



Null CTRL

METODERAPPORT TIL SKUP-PRISEN 2013

ESPEN SANDLI

LINN KONGSLI HILLESTAD

OLA STRØMMAN

An aerial photograph of a city street, likely in Oslo, Norway, showing a mix of residential and commercial buildings, trees, and a railway line. Several teal dots are overlaid on the image, marking specific locations. One dot is near the top right, another near the bottom right, and a cluster of three dots is in the lower center. A semi-transparent grey box with the IP address is positioned over one of the dots in the lower center.

IP 190.55.45.6

Innsendere:

Linn Kongsli Hillestad, Espen Sandli og Ola Strømman

Prosjekt:

Null CTRL - en dokumentarserie om sviktende datasikkerhet i private hjem, bedrifter og det offentlige rom.

Redaksjon:

Dagbladet
v/ Nyhetsavdelingen
Boks 1184 Sentrum
0107 Oslo
Telefon: 24 00 10 00

Kontaktperson:

Arve Bartnes
Nyhetsleder
Mobil: 91164223
e-post: aba@dagbladet.no

Innhold

1. Innledning.....	3
2. Slik startet det: Den bleke kommandøren	3
3. Sentrale problemstillinger.....	4
4. Hva er nytt?	4
5. Organisering av arbeidet.....	5
6. Metoder og kildebruk.....	6
6.1 Kartlegging og forståelse	6
"Farlig verktøy"	6
6.2 Utvikling av søketermer.....	7
6.3 Søk i databasen	8
Ulike porter	10
Målrettede søk.....	11
Automatiserte søk	12
6.4 Digitalt detektivarbeid.....	13
Jakten på "Tommy"	14
Kikkere fra hele verden	16
Tut-tut	17
6.6 Detektivarbeid i felt	17
Gatelangs i tre byer	18
Jakten på det røde kjøleskapet.....	19
6.7 Konfrontasjon og kildekritikk	19
"Dette er da ikke problematisk"	20
Video som metode	22
6.8 Beskjed til ukjent leser.....	23
6.9 Egenutviklet test-motor.....	24
7. Spesielle erfaringer	25
7.1 Blindveier.....	25
7.2 Overraskende reaksjoner.....	25
Takk!.....	25
Tette bånd.....	25
7.3 Egen sikkerhet.....	26
8. Etiske og juridiske problemstillinger	26
8.1 Egendefinerte regler.....	26
8.2 Varsling av aktører.....	27
9. Konsekvenser.....	28
Generelle konsekvenser	29
Hva andre sier	29
10. Liste over publiserte saker	30

1. Innledning

Trolig for første gang har to journalister fysisk testet datasikkerheten for et helt land. Gjennom serien ["Null CTRL"](#) viser vi – helt konkret og reelt – hvordan uvitenhet og uforsiktighet rammer privatpersoner, bedrifter og kritisk infrastruktur.

Med noen få tastetrykk er det mulig å styre naboens web-kamera, åpne konkurrentens database eller ta kontrollen over vitale styringssystemer.

Dagbladet viser hvordan sviktende datasikkerhet åpner veien for svindel, sabotasje, spionasje, terrorisme og andre kriminelle handlinger. Vi viser hvordan giganten Statoil, som bruker millioner av kroner på IT-sikkerhet, ble blottlagt av underleverandører. Hvordan offentlige instanser har lagt ut beredskapsdokumenter ubeskyttet på nett.

Vi viser også hvordan privatpersoner rammes av at uvedkommende kan lese private dokumenter, se hvilken pin-koder som brukes i butikken, se levende bilder fra private hjem eller leser hva arbeidsgiveren skriver om ansatte i filer han trodde var sikret.

Målet har vært å bevege oss vekk fra de mange teoretiske scenarioene. Vi har selv søkt – og funnet – konkrete eksempler på sviktende datasikkerhet. På jakt etter de gode sakene har vi reist land og strand rundt og advart privatpersoner, bedrifter og offentlige instanser om tabber og lovbrudd de ikke visste de begikk.

"Det som er skremmende, er hva journalister i Dagbladet uten spesielle datakunnskaper er i stand til å finne. Hva da med statsmakter, organiserte kriminelle og hackere?", sier seniorrådgiver Vidar Sandland ved Norsk Senter for Informasjonssikring (Norsis).

"Null CTRL" er en digitalserie spesielt laget for Dagbladet.no og DBTV, med en helhetlig publiseringsplan for kvalitetsjournalistikk på nett. Med temaet datasikkerhet har det ligget i kjernen av prosjektet å introdusere ny journalistisk metode, kombinert med nye virkemidler og ny utnyttelse av digital presentasjon. Et ellers komplisert tema er på denne måten presentert forståelig for et bredt publikum.

2. Slik startet det: Den bleke kommandøren

"Jeg ble jo litt blek, med tanke på hva som kunne misbrukes", sa kommandør Jan Sommerfelt-Pettersen i Sjøforsvaret til [Dagbladet 14. februar 2013](#).

Vi hadde konfrontert kommandøren med store mengder forsvarsdokumenter som lå åpent på nett via hans eksterne lagringsenhet. Den private enheten var vi blitt tipset om av en innringer, som oppga en IP-adresse. Ved å taste IP-adressen inn i nettleseren, kom vi rett inn på den åpne serveren med alle dokumentene, uten å taste ett eneste brukernavn eller passord. Under det relativt korte arbeidet med artikkelen ble vi interessert i å finne ut: Hvordan er det mulig å finne en slik server? Finnes det mange slike? Vet folk at data de tror er sikret ligger åpent for alle, kun ved hjelp av et par tastetrykk?

I en samtale med en datakyndig kilde, ble vi introdusert for et dataverktøyet Shodan - beskrevet av enkelte som ["verdens farligste søkemotor"](#). Søkemotoren kan benyttes til å finne enheter koblet til Internett, det vil si alt fra databaser og servere til overvåkingskameraer.

Som journalister så vi umiddelbart varsellampene blinke – og et enormt potensiale. Sjefen så det samme, og ringte Dagbladets advokat. Det ble starten på mange måneder med intens datagraving.

Før arbeidet i det hele tatt startet, utarbeidet vi en etisk og juridisk plattform, med klare avgrensninger for prosjekt og arbeidsmetoder. (Etikk er redegjort for i kapittel 7.1).

3. Sentrale problemstillinger

Når to reportere satte seg fore å granske rikets datasikkerhet, meldte det seg umiddelbart en utfordring: “Dette vet vi ingenting om!”

Linn og Espen spilte aldri Space Invaders, skrev aldri koder på Commodore eller samlet colaflasker rundt PC-skjermen på ungdomsrommet. Vi er flinke gravere, men var på ingen måte dataeksperter.

Problemstillingen ble derfor definert slik:

”Hva kan enhver amatør finne åpent på nett, uten å taste et eneste passord - og hvordan kan det misbrukes?”

Som vi skal presentere videre, var funnene så sjokkerende og omfattende at vi på skrivende tidspunkt fortsatt publiserer saker begrunnet i den samme problemstillingen.

4. Hva er nytt?

Null CTRL er trolig første gang journalister har kartlagt datasikkerheten i et helt land, via egne søk etter reelle eksempler på sviktende sikkerhet. Seriens omfang er ifølge internasjonale eksperter unik også i internasjonal målestokk. Her er noen konkrete eksempler:

- Vi fant over 2500 såkalte “styringssystemer” i Norge er åpent koblet til nett, med minimal eller ingen sikkerhet. 500 av systemene Dagbladet fant kontrollerer industriell eller samfunnskritisk infrastruktur, og brukes i alt fra forsvar og helse til oljebransjen og i kollektivtransport.
- På tross av at FBI advarte mot sårbare versjoner av styringssystemer for bygninger høsten 2012, kartla Dagbladet 290 slike systemer koblet til Internett i Norge. Systemene kontrollerer alt fra lys, varme og ventilasjon til låsemekanismer og brannalarmer. Sikkerhetshullene fantes i navngitte banker, en militærleir, store kontorbygg, skoler, sykehjem og en domstol.
- Dagbladet fant 15 digitale inngangsporter til Jernbaneverkets brannalarmsentraler.
- Dagbladet har avdekket 2048 norske overvåkingskameraer på Internett. Alle med nettilgang kunne se levende bilder fra private hjem, utesteder, restauranter, butikker, arbeidsplasser og andre offentlige steder.
- Dagbladets viser hvordan sikkerhetshull blir utnyttet. Ett kamera på ei hytte i Nord-Trøndelag ble f.eks besøkt 98 ganger på ei uke av personer fra 12 land. Eierne visste ingenting.

- Når moderne printere uten passordbeskyttelse kobles til nett, kan hvem som helst få tilgang til lagrede dokumenter eller skanne dokumenter som ligger i printeren. Dagbladet fant 1781 slike printere koblet til nett i Norge.
- Dagbladet har lokalisert flere tusen servere i Norge koblet direkte til Internett, søkbare og uten passordbeskyttelse. Dette betyr at uvedkommende kan få tilgang til alt fra bilder til dokumenter og programfiler. Både private servere, bedriftsservere og servere tilhørende det offentlige er eksponert.
- Dagbladet fant en åpen server med sensitive data om kunder av Oslo Taxi. Blant 5958 registrerte kunder fant vi identitet og oppholdsadresse for barn med hemmelig ID, under barnevernets omsorg.
- Dagbladet har vist hvordan store oljeselskap eksponeres av sviktende datasikkerhet hos underleverandører og konsulenter. Sensitive dokumenter berørte noen av verdens største oljeselskaper, både norske og internasjonale.
- Vi fant detaljert informasjon om Ørland flystasjon, Norges nye kampflybase. Dokumentene inneholdt informasjon som kunne misbrukes, ifølge Luftfartstilsynet og Cyberforsvaret (Forsvarets gren med ansvar for informasjonsteknologi).
- Dagbladet fant åpne servere for brannberedskapen i 39 av 44 kommuner i Nordland. Her fantes blant annet beredskapsdokumenter, interne brukernavn og passord og informasjon om fabrikk-, tunnel- og flyplassikkerhet.

“Null CTRL” har en egen hjemmeside. Den finner du her: <http://www.dagbladet.no/nullctrl/>

5. Organisering av arbeidet

Alle søk er gjennomført og bearbeidet redaksjonelt av Linn K. Hillestad og Espen Sandli. Hoveddelen av de digitale undersøkelsene og feltarbeidet er gjennomført på heltid i perioden fra påske til september 2013 (bare avbrutt av sommerferien). Første sak ble publisert i oktober. Etter dette jobbet vi heltid fram til desember 2013 med utfyllende feltarbeid og utarbeidelse av nye saker.

Selv om Linn og Espen har tatt enkelte turnusvakter og ved behov bidratt i avdelingens øvrige dekning av nyhetshendelser, har dette vært unntaket. Det er i hele perioden investert mye tid i Null CTRL, noe resten av Dagbladets nyhetsavdeling med sin dugnadsånd har båret merbelastningen av.

Heller enn å lukke prosjektet inne på et mørkt datarom, har vi hatt motsatt innfallsvinkel. Vi har sittet midt i nyhetsredaksjonens åpne landskap, som en del av dagskiftet. Det har medført spørsmål fra nysgjerrige forbipasserende kolleger, men har først og fremst bidratt til avmystifisering (“nei, vi hacker ikke”) og inkludering i prosjektet.

Redaksjonell utvikler Ola Strømman skulle opprinnelig bistå journalistene med visuelle elementer for publisering (plotting av kart, interaktive grafikker, layout-profil m.m), samt datatekniske råd og hjelp. Med stor grad av nysgjerrighet la han imidlertid merke til flere oppgaver Espen og Linn utførte mer tungvint enn han fant nødvendig. Etter hvert ble han en integrert kraft i prosjektet. Han utviklet flere tekniske hjelpemidler som lettet arbeidet med våre datasøk. Mer informasjon om ulike metodeverktøy finnes i kapittel 6.3.

Disse har også bidratt: Arve Bartnes (reportasjeleder), Øistein Norum Monsen (video/foto/regi), Kjell Audun Aas og Tom-Marius Olsen (grafikk/design), Therese Doksheim

og Torgeir P. Krokfjord (reportasje-bistand), Eirik Vale Frogner, samt Thomas Rasmus Skaug, Sveinung U. Ystad og Benjamin Ward (video/foto).

I forkant av publisering hadde vi to heldagsseminarer utenfor huset for gjennomgang av funn og potensielle saker med ledere og nøkkelpersoner.

6. Metoder og kildebruk

6.1 Kartlegging og forståelse

Verktøyet vi bruker for søk etter enheter koblet til nett heter Shodan. Det fungerer ikke på samme måte som Google, Yahoo eller andre tradisjonelle søkeverktøy på Internett. Mens du i Google skriver inn ett eller flere ord for å finne fram til ulike nettsider, søker du i Shodan etter spesifikke enheter og programvare.

Før vi kunne begynne å søke, måtte vi vite hva det var vi lette etter. Vi fant avisartikler om tidligere enkeltfunn, men de var til liten hjelp. Alle var basert på tips fra sikkerhetseksperter, ikke egen research. Ingen av dem ga konkret informasjon om hvordan vi skulle søke.

Vi fant imidlertid fram til en masteroppgave, som benyttet Shodan som verktøy, og denne ga oss en pekepinn på hvordan vi kunne gå fram. Vi innså også at kunnskap om søkemotoren ikke var nok, og søkte blant annet i elektroniske postjournaler og ba om innsyn i dokumenter vedrørende datasikkerhet, for eksempel en bekymringsmelding om datasikkerheten i et elektronisk resepsystem.

Samtidig bestemte vi oss for å kontakte internasjonale eksperter og tidlig gå i dialog med dem. Vi satte oss på flyet til universitetsbyen Cambridge, hvor vi møtte sikkerhetsekspert Eireann Leverett. I Luzern i Sveits var vi på en sikkerhetskoneranse, hvor vi hadde avtalt et møte med Shodan-grunnlegger John Matherly. Disse kildemøtene ga oss uvurderlig kunnskap å bygge videre på.

Matherly omfavnet også prosjektet, og ga oss tilgang til hele Shodans database. Dette skulle vise seg å bli svært nyttig seinere, til utvikling av egne søkeverktøy og test-motor. Matherly er holdt delvis orientert om framdrift, men har ikke på noe tidspunkt deltatt som ressurs i vår research.

"Farlig verktøy"

Shodan ble lansert i 2009, og er i tabloide ordelag beskrevet som ["verdens farligste søkemotor"](#).

Søkemotoren kan være en snarvei for hackere, men kan bare vise hvor du skal logge deg inn. Den gir ingen hjelp til å knekke koder for å bryte seg inn. Hackere trenger heller ikke Shodan for å finne de åpne dørene, dette er kunnskap de har hatt lenge. De skyr også søkemotoren, fordi det er en betalt tjeneste, hvor du er ikke anonym.

Søkemotoren er et verktøy utviklet for å bevisstgjøre systemteknikere, utviklere, systemeiere og andre i bedre forståelse av datasikkerhet. Vi var ingen av delene, men så et enormt og hittil uutnyttet potensiale i testing som journalistisk metode. For å få det til, måtte vi fylle på med

mye av kompetansen vi manglet, datafaglig og innen hvert tematiske område vi ønsket å undersøke. Den veien var lang - og bratt.

6.2 Utvikling av søketermer

I motsetning til Google er ikke Shodan ettergivende for stavfeil. Den gjetter ikke og hjelper deg ikke på vei. Feil ord = feil/null treff.

Skriver du for eksempel “styringssystem” i søkefeltet, får du ikke et eneste treff. I stedet søker man etter spesielle elektroniske “fingeravtrykk”. Dette er informasjon om enheter koblet til nett. Informasjonen er det enheten selv som sender fra seg, ofte via programvaren. Et slikt fingeravtrykk kan for eksempel være versjonsnummeret (v1.1.2) til en helt konkret enhet fra en helt konkret produsent (eller forkortelser av disse), og denne informasjonen kommer opp i et såkalt informasjonsbanner for hvert enkelt treff. Søkeordene er gjerne sammensatte.

Du må altså vite ganske mye om hva du vil finne - om du ønsker å finne det. I begynnelsen brukte vi ukesvis på å lete oss fram til kunnskap som kunne gi meningsfulle søkeord.

Vi lette ulike steder etter søketermer vi kunne bruke som utgangspunkt. For styringssystemer, tok vi for eksempel utgangspunkt i [Eireann Leveretts masteroppgave](#) og diskusjonstråder fra hackerfora. Det er imidlertid ulikt fra land til land hva som er de mest utbredte styringssystemene.

Etter hvert ønsket vi derfor også spesifikke søkeord for Norge. Dette gjorde vi blant annet ved Google-søk på nettet etter bilder av ulike kontrollrom, for deretter å identifisere mulige styringssystemer på disse bildene. I tillegg gjennomgikk vi ulike rapporter og snakket med kilder med kunnskap om de ulike bransjene vi var særlig interesserte i.

Deretter tok vi for oss den informasjonen vi fikk tilbake via Shodan når vi fikk treff på systemer som kunne gi gode reportasjer. Informasjonen som gikk igjen i treff, dannet grunnlag for nye søk. Desto mer presist fingeravtrykket kan defineres, desto flere liknende treff er det sannsynlig å finne. Denne prosessen innebar mye prøving og feiling med ulike søkeord og kombinasjoner.

The screenshot displays a Shodan search result for the 'University of Lagos'. It is divided into three main sections: 'Services', 'Top Countries', and 'Server Information'.

Services	
HTTP	15,931
HTTPS	2,218
HTTP Alternate	9
Telnet	5

Top Countries	
United States	4,785
China	921
Brazil	898
Italy	789
United Kingdom	727

University of Lagos
Added on 01/05/2013
Lagos
Details

HTTP/1.0 200 OK
Date: Tue, 16 Mar 1993 18:07:15 GMT
Server: **cisco-IOS**
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html
Expires: Tue, 16 Mar 1993 18:07:15 GMT
Last-Modified: Tue, 16 Mar 1993 18:07:15 GMT
Cache-Control: no-store, no-cache, must-revalidate
Accept-Ranges: none

Skjerm bilde: Informasjonsbanneret til et tilfeldig treff i Shodan. Serverinformasjonen er et eksempel på et fingeravtrykk.

Vi oppdaget at søketermene også bør ekskludere mest mulig av det unyttige - det vil si andre treff enn de vi leter etter. Det kan være snakk om flere tusen slike i et søk. Etter hvert lærte vi

oss å luke ut negative funn via søketermer som bidrar til å fjerne unyttige treff. Det gjør vi ved utstrakt bruk av minusord (ord eller tall søket ikke skal inneholde).

Eksempel på søketerm: v111.1.2 -404 -atp -401 -301 port:80 country:no

Termen over er konstruert som et eksempel på et søk. Det er et etisk poeng at vi ikke bidrar til å spre faktiske søketermer som kan føre noen inn på styringssystemer eller andre sårbarheter.

Termen over er dog svært lik et reelt søk. Som søket prøver å vise, jakter vi i eksempelet på en versjon ("v") av en bestemt programvare koblet til nett.

"-404" luker ut treff som ikke lenger finnes.

"-atp" er et fiktivt uttrykk for å luke vekk uinteressante servere

"-401" luker ut treff som krever autorisasjon

"-301" luker ut treff som er fjernet fra nett permanent.

"port:80" begrenser søket til http

"country:no" begrenser søket til adresser registrert i Norge

På grunn av antall søk og treff, var det nødvendig å holde en pinlig nøyaktig oversikt over alle søkeord og loggføre treff helt fra begynnelsen. Til dette valgte vi Excel. Ifølge loggføringen har vi benyttet minst 826 selvstendige søketermer, i separate søk. Når vi tar med blindspor og feilslåtte søk som aldri ble notert, har vi reelt testet mer enn tusen unike søketermer.

6.3 Søk i databasen

Uansett hvor spesifikke søketermene er, må treffene testes ved å oppsøke de relevante IP-adressene. Med et godt søk er kanskje 4 av 10 treff interessante, men ofte er det ett av 50 eller ett av 250 treff som viser seg å være av interesse. Hva som er hva vet vi ofte ikke før vi har oppsøkt IP-adressen og sett hva den konkret inneholder. I time etter time, flere måneder i strekk, har vi sittet foran dataskjermen og manuelt gått gjennom IP-adresser. På det meste har vi gått gjennom og sjekket over 2000 treff på ett enkelt søk.

Totalt har vi undersøkt 535 320 unike norske IP-adresser og 707 358 åpne porter.

Shodan er ikke konstruert for den mengden søk vi har gjort i forbindelse med Null CTRL. Vi savnet blant annet muligheten for sortering av søk og en ensides visning av resultatene for å få en bedre oversikt. For å benytte søkemotoren mest mulig effektivt, fant vi det derfor nødvendig å utvikle vårt eget søkeverktøy. Vi spurte derfor John Matherly om vi kunne få tilgang til et ubegrenset antall søk via et API, et programmeringsgrensesnitt som ga oss tilgang til innholdet i Shodans programvare. Det brukte vi til å lage vår egen, modifiserte versjon av søkeverktøyet.

Dette ga oss også muligheten til å benytte flere ulike søketermer samtidig og presentere resultatene fra disse søkene på samme side, noe som var svært viktig i vår research. I tillegg kunne vi legge til egne filtre.

Ekstrafilter for OR-søk: (feks: port:80 -401)

☐ Vis søketekst ☒ Skipp after-begrensning

Ola-filter: ikke rør! ;-)

default filter:
'after:10/10/2013 country:no'

1600 treff etter

update	ip	port	city	org	hostname(s)
2014.01.08:		8080		Telenor Norge AS	8.132.172.tmi.telenormobil.no
2014.01.08:		8080		Telenor Norge AS	6.19.77.tmi.telenormobil.no
2014.01.08:		8080		Telenor Norge AS	8.145.243.tmi.telenormobil.no
2014.01.08:		80		Broadnet AS	:197.banetele-cust.com
2014.01.07:		8080		Telenor Norge AS	8.130.112.tmi.telenormobil.no
2014.01.07:		8080		Telenor Norge AS	6.175.59.tmi.telenormobil.no
2014.01.07:		8080		Telenor Norge AS	6.29.179.tmi.telenormobil.no
2014.01.07:		8080		Telenor Norge AS	8.157.160.tmi.telenormobil.no
2014.01.07:		8080		Telenor Norge AS	6.28.35.tmi.telenormobil.no
2014.01.07:		8080		Telenor Norge AS	8.150.6.tmi.telenormobil.no
2014.01.07:		8080		Telenor Norge AS	6.184.245.tmi.telenormobil.no
2014.01.07:		8080		Telenor Norge AS	6.171.217.tmi.telenormobil.no
2014.01.06:		8080		Telenor Norge AS	6.187.62.tmi.telenormobil.no
2014.01.06:		8080		Telenor Norge AS	6.21.124.tmi.telenormobil.no

Skjermbilde: Egenutviklet søkeverktøy mot Shodan, laget av Dagbladet

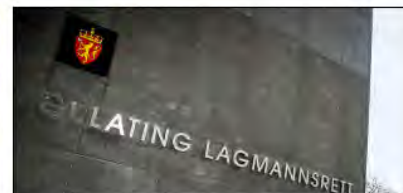
Disse benyttet vi blant annet i arbeidet med tre artikler om sårbare kontrollsystemer for bygninger, publisert 27. november.



Dette er lista over norske bygg hackere kan ta kontroll over

Dagbladet fant sårbare kontrollsystemer i 290 bygg tilhørende banker, skoler, sykehjem - og en militærleir. [Les mer](#)

Skjermbilde: Artikler publisert på Dagbladet.no i november 2013.



Domstolene sjekker datasikkerheten etter «Null CTRL»-avsløring

- Vi har nok ikke hatt tilstrekkelig fokus. [Les mer](#)



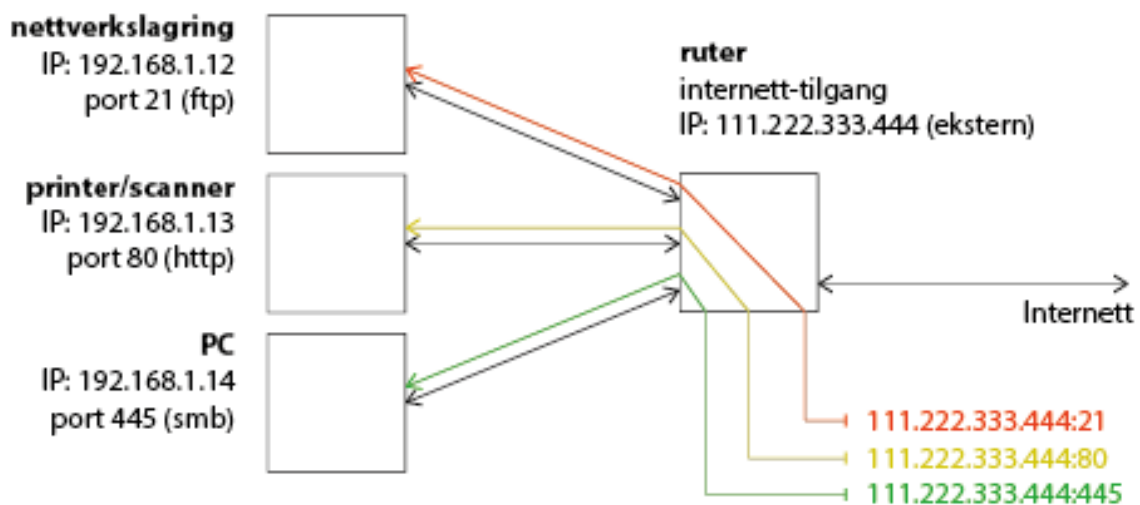
- Dette vil være spesielt uheldig for vårt sykehjem

Sårbart kontrollsystem brukes til å styre lys og varme. [Les mer](#)

Den omtalte sårbarheten var knyttet til programvareversjon, og vi var derfor nødt til å kartlegge alle de spesifikke versjonene av det aktuelle systemet. Dette gjorde vi ved å legge til en kolonne med informasjon om programvareversjon i Dagbladets egenutviklede søkeverktøy.

Ulike porter

Noe av vår tekniske frustrasjon var knyttet til de ulike “portene” vi måtte undersøke. Her følger en liten forklaring på dette: Mange ulike enheter kan kobles til ett nettverk, og når disse igjen kobles til Internett via en ruter, får de en felles IP-adresse for kommunikasjon ut mot Internett. Denne IP-adressen er unik, og kan for eksempel sammenlignes med et telefonnummer. For å nå de ulike enhetene fra andre deler av Internett, adresseres de med forskjellige “porter”. Disse portene kan betraktes som ulike interntelefonnumre. Skissen under viser hvordan IP-adresser og porter henger sammen.



Skisse: Slik kan ulike porter lede inn til forskjellige enheter koblet til samme eksterne IP-adresse

Det finnes 65 535 porter som kan brukes, og vi har undersøkt de vanligste, deriblant http (port 80 og 8080) og https (port 443 og 8443). Disse henviser til vanlige nettsider som kan besøkes med vanlig nettleser, og er dermed de portene folk flest forbinder med Internett.

I tillegg har vi sett på FTP (port 21), SMB (port 443) og MySQL (port 3306), som er spesielle porter for lagring og databaser. Den siste vi har fokusert på er telnet (port 23), en protokoll som ofte brukes til styringssystemer.



```
ca. Telnet
+---<C> Copyright by HONEYWELL Technology Solutions Bangalore 2001-2009---+
+--- B A D M A N Main Menu ---+
+-----+
FIRMWARE VERSION -----> BMA-3 SUSI Server 1.0.2
SYSTEM UP TIME -----> 18 days 04:33:50
CURRENT SYSTEM TIME --> 18-APR-2013 17:25:56
+-----+
1. Board Information
2. Subsystem Overview
3. Network Statistics
4. Active Point Statistics
5. Backup/Restore Statistics
6. Point Monitor
7. SUSI Interface Monitor
8. Trace Channel Monitor
9. Global State Info
A. MTOS State Analyzer
B. Memory Usage Monitor
C. Event Handler Info
D. RACL/COS bit Overview
E. Bootloader Shell
F. Board Restart
+-----+
Please select:
+-----+
```

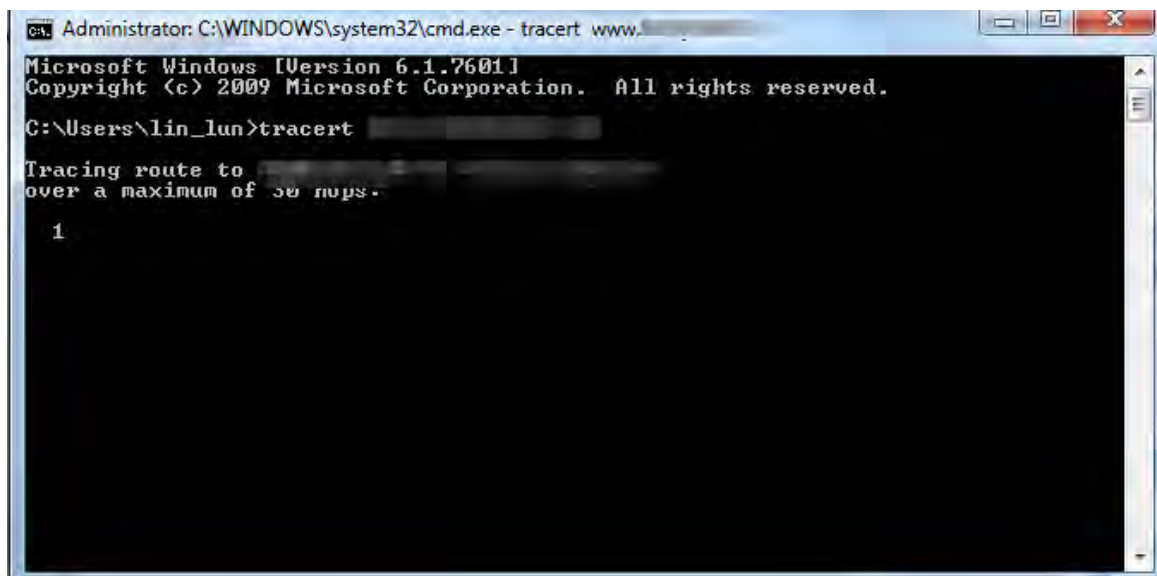
Skjerm bilde: Eksempel på inngang til et styringssystem via telnet.

Måltrettede søk

Alle søkene vi hittil har nevnt er rettet mot enheter, programvare eller porter. I slike søk er det tilfeldig om sikkerhetshullene vi finner berører privatpersoner, bedrifter eller offentlige institusjoner.

Men vi var særlig interesserte i å granske datasikkerheten til samfunnsskrittiske institusjoner, da spesielt selskaper eller instanser innen olje, kraft, kollektivtransport, luftfart, helse, forsvar og myndighetsutøvelse. Vi var derfor nødt til å gå mer måltrettet til verks.

I Shodan kan man også søke på konkrete IP-adresser. Vi kartla derfor først hvilke selskaper og institusjoner vi ønsket å granske spesifikt. Deretter laget vi oss en oversikt over hvilke IP-adresser de respektive benytter. Adressene fant vi ved å gå til respektives hjemmeside, kombinert med funksjonen "tracert" i Windows' kommandolinje (se bilde under). Ved å finne én IP-adresse, kunne vi også søke oss fram på IP-range, serien av adresser mange private og offentlige virksomheter disponerer.



```
Administrator: C:\WINDOWS\system32\cmd.exe - tracert www...
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\lin_lun>tracert [redacted]

Tracing route to [redacted]
over a maximum of 30 hops:

 1
```

Skjerm bilde: Slik finner du IP-adressen fra en nettside

I tillegg gjorde vi konkrete søk på navn på registrerte *eiere* av IP-adresser. Et eksempel på ett slikt søk er “org:jernbaneverket”. Dette søket ga oss 18 treff på port 80 (http). To av disse treffene skulle vise seg å være digitale inngangsporter til brannalarmsentraler i Jernbaneverkets infrastruktur.

De to vi fant, brukte vi til å lage et fingeravtrykk på hva slags bannerinformasjon brannsentralene ga når de var koblet til nett. Fingeravtrykket vi laget, gjorde at vi til slutt fant 15 innganger til brannsystemet. Disse er nå lukket.

To databaser tilhørende Oslo Taxi ble også funnet på denne måten. I en av disse lå det informasjon om 5859 drosjekunder - mange med svært sensitive data som potensielt kunne misbrukes. Ifølge Datatilsynet kunne informasjon i basen sette barns liv i fare.



Skjerm bilde: Artikler publisert på Dagbladet.no i november 2013.

Automatiserte søk

Det ble tidlig klart at mange av søkene resulterte i en u håndterlig mengde treff på noen bestemte porter. Det gjaldt FTP (ca. 35 000 treff), SMB (ca. 8500 treff), MySQL (ca. 6000 treff) og “Index of” (ca. 3000 treff).

Med så mange potensielt sårbare servere, er det u håndterlig å gå gjennom alle manuelt. Løsningen ble å sette opp automatiserte prosesser som kontrollerte resultater på disse portene. Disse jobbene ble kjørt via linux/php. Hver jobb kunne ta en dag eller to og resulterte i en automatisert rapport med oversikt over deler av innholdet. På denne måten hadde vi tilgang til en enkel og lettlest oversikt som kunne gi en pekepinn på om det fantes noe av journalistisk interesse på serveren.

SHARE	TYPE	READABLE	DIRS	FILES	COMMENT
IPC\$	IPC	0	-		IPC Service (My Book Live Duo Personal Cloud Storage)
	Disk	1	30	10	
<u>Forskrifteretningslinjer</u>					
+ 6 filer					
<u>Diverse skema</u>					
+ 22 filer					
<u>DIETI</u>					
+ 4 filer					
<u>Hvorfor bruke oss</u>					
+ 11 filer					
<u>TAUSHETSSKJEMA for</u> <u>FENGSEL</u>					
+ 4 filer					

Skjerm bilde: Eksempel fra FTP-rapport generert i oktober 2013

Automatiserte søk er ikke benyttet i andre søk enn de nevnte. Alle rapportene ble kjørt tre ganger, med flere ukers mellomrom, og resulterte i flere gode saker, deriblant artikkelen om store oljeselskaper som blir blottlagt av konsulenter og underleverandører.

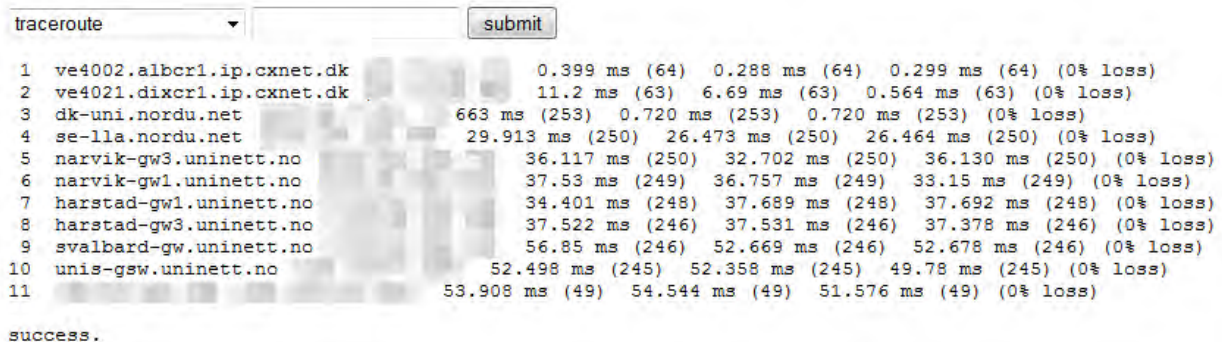


Faksimile: Dagbladet 9. desember 2013

6.4 Digitalt detektivarbeid

Som vist, kan det være vanskelig å søke og finne enheter på nett. Men det å spore opp funnene i den virkelige verden, er enda vanskeligere.

Det finnes en rekke nettbaserte verktøy for å finne eiere av IP-adresser, som for eksempel www.whois.net. Men dersom IP-adressen er registrert på et mindre selskap eller en privatperson, er det ofte nettleverandøren som står som eier (ikke kunde). Nettleverandøren har taushetsplikt og oppgir kun informasjon om IP-adresser etter hjemlet henvendelse fra politiet. En mulighet kan da være å bruke digitale verktøy som forsøker å spore IP-adressens koblinger tilbake til den virkelige eieren, for eksempel www.openbgp.org. I noen tilfeller hvor IP-eier er en mellomstor bedrift eller institusjon, lyktes vi å spore opp eier på denne måten. Ett eksempel er skjermbildet under.

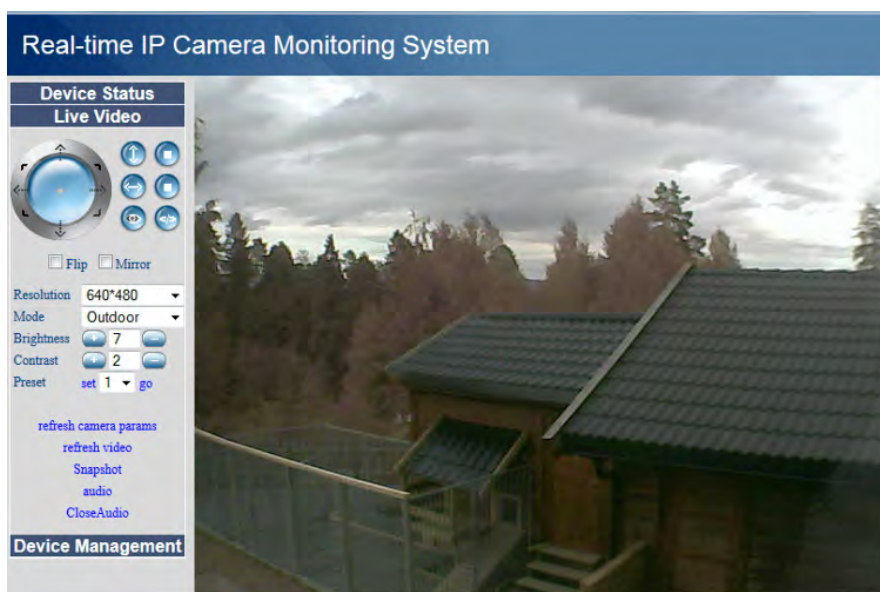


Skjermbilde: Digitalt verktøy som sporer ruten til en IP-adresse.

Her har vi søkt etter informasjon om en konkret IP-adresse til et styringssystem vi fant. For å finne eieren, ser vi hvilke servere internettrafikken går gjennom. Tjenesten vi brukte ligger i Danmark og derfor er de første oppføringene danske. Så går den over til uninett.no, som blant annet er nettleverandør for forskningsmiljøene i Norge. Ut fra navnene på serverne ser vi at trafikken går nordover til Harstad, Svalbard og så til slutt: Universitetssenteret på Svalbard.

Dette konkrete verktøyet ga oss ingen konkrete saker, men vi fikk luket ut flere treff vi mente ikke var interessante, da vi fant ut hvem som var eieren.

Jakten på "Tommy"



Skjermbilde: Åpent, privat overvåkingsskamera funnet via Shodan.

I mange tilfeller kommer nevnte verktøy til kort, særlig når privatpersoner er involvert. Vi var derfor ofte nødt til å nøste oss fram til eieren på helt andre måter.

Skjermbildet over viser et nettbasert styringspanel tilhørende et privat overvåkingskamera vi fant. Som skjermbildet viser, filmer det mot en hundegård (nederst til venstre). I tillegg kan du se noe skog i bakgrunnen. Styringspanelet lå helt ubeskyttet på nett, og hvem som helst kunne derfor ta styring over kameraet - for eksempel ved å dreie det 180 grader rundt. I dette tilfellet ville det da filme innendørs, på eierens kjøkken. I tillegg til at de aller fleste vil oppleve det svært ubehagelig at uvedkommende kan se bilder fra deres private hjem, kan slike kameraer også misbrukes til å for eksempel kartlegge verdisaker eller se når det er noen hjemme. Vi ønsket å varsle eieren om det åpne kameraet. Men hvor skulle vi begynne?

Først brukte vi et nettbasert verktøy for å få tilgang til informasjon om IP-adressens fysiske beliggenhet (<http://www.iplocation.net/>). Dette verktøyet benytter fire forskjellige baser for å undersøke geografisk lokalisering. To av disse oppga at kameraet befant seg på Dokka, de to andre at det befant seg på Lillehammer. Det var ikke nok til å lokalisere et hus med trær og hunder.

I styringspanelet fant vi informasjon om det trådløse nettverket kameraet var koblet til, og at dette het "Tommy84". Vi tenkte derfor at kameraeieren muligens het Tommy og var født i 1984. Vi søkte derfor i Bizweb og gikk gjennom alle oppføringer av personer som heter Tommy, med rett alder, bosatt på Lillehammer, Dokka og omegn. Deretter sjekket vi adressene vi fant i Google Street View for å se om hus kunne stemme med kamerabildet. Vi fant ingen som passet.

Vi prøvde deretter å gå mer systematisk gjennom Google Maps og Google Street View for å finne huset, ved å panorere gate for gate. Det ga ingen resultater. Telefonsamtaler med lokale eiendomsmeglere, taxisjåfører og dyrebutikker tok oss heller ingen vei.

Vi tok derfor en fot i bakken, og tenkte: "Hva viser egentlig bildet?". Konkret hadde vi tre ting å gå på: Hundegården, hvor vi hadde sett to rottweilere og en liten, hvit spissnutet hund, navnet Tommy og Oppland fylke, hvor kameraet trolig befant seg. Vi prøvde derfor en kombinasjon av søkeordene "kennel", "tommy" og "oppland" i Google. Etter en gjennomgang av litt ymse treff, kom vi over et blogginnlegg om premiehunden Tommy, en japanesisk spitz (spissnutet hvit hund). Innlegget var skrevet av eieren, og vi fant vedkommendes adresse på Gjøvik. Et oppslag i Google Maps viste at dette så ut til å være huset vi lette etter. Vi oppsøkte eieren, som ble helt forferdet over at kamerabildene var tilgjengelige for alle - men veldig glad for å bli varslet. Sikkerhetsinnstillingene i overvåkingskameraet endret han med en eneste gang.

Overvåket av eget kamera

Trond Kristiansen hadde aldri forestilt seg at kameraet han hadde plassert på kjøkkenet og datterens soverom kringkastet lyd og bilder rett ut på Internett.

Trond Kristiansen
Egen Sandli
Thomas Rasmus Skjau

GNVH (Dagbladet): -Datteren er veldig skummelt, sier Trond Kristiansen til Dagbladet.

For snart en tiår ligger han på overvåkingskameraet så han kan se både en øye med hundene i husholdningen, og uansett kjøkkenet.

Kameraet plasserte Kristiansen opp på arbeidsbordet, hvor det er en finnet kameraarm som kan kringkastes, tryk på den røde knappen og du kan se bildet på skjermen.

Trond Kristiansen ikke viser, er at kameraet også var tilgjengelig på den offentlige IP-adressen, hvor det var en finnet kameraarm som kan kringkastes, tryk på den røde knappen og du kan se bildet på skjermen.

Uvilkommende kunne derfor ta styring over kameraet via nettet i nettverken og å se det på 180 grader så de så rett inn på kjøkkenet.

-Og dette kan hvem som helst gjøre, mener det eke Kristiansen spikket på Dagbladet hvor han er fribilg og bare enkelt det er.

På barnerommet

Et uke før Dagbladet gjorde han oppmerksom på at kameraet tilgjenglig for alle, hadde han flyttet det ned på datterens soverom.

Nor som ikke er vanlig er å ferdig gjer for å holde et øye med barna, i forbindelse med en overvåkingskameraet.

Ko overvåkingskameraet koble til nettet. Av disse er flere plassert på barnerommet.

Kall det en nysserom hushold, sier Kristiansen.

-Sånn som det er greit at folk ut på kjøkken, men at de skal ha tilgang til soverommet til datteren min, det er jeg ikke så glad for.

Selv kan han følge ned på kameraet via en app på mobil, og han demonstrerer hvordan han enkelt

kan se på kameraet, bare lyd og bilder og oppsett.

I utgangspunktet veldig praktisk, så ligger ikke alle andre har den samme muligheten. Dagbladet er kjent med at overvåkingskameraet, har vært inne på Kristiansens kamera, men kan ikke avsløre hvor mange.

Bekymret for kriminelle

-Det ferske jeg tenker på, er jo kriminelle. Med tanke på at de faktisk ser inn i så høyt det, så kan de jo se det som er veldig i øyeblikket. Men det er jo en ting. Noe annet er faktisk å bli overvåket av dine egne kameraer uten at de er klar over det, sier han.

Han mener levestandarden av slike kameraer har et opplysningsnivå.

Kameraet er jo utstyrt med en nettside eller en nettsidekobling, og de kan jo holde det opp med min ruter, som er passordbeskyttet, og det er det ikke mine tenker at noen som kunne på inn og utplassering på et kamera. Det kan være og ikke se for meg i mine vilkår.

Han varner at de vil følge opp kameraovervåkingen etter Dagbladets avsløring.

Tilgjenglig

Kristiansen får støtte av direktør Bjørn Erik Thon i Dataforvaltningen, som mener en av årsaker til problemet er at denne typen kameraer er blitt så lett tilgjengelige for folk.

-Dette er jo ganske avansert teknologier. Derfor er det viktig å ha en offentlig opplysning i hvordan de setter opp passord og hvordan de sikrer datene sine. Det har bransjen et ansvar, sier Thon til Dagbladet.

Han varner at de vil følge opp kameraovervåkingen etter Dagbladets avsløring.

Tilgjenglig

Ettersom en IP-adressert utgangspunkt er anonym for andre enn nettsideovervåking, er det på ingen måte usannsynlig å finne fram til denne overvåkingskameraet.

For det første kan du finne ut hvilke IP-adresser som er plassert via et enkelt lokaliseringssøk av IP-adressen på kameraet. Slik fant Dagbladet ut at dette aktuelle kameraet var plassert i Oslo.

Samtidig var brukeren av IP-adressen oppgitt kameraovervåking og husholdningskameraet tilhørte den samme personen. Ved å se på IP-adressen, og på den IP-adressen som er registrert i Google, fant Dagbladet en spesiell person, og dermed også kameraet.

-Skummelt hvor enkelt det kan være, mener Trond Kristiansen, som nå har fjernet kameraet fra nettet.

Si også kommentar side 5.

SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans kringkastet bilder og lyd rett ut på Internett. Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom.

Foto: Thomas Rasmus Skjau

FAKTA

Slik sikrer du kameraet ditt

Selv om overvåkingskameraet er koblet til det interne nettverk, betyr det ikke at det er trygt. Hvis du har et kamera, kan kameraet fortsatt være tilgjengelig for andre via din offentlige IP-adresse.

Derfor er det viktig å beskytte kameraet med brukernavn og et solid passord.

I noen tilfeller kommer kameraer med et standardpassord fra leverandøren, som for eksempel «admin». Disse er ofte allment kjent, og må derfor byttes med en gang du installerer kameraet.

Generelt må du alltid huske å skifte passord regelmessig. Dette kan du gjøre via en nettside eller via en app. Hvis du har et kamera, er det viktig å oppdatere til siste versjon av det som er anbefalt.

Derom du har installert et kamera på et offentlig sted, som i en butikk eller restaurant, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

TIPS

055

FAKTA

NULL CTRL

Tenk deg at du med noen få klikk på en knapp over kontrollen av kameraet, kan se bilder fra kjøkkenet og datterens soverom.

Apert databasen til kameraet, kan du finne ut hvilke IP-adresser som er plassert på kameraet.

Etter det har du installert et kamera på et offentlig sted, er det viktig å sette seg inn i regelverket for kamerainstallasjon på de vet at det ikke er ulovlig som opp i tillegg må ikke kameraer midles inn til datanettet.

Kilde: Anette Sævi for Informasjonssenteret / Dataforvaltningen

6.5 Kartgrafikk

Vi laget også [en interaktiv kartgrafikk](#) av trafikken inn til kameraet i Nord-Trøndelag for å gi et bilde av den omfattende aktiviteten. Til dette brukte vi Google Maps med egne geometri-biblioteker (ekstra kode) for utregning av avstander til plotting av linjer og ikoner. Bildene og linjene byttes ut med kraftigere fargelag når musepekeren føres over.

I tillegg ønsket vi å tydeliggjøre omfanget av i funnene våre i flere andre saker ved bruk av kartgrafikk. Kartene er plottet med json-objekter direkte på Google Maps.

Totalt har vi laget kart med plassering av:

- Overvåkingskameraer
- Servere som oppgir sitt standardpassord
- SMB - deling av mapper
- Dreambox - satellittbokser (pirater)
- FTP - deling av filer
- Fjernstyring av PC-er (RDP)
- Telnet
- Eksterne lagringsenheter (NAS)
- Styringssystemer
- Niagara - sårbare versjoner av styringssystem for bygninger
- Printere



Skjerm bilde: Eksempel på kartgrafikk. Dette viser antall styringssystemer Dagbladet fant.

Tut-tut

I forbindelse med research av en togrelatert sak, slet vi med å finne ut av noen bestemte målere. Vi forsto det var strømmålere vi hadde funnet, men ikke hvorfor cirka 500 lå åpent.

I et forsøk på å forstå mer, lastet vi ned GPS-loggfiler fra målerne og plottet posisjonering over tid. Vi kunne da spille av målerne bevegelser i et kart. Sluttresultatet ble at vi uten å vite det hadde laget oss en digitalisert modelljernbane hvor et døgns gods- og persontrafikk suste rundt. Det skal sies at NSBs sanntidstabeller er mer nøyaktige og oppdaterte, og dette ble derfor aldri en sak. Jernbaneverket kunne imidlertid ikke forklare hvorfor så mange lå åpent, og har seinere sikret utstyret.

6.6 Detektivarbeid i felt

Selv om Null CTRL er basert på ny, digital journalistisk metode, har vi i vårt arbeid vært avhengige av visse, helt tradisjonelle metoder, noe vi har brukt minst like mye tid på som datagraving. Ingen datamaskin kan erstatte banking på dører, møtet med mennesker ansikt til ansikt, konfrontasjon, letingen etter åsteder og forklaringer i felt, blant folk. Her er et par eksempler:



Skjermbilde: Overvåkingskamera som sender levende bilder av festende ungdom ut på nett.

Et overvåkingskamera vi fant, filmet med meget høy kvalitet gjestene inne på et utested. Her så og hørte vi fulle, unge mennesker hygge seg en lørdag kveld. Rett foran kameraet sto et ungt par og klinte. Nattklubben filmet altså intetanende gjester i intime situasjoner og kringkastet bildene åpent ut på Internett. I tillegg var kameraet etter alle solemerker ulovlig satt opp. Vi mente dette var en alvorlig sak, og ville varsle utestedet.

Men hvilket utested var det? Og hvor? Ifølge geolokaliseringen i Shodan, befant det seg i Stavanger. Vi dro dit, oppsøkte alle byens utesteder, men kunne ikke finne noe som passet. Lokalkjente dro ikke kjensel på stedet vi kunne vise bilder av. Etter tolv timer ga vi opp.

Et grundigere søk med geolokalisering, viste også Oslo som mulig sted. På ny gikk vi på leting gatelangs, forhørte oss med utelivskilder og satt i timesvis og sjekket utesteders inventar via bilder på nett. Ikke noe passet. Dette er et eksempel på hvordan geolokalisering kan være misvisende, og ikke kan erstatte arbeid i felt.

På en videosnutt oppdaget vi en person rope over all annen lyd: “Vi kan ikke slepe med oss alt dette utstyret gjennom hele Drammen”. Etter en kjapp sjekk på nettet, fant vi riktig sted: Nattklubben Klubbteateret. Vi dro dit en fredag kveld og snakket med ungdommer for å prøve å finne ut hvem paret fra videoen var. Til slutt traff vi en som kjente dem. Vi snakket seinere med paret, som nettopp hadde innledet et forhold. Ingen av dem ønsket å la seg intervju, men samtykket til at vi brukte en sladdet versjon av klinesekvensen. Paret var lite fornøyd med nattklubbens datasikkerhet.

I den påfølgende konfrontasjonen med Klubbteaterets ledelse, filmet vi deler av intervjuet fra Oslo, via nattklubbens eget overvåkningskamera.

Jakten på det røde kjøleskapet

Ett av de mest teknisk avanserte overvåkingskameraene vi fant i våre søk, filmet en stue med åpen kjøkkenløsning, et rødt kjøleskap og et lite, rundt spisebord. Over kjøkkenet var det en glasshems med store, runde skruer i stål. Via kameraets tekniske funksjoner var det mulig å gjøre opptak, høre lyd og snakke til de menneskene som befant seg i leiligheten.

Vi ønsket å komme i kontakt med eieren, både for å advare vedkommende, og for å rette en intervjuforespørsel for å illustrere følgene av sviktende datasikkerhet i private overvåkingskameraer. Vi vurderte det som uansvarlig, og i strid med de etiske og juridiske grunnreglene våre, å snakke til eieren via kameraet hans. Og ikke minst, vedkommende kunne ha fått et illebefinnende hvis Dagbladet plutselig snakket til ham via kameraet på veggen. Så hvordan skulle vi finne ham?

Den eneste informasjonen vi hadde å gå på, var at leiligheten ifølge geolokaliseringen av IP-adressen trolig befant seg i Stavanger. I tillegg visste vi altså hvordan kjøkkenet og stua så ut. Vi ønsket imidlertid ikke å sende rundt skjermbilde av leiligheten elektronisk, i tilfelle det skulle komme på avveie.

Vi hadde også informasjon om merke og modell på overvåkingskameraet, og begynte å snakke med en av de norske leverandørene for å finne ut mer om selve kameratypen. Da fant vi ut at kameraet var relativt dyrt og svært avansert, og derfor ikke vanlig blant privatkunder. Den aktuelle modellen var gått ut av produksjon for flere år siden. Kunne det være snakk om en pendlerleilighet som tilhørte en bedrift, som brukte et eldre kamera til å overvåke de ansatte som bodde der?

Basert på det interiørbildet vi hadde, tenkte vi at det trolig var snakk om en liten toromsleilighet. Vi lette derfor først etter lignende leilighetstyper på Finn.no. Der søkte vi etter "alkove" og "hems" i eiendom under 55m², uten geografisk begrensning. Dette ga oss flere interessante treff, og det var særlig to gater som gikk igjen. I tillegg snakket vi med en utleiemegler i Stavanger. Basert på våre beskrivelser, mente han at leiligheten trolig lå på én av tre konkrete adresser i de gatene vi hadde kommet fram til via våre søk på Finn.no. Vi bestemte oss for at vi hadde nok informasjon til å reise til Stavanger og banke på dører, på tross av at det fortsatt var litt som å lete etter ei nål i en høystakk.

De aktuelle leilighetsbyggene var svære, og etter å ha gått fra dør til dør på to av adressene uten hell, besøkte vi den samme utleiemegleren vi hadde snakket med på telefon, for å vise fram skjermbildet fysisk. Basert på skruene på hemsen, mente flere på meglerkontoret at leiligheten trolig lå på den tredje adressen vi ennå ikke hadde besøkt. Her hadde vi hellet med oss. Etter å ha ringt på flere dører, traff vi eieren av leiligheten med det røde kjøleskapet. Det viste seg å være en mann som jobbet med overvåkingskameraer, og dette var grunnen til at han hadde et såpass avansert kamera. Vedkommende ønsket imidlertid verken navn eller bilde på trykk i Dagbladet, noe vi selvfølgelig måtte respektere. Dette er bare ett eksempel på funn vi har lagt ned mye tid på å finne ut av, som ikke har resultert i noe på trykk.

6.7 Konfrontasjon og kildekritikk

I forbindelse med Null CTRL, har vi gjort feltarbeid i Oslo, Drammen, Gjøvik, Fredrikstad, Hønefoss, Lillehammer, Bergen, Stavanger, Stathelle, Moss, Kviteseid, Otta, Trondheim, Bjugn, Frosta, Bodø, Lofoten og Sortland, samt et par steder vi ikke kan oppgi av hensyn til

anonymitet. Deler av feltarbeidet innebar ordinære intervjuer med personer eller bedrifter berørt av sviktende datasikkerhet og deres reaksjoner på Dagbladets funn.

Men i flere tilfeller var konfrontasjonene langt mer kompliserte, fordi det er vanskelig å vite hva styringssystemene vi fant i hvert enkelt tilfelle kontrollerer. Vi kan heller ikke teste systemene, fordi vi ikke vet hva slags konsekvenser det vil få. Problematikken kan sammenlignes med at du finner en lysbryter, men ikke kan se hvor det blir mørkt hvis du trykker på den. Vi visste dermed ikke om funnene kunne misbrukes av personer med ondsinnede hensikter, og hvorvidt det var problematisk at materialet lå åpent tilgjengelig på Internett eller ikke, den grunnleggende journalistiske motivasjonen for prosjektet.

“Dette er da ikke problematisk”

24. oktober 2013 hadde Dagbladet.no en artikkel på trykk om åpne inngangsporter til Jernbaneverkets alarmsentraler.



- Kan vi få lov til å trykke her nå?
- Nei, absolutt ikke, absolutt ikke

Dagbladet fant inngangsportene til 15 av Jernbaneverkets brannalarmsentraler åpent på Internett.
[Les mer](#)



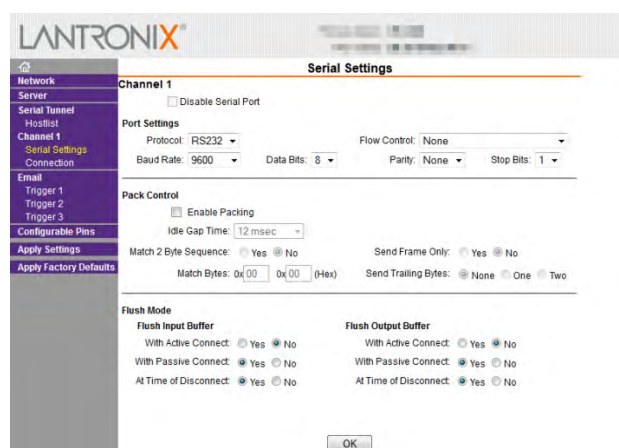
- Det er svært alvorlig, det bør bekymre noen hver

Reagerer på sikkerhetshull hos Jernbaneverket.
[Les mer](#)

Skjerm bilde: Artikler publisert på Dagbladet.no i oktober 2013.

Som med flere andre saker om styringssystemer, var denne artikkelen resultat av møysommelige konfrontasjoner med de involverte.

Vi begynte arbeidet med en rekke funn som så slik ut:



Skjerm bilde: En av inngangene til Jernbaneverkets alarmsentraler

Styringssystemet over var registrert med en IP-adresse tilhørende Jernbaneverket, men hva i alle dager kan man kontrollere via akkurat dette panelet? I og med at kollektivtransport kan være særlig utsatt for sabotasje via Internett, og Jernbaneverket er et stort statlig selskap som burde ha kontroll på datasikkerheten, ønsket vi å granske de 15 panelene nærmere.

Vi visste at Lantronix-servere ofte brukes til ekstern kontroll av utstyr over Internett, men ikke hva Jernbaneverket i dette tilfellet konkret hadde koblet systemet opp mot i sin infrastruktur. Vi plottet IP-adressene i et kart for å se om den geografiske plasseringen kunne gi oss et nærmere hint om hva dette var, men ble ikke spesielt klokere.

Uten svar, men med spørsmål, avla vi Jernbaneverket en visitt og viste dem hva vi hadde. Etter flere runder på e-post, telefon og ansikt til ansikt med ulike personer i Jernbaneverket, fikk vi etter hvert vite at dette var inngangsporter til brannalarmsentraler i Jernbaneverkets kraftforsyning. Med tilgang til panelene kunne uvedkommende ha hindret Jernbaneverket å få informasjonen fra de respektive brannsentralene.

Likevel var omkvedet: “Det er veldig flott at dere setter fokus på datasikkerhet, men akkurat dette er ikke problematisk”.

Vi spurte derfor om det var greit at vi testet en av knappene i et panel. Svaret var kort og kontant: “Nei, det må dere absolutt ikke gjøre.” Det ble også ble vinklingen på reportasjen.

Dette illustrerer problemene vi møtte når vi var avhengig av involverte parter for å finne ut hva et spesifikt system styrte. Noen prøvde å hevde systemet var helt ufarlig, andre at det var snakk om et helt annet system. Vi etterstrebet derfor alltid å ha sikret oss så god informasjon om systemene som mulig, gjennom bakgrunnsamtaler med leverandører, teknisk kyndige kilder og kilder med kjennskap til den aktuelle bransjen involvert. I tillegg satte vi oss inn i bruksanvisninger for kompliserte systemer. Vi måtte også utøve en kontinuerlig kildekritikk, teste påstander med andre kilder, og i noen tilfeller ha gjentatte møter med involverte parter, før vi satt med et helhetlig bilde vi kunne bruke i reportasjen.

Et annet eksempel på vanskelige intervjuobjekter, er saken om sensitive, sivile dokumenter vedrørende Ørland flystasjon, som en ansatt la i en åpen server ved en feil.



NY INFORMASJON: Store dokumenter om Ørland flystasjon lå tilgjengelig på en videregående skole, privat nettside og en kafe i Cyberforsvaret.

La ut dokumenter om Norges nye kampfly-base ved en feil

Detaljerte dokumenter om Ørland flystasjon lå åpent på Internett. En potensiell fare for rikets sikkerhet, mener kilden i Cyberforsvaret. Ufarlig, mener Luftforsvaret.

NY KAMPFLYBASE: Ørland flystasjon er en av Luftforsvarets to hovedflystasjoner, og opererer F16 jagerfly, redningshelikoptere og helikopter med våpen. I juni i fjor vedtok Stortinget at Ørland skal bli Norges nye kampflybase. Foto: Mikkel Østland

NY INFORMASJON: Store dokumenter om Ørland flystasjon lå tilgjengelig på en videregående skole, privat nettside og en kafe i Cyberforsvaret.

Detaljerte dokumenter om Ørland flystasjon lå åpent på Internett. En potensiell fare for rikets sikkerhet, mener kilden i Cyberforsvaret. Ufarlig, mener Luftforsvaret.

NY KAMPFLYBASE: Ørland flystasjon er en av Luftforsvarets to hovedflystasjoner, og opererer F16 jagerfly, redningshelikoptere og helikopter med våpen. I juni i fjor vedtok Stortinget at Ørland skal bli Norges nye kampflybase. Foto: Mikkel Østland

NY INFORMASJON: Store dokumenter om Ørland flystasjon lå tilgjengelig på en videregående skole, privat nettside og en kafe i Cyberforsvaret.

Detaljerte dokumenter om Ørland flystasjon lå åpent på Internett. En potensiell fare for rikets sikkerhet, mener kilden i Cyberforsvaret. Ufarlig, mener Luftforsvaret.

NY KAMPFLYBASE: Ørland flystasjon er en av Luftforsvarets to hovedflystasjoner, og opererer F16 jagerfly, redningshelikoptere og helikopter med våpen. I juni i fjor vedtok Stortinget at Ørland skal bli Norges nye kampflybase. Foto: Mikkel Østland

Faksimile: Dagbladet 29. oktober 2013

På tross av at dokumentene var svært detaljerte, var vi ikke sikre på om det var sensitiv informasjon eller ikke. En rekke offentlige etater hevdet at dette var helt ufarlig informasjon. Men i Cyberforsvaret fikk vi beskjed om at det utgjorde “en fare for rikets sikkerhet”. Vi fortsatte presset på andre etater. Her er en dialog med Luftfartstilsynet, etter at Dagbladet hadde sendt over dokumentene:

Luftfartstilsynet: “Dette dreier seg om lokale prosedyrer for lufttrafikkjenesten og majoriteten av opplysningene ligger tilgjengelig i AIP (Aeronautical Information Publication, Norway), som er offentlig informasjon.”

Dagbladet: “OK, har du noen lenke til hvor jeg finner dette? Det er jo mye spesifikk informasjon om denne flyplassen.”

Luftfartstilsynet: “Du finner AIPen her: <https://www.ippc.no/ippc/index.jsp>”

Dagbladet: “Den har jeg funnet, men jeg finner ingen av de dokumentene jeg sendte dere her, kunne du ha gitt meg en pekepinn på hvor jeg finner de hen?”

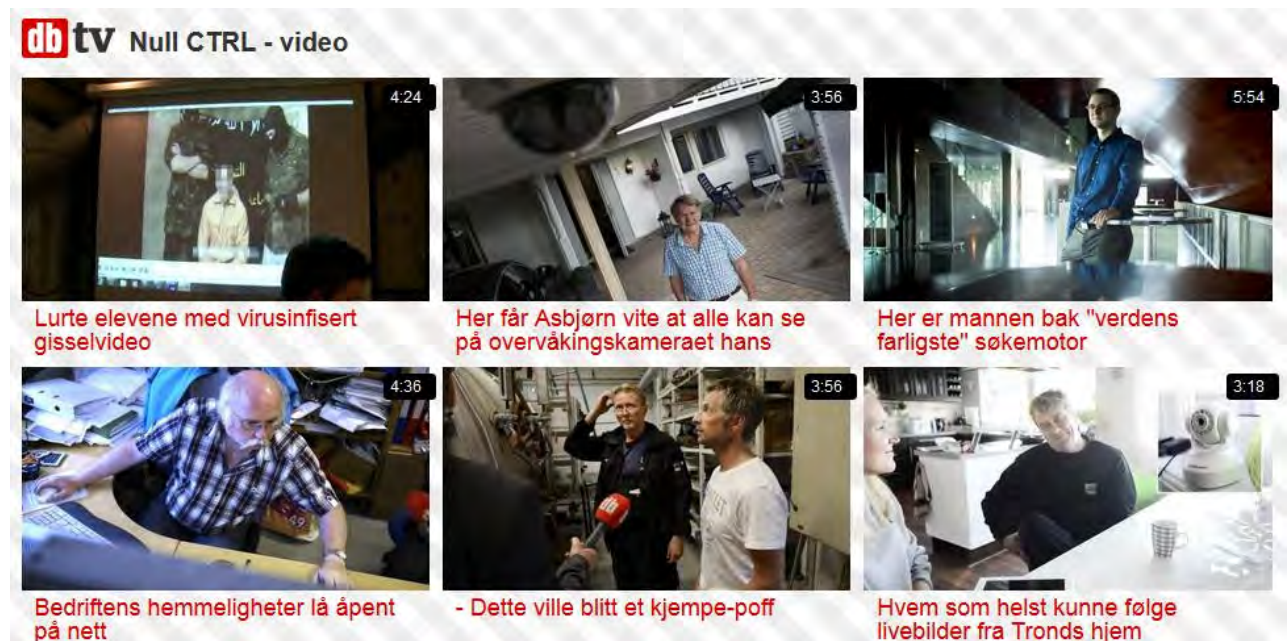
Det kunne vedkommende ikke, og vi ble til slutt henvist til en annen leder. Denne medga at flere av dokumentene ikke er offentlige - og at de kunne misbrukes.

Video som metode

I konfrontasjoner med enkelte rammet av dårlig datasikkerhet, var den første kommentaren at “Da må dere ha hacket oss”. Det hadde vi forutsett, og hadde derfor på forhånd filmet hvordan vi via PC gikk inn på styringssystemer, servere og kameraer. Slik kunne vi dokumentere at vi ikke tastet passord eller gjorde kompliserte datatekniske øvelser for å få tilgang.

Svært mange konfrontasjoner i felt er også filmet fra begynnelse til slutt for å dokumentere at vi har varslet eier, i tilfelle det skulle oppstå problemer i ettertid eller eventualiteter underveis. Vi visste at sviktende datasikkerhet kunne være et følsomt tema for mange, og tok derfor forholdsregler.

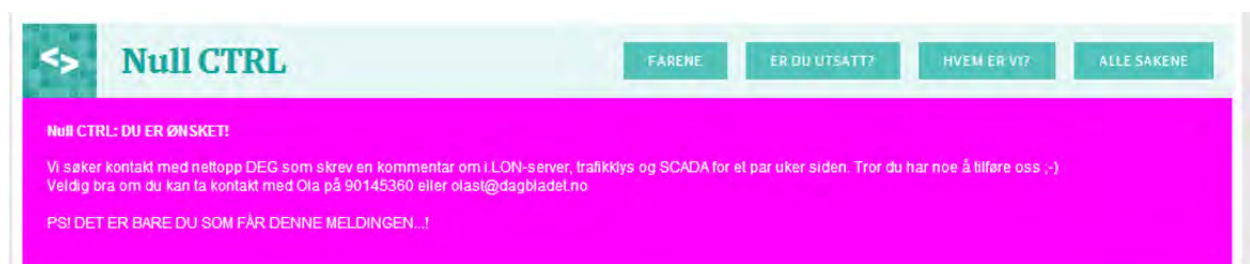
Øistein Norum Monsen har vært seriens videoansvarlig, med regi på et stort videomateriale som har resultert i en egen videoserie publisert på Dagbladet.no. Video er også benyttet for å vise konkret hvordan kameraer, printere og styringssystemer kan misbrukes av hvem som helst via nettet.



6.8 Beskjed til ukjent leser

For hver sak som ble publisert, kom det inn stadig nye tips via prosjektets egen tipsmail nullctrl@dagbladet.no. I tillegg ble kommentarfeltene fort fylt, noen ganger med gode innspill. Tidlig i serien var det et innlegg i et kommentarfelt vi fattet særlig interesse for, fordi vedkommende som skrev kommentaren så ut til å ha god kjennskap til et spesielt styringssystem som vi hadde funnet mange av, men ikke forstod. Systemet brukes etter alt å dømme til å kontrollere gatelys. Vi ønsket derfor kontakt for å forstå mer.

Avsender av innlegget var anonym, og det eneste vi kjente var IP-adressen. Vi la derfor på en ekstra boks på alle Null CTRL-artiklene, som oppfordret den aktuelle leseren til å ta kontakt med oss. Boksen vises kun på vedkommendes IP-adresse



Skjerm bilde: Boks koblet mot IP-adresse, med oppfordring om å ta kontakt

Dette er første gang vi har utviklet et verktøy for å komme i kontakt med en konkret tipser. Per 6. januar er boksen vist for leseren 42 ganger, men ingen har foreløpig tatt kontakt. Utviklingen av denne boksen fikk oss imidlertid til å innse hvor viktig det var å utvikle egne, interaktive verktøy i forbindelse med Null CTRL. Neste metode ble en knallsuksess.

6.9 Egenutviklet test-motor

Vi avdekket etter hvert så mange og store svakheter i norsk datasikkerhet, at vi ønsket å gi leserne hjelp på veien. Det ble starten på [en egenutviklet test-funksjon](#) Dagbladet.no nå tilbyr, hvor alle kan sjekke om de er registrert med utstyr liggende åpent på nett.

Den automatiserte tjenesten ble utviklet av Dagbladet etter avtale med Shodan-grunnlegger John Matherly. Leseren kan selv slå opp egen IP-adresse i en statisk database og få svar på om IP-adressen er registrert med noen kjente feil, og eventuelt en beskrivelse av hva den potensielle risikoen er.

Det er lagt inn en sikkerhetssjekk så ingen andre kan bruke testen og presentere den som sin egen på annen nettside. For å forhindre bruk av vår test til vilkårlige oppslag, samt forenkle bruken for leserne, bruker vi den IP-adressen leseren gjør forespørselen fra. En av fire som har tatt Dagbladets test har hatt åpne porter.

I og med at Shodans database er statisk, er testen kun å betrakte som en veileder. Den gjør ingen sanntidssjekk av IP-adressene, men slår opp i en base hvor IP-adressene allerede er kontrollert. Dette betyr at det kan være åpent utstyr på en IP-adresse som ikke slår ut på testen, fordi det ble koblet til etter at kontrollen ble gjennomført. På den andre siden vil testen heller ikke oppdateres dersom åpent utstyr blir sikret i etterkant. I helt spesielle tilfeller, hvor en bruker har overtatt en tidligere brukt IP-adresse, kan testen vise resultater fra andre kunder hos samme leverandør. Dette har vi vært nøye med å presisere for leserne.



Skjerm bilde: En IP-adresse registrert med flere sikkerhetshull.

7. Spesielle erfaringer

7.1 Blindveier

I noen tilfeller er det ikke mulig å finne ut hvem som faktisk eier systemer vi finner. Det er i tilfeller hvor IP-adressen bare er registrert på nettleverandøren, som har taushetsplikt. Noen ganger måtte vi derfor bare innse at vi ikke kom i mål, og skrinla saken. I saker med potensielt kritiske systemer varslet vi da Nasjonal sikkerhetsmyndighet (NSM) og/eller internettleverandør, slik at sikkerhetshullene i det minste ble lukket.

Vi har også eksempler hvor vi har misforstått hva vi ser. Vi har funnet tilsynelatende kritiske styringssystemer åpne på nett - for eksempel til to vindmølleparker i Midt-Norge. Lederne i energiselskapet som eide systemet fikk hakeslepp da de så styringsfunksjonene vist på Dagbladets PC. Men i tett dialog fant vi sammen ut at styringssystemet ikke kontrollerte drift av møllene eller kraftleveranse og i virkeligheten bare kunne brukes til strømvlesing. Ved overgangen til 2014 har vi fortsatt store mengder saker vi ikke har løst, og kanskje aldri kommer til å rekke over.

7.2 Overraskende reaksjoner

Takk!

Vi har oppsøkt svært mange mennesker med dårlig datasikkerhet. For noen har konsekvensene vært store, privat, jobbmessig eller økonomisk. Derfor forventet vi at enkelte ville kunne reagere sterkt når vi banket på døra og viste dem hvordan de var tatt med buksa nede. Vi forventet litt ubehag. Det skjedde ikke.

Med få unntak, har alle reagert overraskende positivt. Den allmenne reaksjon, er at eierne av problemet takker for at de blir advart. Et eksempel er bedriften Lofotnett, som leverte betydelige mengder IT-tjenester. Her fant vi en server med blant annet kundenes passord liggende åpent tilgjengelig på nett.

“Jeg ser for meg at det er kroken på døra for det her firmaet, så alvorlig ser jeg på at den her type informasjonen har kommet ut. Men gud fader jeg er glad for at jeg ble gjort oppmerksom på det, slik at jeg kan få berga det som er”, sa eier og daglig leder Jarl Salomonsen minutter etter at han forsto alvoret bak Dagbladets besøk hos ham.

Bedriften har seinere begjært oppbud.

Tette bånd

På tross av at det finnes flere offentlige instanser involvert i norsk datasikkerhet, viste det seg i noen tilfeller vanskelig å få konkrete uttalelser om våre ulike funn.

I de mest alvorlige sakene, er for eksempel NSM den offentlige instansen det ville være mest naturlig å innhente kommentarer fra. De største samfunnsaktørene i Norge er imidlertid “kunder” av NSM, og sikkerhetsmyndigheten ønsker ikke å kommentere saker direkte relatert til disse.

Problematikken ble forsterket av at involverte selskaper kunne være svært ordknappe selv. I ett tilfelle satt vi i en situasjon hvor NSM oppfordret oss på det ytterste til å vente et par dager ekstra med publisering, fordi de mente dokumentene på serveren vi fant virket så sensitive at dette var nødvendig. De ønsket imidlertid ikke å ha noen konkrete kommentarer på trykk. De

berørte parter ville heller ikke kommentere utover enstavelsesord. Vi kunne dermed ikke formidle hvor alvorlig saken egentlig var.

7.3 Egen sikkerhet

Ved å publisere en omfattende artikkelserie om sviktende datasikkerhet, forsto vi at vi ville kunne eksponere oss for hackere og andre som ville granske om Dagbladet hadde orden i eget hus - og muligens utnytte eventuelle sikkerhetshull.

Vår driftsleverandør av web-tjenester, Basefarm, ble derfor tidlig varslet om serien som skulle komme og fulgte godt med i de første dagene etter lansering. I tillegg mente vi det var en viss risiko for at reportere og fotografer med byline i Null CTRL kunne bli utsatt for inntrengningsforsøk, så vi foretok også en gjennomgang av egen datasikkerhet i forkant av publisering.

Dagbladets ansatte fikk tidlig mulighet til å sjekke sin egen hjemmesikkerhet med testen Dagbladet utviklet. I denne forbindelse ble noen hull funnet og tettet. Totalt 17,5 prosent av de ansatte som tok testen hadde åpne enheter registrert på sin IP-adresse. 75 porter sto åpent totalt. Som ventet ble vi ganske raskt kontaktet av et par eksperter som hadde tatt for seg sikkerheten til Dagbladet.no. En av disse leverte en skriftlig oppskrift på konkrete sikkerhetshull som berørte både Dagbladet og VG. Disse ble fulgt opp og tettet. VG ble varslet på ledernivå. I tillegg mottok vi et par e-poster fra hackere uten edle motiver, med mer eller mindre fordekke trusler.

8. Etiske og juridiske problemstillinger

8.1 Egendefinerte regler

Hvor går grensen etisk og juridisk når du gransker datasikkerhet? Dette er et komplisert spørsmål, med mange gråsoner og regler det kan være vanskelig å orientere seg i. I Norge er det få klare domsavsigelser å lære av, men Høyesterett har blant annet trukket et skille mellom gode og onde hensikter.

Før vi begynte å gjøre research, gikk vi mange runder på hvordan vi kunne gå fram. Vi drøftet prosjektet med vår advokat og definerte noen klare grenser vi ikke kunne krysse. I tillegg snakket vi med norske og internasjonale IT-eksperter som har gjort noe tilsvarende undersøkelser, for å få et innblikk i hvordan de forholdt seg til etiske og juridiske spørsmål rundt testing av datasikkerhet. Underveis har vi hatt dialog med NSM, Norsis og andre myndigheter.

Den første regelen vi ble enige om, var at vi aldri skulle teste ett eneste passord. Vi skulle heller ikke teste standardpassord, som mye utstyr blir levert med fra leverandøren, selv om det er et velkjent problem i sikkerhetsmiljøene at disse passordene ofte ikke byttes ut. Vi skulle kun granske enheter som lå åpent tilgjengelig på nettet, uten noen som helst beskyttelse. Dette gjaldt også tilfeller hvor passordene bokstavelig talt ble servert.



Skjerm bilde: Eksempler på enheter som oppgir passord, men som vi av etiske grunner ikke har testet

Det betyr at vår kartlegging av datasikkerhet stopper der det må testes passord. For personer med andre etiske og juridiske vurderinger enn oss, ville det imidlertid trolig vært så enkelt å ta seg inn. Omfanget av sårbare systemer i Norge er derfor sannsynligvis langt større enn vi har avdekket.

Regel nummer to er at vi aldri skal gjøre noe med systemene vi finner, med mindre vi har eksplisitt tillatelse fra eieren. Vi kunne for eksempel ikke sjekke hvordan et styringssystem fungerte eller hvorvidt det var mulig å endre dokumentene i en database. I tillegg var det viktig for oss å aldri skjule IP-adressen vår når vi utførte granskingen. Dersom noen ønsket å spore IP-adressen vår, ville de derfor med en gang se at den var registrert på AS Avishuset Dagbladet.

Det må presiseres at vi ikke har gjort noen form for portscanning i våre undersøkelser, men kun gjennomført søk mot en statisk database. Vi har også avslørt minst mulig om de søketermene vi har brukt, så søkene våre ikke kan repeteres av folk med andre hensikter.

I omtale av privatpersoner og private data, har vi kun publisert saker hvor personene har samtykket til dette. Vi har varslet en rekke privatpersoner som ikke ønsker omtale. Flere artikler kunne også ha vært skrevet mer individorientert og konfronterende enn vi har valgt å gjøre. Men vi har løst det slik fordi vi i enkelte tilfeller har vurdert at det er en urimelig stor belastning å henge ut en underordnet enkeltperson på vegne av en dataglipp. Ingen selskaper eller offentlige instanser har motsatt seg publisering.

8.2 Varsling av aktører

Det har vært grunnleggende viktig for oss at de personene vi har konfrontert med sikkerhetshull har fått god tid til å sikre sine data før publisering av saken. Vi har derfor flere ganger avventet

publisering til sikkerhetshullene var tettet. I en rekke tilfeller har vi også avventet at flere hundre brukere med tilsvarende sikkerhetssvikt har fått rimelig tid til å rydde opp. Vi har også holdt igjen saker i forbindelse med sikkerhetssvikt hvor eieren av problemet ikke har ønsket å innse at det eksisterer et problem.

Vi varslet også også aktører som ikke ble omtalt i våre artikler, men som var eksponert for lignende sikkerhetshull, ettersom vi ikke ønsket at serien skulle oppfordre til hacking. Dersom vi ikke fant eieren av IP-adressen, varslet vi enten NSM eller internettleverandør, avhengig av alvorlighetsgrad. Internettleverandør varslet deretter eier. Totalt har Dagbladet meldt inn rundt 2500 mulig kritiske IP-adresser.

I tilfellene hvor internettleverandør ble varslet (mindre alvorlige sikkerhetshull), måtte vi søke opp registrert eier av alle IP-adressene og lage lister med alle nettleverandørene, et tidkrevende arbeid.

I noen spesielle tilfeller mente også internettleverandøren at selv ikke de kunne varsle eieren om sikkerhetshullet, fordi de av personvern hensyn ikke kunne koble IP-adresse med kundeinformasjon. Vi ga da adressen videre til sikkerhetsmyndighetene.

9. Konsekvenser

Serien “Null CTRL” har ikke én konsekvens, den har flere tusen. De fleste av våre artikler beskriver feil vi har funnet, som leder til reaksjon og konsekvens.

For eksempel er følgende konkrete sikkerhetshull tettet som direkte følge:

- Fem åpne servere med sensitive data om norsk oljeindustri er stengt ned
- 39 kommuner i Nordland har fått tryggere brannberedskap
- Du kan ikke lenger spore opp barn på med hemmelig ID via Oslo Taxi, som har fjernet sensitive data om inntil 5958 kunder
- Sensitive dokumenter om Norges nye kampflyplass finnes ikke lenger på nett
- Lofotnett har ikke lenger kundenes passord liggende åpent på nett
- Du kan ikke lenger se ungdom fylle og kline på Klubbteateret
- 290 navngitte bygg innen skole, helse og forsvar er ikke lenger sårbare
- Du kan ikke lenger tukle med Jernbaneverkets brannalarmer
- Minst et tresifret antall overvåkingskameraer er sikret eller fjernet fra nett.
- Uvedkommende kan ikke lenger følge med på kundenes tasting av pin-koder på Frostasenteret.
- Det går ikke lenger å følge gjestene på hjemmesiden til Cafe Sør og åpent kamera på Jacob Aalls.
- Kikkere fra hele verden får ikke lenger se live-TV fra et soverom i Nord-Trøndelag.
- Fiskebollefabrikken Vesteraalens er mindre utsatt for potensiell terror/sabotasje.
- Flere tusen kunder er advart mot mulig feil ved rutere fra to ulike bredbåndsløseleverandører.
- Beboere i en rekke leilighetsbygg er ikke lenger sårbare for sabotasje mot varmestyringen.
- En industriell robot tilhørende et Statoil-selskap kan ikke lenger styres av uvedkommende.
- Avanserte printere med åpne og tilgjengelige dokumenter, er lukket Norge rundt.
- Viasats kunder er ikke lenger utsatt for lekkasje av fakturainformasjon.

- Uvedkommende kan ikke lenger spore kunder ved inntil 40 taxi-sentraler i Norge og Danmark.
- Bemanningsbyrået Veksthuset har ikke lenger sensitive data om jobb-kandidater åpent på nett.
- Hvem som helst kan ikke lenger styre tog-vaskehallen i Stockholm.
- Et irsk fylke fjerner kloakksystemet fra åpen nett-løsning.

Alle sakene finner du her: <http://www.dagbladet.no/nullctrl/>

Generelle konsekvenser

- 2500 potensielt kritiske IP-adresser er meldt inn til NSM, eiere og/eller nettleverandører
- Flere tusen sikkerhetshull er tettet som direkte følge av Null CTRL
- Privatpersoner, bedrifter og samfunnsaktører er bevisstgjort om datasikkerhet
- En av fire som har benyttet Dagbladets test-motor har fått varsel om en eller flere åpne porter som bør undersøkes nærmere
- Norsis og Datatilsynet har på bakgrunn av Null CTRL utarbeidet ny veileder for sikring av web-kamera.
- Justis- og beredskapsminister Anders Anundsen har varslet at han ser for seg endringer i lovverket.

Hva andre sier

Seriens betydning for bevisstgjøring av privatpersoner, bedrifter og myndigheter, førte til at Dagbladet i år ble tildelt databransjens egen fagpris, Rosing-prisen. Juryen skriver blant dette om konsekvenser for landets IT-sikkerhet:

“....gjennom en lengre periode og stor innsats har satt informasjonssikkerhet på dagsorden for veldig mange - og utøvd en rolle som har gitt resultater langt utover sin vanlige og forventede funksjon. Vinneren har igjennom sitt arbeid bevisstgjort både vanlige private personer, bedrifter, media og myndigheter.

Vinneren utmerker seg ved å bruke gravejournalistikk, nærbilder og menneskelige fortellinger om sikkerhetsmessige konsekvenser.

Resultatet gjør informasjonssikkerhet og sårbarheter forståelig på et nivå folk kan forstå og relatere seg til og vinneren kan vise til omfattende resultater av å teste datasikkerheten for hele Norge.

Et sekssifret antall IP-adresser og enheter på nett er undersøkt, og flere tusen kritiske systemer er avslørt som sårbare. Arbeidet har medført at flere instanser har varslet om regelendringer og nye veiledninger. Totalt er et firesifret antall sikkerhetshull lukket som direkte følge av arbeidet.”

Juryens begrunnelse

“I've been following the stories and it's far beyond any expectations I had. It's very unusual for me that journalists are able to research this sort of stuff without my hand-holding. You guys are the only ones that showed technical competence out of all the newspapers/TV stations etc. that I've worked with. It's seriously impressive.

John Matherly, Shodan-grunnlegger

”Dagbladet har i artikkelserien «Null CTRL» påvist en rekke svakheter i datasikringen i Norge (...) Cyberkriminalitet har blitt en storindustri, mer lukrativ enn narkohandel, ifølge Interpol. Dagbladet gjør derfor et viktig bidrag til å øke sikkerheten for oss alle ved å sette søkelyset på eksponeringen ny teknologi utsetter oss for.”

Niklas Vilhelm, Nasjonal sikkerhetsmyndighet

10. Liste over publiserte saker

Dato	Tittel	Plattform
02.10.2011	Dagbladet fant 2048 norske overvåkings-kameraer på Internett	NETT
02.10.2011	Her fester og kliner de unge gjestene for åpent kamera	NETT/DBTV
02.10.2011	Politi- og idrettskjendis filmet på jobb i sivil	NETT
03.10.2011	Alle ser deg	PAPIR
03.10.2011	Her kan du se pinkoder, safen og naboene ta solarium	NETT/DBTV
03.10.2011	«Skremmende», «uakseptabelt», «skummelt», «forferdelig»	NETT
04.10.2011	Her filmer Dagbladet med restaurantens eget kamera	NETT/DBTV
04.10.2011	Her har de filmet datene dine og sendt dem direkte på nett	NETT/DBTV
04.10.2011	Vil ta affære etter Dagbladets kamera-avsløringer	NETT
05.10.2011	Her får Asbjørn vite at overvåkingskameraet hans ligger åpent på nett	NETT/DBTV
05.10.2011	Overvåket av eget kamera	PAPIR
05.10.2011	Hvem som helst kunne følge livebilder fra Tronds hjem	NETT/DBTV
06.10.2011	Hele verden spionerte på soverommet i norsk hytte	NETT
07.10.2011	Hele verden spionerte på soverommet i norsk hytte	PAPIR
07.10.2011	- Den nye trenden er å hacke forbrukerelektronikk	NETT
08.10.2011	- Slike opptak kan enkelt brukes til utpressing	NETT
08.10.2011	ALARM! Nødsentralen lå åpen på nett	PAPIR
08.10.2011	- Fatter ikke at det er mulig	PAPIR
08.10.2011	ALARM! Nødsentralen lå åpen på nett	NETT/DBTV
08.10.2011	- Fatter ikke at det er mulig	NETT
08.10.2011	- Dette er ufattelig sløvt. Særlig etter 22. juli og alt fokuset vi har	NETT

hatt på beredskap og sikkerhet i samfunnet

09.10.2011	- Om en faen vil sprengre dette, er det bare å skru igjen her...	PAPIR
09.10.2011	<u>- Om en faen vil sprengre dette, er det bare å skru igjen her...</u>	NETT/DBTV
09.10.2011	<u>- Det er klart dette kan brukes til sabotasje: Kystvakta og kjøpesenteret ligger rett ved</u>	NETT
10.10.2011	Varslet - men fant ikke feil	PAPIR
10.10.2011	<u>- Jeg husker vi ble varslet, men vi fant ingen feil</u>	NETT
13.10.2011	- Ingen tør å ta tak i det	PAPIR
13.10.2011	<u>- De er fullstendig tafatte hele gjengen</u>	NETT/DBTV
14.10.2011	Kundenes sensitive data lå åpent på nettet	PAPIR
14.10.2011	<u>«Det er et forferdelig sjokk - og trolig kroken på døra»</u>	NETT/DBTV
15.10.2011	Lurer seg inn din bakdør	PAPIR/PLUSS
17.10.2011	Ute av styring	PAPIR
17.10.2011	<u>- I verste fall kan liv gå tapt</u>	NETT
17.10.2011	<u>Her kan Dagbladet skru av varmen i et kvartal</u>	NETT
17.10.2011	<u>14-åring fjernstyrte trikker, fire sporet av og 12 personer ble såret</u>	NETT
17.10.2011	<u>Dette systemet styrer produksjonsroboten til et Statoil-selskap</u>	NETT
18.10.2011	- Det er ikke et spørsmål om, men når vi blir angrepet	PAPIR
18.10.2011	<u>- Det ikke er et spørsmål om vi blir utsatt for et sånt angrep, det er et spørsmål om når</u>	NETT/DBTV
21.10.2011	Vokt deg for printerspionasje	PAPIR
21.10.2011	<u>- Lå dette åpent på nett?! Jeg ante ikke at det gikk an engang</u>	NETT/DBTV
23.10.2011	<u>Slik avslører Dagbladet råtten sikkerhet på norske PC-er</u>	NETT
23.10.2011	<u>Her er mannen bak «verdens farligste søkemotor»</u>	NETT/DBTV
23.10.2011	<u>Så lett beskytter du deg</u>	NETT
23.10.2011	<u>Sjekk din datasikkerhet med Dagbladets testmotor</u>	NETT
24.10.2011	<u>- Kan vi få trykke her nå? Nei, absolutt ikke, absolutt ikke</u>	NETT
24.10.2011	<u>Slik sto det til med Dagbladets datasikkerhet</u>	NETT
25.10.2011	<u>- Det er svært alvorlig, det bør bekymre noen hver</u>	NETT

28.10.2011	Blottlagt av Get	PAPIR
28.10.2011	Er din PC sikker?	PAPIR
28.10.2011	Thomas' Get-boks lå åpen ut mot nettet	NETT
29.10.2011	Hver fjerde har mulig svikt i datasikkerheten	NETT
29.10.2011	- En fare for rikets sikkerhet	PAPIR
29.10.2011	La ut dokumenter om ny kampflybase ved en feil	NETT
30.10.2011	- Det er så alvorlig at vi har stengt tjenesten	NETT
30.10.2011	Så sårbar er du hjemme i din egen stue	NETTGRAFIKK
25.11.2011	Barn på hemmelig adresse blottlagt av dataglipp	NETT/DBTV
25.11.2011	- Jeg reagerer med skrekk	NETT
25.11.2011	- Det kan sette barn i fare om dette kommer ut	NETT
25.11.2011	Oslo kommune vurderer avtalen med Oslo Taxi	NETT
26.11.2011	Dagbladet har overlevert 2500 IP-adresser til NSM, eiere og leverandører	NETT
26.11.2011	Dagbladet fant åtte åpne drosje-servere på nett	NETT
27.11.2011	Slik kan hackere ta kontroll i norske banker, skoler, sykehjem - og en militærleir	NETT
27.11.2011	- Dette vil være spesielt uheldig for vårt sykehjem	NETT
27.11.2011	Domstolene sjekker datasikkerheten etter «Null CTRL»-avsløring	NETT
09.12.2011	Fant sensitive dokumenter om norsk oljebransje - lå åpent på nett	PAPIR
09.12.2011	Sensitive dokumenter om norsk oljebransje lå åpent på nett	NETT
09.12.2011	- I verste fall kan dette føre til tap av verdier i 100-millionersklassen	NETT
10.12.2011	- Tabben jeg aldri skal gjøre igjen	PAPIR
10.12.2011	Slik blottlegges dokumenter	PAPIR
10.12.2011	- Den feilen gjør jeg ikke igjen	NETT
10.12.2011	Slik blottlegges dokumenter på Internett	NETT
10.12.2011	Trodde de måtte taste navn og passord for å komme inn på bedriftens server	NETT
11.12.2011	Sjefen er dataversting	PAPIR

11.12.2011	- Dette har ikke noe i offentligheten å gjøre	NETT
12.12.2011	Frykter hacking av strømmettet	PAPIR
12.12.2011	- Denne typen tiltak gjør oss mer sårbare for ondsinnede angrep	NETT
19.12.2011	- Er det tilgang til kontrollpanelene eller at det går alarmer dere reagerer på?	NETT
20.12.2011	Skjerper datasikkerheten	PAPIR
20.12.2011	Her kan hvem som helst kontrollere vaskeanlegget til lokaltogene i Stockholm	NETT
20.12.2011	Her er kloakksystemet til et helt irsk fylke	NETT
22.12.2011	- Konsekvensene ved et angrep er større enn man forestiller seg	NETT
22.12.2011	- Hva frykter du mest? - Det vet jeg ikke om jeg vil si...	NETT
12.01.2012	Avslører demente med nøkkel i lomma, dialysepasienter og elever som skal stoppes fast	NETT

Engelske artikler:

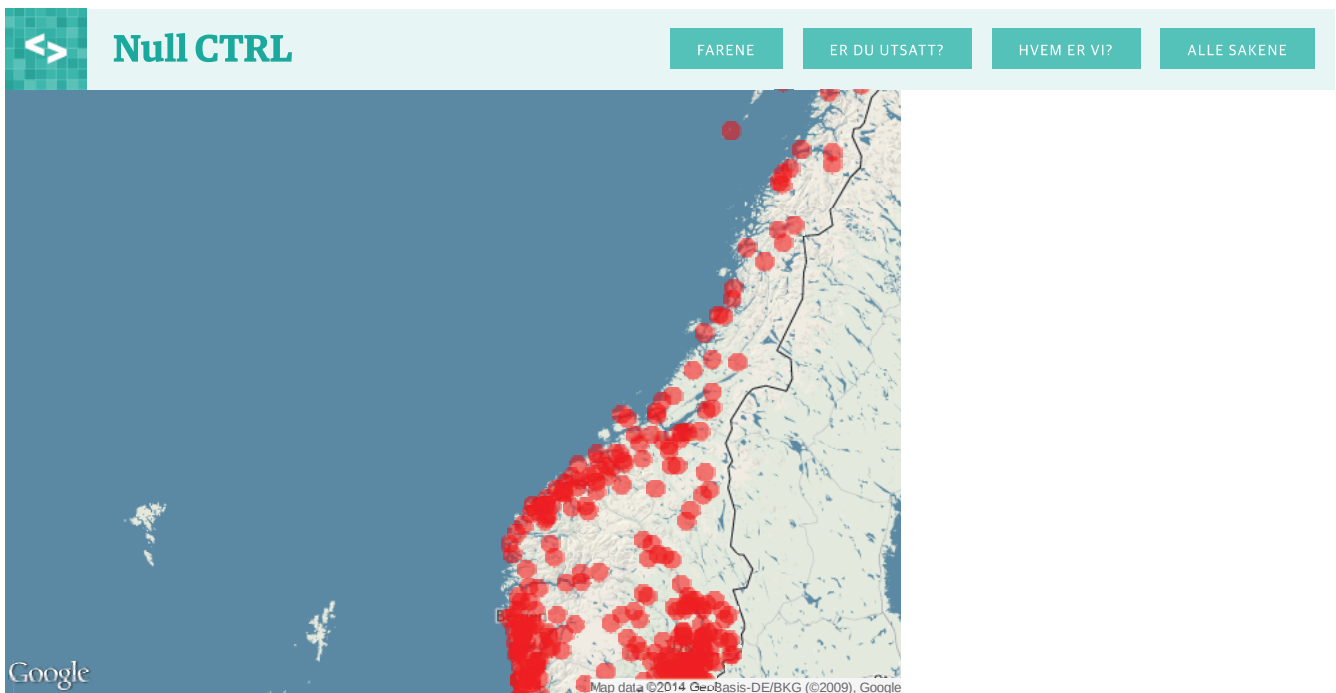
06.01.2012	Here is the wastewater system for an entire Irish county	NETT
06.01.2012	Journalists warned system owners and Norwegian NSA of 2500 critical data flaws	NETT
06.01.2012	Digital footprints - how safe are you?	NETTGRAFIKK
06.01.2012	Test your computer security with one click	NETT
06.01.2012	The actual test	NETT

Prosjektets hjemmeside finner du her: www.dagbladet.no/nullctrl

Linn Kongsli Hillestad /s/ Espen Sandli /s/ Ola Strømman /s/

Oslo, 19. januar 2014

VEDLEGG



STOREBROR SER DEG: Dette kartet viser antall kameraer som ligger koblet på nettet i Norge. Ved å zoomme inn på kartet kan du se hvor de ulike kameraene befinner seg. Grafikk: Ola Strømman

Dagbladet fant 2048 norske overvåkings-kameraer på Internett

Her kan hvem som helst se levende bilder fra private hjem, butikker, barer og restauranter uten at eierne vet det.



LINN KONGSLID HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): En liten baby ligger og sover søtt blant suttekluter og kosedyr et sted på Østlandet. Over senga har foreldrene satt opp et overvåkingskamera som filmer kontinuerlig, trolig så de kan holde et øye med ungen til enhver tid.

Det de sannsynligvis ikke vet, er at hvem som helst kan følge med på barnet deres når det ligger i senga.

Overvåkingskameraet er nemlig koblet til Internett - uten beskyttelse av brukernavn eller passord - noe som betyr at alle med internettilgang kan se kamerabildene.

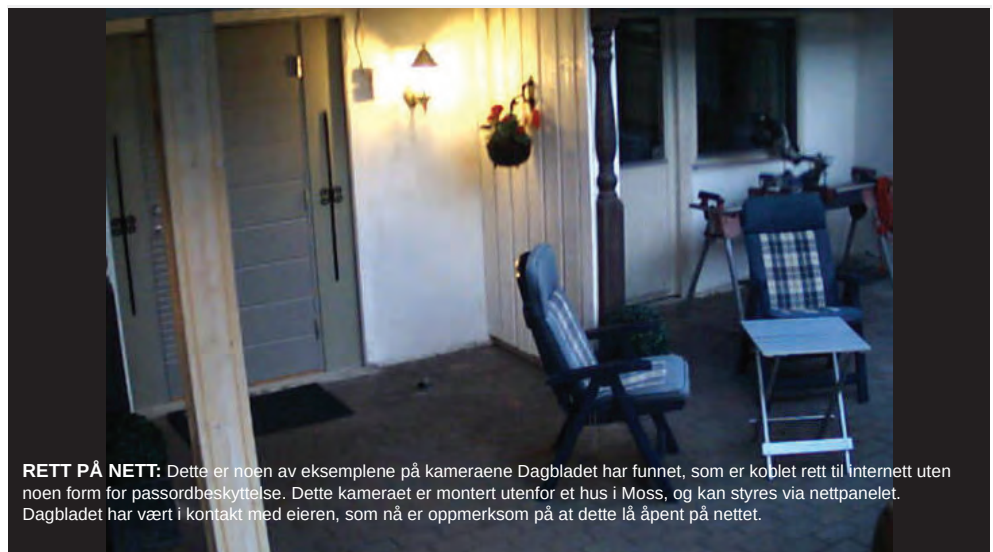
Om dette er ikke det eneste.

Vidåpent

I forbindelse med [en artikkelserie om datasikkerhet](#) har Dagbladet funnet 2048 norske overvåkingskameraer som ligger

Det som filmes er ikke noe offentligheten har noe med. Dette er noe som skjer på arbeidsplasser og i private hjem, og da er det veldig viktig at tilgangen til de bildene vi her har sett er begrenset til et fåtall personer.

Direktør Bjørn Erik Thon i Datatilsynet



RETT PÅ NETT: Dette er noen av eksemplene på kameraene Dagbladet har funnet, som er koblet rett til Internett uten noen form for passordbeskyttelse. Dette kameraet er montert utenfor et hus i Moss, og kan styres via nettpanelet. Dagbladet har vært i kontakt med eieren, som nå er oppmerksom på at dette lå åpent på nettet.

ute på Internett, og har vært inne på over 250 av disse.

Mange overvåkingskameraer blir levert uten noen som helst form for passordbeskyttelse, så dersom ikke brukeren selv installerer dette, er kameraet i prinsippet like tilgjengelig som en norsk nettavis.

Lydoverføring

Uten å taste noen form for passord, har Dagbladet derfor fått tilgang til livebilder fra [en nattklubb](#), barer, restauranter, butikker - og private hjem. Mange av kameraene kan styres via panelet som kommer opp i nettleseren, og flere har lydoverføring.

Det betyr i praksis at hvem som helst kan snakke til intetanende privatpersoner hjemme i stua via deres eget webkamera.

I tillegg er det mulig å opprette passord som midlertidig sperrer deg ute fra ditt eget kamerasystemet.

Solsenger og badestamp

Det er mange eksempler på videobilder som kringkastes rett ut på nett, fritt for alle.

Noen overvåker badestampen eller solstolene ute på terrassen, andre lysekronene og de persiske teppene hjemme i stua. I tillegg finner du lysthus, fjøs, hytter, kjøkken og parkeringshus. Kiosker, bensinstasjoner, en kinosal og undervisningsrom på skoler.

En Joker-butikk hadde et kamera hvor du via et nettbasert kontrollpanel kunne zoome inn på ansatte som taster adgangskoden til ytterdøra.

- Dette i strid med våre sikkerhetsrutiner. Vi har vært i kontakt med butikken det gjelder og gjort dem oppmerksomme på at dette ikke er akseptabelt. Vi har nå sørget for at butikken har koblet fra kameraet, og vi skal påse at det ikke gjentar seg, skriver informasjonsansvarlig Anette Grønby Rein i Kjøpmannshuset Norge i en e-post til Dagbladet.

Sikkerhetsbrudd

Direktør Bjørn Erik Thon i Datatilsynet reagerer kraftig på alle de åpne kameraene.



ÅPENT KAMERA: Kameraet på utestedet Klubbteateret i Drammen sendte videostrømmen rett på nett. Video: Øistein Norum Monsen / Dagbladet.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



REAGERER: Direktør Bjørn Erik Thon i Datatilsynet (i midten) mener flere av eksemplene Dagbladet viser er svært alvorlige. Her sammen med seniorrådgiver Stian D Kringlebotn og seniorrådgiver Guro Skåltveit. Foto: Benjamin A. Ward / Dagbladet

- Det som filmes er ikke noe offentligheten har noe med. Dette er noe som skjer på arbeidsplasser og i private hjem, og da er det veldig viktig at tilgangen til de bildene som vi her har sett er begrenset til et fåtall personer, sier han etter at Dagbladet har vist ham noen av kameraene som ligger åpne på nettet.

Thon påpeker at noe av informasjonen som filmes kan være svært avslørende for den enkelte, særlig når det er mulig å høre lyd.

I tillegg kan de åpne kameraene innebære en sikkerhetsrisiko, blant annet fordi tyver kan se hvor verdisaker befinner seg.

- Her er det et helt klart sikkerhetsbrudd som har skjedd hos en del av disse bedriftene — og for så vidt privatpersonene, sier han.

Ulovlig overvåkning

Dagbladet har i forkant av publisering sendt varsel om alle de sensitive kameraene til de ulike internettleverandørene. Seniorrådgiver Vidar Sandland i Norsk Senter for Informasjonssikring (Norsis) tror problemet med de åpne kameraene skyldes manglende teknisk kunnskap.

- Folk vet ikke hva de driver med, og plutselig er kameraet tilgjengelig for millioner av mennesker der ute, sier han til Dagbladet.

Flere av kameraene Dagbladet har funnet viser harmløse bilder fra offentlige steder, hvor ingen mennesker kan identifiseres. Mange er imidlertid av en helt annen art, både når det gjelder teknisk kvalitet og motiv, enn kameraene på [lister over offentlig tilgjengelige overvåkingskameraer](#) i Norge.

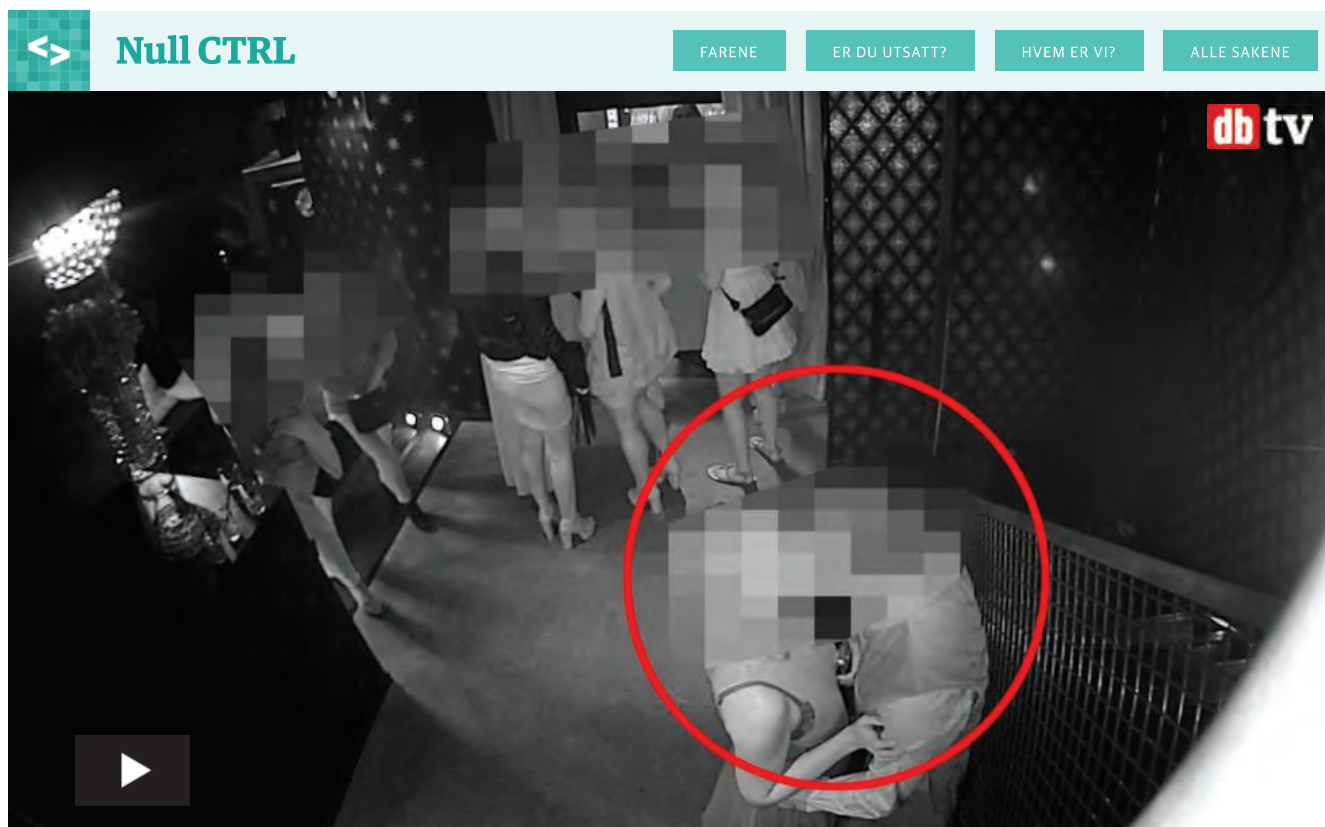
I tillegg er bruken av slike kameraer omfattet av strenge reguleringer, og Sandland påpeker at flere av de kameraene Dagbladet har funnet ikke engang er lovlig satt opp.



MANGLER KUNNSKAP: Seniorrådgiver Vidar Sandland i Norsk Senter for Informasjonssikring er ekspert på IT- og informasjonssikkerhet. Han mener folk legger overvåkingskameraene sine ut på nett fordi de ikke vet bedre. Foto: Øistein Norum Monsen / Dagbladet



Her fester og kliner de unge gjestene for åpent kamera, publisert onsdag 2. oktober 2013 kl. 12:12



RETT PÅ NETT: Kameraet på utestedet Klubbteateret i Drammen sendte videostrømmen rett på nett. Video: Øistein Norum Monsen/Dagbladet

Her fester og kliner de unge gjestene for åpent kamera

Men de vet det ikke selv.



ESPEN SANDLI
esan@dagbladet.no



SVEINUNG U. YSTAD
sys@dagbladet.no



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ØISTEIN NORUM MONSEN
onm@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

DRAMMEN (Dagbladet): Foto/Video

Utelivsbaronene bak Vulkan, Nox og Stravinsky har spredt suksessoppskriften fra Oslo til [Klubbteateret](#) i Drammen. Men vernet av gjestenes privatliv har de ikke vært like heldige med.

Via nattklubbens eget kamera har hvem som helst kunnet følge med på hvem som er på byen, hvem de er sammen og hvem som for anledningen kliner med hvem.

Kan føle seg krenket

Utestedets overvåkningskamera er ett av [2048 norske overvåkningskameraer](#) [Dagbladet fant på nett](#) i forbindelse med [en artikkelserie om datasikkerhet](#). Videostrømmen lå på Internett uten noen form for passordbeskyttelse. Det opprører Datatilsynet:

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

- Det er skremmende, sier direktør Bjørn Erik Thon i Datatilsynet.

Dagbladet har vært i kontakt med ungdommer fra overvåkningsvideoen som følger det svært ubehagelig å bli filmet på denne måten, og som ønsker å være anonyme.

Thon mener både gjester og ansatte som filmes på denne måten med rette kan føle seg krenket.

- Det kan være avslørende informasjon. Det er bilder av gjester og av ansatte, og det er klart at dette er jo noe som absolutt ikke har noenting på et offentlig nett å gjøre, sier Thon.

- Burlesk og teater

Hvor lenge gjestene på Klubbteatret er blitt filmet «live» er uvisst. Nattklubben åpnet i fjor høst. Lokalavisa Drammens Tidende skrev da at utestedet i «[bråkmakergata](#)» var den største satsingen der på denne siden av 2000-tallet.

- Dette må være et av landets råeste nattklubblokaler, uttalte medeier Bo Vivike til [dt.no](#).

Medinvestor og tidligere sandvolleyballstjerne Jørre Kjemperud sa bare «Au» på spørsmål om hva det hadde kostet å pusse opp stedet.

- Vi blander mange stilarter, her oppe er det en krysning av burlesk og teater, sa Vivike.

- En glipp

Men at gjestene skulle vises på nett, sekund for sekund i hele åpningstida, var aldri meningen.

- Nei. Dette er en glipp. Og den skal vi ta tak i med en gang, sier markedsansvarlig Martin Hellström ved Klubbteatret til Dagbladet

Overfor Dagbladet er han opptatt av at vi ikke skal filme ham.

- Jeg vil ikke på TV, sier Hellström.

- Så det er bare gjestene dine som skal på TV?

- Jeg ønsker ikke å være med på det, så det får dere bare respektere. Men jeg svarer på spørsmål, sier Hellström.

Det tekniske opplegget kjenner ikke Hellström til, men lover å ringe vedkommende som er ansvarlig for datasikkerheten.

- Løssluppet og privat

Seniorrådgiver Vidar Sandland ved Norsk senter for informasjonssikring (Norsis) er ikke imponert:



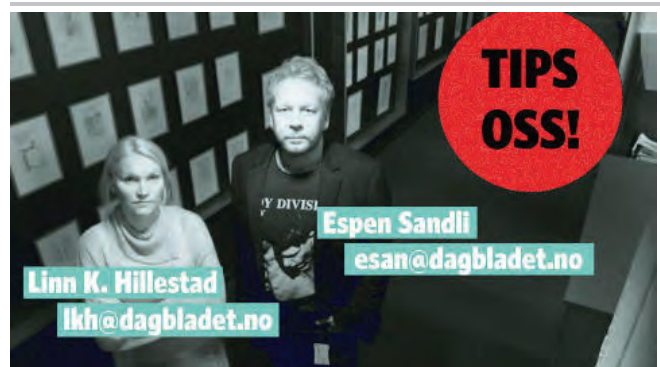
ÅPENT PÅ NETT: Dette styringspanelet fant Dagbladet åpent og usikret på nett. Det gir tilgang til et avansert overvåkningskamera inne på nattklubben Klubbteatret i Drammen. Foto: Skjermdump



POPULÆRT STED: Klubbteatret er en populær nattklubb i Drammen. Foto: Sveinung U. Ystad/Dagbladet



ADVARER: Vidar Sandland er seniorrådgiver i Norsis og ekspert på IT og informasjonssikkerhet. Foto: Øistein Norum Monsen / DAGBLADET



- Dette er absolutt ikke bra, for det går jo på personvernet til kundene. Det her er jo ikke lov engang, sier han.

Filmingen av gjestene skjer med lyd. Når musikken ikke overdøver alt, har man kunne høre samtale som pågår i rommet.

- Konsekvensene av at dette ligger åpent er jo at personer som ikke ønsker å informere at de har vært på de stedene, eller at personlige samtaler blir spredd overalt på internett... Dette kan være ganske katastrofalt for den enkelte, sier Sandland.

Og legger til:

- Det er jo på et utested, hvor det sannsynligvis drikkes alkohol, folk blir litt løsslupne, de gjør kanskje ting som de ikke vil at andre skal se, de snakker om ting som kanskje ikke noen andre enn de to som snakker sammen burde vite om. Det her kan faktisk talt få katastrofale konsekvenser for den enkelte hvis disse filmene og lydopptakene kommer på avveie.

- Ikke akseptabelt

- Det skal veldig mye til for at overføring av lyd tillates, spesielt i kombinasjon med levende bilder. Og at det er mulig å gå inn og se hvem som er på en nattklubb er på ingen måte akseptabelt. Det er veldig alvorlig, sier direktør Bjørn Erik Thon i Datatilsynet til Dagbladet.

Han reagerer også sterkt på at det er mulig for hvem som helst å gjøre opptak av bilder og lyd via det åpne styringspanelet.

- Det er helt klart at ingen som er på en nattklubb regner med å bli overvåket, og dette er jo et overvåkingsinstrument. Det er en krenkelse av personlig integritet, sier han.

- Innbrudd

Det avanserte overvåkningskameraet ble tatt vekk fra nett samme dag Dagbladet oppsøkte Klubbteateret. Ifølge nattklubbens tekniker er det ikke gjort feil under installeringen av overvåkningskameraet.

I stedet oppgis det at manglende sikkerhet kan skyldes en PC som skal ha blitt stjålet fra utestedet for en tid tilbake, og at informasjon fra den maskinen kan ha blitt brukt til å hacke kamerasystemet.

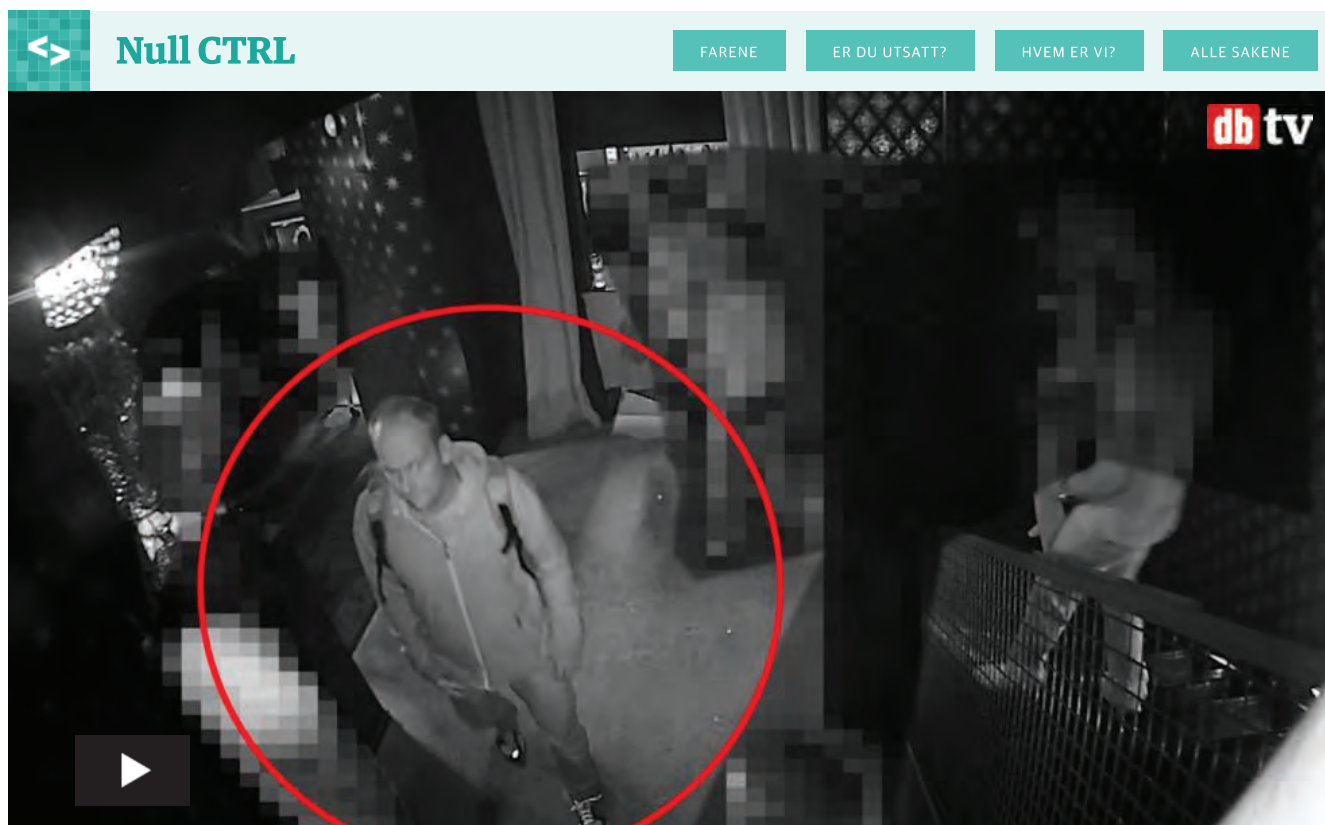
Klubbteateret

- Nattklubb i Drammen.
- Selskapet Engene 12 Drift AS eies av Strav Holding (50 prosent), og TQ Holding (25 prosent).
- Brødrene Jørre Kjemperud og Kim Hellum eier 12,5 prosent hver.
- Bo Vivike eier La Belle Sole på Solli Plass i Oslo. Åpnet Bar Bygdøy Allé i 2009, senere Bar Tjuvholmen og Bar Vulkan. Eier Strav Holding sammen med Jørn Morten Grønneberg.
- Klubbteateret åpnet for allmennheten i oktober 2012.

Kilde: dt.no



KRITISKE: Datatilsynets seniorrådgiver Stian D Kringlebotn, direktør Bjørn Erik Thon og seniorrådgiver Guro Skåltveit studerer Dagbladets videomateriale. Foto: Benjamin A. Ward / Dagbladet



PÅ JOBB I SIVIL: Overvåkingskameraet på utestedet Klubbteateret i Drammen sendte video av politiets innsatsleder Geir Oustorp rett på nett.

Her filmes politi- og idretts- kjendisen på jobb i sivil

Politi og ungdom overvåket ulovlig. Men det ønsker ikke politiet å mene noe om.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLID HILLESTAD
lkh@dagbladet.no

DRAMMEN (Dagbladet): Dagbladet har avdekket hvordan unge personer på nattklubben Klubbteateret i Drammen [fester og kliner for åpent kamera](#), uten at de selv vet om det.

Men det er ikke bare ungdom på fest som avdekkes via overvåkingskameraet. Natt til søndag 25. august ble innsatsleder Geir Oustorp ved Søndre Buskerud politidistrikt selv et offer.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

«Semikjendis»

Det kjente håndballeset, trener- og politiprofilen Oustorp, er imøtekommende når Dagbladet viser ham bildene fra nattklubbens overvåkingskamera, som lå åpent på nett for alle som ønsket å se.

Ifølge ham selv var det i embets medfør han ble fanget opp av

kameraet på nattklubben.

Hans arbeidsgiver bekrefter at innsatsleder Oustorp jobbet i sivil i forbindelse med en større folkemønstring som fant sted i Drammen på det tidspunktet.

- Ikke naturlig

Men når Dagbladet ber om å få intervju Oustorp som et eksempel på en tilfeldig person fanget opp av ulovlig overvåkning, blir avisa nektet dette:

- Vi har tatt en runde på dette internt. Geir Oustorp var på jobb som tjenestemann denne kvelden, og i sin rolle som det er det ikke naturlig at han uttaler seg om denne konkrete saken, skriver kommunikasjonsrådgiver Anne Malm Monstad i en e-post til avisa.

Hun legger til:

- At han var i sivil på jobb, selv om han er et kjent ansikt som både politimann og håndballtrener, er også et element som gjør at det ikke er ønskelig å stille til intervju i forhold til problemstillingen, skriver hun.

Oustorp har tidligere gitt Dagbladets lesere [en personlig, sterk og gripende skildring av de tøffeste øyeblikkene](#) han og kolleger opplevde etter terrorangrepet på Utøya.

- Tilfeldig

Dagbladet har snakket med ungdom som er filmet av det samme kameraet, og som opplever det krenkende og ubegagelig. Dagbladet ba derfor om å få et intervju med Oustorps overordnede, med henvisning til politiet som talspersoner for rett og galt, preventiv effekt og overordnet samfunnsansvar.

Det nekter stasjonsledelsen å være med på.

- Politiet, ved undertegnede i Søndre Buskerud politidistrikt, ønsker ikke å kommentere denne saken, skriver stasjonssjef Jan Erik Strøm i en e-post.

Han utdyper dette på følgende måte:

- Det kameraet som det her er snakk om er ikke rettet spesielt mot politiets arbeid. Denne saken dreier seg om, slik vi ser det, utplassering og bruk av overvåkingskamera. At det «tilfeldigvis» er en profilert politimann/håndballtrener som er fanget opp av kameraet kan vi ikke se har betydning for slik utplassering av overvåkingskamera, skriver han.

- Skremmende

Utestedets overvåkingskamera er ett av [2048 norske overvåkingskameraer](#) Dagbladet fant på nett i forbindelse med [en artikkelserie om datasikkerhet](#). Det var som et eksempel på dette Dagbladet søkte politiets medvirkning.

Videostrømmen fra Klubbteateret lå på Internett uten noen form for passordbeskyttelse. Det opprører Datatilsynet:

- Det er skremmende, sier direktør Bjørn Erik Thon.

Seniorrådgiver Vidar Sandland ved Norsk senter for informasjonssikring (Norsis) er heller ikke imponert:



RETT PÅ NETT: Et overvåkingskamera ved utestedet Klubbteateret i Drammen sendte livebilder rett på nett. Video: Øistein Norum Monsen/Dagbladet.



PROFIL: Geir Oustorp er tidligere landslagsspiller i håndball, profilert trener og politimann. Arkivfoto: Lise Åserud / NTB Scanpix

Geir Oustorp (41)

- Profilert politimann (innsatsleder) i Drammen.
- Var blant de første på Utøya etter pågripelsen av Anders Behring Breivik, hvor han våket over de døde hele natta.
- 91 kamper for herrelandslaget i håndball, 317 mål, i perioden 1992-2004.
- Tidligere trener for Drammen Håndballklubb (herrer) og Byåsen (damer). Nå i trenerteamet til Glassverket (damer).
- Spilte i blant annet DHK, TuS Nettelstedt (Tyskland) og Sandefjord.

Kilder: [handball.no](#) / [Dagbladet](#)



NEKTER INTERVJU: Stasjonssjef Jan Erik Strøm ved Drammen

- Dette er absolutt ikke bra, for det går jo på personvernet til kundene. Det her er jo ikke lov engang, sier han.

Live og med lyd

Filmingen av gjestene skjer med lyd. Når musikken ikke overdøver alt, har man kunne høre samtalene som pågår i rommet.

- Konsekvensene av at dette ligger åpent er jo at personer som ikke ønsker å informere at de har vært på de stedene, eller at personlige samtaler blir spredt overalt på internett... Dette kan være ganske katastrofalt for den enkelte, sier Sandland.

Beklager glippen

Det avanserte overvåkningskameraet ble tatt vekk fra nett samme dag Dagbladet oppsøkte Klubbteateret. Ifølge nattklubbens tekniker er det ikke gjort feil under installeringen av overvåkningskameraet.

- Dette er en glipp. Og den skal vi ta tak i med en gang, uttalte markedsansvarlig Martin Hellström ved Klubbteateret [da Dagbladet oppsøkte nattklubben.](#)

politikammer sier nei til å la Geir Oustorp stille til intervju. Oustorps sjef og Strøm selv nekter også å la seg intervju av Dagbladet. Arkivfoto: Lise Åserud / NTB Scanpix



Tips oss på fullctrl@dagbladet.no

ALLE SE

Overvåkingskameraer viste pinkoder, s

Dagbladet fant 2048 norske overvåkingskameraer på Internett, med levende bilder fra private hjem, barer og butikker. 16 av dem overvåket uvitende kunder ved Frostasenteret.

NY SERIE - NULL CTRL



Espen Sandli
esan@dagbladet.no



Linn Kongsli Hillestad
llu@dagbladet.no



Øistein Norum Monsen
onm@dagbladet.no

FROSTA (Dagbladet): Inn i butikken kommer en dame gående. Hun stopper ved Post i butikk, setter inn kredittkortet og taster sin pinkode. Via et overvåkingskamera i taket kan alle som har ønsket det kunnet følge med henne og andre kunder som taster sine koder.

Via det samme kameraet kan man se Postens dataskjerm.

Dette er bare ett av 16 overvåkingskameraer ved Frostasenteret i Nord-Trøndelag som har ligget åpent på nettet, uten passordbeskyttelse.

Vidåpent

Disse er noen av de 2048 norske overvåkingskameraene Dagbladet har funnet på Internett i forbindelse med en artikkelserie om datasikkerhet.

Uten å taste noen form for passord, har vi fått tilgang til livebilder fra en nattklubb, barer, restauranter – og private hjem.

Mange overvåkingskameraer blir nemlig levert uten noen som helst form for passordbeskyttelse, så dersom ikke brukeren selv installerer dette, er kameraet i prinsippet like tilgjengelig som en norsk nettavis.

Safe og sol

Ett av kameraene på kjøpesenteret i Frosta er montert slik at man kan følge med på det indre liv på bakrommet av Coop Prix-butikken. Her står en safe i hjørnet og man kan potensielt se når den eventuelt står åpen eller når det legges verdier i den.

På lista over 16 tilgjengelige kameraposisjoner finner man en av bygdas frisører og det lokale solstudioet.

Alt dette er kameraer som Dagbladet fant åpent på Internett og uten noen form for passordbeskyttelse. Med andre ord har det vært fritt tilgjengelig for alle og enhver. Og slik har det vært en stund.

– Dette skal jo ikke ligge åpent,

men lukket og låst bak en brannmur og med passordbeskyttelse, sier daglig leder Jan Inge Røkke ved Frostasenteret.

– Mager trøst

Men slik var det ikke da Dagbladet møtte ham på Frosta.

– Her er det noe som er som det ikke burde være, så det må jeg inn og finne ut av, sier Røkke.

Han er ikke spesielt glad for at det har skjedd. Den lille kommunen med 2600 innbyggere er ikke mer enn ei lita bygd, hvor de fleste kjenner hverandre.

– Jeg trodde jo det var rimelig sikkert, sier Røkke ettertenksomt.

– Om det er noen trøst, er du ikke den eneste.

– Det er en mager trøst, sier Røkke.

Flyttet feil

Frostasenteret kjøper sikkerhetstjenester av Nokas.

– Jeg har jo ikke teknisk kompetanse til å si så mye om hva som har skjedd, men skal kontakte Nokas og leverandøren for å finne ut av det, sier Røkke.

Etter Dagbladets besøk på Frostad, ble anlegget ifølge Røkke umiddelbart koblet fra nett.

– I forbindelse med service på en harddisk og montering av annet utstyr har det skjedd en feil med plassering av PC, skriver Røkke i en e-post.

Han har også oversendt Dagbladet en rapport fra Nokas Teknisk AS, hvor det framgår feilen skyldes at utstyr ble flyttet fra en ruter til en annen.

Kan se hjemmefra

I butikken er alle kameraer koblet via fysiske kabler. En overføring til nett er derfor ikke nødvendig. Butikken har imidlertid funnet det praktisk å kunne koble seg på hjemmefra, som det heter i rapporten.

Den eksterne påloggingen skal nå være passordbelagt, skriver Nokas.

Seniorrådgiver Vidar Sandland ved Norsk senter for informasjonssikkerhet (NorSIS) er ikke imponert:

– Dette er absolutt ikke bra, for det går jo på personvernet til kundene, sier han.

– Slurv

Han får støtte av direktør Bjørn Erik Thon i Datatilsynet:

– Det som filmes og det som vi har sett i disse reportasjene er ikke noe offentligheten har noe med. Dette er noe som skjer på arbeidsplasser, og da er det veldig viktig at tilgangen til de bildene som vi har sett er begrenset til et fåtall personer, sier han.



AVANSERT: Med dette høyoppløselige overvåkingskameraet kan man definere egne kamerautsnitt fra i

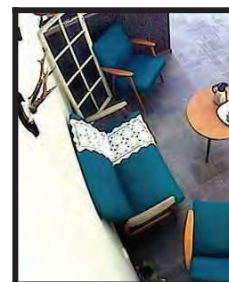


16 KAMERAER: Oversikten viser hvilke tilgjengelige kamera man hadde ved Frostasenteret. Alle disse har stått åpne og uten passordbeskyttelse. Foto: Skjermdump

FØLG SAKEN

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av nabosens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no



KLIPP: Her kunne man følge ventet på neste hårklipp.



R DEG

afe og at naboene tok solarium

Slik beskytter du bankkortet, Iphonen og Ipaden

Har du tenkt på hva slags bakgrunnsbilde du har på smarttelefonen din? Det kan hende du bør skaffe deg et nytt et.



Therese Dokshim
tdo@dagbladet.no

- Vi er nok litt naive, sier IT-ekspert Per Thorsheim. I forbindelse med Dagbladets avsløringer om svikt i norsk data-sikkerhet ber Dagbladet ham om tips til hvordan man beskytter pin-koder og digitale duppedingser.

Og det er tilsynelatende ikke så mye som skal til. En smart løsning her, et enkelt tastetrykk der - og vips, så er du, så godt som, sikret.

KORT OG PINKODER:

- Skaff deg et kort som ikke krever at pin-kode tastes når du handler for under 200 kroner. Da trenger du bare taste koden ved større beløp, og minsker risikoen for at noen skal «ta» pin-koden din, sier Thorsheim. Med en maks grense er på 200 kroner er det liten økonomisk gevinst for folk som er ute etter pengene dine, skulle de få tak i kortet ditt.

- Aldri legg fra deg kortet i baren, selv om det kanskje «blir enklere» når regningen skal gjøres opp etter en fuktig kveld på byen. - Du skal til enhver tid kunne se kortet ditt. Er du på restaurant, og servitøren tar med kortet ditt inn på kjøkkenet eller til baren for å ta betalingen din - da har du blitt grådig lurt, sier Thorsheim.

- Hold en hånd eller veske over pinkoden når du taster koden din. Det finnes kriminelle som monterer opp filmkameraer for eksempel på minibanken. Det er helt tydelig at de som holder en hånd over mens de taster er mindre utsatt for kriminelle handlinger.

MOBIL OG DIGITALE DUPPEDINGSER:

De aller fleste av oss har gjerne bakgrunnsbilde på telefonen av en fin solnedgang, kjæresten eller av en søt hund. Det er utrolig dumt, skal vi tro ekspertene.

- Hvis du mister telefonen din og har på tastelås på telefonen slik at den er låst når noen finner den - vil finneren til slutt gi opp å finne deg fordi det ikke er noe på den som tilsier at den er din. Et tips er å heller ha bilde av seg selv sammen med eier-skapelig info slik at folk kan søke deg opp.

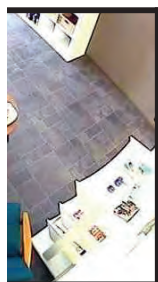
- Gjør det samme på Macen eller på PC-en: - Fest en klisterlapp med navn og nummer på dataen, slik at folk kan kontakte deg om de skulle finne PC-en eller Macen du har forlagt på cafeen, flyplassen eller på bus-sen, oppfordrer Thorsheim.

Se mer på

db tv



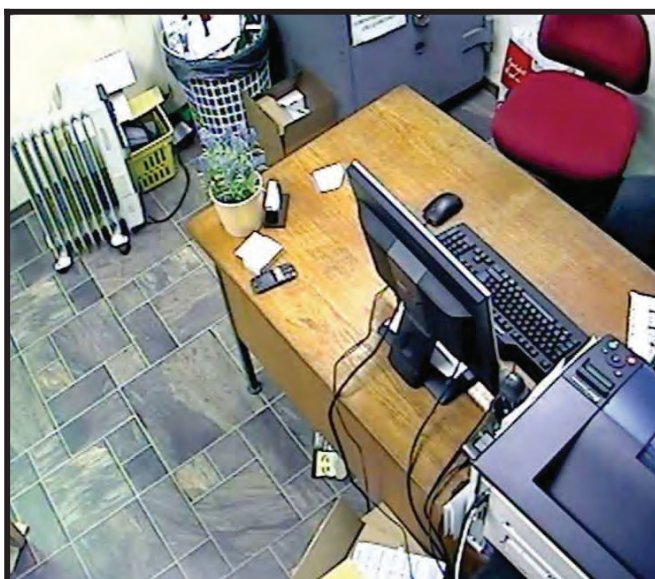
Post i butikk. For eksempel kan man potensielt se pinkoder og annen sensitiv informasjon fra kortautomaten, safen eller PC-en. Foto: Skjermdump



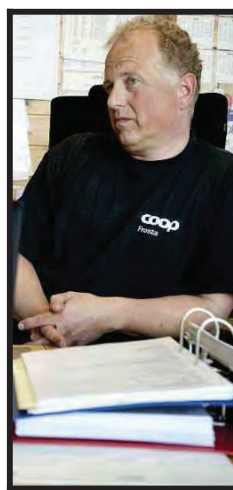
med på hvem som Foto: Skjermdump



EKSPERT:
Vidar Sandland er senior-rådgiver i NorSIS og ekspert på IT og informasjons-sikkerhet. Foto: Øistein Norum Monsen

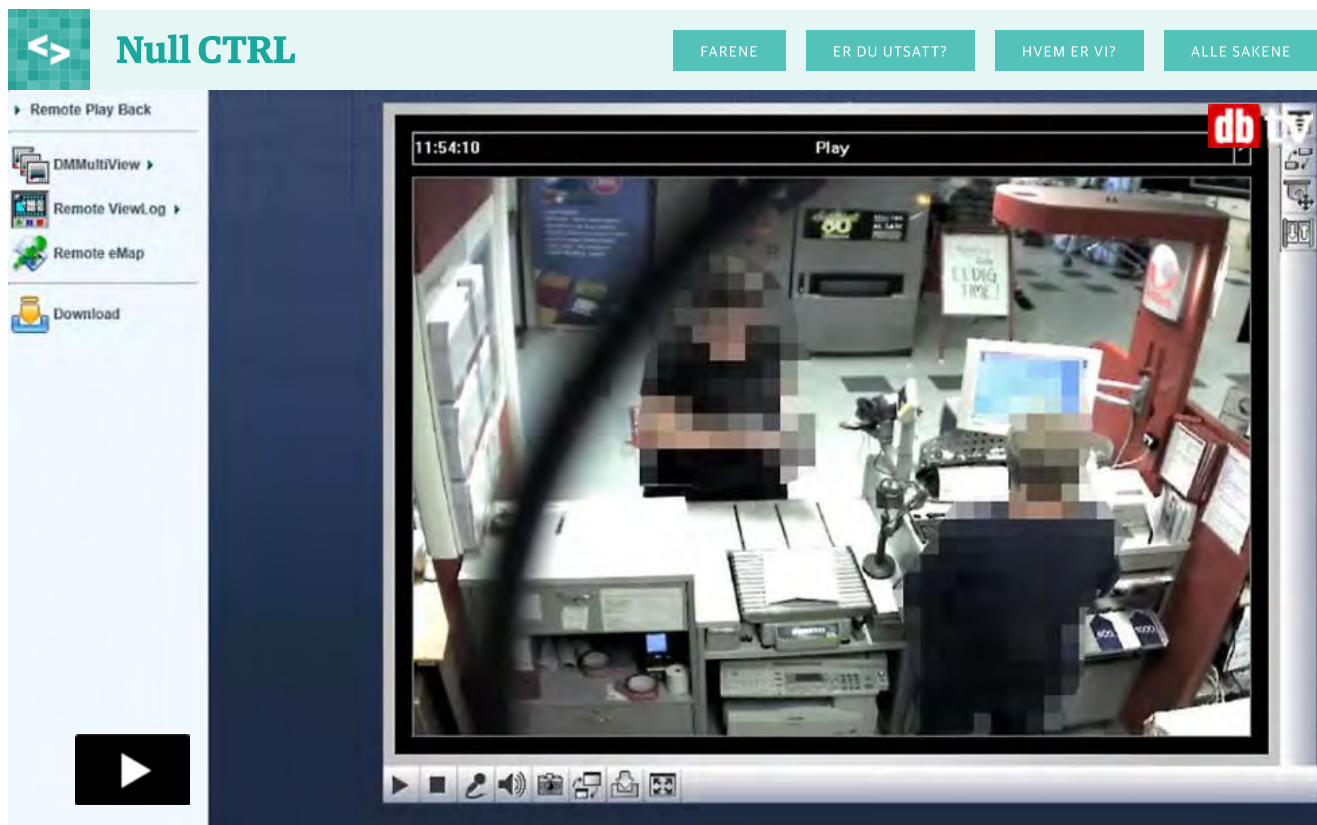


SAFEN: Et kamera overvåket butikkens kontor på Frostasenteret. Her kan man potensielt se når safen i hjørnet er fylt med verdier. Foto: Skjermdump



UVITENDE: Jan Inge Røkke er daglig leder ved Frostasenteret og opplyser til Dagbladet at han var helt uvitende om at senterets overvåkingssystem lå åpent for alle på nett. Foto: Øistein Norum Monsen

Her kan du se pinkoder, safen og naboene ta solarium, publisert torsdag 3. oktober 2013 kl. 10:35



VIDEOSTRØM: Et kamera står plassert bak skranken i Post i butikk på Frostasenteret nord for Trondheim. Via dette har man hatt full oversikt over personer som kommer for å ta ut penger, betale regninger eller hente pakker. Pinkoder og kontoinformasjon på PC-skjermen kan være synlig. Totalt lå 16 av senterets overvåkingskameraer tilgjengelig på nett. Video: Øistein Norum Monsen / Dagbladet

Her kan du se pinkoder, safen og naboene ta solarium

Dagbladet fant kjøpesenterets 16 overvåkingskameraer åpne for alle på nettet.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLIE HILLESTAD
lkh@dagbladet.no



ØISTEIN NORUM MONSEN
onm@dagbladet.no

FROSTA (Dagbladet): Inn i butikken kommer en dame gående. Hun stopper ved Post i butikk, setter inn kredittkortet og taster sin pinkode.

Via et overvåkingskamera i taket kan alle som har ønsket det kunnet følge med henne og andre kunder som taster sine koder. Via det samme kameraet kan man se Postens dataskjerm.

Dette er bare ett av 16 overvåkingskameraer Dagbladet fant ved [Frostasenteret](#) i Nord-Trøndelag.

Senterets kameraer er blant [2048 norske overvåkingskameraer](#) [Dagbladet fant på nett](#) i forbindelse

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

med [en artikkelserie om datasikkerhet](#).

Safe og sol

Ett annet kamera er montert slik at man kan følge med på det indre liv på bakrommet av Coop Prix-butikken.

Her står en safe i hjørnet og man kan potensielt se når den eventuelt står åpen eller når det legges verdier i den.

På lista over 16 tilgjengelige kameraposisjoner finner man en av bygdas frisører og det lokale solstudioet.

Alt dette er kameraer som Dagbladet fant åpent på Internett og uten noen form for passordbeskyttelse. Med andre ord har det vært fritt tilgjengelig for alle og en hver. Og slik har det vært en stund.

- Dette skal jo ikke ligge åpent, men lukket og låst bak en brannmur og med passordbeskyttelse, sier daglig leder Jan Inge Røkke ved Frostasenteret.

- Mager trøst

Men slik var det ikke da Dagbladet møtte ham på Frosta.

- Her er det noe som er som det ikke burde være, så det må jeg inn og finne ut av, sier Røkke.

Han er ikke spesielt glad for at det har skjedd. Den lille kommunen med 2600 innbyggere er ikke mer enn ei lita bygd, hvor de fleste kjenner hverandre.

- Jeg trodde jo det var rimelig sikkert, sier Røkke ettertenksomt.

- Om det er noen trøst, er du ikke den eneste.

- Det er en mager trøst, sier Røkke.

- Skjermet

I ettertid ønsker Røkke å presisere følgende angående pinkoder:

- Tastaturet på terminalen er plassert med skjerm foran tallene, slik at det er lesbart kun fra kundens side, sier Røkke.

Han hevder det ikke skal være mulig å se pinkoden, verken fra kameraet i Post i butikk eller fra



UVITENDE: Jan Inge Røkke er daglig leder ved Frostasenteret og opplyser til Dagbladet at han var helt uvitende om at senterets overvåkingsystem lå åpent for alle på nett. Foto: Øistein Norum Monsen / DAGBLADET



16 KAMERA: Oversikten viser hvilke tilgjengelige kamera man hadde ved Frostasenteret. Alle disse har stått åpne og uten passordbeskyttelse. Foto: Skjerm dump



RETT PÅ NETT: Kameraet på utestedet [Klubfteateret viste festglad og klinende ungdom](#). Videostrømmen gikk rett på

kameraet på motsatt side.

nett. Video: Øistein Norum Monsen/Dagbladet.

Flyttet feil

Frostrasenteret kjøper sikkerhetstjenester av Nokas.

- Jeg har jo ikke teknisk kompetanse til å si så mye om hva som har skjedd, men skal kontakte Nokas og leverandøren for å finne ut av det, sier Røkke.

Etter Dagbladets besøk på Frosta, ble anlegget ifølge Røkke umiddelbart koblet fra nett.

- I forbindelse med service på en harddisk og montering av annet utstyr har det skjedd en feil med plassering av PC, skriver Røkke i en e-post.

Han har også oversendt Dagbladet en rapport fra Nokas Teknikk AS, hvor det framgår feilen skyldes at utstyr ble flyttet fra en router til en annen.

Kan se hjemmefra

I butikken er alle kameraer koblet via fysiske kabler. En overføring til nett er derfor ikke nødvendig. Butikken har imidlertid funnet det praktisk å kunne koble seg på hjemmefra, som det heter i rapporten.

Den eksterne påloggingen skal nå være passordbelagt, skriver Nokas.

Seniorrådgiver Vidar Sandland ved Norsk senter for informasjonssikring (Norsis) er ikke imponert:

- Dette er absolutt ikke bra, for det går jo på personvernet til kundene, sier han.

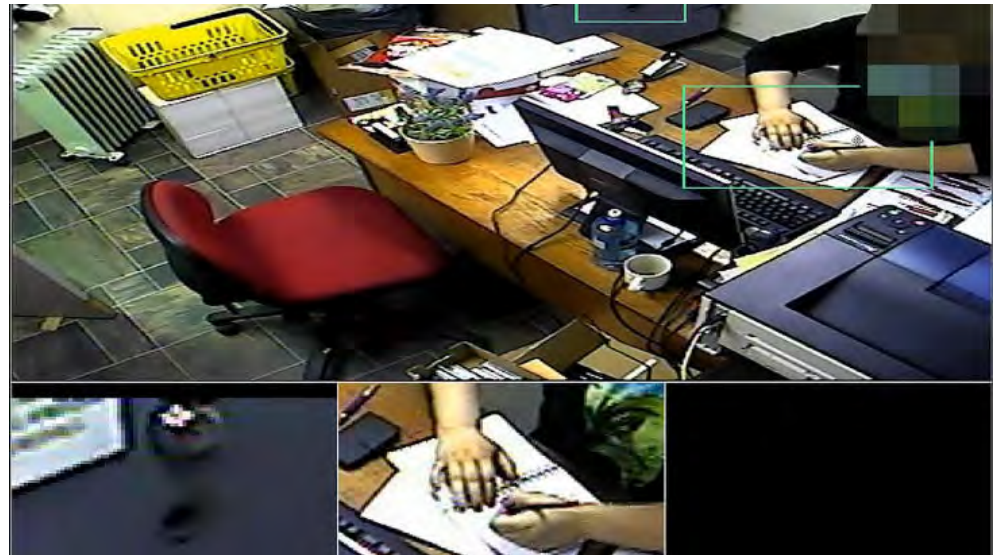
- Slurv

Han får støtte av direktør Bjørn Erik Thon i Datatilsynet:

- Det som filmes og det som vi har sett i disse reportasjene er ikke noe offentligheten har noe med. Dette er noe som skjer på arbeidsplasser, og da er det veldig viktig at tilgangen til de bildene som vi her har sett er begrenset til et fåtall personer, sier han.

Og legger til:

- Her er det et helt klart sikkerhetsbrudd som har skjedd hos bedriftene, som har slurvet med sikkerheten. Som vi så her - betalingsautomater, kassaapparater - det er klart at dette er noe som absolutt ikke har noenting på et offentlig nett å gjøre.



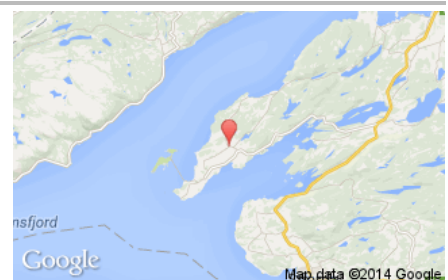
SAFEN: Et kamera overvåket butikkens kontor på Frostasenteret. Her kan man potensielt se når safen i hjørnet er fylt med verdier. Foto: Skjermdump



EKSPERT: Vidar Sandland er seniorrådgiver i Norsis og ekspert på IT og informasjonssikkerhet. Foto: Øistein Norum Monsen / DAGBLADET



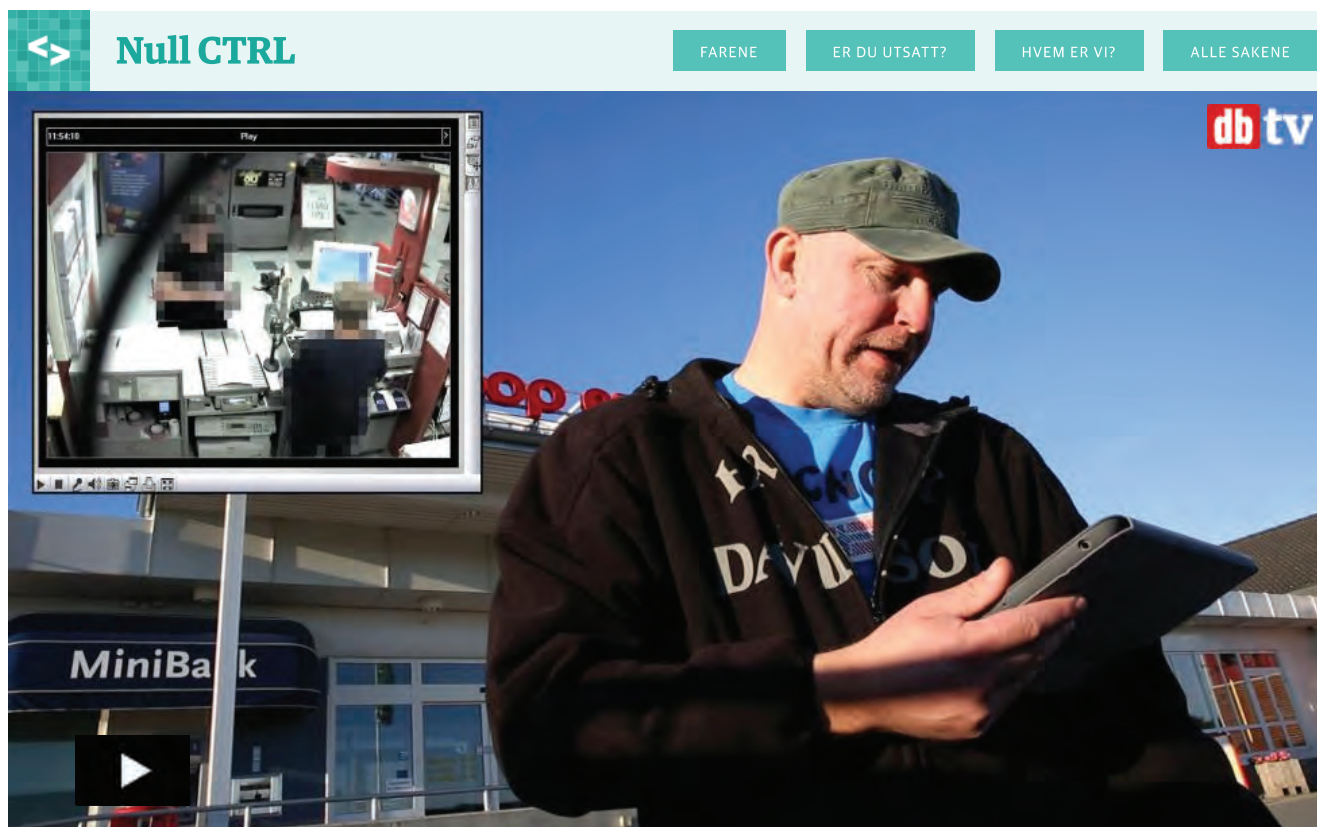
Tips oss på nullctrl@dagbladet.no



Frosta

[Se større kart](#)

«Skremmende», «uakseptabelt», «skummelt», «forferdelig», publisert torsdag 3. oktober 2013 kl. 17:18



SKREMT: Harry Stene likte ikke at 16 overvåkingskameraer på Frostasenteret har ligget åpent på internett. Video: Ole Morten Melgård / Øistein Norum Monsen / Dagbladet.

«Skremmende», «uakseptabelt», «skummelt», «forferdelig»

Frostasenterets kunder reagerer kraftig på klippene fra senterets overvåkingskameraer.

OLE MORTEN MELGÅRD
olemorten@yahoo.com



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

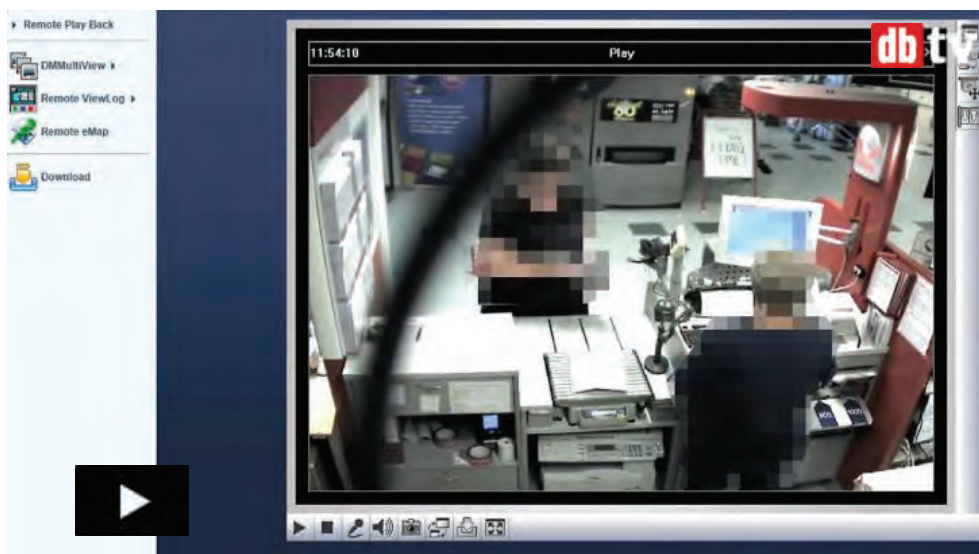
FROSTA/OSLO (Dagbladet): - Og dette trengte du ingen kode for å komme inn på?! sier Erik Rosø.

Dagbladet møter ham utenfor Frostasenteret i Nord-Trøndelag, som hadde [16 overvåkingskameraer liggende åpent ute på internett](#) uten noen form for passordbeskyttelse. Her kunne hvem som helst zoome inn på betalingsterminaler, dataskjermer - og butikkens safe.

- Jeg vet ikke hva jeg skal si, jeg er litt sjokkert, egentlig, sier Rosø.

- Ikke greit

Han er ikke den eneste av senterets kunder som reagerer på Dagbladets avsløringer. Harry Stene er på handleturn sammen



AVANSERT SYSTEM: Et kamera står plassert bak skranken i Post i butikk på Frostasenteret. Totalt lå 16 av senterets overvåkingskameraer tilgjengelig på nett, men blant annet mulighet for å zoome. Video: Øistein Norum Monsen/Dagbladet.

med datteren Mina når Dagbladet møter ham.

- Dette er ikke bra. Det er greit med kameraer hvis noen stjeler og sånt, men ikke å bli overvåket så alle kan følge med på hva du holder på med, sier han, og viser datteren videoklippet.

- Jeg synes ikke noe spesielt om dette, jeg gjør ikke det.

Frostasenterets overvåkingskameraer filmet blant annet Post i butikk, solstudioet og kontoret hvor ansatte satt og jobbet. Etter at Dagbladet før sommeren gjorde dem oppmerksom på at det lå åpent tilgjengelig på internett, ble det raskt fjernet.

Feil med plassering

Daglig leder Jan Inge Røkke ved Frostasenteret kjente ikke til at kameraene lå helt ubeskyttet da Dagbladet møtte ham på Frosta.

- Jeg trodde jo det var rimelig sikkert, sier Røkke ettertenksomt.

- Om det er noen trøst, er du ikke den eneste.

- Det er en mager trøst, sier Røkke.

Etter Dagbladets besøk fant han ut at det hadde skjedd en feil med plassering av PC i forbindelse med service på en harddisk og montering av annet utstyr.

Han har også oversendt Dagbladet en rapport fra Nokas Teknikk AS, som leverer sikkerhetstjenester til Frostasenteret, hvor det framgår feilen skyldes at utstyr ble flyttet fra en router til en annen.

- Skjermet

I ettertid ønsker Røkke å presisere følgende angående pinkoder:

- Tastaturet på terminalen er plassert med skjerm foran tallene, slik at det er lesbart kun fra kundens side, sier Røkke.

Han hevder det ikke skal være mulig å se pinkoden, verken fra kameraet i Post i butikk eller fra kameraet på motsatt side.

- Forferdelig

Bjarne Broder Krog og Liv

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL



UVITENDE: Daglig leder Jan Inge Røkke ved Frostasenteret visste ikke at 16 av senterets overvåkingskameraer lå tilgjengelig på nett. Etter Dagbladets besøk fant han ut at problemet skyldtes at utstyret ble flyttet fra en router til en annen. Foto: Øistein Monsen / Dagbladet



SKEPTISKE: Bjarne Broder Krog og Liv Leth-Olsen er kunder på Frostasenteret, og reagerer på at overvåkingskameraet deres har ligget åpent. Foto: Ole Morten Melgård / Dagbladet

Leth-Olsen er glade for at overvåkingssystemet nå er fjernet fra internett, men ble likevel skremt av Dagbladets filmklipp.

- Jeg synes det er forferdelig at ansatte og kundene kunne bli overvåket. De sitter jo og jobber her, og blir overvåket alle sammen, sier Leth-Olsen.

- **De bør jo få seg en smekk de som har satt opp det systemet. Det er det ikke noen tvil om. Sånn skal det ikke være, supplerer Krog.**

- *Hva tenker dere om at folk kan ha zoomet inn når dere har slått inn pinkoden?*

- Det er skremmende, sier Krog.

- Uakseptabelt, legger Leth-Olsen til.

- Det blir jo en vekker for oss også, som bruker det. Vi må se oss rundt.

Sikkerhetsbrudd

Datatilsynet er ikke imponert.

- Her er det et helt klart sikkerhetsbrudd som har skjedd hos bedriftene, som har slurvet med sikkerheten. Som vi så her - betalingsautomater, kassaapparater - det er klart at dette er noe som absolutt ikke har noenting på et offentlig nett å gjøre, sier direktør Bjørn Erik Thon til Dagbladet.

Kunde Michael Skogen tenker spesielt på de ansatte ved senteret som er blitt overvåket på jobb.

- *Hva er det største problemet med at det har vært sånn?*

- Det er jo at folk kan få informasjon om stedet og i verste fall innbrudd og tyveri. Folk kan jo utnytte seg av det og følge med på andre folk, sier han.

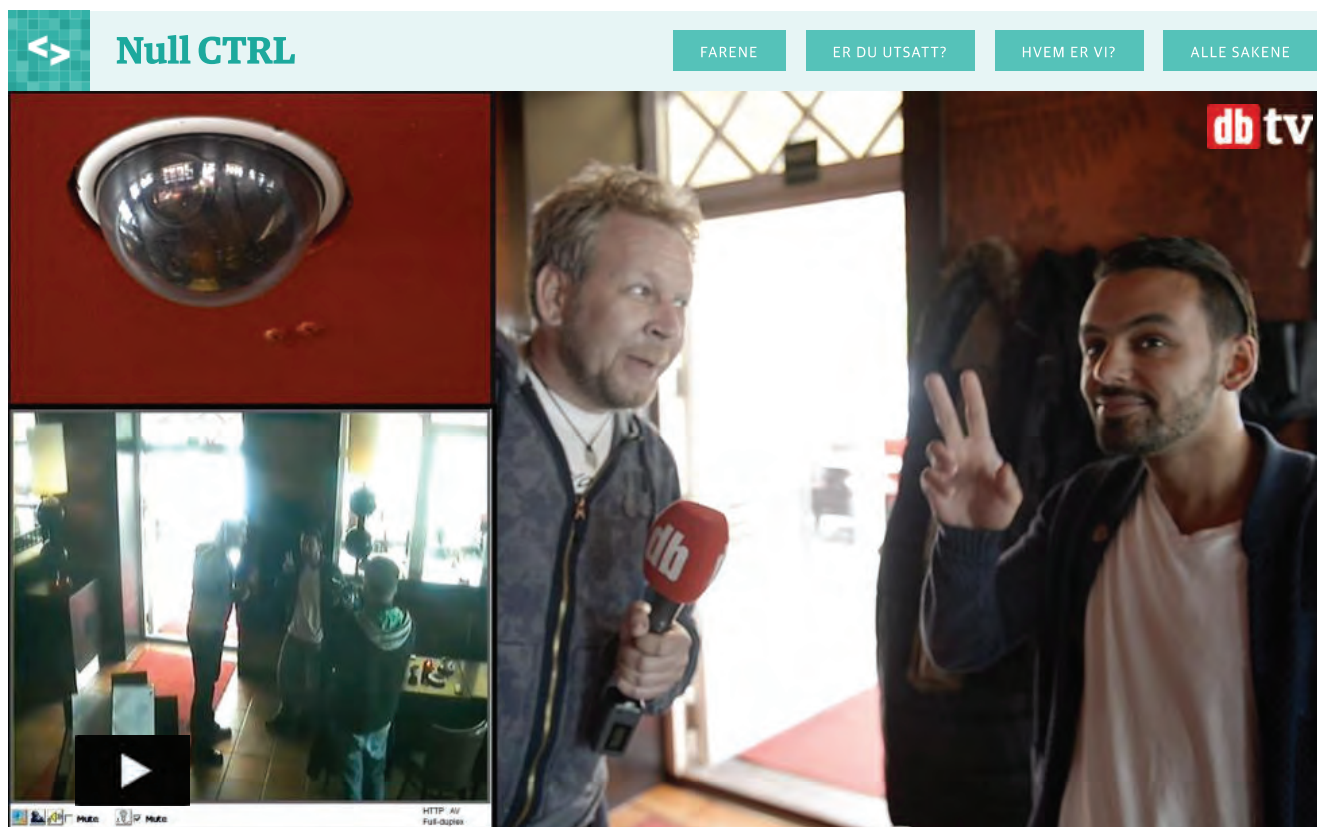


RETT PÅ NETT: Kameraet på utestedet Klubbteateret i Drammen, sendte videostrømmen rett på nett. Video: Øistein Norum Monsen/Dagbladet.



Tips oss på nulctrl@dagbladet.no

Her filmer Dagbladet med restaurantens eget kamera, publisert fredag 4. oktober 2013 kl. 09:52



VINKET TIL KAMERAET: På nettet fant Dagbladet et avansert overvåkingskamera som filmet inne på restauranten Jacob Aall i Fredrikstad. Videostrømmen lå åpent og ubeskyttet av passord. Hvor lenge det har ligget slik, er ikke kjent. Video: Øistein Norum Monsen/Dagbladet.

Her filmer Dagbladet med restaurantens eget kamera

Overvåking av gjester og ansatte havnet rett på nett.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLI HILLESTAD
llu@dagbladet.no



ØISTEIN NORUM MONSEN
onm@dagbladet.no

FREDRIKSTAD (Dagbladet): Tenk deg at du sitter på en restaurant med venner, kollegaer eller forretningsforbindelser - og uten at du vet det, kan alle som ønsker det se og høre deg via Internett.

En absurd tanke?

På restauranten Jacob Aall i Fredrikstad kan det godt ha skjedd. På nettet fant Dagbladet et avansert overvåkingskamera liggende åpent og ubeskyttet. Hvor lenge det har ligget slik, er ikke kjent.

- Det var jeg ikke klar over, sier daglig leder Motaz Gomah ved Jacob Aall i Fredrikstad.



OVERRASKET: Daglig leder Motaz Gomah ved Jacob Aall i Fredrikstad, visste ikke at kameraet som overvåker restaurant lå tilgjengelig og ubeskyttet på nett. Video: Øistein Norum Moinsen/Dagbladet.

Dagbladet tester

Tenk deg at du med et tastetrykk

kan styre naboens web-kamera, åpne konkurrentens database eller ta kontrollen over vital samfunnssikkerhet.

I en serie artikler avslører Dagbladet hvor enkelt det er, og hvilke dramatiske konsekvenser det kan få.

Ved å gå inn på kameraets unike IP-adresse ved Jacob Aall, kunne Dagbladet se alt som foregikk på restauranten. Alle som måtte ønske, kunne gjøre det samme.

- Her må jeg få hjelp av teknikere som kan se på hva som kan ha skjedd, sier Gomah til Dagbladet.



OVERVÅKET: Videostrømmen fra Jacob Aall i Fredrikstad var tilgjengelig på nett for alle som ville se. Foto: Øistein Norum Moinsen/Dagbladet.

Filmet seg selv

Som du kan se i videointervjuet øverst i saken, benyttet Dagbladet restaurantens eget kamera for å filme under intervjuet av Jacob Aalls daglige leder.

Det avanserte overvåkningskameraet kunne styres hvor enn man ønsket rundt i restauranten eller bak disken.

- Det kan se ut til at kameraet er forhåndsinnstilt til å holde spesielt øye med ansatte, stemmer det?

- Nei, det stemmer ikke. Det skal brukes for spesielt å dekke innganger, sier Gomah.

- Men det ser ut som det er satt opp for å overvåke de ansatte.

- Nei. Jeg er helt sikker, sikker Gomah.

Alle rettigheter

Det er et styringspanel til kameraet som lå åpent på nett. I et slikt panel kan alle med tilgang redigere kameraets funksjoner og innstillinger, blant annet om det skal gjøres opptak og om det skal skje med eller uten lyd.

I dette tilfellet har alle som har hatt ønske om det kunnet lagre opptak fra restaurantens overvåkningskamera. Det var ikke restaurantens hensikt da det ble satt opp.

- Det er for sikkerheten, til politiet om det skulle være noe. Bare de som skal ta del av de filene, sier Gomah.

Det avanserte kameraet av type «dome», gir brukeren mulighet til å gjøre detaljerte utsnitt i bildet.

«Creepy»

Dagbladet fant dette kameraet på nett via et søkeprogram, men teknikken er velkjent og utbredt.

I kameraets logg kunne Dagbladet se at også andre hadde besøkt den samme IP-adressen.

En slik bruker hadde trolig også redigert kameraet navn, og døpt det om til «Åpent nett kamera som er creepy».

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: [#null_CTRL](https://twitter.com/null_CTRL)



Vandal-Proof Network Speed Dome Camera



STYRE HJEMMEFRA: Slik ser panelet ut som styrer overvåkningskameraet på Jacob Aall i Fredrikstad. Ved å trykke på pilene til venstre, kan man rotere kameraet rundt i restauranten. På bildet sitter en ansatt og fyller kjøleskapet bak baren. Foto: Skjermdump



Tips oss på nullctrl@dagbladet.no

- Jeg skal få noe til å se på hva som har skjedd, sier Gomah.

- Vi er hacket

I ettertid har restaurantens eiere undersøkt saken. Overfor Dagbladet hevder de at kameraet av typen «vandal proof» opprinnelig var utstyrt med passord og brukernavn, men at noen på et tidspunkt kan ha hacket seg inn og etterlatt det stående åpent.

- Vi ønsker ikke å kommentere saken, men etter at Dagbladet gjorde oss oppmerksomme på problemet, har vi oppgradert sikkerhetssystemet og forhåpentligvis sikret oss mot ytterligere hacke-forsøk, sier regionssjef og medeier Kawal Kahlon i Dilla Holding som eier Jacob Aall-kjeden.

- Skremmende

Datatilsynet reagerer på at slike kameraer kan ligge åpent på nett:

- Det er veldig interessant og veldig skremmende. Det som filmes er ikke noe offentligheten har noe med. Dette er noe som skjer på arbeidsplassen og da er det veldig viktig at tilgangen til de bildene vi her har sett er begrenset til et fåtall personer, sier direktør Bjørn Erik Thon i Datatilsynet.

Han mener både gjester og ansatte som filmes på denne måten kan føle seg krenket:

- Det kan være avslørende informasjon. Det er bilder av restaurantgjester og av ansatte, og det er klart at dette er jo noe som absolutt ikke har noenting på et offentlig nett å gjøre, sier Thon.

Host name : Åpent nett kamera som er creepy

☐ Turn off the LED indicator

☐ Automatically restore DO state after 1 second(s)

☐ Manually set your daylight saving time

Note: You can set your Daylight Saving Time rules

Start

End

Date: 03/01 [mm/dd]

Time: 00:00 [hh:mm]

Date: 10/01 [mm/dd]

Time: 00:00 [hh:mm]

☒ Keep current date and time

☒ Sync with computer time

PC date: 2013/05/27 [yyyy/mm/dd]

PC time: 13:15:33 [hh:mm:ss]

☐ Manual

Date: 2013/05/27 [yyyy/mm/dd]

Time: 11:16:21 [hh:mm:ss]

☐ Automatic

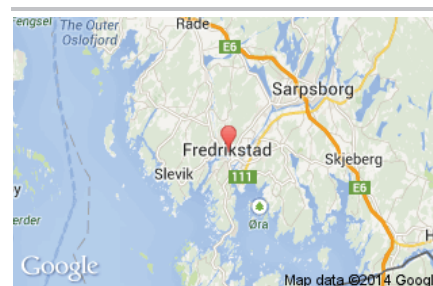
NTP server: skip to invoke default server

Time zone: GMT

Update interval: One hour

Save

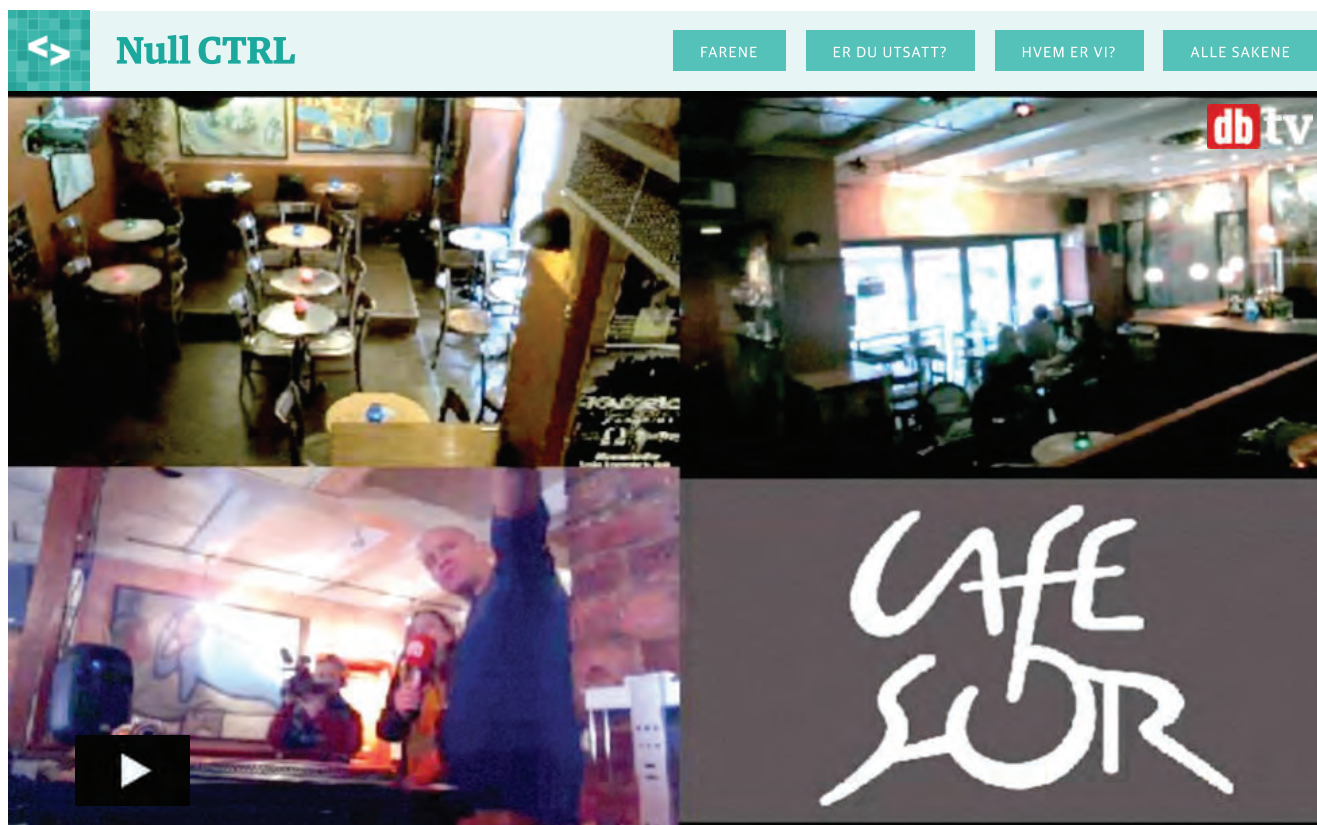
ALLE RETTIGHETER: Ettersom dette panelet ikke var utstyrt med noe passordbeskyttelse, har hvem som helst kunnet gå inn og redigere kameraets funksjoner og oppsett. Øverst har noem døpt det om til «creepy». Foto: Skjermdump



Fredrikstad

[Se større kart](#)

Her har de filmet datene dine og sendt dem direkte på nett, publisert fredag 4. oktober 2013 kl. 12:30



- **BRYTER ALLE REGLER:** Det mener Datatilsynet om Café Sør i Torggata i Oslo, som har satt opp tre overvåkingskameraer som vises som en direktesending på kafeens nettside. Daglig leder trodde det var lovlig. Video: Lise Rafaelsen / Dagbladet

Her har de filmet datene dine og sendt dem direkte på nett

- De bryter alle regler. Det er ikke lov, sier Datatilsynet.



THERESE DOKSHEIM
tdo@dagbladet.no



LISE RAFAELSEN
lra@dagbladet.no

(Dagbladet): Du tenker kanskje at du på kafé, restaurant eller på byen kan føle deg trygg på at det kun er de du er sammen med som vet at du er der. Det var kanskje naivt.



De bryter alle reglene som finnes rundt datasikkerhet.

Guro Skåltveit, seniorrådgiver i Datatilsynet.

På Café Sør i Torggata i Oslo filmer tre bitte små kameraer fra hver sin vinkel, 24 timer i døgnet - og hvem som helst kan se «direktesendinga» på kafeens [hjemmeside](#).

- En morsom gimmick

Dagbladet tar i forbindelse med en [artikkelserie om datasikkerhet](#), hvor blant annet [2048 norske overvåkingskameraer på nett er blitt avdekket](#), turen innom Oslo-kafeen. Daglig leder bekrefter at de filmer gjestene sine.

- Ja, vi har tre kameraer her. Jeg

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

har aldri fått indikasjoner på at dette er ulovlig. Vi gjør dette i et forsøk på å få bukt med kriminalitet, siden vi ligger i Torggata og er kjent med at det skjer mye i området.

- Dessuten er det en morsom gimmick i et samfunn hvor folk er på nettet hele tida og vil vite hva som skjer, sier daglig leder Laurent Vacarissas.

Møtet med daglig leder og kafeens gjester ser du i videoen øverst i denne saken.

- Bryter med alle regler

Datatilsynet sier denne typen overvåking er regelrett ulovlig.

- Det er veldig problematisk. Det er ikke lov. Punktum. Webkameraer i seg selv lov i den forstand at du har lov til å filme været på torget eller en trafikk situasjon, men det er ikke lov når du kan kjenne igjen folk. Her er det ikke vanskelig å kjenne igjen folk, du ser alt fra klær til hår og hvem som sitter og prater sammen, sier seniorrådgiver Guro Skåltveit til Dagbladet.

- De bryter alle reglene om datasikkerhet som finnes, sier hun.

- Forventer en privat stund

Dagbladet snakker med flere kafégjester, og ingen er klar over at besøket blir direktesendt.

- Jeg ante ikke at de filmet her. Det er ganske utrolig, jeg kjenner jeg blir kvalm. Man har ikke kontroll, man har på en måte ingen ting man skulle sagt, sier Kenneth Akselsen.

- Man kan godt si at det er en bagatell at man blir filmet på kafé, men når det legges sammen med annen overvåkning er det alvorlig. De sjeldne gangene jeg går på kafé forventer jeg å ha en privat stund med dem jeg drikker kaffe med. Ikke at det ligger ute på nettet, sier han.

Skåltveit i Datatilsynet mener overvåkingen er svært grov.

- Jeg kan ikke se en eneste regel de ikke har brutt. Det finnes ingen unnskyldning som kan forsvare slike grove lovbrudd.

- Aldri prøvd å skjule det

Daglig leder trodde filmingen var lovlig så lenge de ikke tar opptak



- TRODDE DET VAR LOV: Daglig leder ved Café Sør sier til Dagbladet at han forstod det som at kameraovervåkingen var lovlig. Han sier han vil endre praksisen dersom de blir bedt om det. Foto: Lise Rafaelsen / Dagbladet



FILMER DEG: Dette er ett av de tre kameraene som filmer deg inne på Café Sør i Oslo. Stedet fungerer som både kafé, utested og konsertsted. Trygt hjemme i sofaen kan andre se livebilder fra stedet, dag og natt. Foto: Lise Rafaelsen / Dagbladet



RETT PÅ NETT: Kameraet på utestedet Klubbteateret i Drammen, sendte videostrømmen rett på nett. Her kliker og fester ungdommen for åpent kamera. Video: Øistein Norum Monsen / Dagbladet



Jeg trodde det var greit så lenge folk ble informert om det. Vi har alltid vært åpne om dette, og aldri prøvd å skjule at vi filmer her.

eller lagrer det som filmes.

Laurent Vacarisas, daglig leder ved Café Sør.

- Jeg trodde det var greit så lenge folk ble informert om det og så lenge vi ikke tok opptak av det. Vi har alltid vært åpne om dette, og aldri prøvd å skjule at vi filmer her, sier han.

Men skiltene rundt om på kafeen er bitte små og nesten umulig å se med mindre man vet hvor de er plassert. På små skilt står det «TV og video» sammen med et bilde av et overvåkningskamera. Det står derimot ingenting om at det kameraet filmer kan streames på nettet.

- Jeg ante ikke at man blir filmet her. Det første jeg tenker er «tenk hvis jeg hadde vært på en første date», for eksempel, sier Elise Andersen Vegard (25).

- Blir utilpass

Det er første gang hun og mora er på Café Sør. De blir vist kameraene, hvorav ett av dem er lokalisert en halv meter fra dem, av Dagbladet.

- Jeg føler meg nesten litt utilpass nå når jeg vet at jeg blir filmet av et sånt kamera. Vi så ingen skilt eller noen ting da vi gikk hit. De skiltene jeg nå ser er satt opp, ser ut som er til å forklare at det blir overvåket av sikkerhetsmessige grunner. Ikke at det ligger ute på nett så alle kan se det, sier Vegard.

Mens Dagbladet er på kafeen, endres det man kan se på nettet. Streamingen går fra å omfatte alle kameraene til å kun vise ett av kameraene.

- Vil fjerne kameraene

Datatilsynets seniorrådgiver er kritisk til Café Sørs metoder.

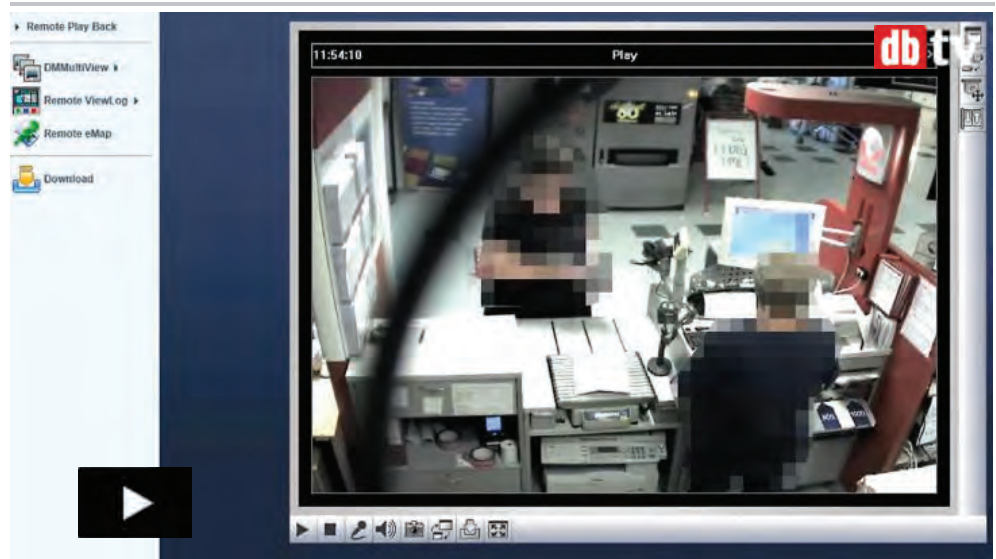
- Jeg har selv sjekket kameraet på hjemmesida deres, og du kan klart og tydelig se hvem som er der, klærne deres og hvem de er sammen med. Det er ikke greit. Jeg tror ingen ville gått dit, hadde de visst at de ble filmet og lagt ut på nettet, sier hun.

Daglig leder vil endre praksisen og ta ned kameraene dersom han får pålegg om det, opplyser han til Dagbladet.

- Hvis Datatilsynet ber oss fjerne kameraene, så skal vi gjøre det. Vi ønsker ikke å drive med ulovligheter, sier Vacarisas.



PÅ JOBB I SIVIL: Overvåkningskameraet på utestedet Klubbteateret i Drammen sendte video av politiets innsatsleder Geir Oustorp rett på nett. Video: Øisten Monsen / Dagbladet



ALLE KAN SE: Et kamera står plassert bak skranken i Post i butikk på Frostad senter nord for Trondhjem. Totalt lå 16 av senterets overvåkningskameraer tilgjengelig på nett. Video: Øistein Norum Monsen / Dagbladet



Tips oss på nullctrl@dagbladet.no



ALARMERT: Seniorrådgiver Stian D Kringlebotn, direktør Bjørn Erik Thon og seniorrådgiver Guro Skåltveit ved Datatilsynet ser på Dagbladets reportasjer om overvåkingskameraer som ligger vidåpne på internett. Nå vil de holde leverandørene i øra så de gir kundene skikkelig opplæring i sikkerhet. Foto: Benjamin A. Ward / Dagbladet

Vil ta affære etter Dagbladets kamera-avsløringer

Datatilsynet mener leverandørene også har ansvar for at overvåkingsbilder kringkastes rett ut på Internett.



LINN KONGSLØ HILLESTAD
llu@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



THERESE DOKSHEIM
tdo@dagbladet.no

(Dagbladet): Se for deg at du nettopp har satt deg ned med et glass vin, enten hjemme i stua, på en bar eller restaurant. Skuldrene har nettopp senket seg etter en hektisk dag på jobb.

Men idyllen hadde nok slått sprekker dersom du hadde visst at fremmede samtidig iakttok deg via internett - noe som ikke bare er en hypotetisk mulighet.

Alle kan se

De siste dagene har Dagbladet avslørt at bilder fra overvåkingskameraer over hele landet [kringkastes rett ut på nettet](#), uten passordbeskyttelse, til skue for hele verden.

Og oftest uten at eierne vet om det



- UPROFFE: Helge Veum i Datatilsynet mener det finnes alt for mange som benytter seg av uprofesjonelle overvåkingssystemer, og at det derfor ofte går galt. Foto: Datatilsynet

selv.

Totalt har vi funnet over 2000 norske overvåkingskameraer på internett.

Mange av kameraene kan styres via panelene som kommer opp i nettleseren, og noen av dem har lydoverføring. Dette innebærer at uvedkommende kan lytte til private samtaler via internett, og i noen tilfeller også snakke via kameraene.

- Bransjen har ansvar

Datatilsynet var ikke kjent med problematikken Dagbladet har avdekket, og beskriver situasjonen som «alarmerende».

Nå vil de ta affære, varsler direktør Bjørn Erik Thon.

Han mener det hviler et spesielt ansvar på de som er ute og monterer disse kameraene.

- Selvfølgelig er det også viktig at de som tar i bruk kameraene vet hvordan de brukes. Men dette er jo ganske avansert teknologi. Derfor er det viktig at de får ordentlig opplæring i hvordan de setter opp passord og hvordan de sikrer dataene sine. Der har bransjen et ansvar, sier Thon til Dagbladet.

Også avdelingsdirektøren for tilsyns- og sikkerhetsavdelingen i selskapet, Helge Veum, mener det er her problemet ligger: Det er alt for mange aktører som skaffer seg overvåkingskameraer de ikke klarer å håndtere.

- Det er rett og slett uprofesjonelle løsninger gjort av uprofesjonelle aktører. I dag er det altfor enkelt å skaffe seg overvåkingskameraer, og det finnes lite hjelp å få. Dermed ender folk opp med løsninger de ikke klarer å håndtere. Da er ikke systemene sikre, slik som dere nå viser, sier han.

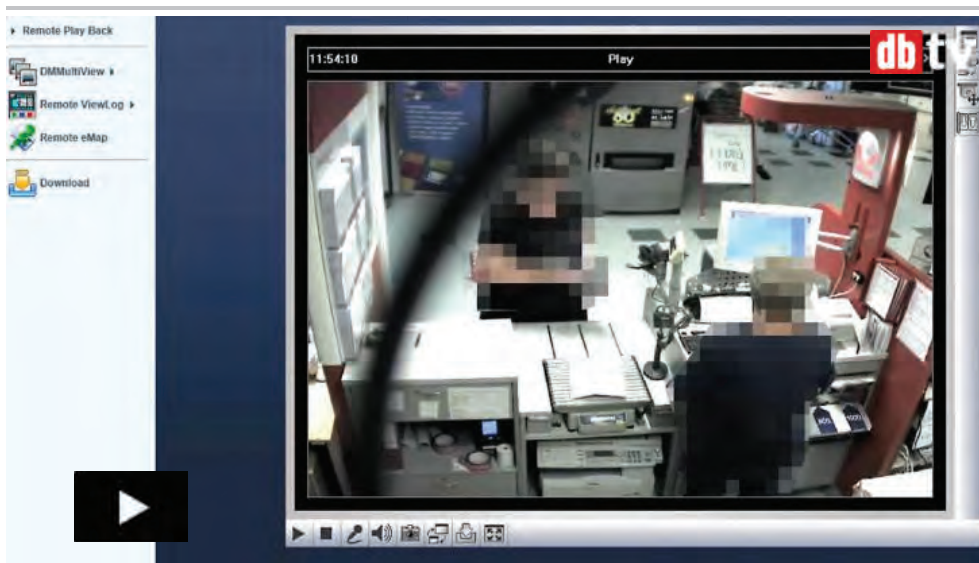
Vil ta kontakt

Direktør Thon forteller at Datatilsynet derfor vil ta kontakt med de største firmaene som driver med kamerainstallasjon, og deres bransjeorganisasjoner, for å få dem til å gi bedre informasjon og opplæring av bedrifter og privatpersoner som har kameraene installert.

- Når vi går på tilsyn til bedrifter som driver med



RETT PÅ NETT: Kameraet på utestedet Klubbteateret i Drammen sendte videostrømmen rett på nett. Video: Øistein Norum Monsen/Dagbladet



SYNLIG FOR ALLE: Et kamera står plassert bak skranken i Post i butikk på Frostad senter nord for Trondheim. Totalt lå 16 av senterets overvåkingskameraer tilgjengelig på nett. Video: Øistein Norum Monsen / Dagbladet

Hva kan du gjøre?

Skulle du oppdage å bli filmet på det du mener er ulovlig vis, er det flere ting du som enkeltperson kan gjøre.

Avdelingsdirektøren for tilsyns- og sikkerhetsavdelingen i Datatilsynet, Helge Veum, har følgende råd:

- Si ifra til stedet det gjelder, og gi dem klar beskjed på at dette ikke er greit. Da kan de sjekke systemene sine og få på plass sikrere løsninger og kryptering.
- **Hører de ikke på deg kan du melde det inn til oss i Datatilsynet, eller eventuelt anmelde det, sier Veum.**
- Det ryddigste er å gå til de som har problemet, slik at de har mulighet til å korrigere det, sier han.

kameraovervåkning er det også viktig at vi sjekker spesielt om de passer på at anleggene er godt sikret mot «innbrudd» utenfra, sier han.

I og med at kameraovervåking potensielt kan være et inngrep i personvernet, drar Datatilsynet jevnlig ut på tilsyn til bedrifter og offentlige instanser som benytter seg av overvåkingskameraer. Kameraovervåking på arbeidsplasser og offentlige steder er også meldepliktig.

Mange glemmer imidlertid å melde fra. Derfor finnes ingen fullstendig oversikt over antall overvåkingskameraer i Norge, men de siste åra har det vært en jevn økning. Datatilsynet estimerer at rundt 20 000 aktører har overvåkingskameraer, privatpersoner ikke inkludert.

Strengte regler

Overvåkingen er regulert av personopplysningsloven, og de som benytter seg av kameraovervåking har selv plikt til å sette seg inn i reglene.

- Generelt sett er det lov å bruke overvåkingskameraer når du har et fornuftig behov for det og bruker kameraene på en fornuftig måte, sier Thon.

Det er for eksempel ikke greit å overvåke en skolegård i skoletida hvis målet er å sikre seg mot hærverk som skjer på kveldstid.

- Det handler om å finne en god balanse mellom personvern på den ene siden og sikkerhet på den andre siden. Og hvis man bruker hodet og bruker fornuft, så klarer man som regel å finne en god balanse der, sier Thon.

Avdelingsdirektøren for tilsyns- og sikkerhetsavdelingen, Veum, sier Datatilsynet gjerne skulle rekke å se på alle tilfellene der overvåkingsregler er brutt.

Det er derimot enklere sagt enn gjort.

- Jeg tror ikke det ville hjulpet særlig om vi i Datatilsynet løp rundt med bøteblokk - jeg tror heller dette må tas opp av tilligtsvalgte slik at de ansatte gjøres oppmerksomme på hvilke tiltak som må til før kameraene er sikret på best mulig måte. Problematikken må rett og slett belyses, sier Veum.



- BRYTER ALLE REGLER: Det mener Datatilsynet om Café Sør i Torggata i Oslo, som har satt opp tre overvåkingskameraer som vises som en direktesending på kafeens nettside. Daglig leder trodde det var lovlig. Video: Lise Rafaelsen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyrte vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL

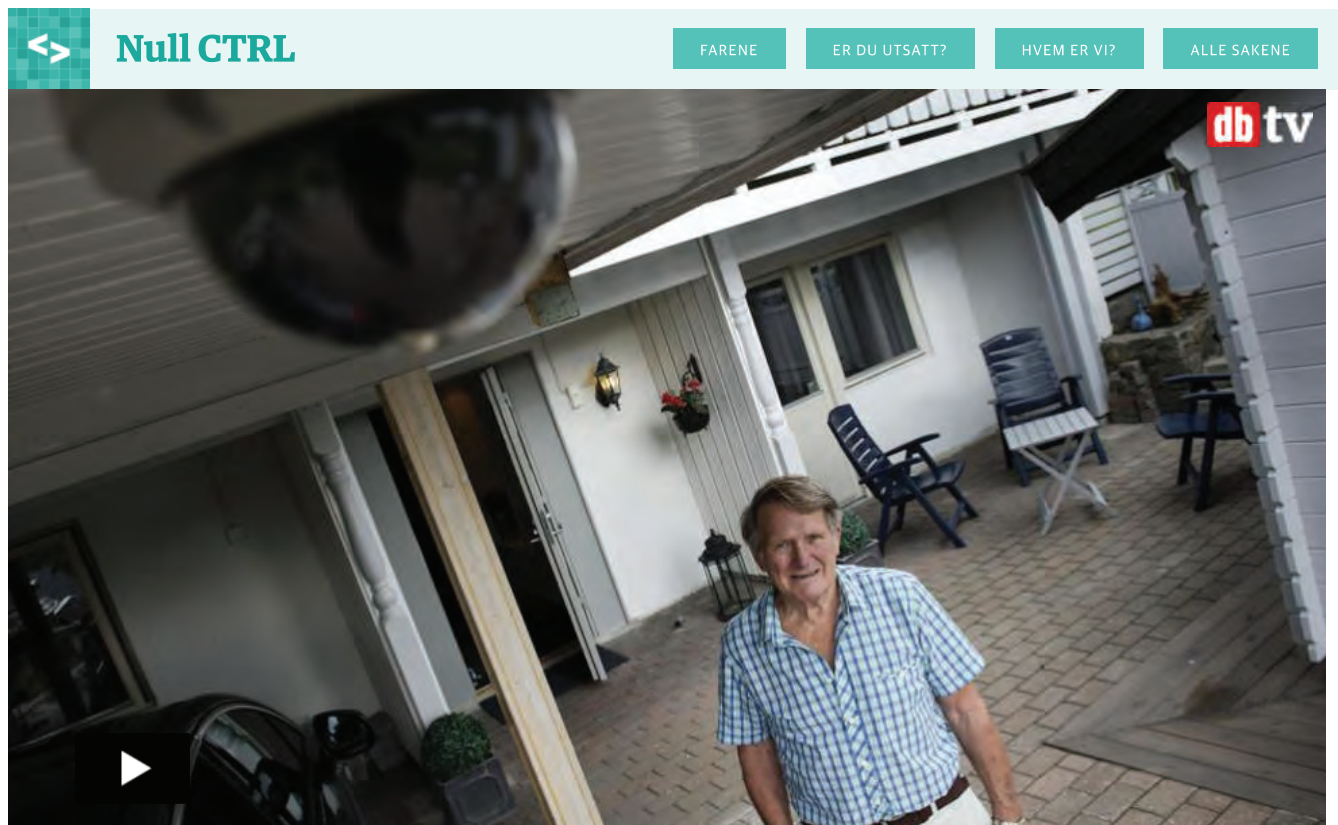


PÅ JOBB I CIVIL: Overvåkingskameraet på utestedet Klubbteateret i Drammen sendte video av politiets innsatsleder Geir Oustorp rett på nett. Video: Øisten Monsen / Dagbladet



SKREMT: Harry Stene likte ikke at 16 overvåkingskameraer på Frostad senter har ligget åpent på internett. Video: Ole Morten Melgård / Øistein Norum Monsen / Dagbladet

Her får Asbjørn vite at overvåkingskameraet hans ligger åpent på nettet, publisert lørdag 5. oktober 2013 kl.



OVERVÅKET: Asbjørn Korsfjord fra Moss var ikke klar over at overvåkingskameraet hans lå åpent på internett. Video: Øistein Norum Monsen/Dagbladet.

Her får Asbjørn vite at overvåkingskameraet hans ligger åpent på nettet

- Jeg hadde aldri hatt mistanke om dette.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



ØISTEIN NORUM MONSEN
onm@dagbladet.no

STATHELLE/MOSS/OSLO
(Dagbladet): Det kan være mange gode grunner til å installere et nettbasert overvåkingskamera. Å sikre seg mot tyveri, sjekke snømengden på hyttetaket, eller se at båten ligger som den skal, for eksempel.

Men hvis du glemmer å beskytte kameraene med passord, kan de fort virke mot sin hensikt.

Over 2000 kameraer

Som [Dagbladet har avslørt](#), ligger over 2000 norske overvåkingskameraer ute på Internett. Det betyr at uvedkommende enkelt kan få tilgang til levende bilder fra [utesteder](#), [restauranter](#), [butikker](#) - og private stuer og soverom.



- **BRYTER ALLE REGLER:** Det mener Datatilsynet om Café Sør i Torggata i Oslo, som har satt opp tre overvåkingskameraer som vises som en direktesending på kafeens nettside. Daglig leder trodde det var lovlig. Video: Lise Rafaelsen / Dagbladet

Noen overvåker babysenga hvor

spedbarnet sover søtt, andre badestampen ute på terrassen.

Mange av kameraene kan styres via panelet som kommer opp i nettleseren, og flere har lydoverføring. Det betyr at vi kunne ha snakket til intetanende privatpersoner hjemme i stua gjennom deres eget web-kamera.

- Farlig

Jan Olaf Stenhaug installerte et overvåkingskamera utenfor døra si hjemme på Stathelle etter at han hadde vært utsatt for hærverk. Kontinuerlig filmer det sitteplassene utenfor inngangen.

Når Dagbladet viser Stenhaug bildene fra kameraet på vår Ipad, blir han temmelig paff.

- Det er rart at dette kameraet skal sende ut på Internett. Jeg var sikker på at dette var helt på innsiden av min egen brannmur, sier Stenhaug, som av denne grunn ikke beskyttet kameraet med passord.

- Det er jo litt farlig hvis alle kan se hva du foretar deg til enhver tid, sier han.

Kameraet er kinesisk, kjøpt på nettstedet Ebay, og selv om det er koblet til Stenhaugs internett, kan alle få tilgang via hans eksterne IP-adresse.

- Jeg hadde aldri hatt mistanke om at dette kunne gå via flere IP-adresser, sier han.

- Ikke bra

Asbjørn Korsfjord fra Moss er i samme situasjon. hans kamera kunne i tillegg styres via panelet i nettleseren.

Dagbladet viser ham livebilder fra overvåkingskameraet hvor vi sammen står utenfor huset hans. Da humrer han godt.

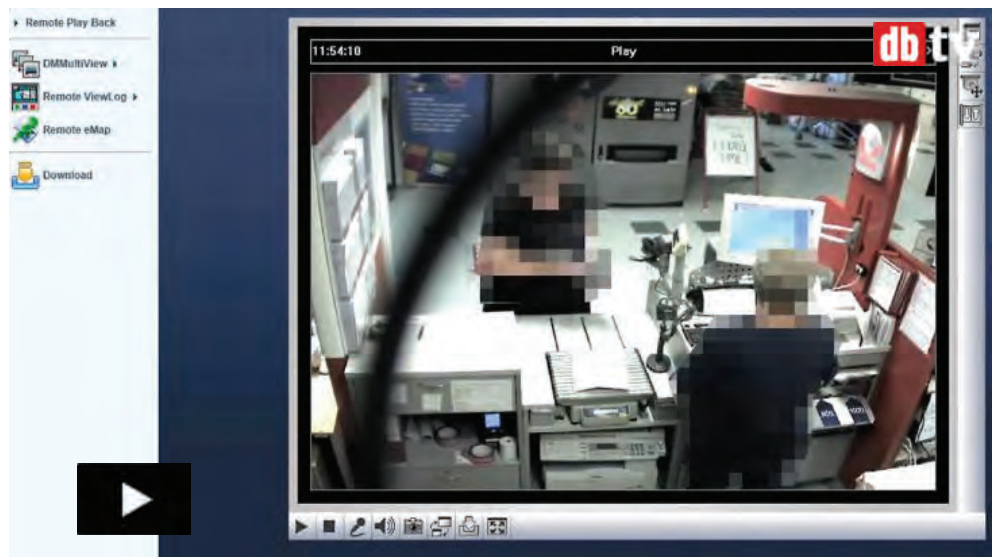
- Jeg har ikke tenkt over dette. Jeg bør vel lage meg ett passord, i hvert fall.

- Det er jo ikke bra det der, at alle kan se, men det har jo ikke noe å si når det er på utsiden, sier han.

- Samtidig kan jo innbruddstyver følge med når det er noen hjemme og ikke.

- Ja, det er riktig det.

Kan misbrukes



SYNLIG FOR ALLE: Et kamera står plassert bak skranken i Post i butikk på Frostasenteret nord for Trondheim. Totalt lå 16 av senterets overvåkingskameraer tilgjengelig på nett, før Dagbladet gjorde dem oppmerksomme på feilen før sommeren. Video: Øistein Norum Monsen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



RETT PÅ NETT: Klubbteateret i Drammen [viste festglad og klinende ungdom](#). Video: Øistein Norum Monsen / Dagbladet

Problemet er nettopp det at du aldri vet hvem som sitter og ser på kameraene, påpeker seniorrådgiver Vidar Sandland i Norsk Senter for Informasjonssikring (Norsis).

- Det kan være nysgjerrige naboer eller bekjente, eller det kan være kjeltringer som bruker dette til å finne ut når du er hjemme og når du er borte, sier han til Dagbladet.

- Og hvis dette kameraet skulle stå inne, er det jo også forferdelig for mange. Da vil jo hvem som helst kunne se og kanskje høre alt som skjer, legger han til.

Billigere og mer avansert

Direktør Bjørn Erik Thon i Datatilsynet tror problemet med åpne kameraer først og fremst skyldes uvitenhet.

- De siste åra har vi sett at kameraene er blitt mye mer avanserte, og samtidig er de blitt billigere og lettere å bruke. Så det er nok ganske mye tankeløshet. Man synes det er greit å ha et kamera, man tror man får bedre sikkerhet, og så er det nettopp det motsatte som skjer, sier han til Dagbladet.

Datatilsynet [vil nå ta affære](#) og sørge for at leverandørene gir kundene sine bedre opplæring.

Så er det heller ikke vanskelig å sikre seg i hvert fall et minimum av beskyttelse.

Mens Dagbladet er på Stathelle, har Jan Olaf Stenhaug i løpet av noen minutter satt opp passordbeskyttelse på web-kameraet sitt. Og vi har ikke lenger tilgang til overvåkingsbildene hans.



Tips oss på nullctrl@dagbladet.no



FILMET INNGANGSDØREN: Jan Olaf Stenhaug installerte et overvåkingskamera utenfor døra si hjemme på Stathelle. Foto: Øistein Norum Monsen/Dagbladet

Overvåket av

Trond Kristiansen hadde aldri forestilt seg at kameraet han hadde plassert på kjøkkenet og datterens soverom kringkastet lyd og bilder rett ut på Internett.

Tekst: **Linn Kongsli Hillestad**
lk@dagbladet.no

Espen Sandli
esan@dagbladet.no

Thomas Rasmus Skaug
tsk@dagbladet.no

GJØVIK (Dagbladet): – Dette er ordentlig skummelt, sier Trond Kristiansen til Dagbladet.

For snart ett år siden kjøpte han et overvåkingskamera så han kunne holde et øye med hundene i hundegården, rett utenfor kjøkkenet.

Kameraet plasserte Kristiansen oppe på mikrobølgeovnen, hvor det sto og filmet kontinuerlig ut av kjøkkenvinduet, trygt på det trådløse nettverket og bak brannmuren hans. Trodde han i hvert fall.

Det Kristiansen ikke visste, er at kameraet også var tilgjengelig på den offentlige IP-adressen hans, uten noen form for passordbeskyttelse.

Uvedkommende kunne derfor ta styring over kameraet via panelet i nettleseren og dreie det 180 grader så de så rett inn på kjøkkenet.

– Og dette kan hvem som helst gjøre, mener du? spør Kristiansen sjokkert når Dagbladet viser ham et filmklipp av hvor enkelt det er.

På barnerommet

Ei uke før Dagbladet gjorde ham oppmerksom på at kameraet lå åpent tilgjengelig for alle, hadde han flyttet det ned på datterens soverom.

Noe som ikke er uvanlig at foreldre gjør for å holde et øye med barna. I forbindelse med en artikkelserie om datasikkerhet, har Dagbladet funnet over 2000 norske overvåkingskameraer koblet til nettet. Av disse er flere plassert på barnerom.

– Kall det en nymotens babycall, sier Kristiansen.

– Sånn sett er det greit at folk ser ut på bikkjer, men at de skal ha tilgang til soverommet til datteren min, det er jeg ikke så glad for.

Selv kan han følge med på kameraet via en app på mobilen, og han demonstrerer hvordan han enkelt

kan snu på kameraet, høre lyd og ta bilder og opptak.

I utgangspunktet veldig praktisk, så lenge ikke alle andre har den samme muligheten. Dagbladet er kjent med at uvedkommende har vært inne på Kristiansens kamera, men kan ikke anslå hvor mange.

Bekymret for kriminelle

– Det første jeg tenker på, er jo kriminelle. Med tanke på at de faktisk ser innsida av huset ditt, så de kan se om det er verdier å stjele. Men det er jo én ting. Noe annet er faktisk å bli overvåket av dine egne kameraer uten at du er klar over det, sier han.

Han mener leverandørene av slike kameraer har et opplysningsansvar.

– Kameraet er jo avhengig av en ruter eller en nettverkstilkobling, og så lenge jeg kobler det opp mot min ruter, som er passordbeskyttet, så var det ikke i mine tanker at noen som kunne gå inn og styre eller se på det kameraet. Dette kunne jeg ikke se for meg i mine vildeste fantasier.

Lett tilgjengelig

Kristiansen får støtte av direktør Bjørn Erik Thon i Datatilsynet, som mener en av årsakene til problemet er at denne typen kameraer er blitt så lett tilgjengelige for folk flest.

– Dette er jo ganske avansert teknologi. Derfor er det viktig at de får ordentlig opplæring i hvordan de setter opp passord og hvordan de sikrer dataene sine. Der har bransjen et ansvar, sier Thon til Dagbladet.

Han varsler at de vil følge opp kameralleverandørene etter Dagbladets avsløringer.

«Tommy»

På tross av at IP-adresser i utgangspunktet er anonyme for andre enn nettleverandøren, er det på ingen måte umulig å finne fram til eierne av overvåkingskameraer.

For det første kan du finne ut cirka hvor kameraet er plassert via et enkelt lokaliseringssøk av IP-adressen på Internett. Slik fant Dagbladet ut at dette aktuelle kameraet trolig befant seg i Oppland.

Samtidig var brukernavnet «Tommy» oppgitt i kamerapanelet, og hundegården kameraet filmet tilsa at eierne trolig drev med hundepoppdrett. Ved å søke «Tommy», «Oppland» og «hundepoppdrett» i Google, fant Dagbladet en spesiell premiehund – og dermed også kameraeierne.

– Skummelt hvor enkelt det kan være, mener Trond Kristiansen, som nå har fjernet kameraet fra nettet.

Se også kommentar side 3.



Dette skulle kameraet filme



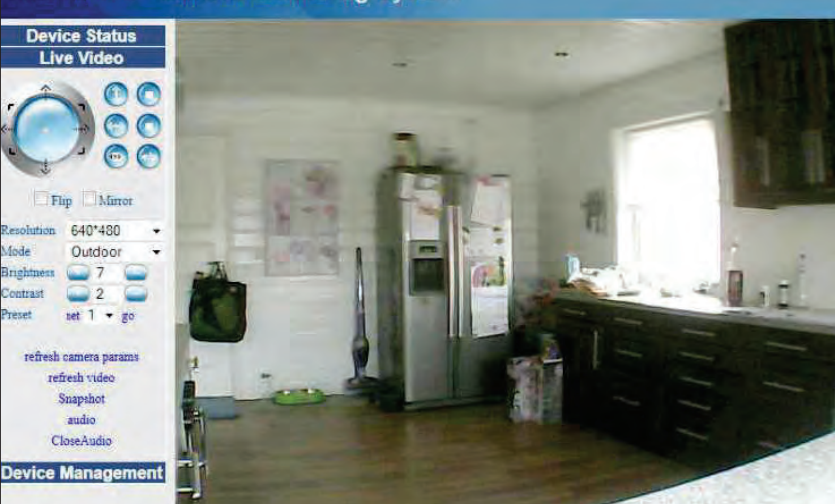
SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans kringkastet bilder og lyd rett ut

” Sånn sett er det greit at folk ser ut på bikkjer, men at de skal ha tilgang til soverommet til datteren min, det er jeg ikke så glad for.

Trond Kristiansen,
eier av overvåkingskamera

eget kamera

Real-time IP Camera Monitoring System



...men så ble det fjernstyrt av andre



PRAKTISK OG ENKELT: Trond Kristiansen kjøpte overvåkingskameraet sitt på nettet, og kan hele tida følge med på livebilder via sin telefon. Men andre hadde også samme muligheten.

Foto: Thomas Rasmus Skaug

FAKTA

Slik sikrer du kameraet ditt

- Selv om overvåkingskameraet er koblet til ditt interne nettverk, beskyttet bak en brannmur, kan kameraet fortsatt være tilgjengelig for andre via din offentlige IP-adresse.
- Derfor er det viktig å beskytte kamerapanelet med brukernavn og et solid passord.
- I noen tilfeller kommer kameraer med et standardpassord fra leverandøren, som for eksempel admin./admin. Disse er ofte allment kjent, og må derfor byttes med en gang du installerer kameraet.
- Generelt må du alltid huske å sikkerhetsoppdatere de elektroniske produktene du har koblet til nettet. Hvis det finnes et sikkerhetshull, er det enkelt for en hacker å utnytte dette og få full tilgang. Derfor må du huske å oppdatere til siste versjon eller det som er anbefalt.
- Dersom du har installert et kamera på et offentlig sted, for eksempel i en butikk eller restaurant, er det viktig å sette seg inn i regelverket for kameraovervåking så du vet at det ikke er ulovlig satt opp. I tillegg må slike kameraer meldes inn til Datatilsynet.

Kilder: Norsk Senter for Informasjonssikring / Datatilsynet

TIPS OSS

Espen Sandli
esan@dagbladet.no

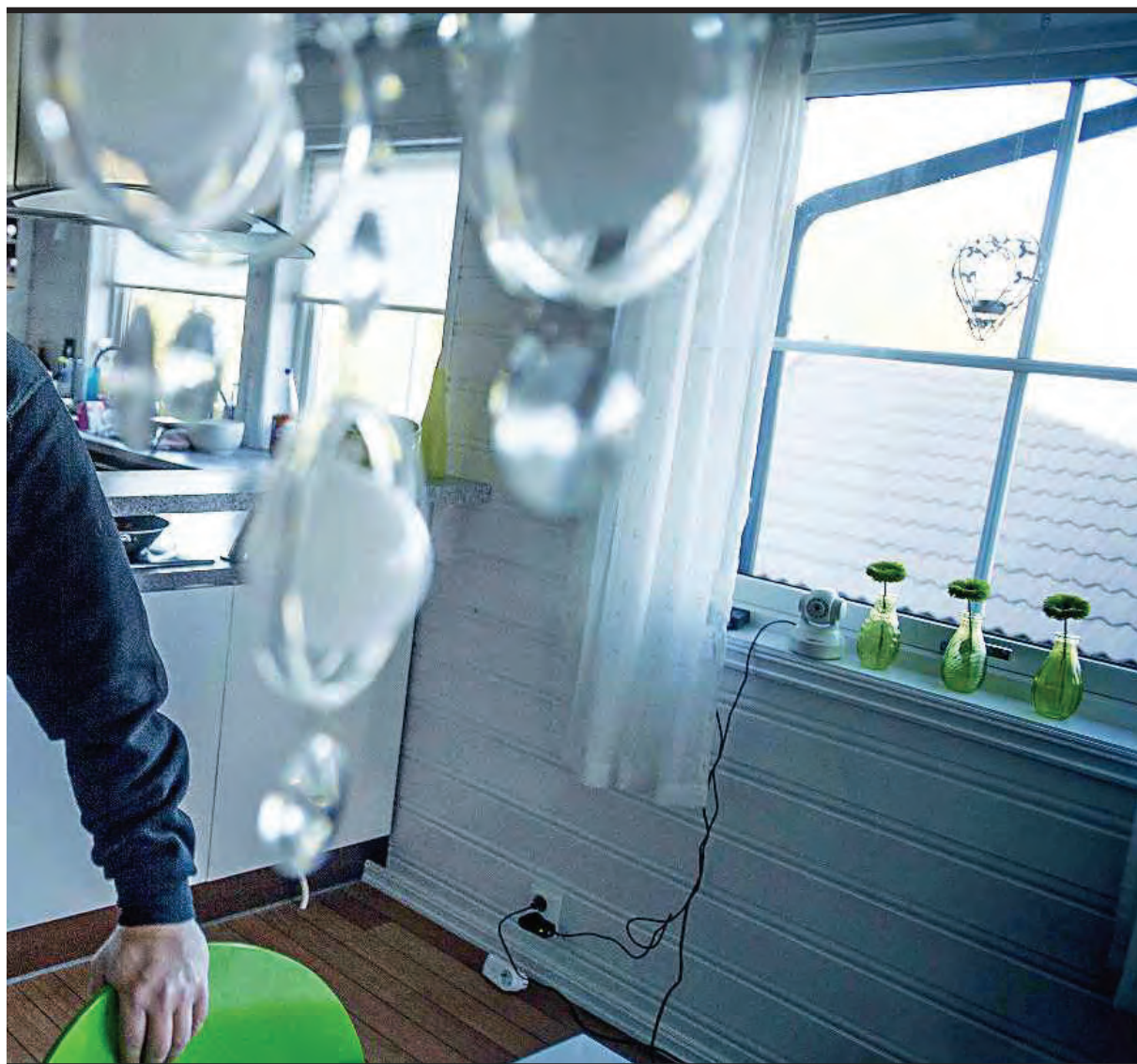
Linn K. Hillestad
lkh@dagbladet.no

Null CTRL

FAKTA

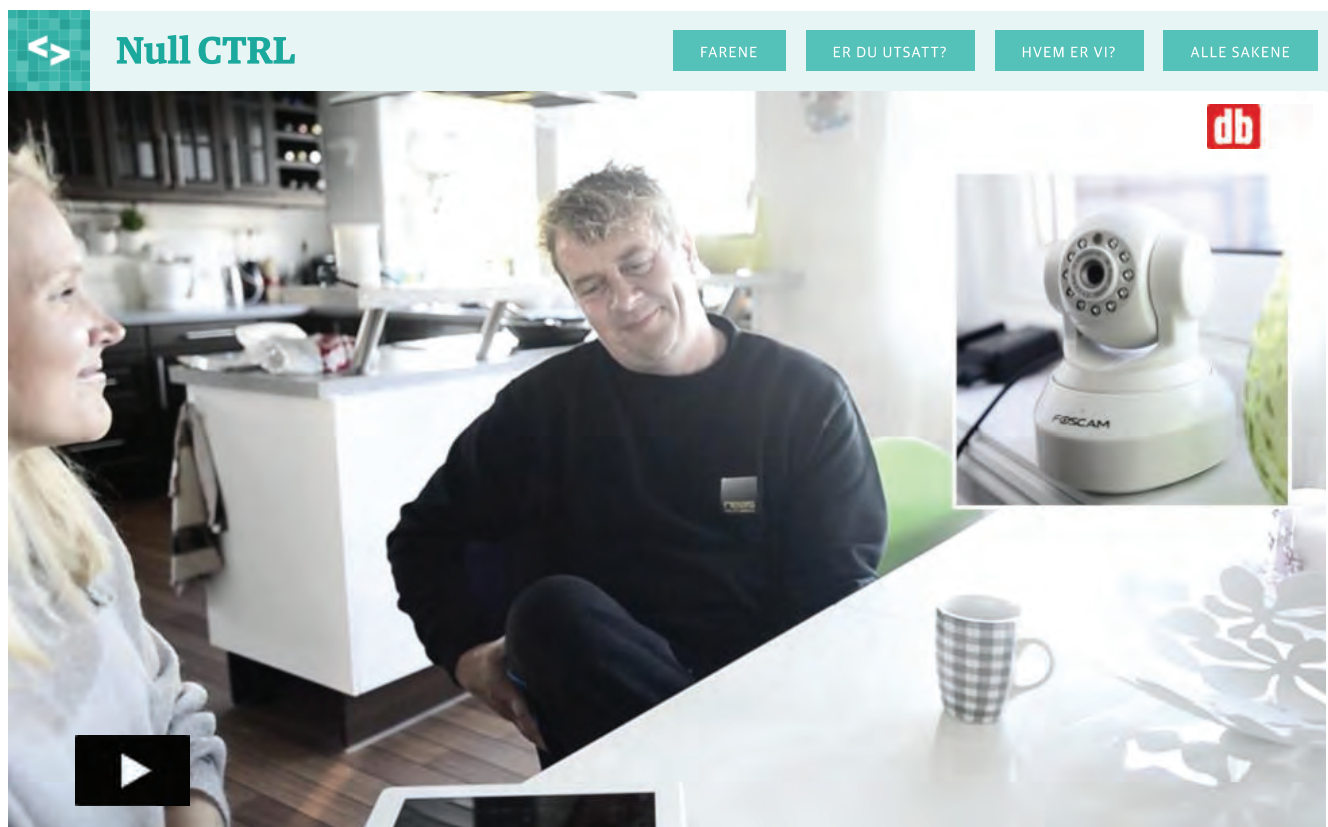
Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens webkamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: dagbladet.no/nullctrl/
- Tips oss på nullctrl@dagbladet.no



på Internett. Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom.

Foto: Thomas Rasmus Skaug



SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans kringkastet bilder og lyd rett ut på Internett. Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet

Hvem som helst kunne følge livebilder fra Tronds hjem

- Dette kunne jeg ikke se for meg i mine vildeste fantasier.



LINN KONGSLIE HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



THOMAS RASMUS SKAUG
tsk@dagbladet.no

GJØVIK (Dagbladet): - Dette er ordentlig skummelt, sier Trond Kristiansen.

For snart ett år siden kjøpte han et overvåkingskamera så han kunne holde et øye med hundene i hundegården, rett utenfor kjøkkenet hans.

Kameraet plasserte Kristiansen oppe på mikrobølgeovnen. Her sto det og filmet kontinuerlig ut av kjøkkenvinduet, trygt på det trådløse nettverket og bak brannmuren hans. Trodde han i hvert fall.

Det Kristiansen ikke visste, er at kameraet også var tilgjengelig på den offentlige IP-adressen hans, uten noen form for passordbeskyttelse.

Uvedkommende kunne derfor ta

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

styring over kameraet via panelet i netteseren og dreie det 180 grader så de så rett inn på kjøkkenet.

- Og dette kan hvem som helst gjøre, mener du? spør Kristiansen sjokkert når Dagbladet viser ham et filmklipp av hvor enkelt det er.

På barnerommet

Ei uke før Dagbladet gjorde ham oppmerksom på at kameraet lå åpent tilgjengelig for alle, hadde han flyttet det ned på datterens soverom.

Noe som ikke er uvanlig at foreldre gjør for å holde et øye med barna. I forbindelse med [en artikkelserie om datasikkerhet](#), har Dagbladet funnet [over 2000 norske overvåkingskameraer koblet til nettet](#). Av disse er flere plassert på barnerom.

- Kall det en nymotens babycall, sier Kristiansen.

- Sånn sett er det greit at folk ser ut på bikkjer, men at de skal ha tilgang til soverommet til datteren min, det er jeg ikke så glad for, legger han til.

I videoen over kan du se en demonstrasjon av hvordan overvåkingskameraet også filmet Dagbladets intervju med Kristiansen. Selv kan han følge med på kameraet via en app på mobilen, og han demonstrerer hvordan han via telefonskjermen enkelt kan snu på kameraet, høre lyd og ta både opptak og bilder.

Bekymret for kriminelle

I utgangspunktet veldig praktisk, så lenge ikke alle andre har den samme muligheten.

- Det første jeg tenker på, er jo kriminelle. Med tanke på at de faktisk ser innsiden av huset ditt, så de kan se om det er verdier å stjele. Men det er jo én ting. Noe annet er faktisk å bli overvåket av dine egne kameraer uten at du er klar over det, sier Kristiansen.

Han mener leverandørene av slike kameraer har et ansvar om å opplyse om at dette faktisk kan skje hvis kameraene ikke sikres godt nok.

- Kameraet er jo avhengig av en ruter eller en nettverkstilkobling, og



RETT PÅ NETT: Klubbteateret i Drammen [viste festglad og klinende ungdom](#). Video: Øistein Norum Monsen / Dagbladet



PRAKTISK OG ENKELT: Trond Kristiansen kjøpte overvåkingskameraet sitt på nettet, og kan hele tida følge med på livebilder via sin telefon. Men andre hadde også samme muligheten. Foto: Thomas Rasmus Skaug / Dagbladet

Slik sikrer du kameraet ditt

- Selv om overvåkingskameraet er koblet til ditt interne nettverk, beskyttet bak en brannmur, kan kameraet fortsatt være tilgjengelig for andre via din offentlige IP-adresse.
- Derfor er det viktig å beskytte kamerapanelet med brukernavn og et solid passord.
- I noen tilfeller kommer kameraer med et standardpassord fra leverandøren, som for eksempel admin/admin. Disse er ofte allment kjent, og må derfor byttes med en gang du installerer kameraet.
- Generelt må du alltid huske å sikkerhetsopdatere de elektroniske produktene du har koblet til nettet. Hvis det finnes et sikkerhetshull, er det enkelt for en hacker å utnytte dette og få full tilgang. Derfor må du huske å oppdatere til siste versjon eller det som er anbefalt.
- Dersom du har installert et kamera på et offentlig sted, for eksempel i en butikk eller restaurant, er det viktig å sette seg inn i regelverket for kameraovervåking så du vet at det ikke er ulovlig satt opp. I tillegg må slike kameraer meldes inn til Datatilsynet.

Kilder: Norsk Senter for Informasjonssikring / Datatilsynet

så lenge jeg kobler det opp mot min ruter, som er passordbeskyttet, så var det ikke i mine tanker at noen som kunne gå inn og styre eller se på det kameraet. Du hører det hvis det går, hvis det flytter på seg, men nei, dette kunne jeg ikke se for meg i mine villeste fantasier.

Lett tilgjengelig

Kristiansen får støtte av direktør Bjørn Erik Thon i Datatilsynet, som mener en av årsakene til problemet er at denne typen kameraer er blitt så lett tilgjengelige for folk flest.

- Dette er jo ganske avansert teknologi. Derfor er det viktig at de får ordentlig opplæring i hvordan de setter opp passord og hvordan de sikrer dataene sine. Der har bransjen et ansvar, sier Thon til Dagbladet.

De [vil nå følge opp kameraleverandørene](#) etter Dagbladets avsløringer.

«Tommy»

På tross av at IP-adresser i utgangspunktet er anonyme for andre enn nettleverandøren, er det på ingen måte umulig å finne fram til eierne av overvåkingskameraer som kringkaster ut på nettet.

For det første kan du finne ut cirka hvor i verden kameraet er plassert via et enkelt lokaliseringssøk av IP-adressen på Internett. Slik fant Dagbladet ut at dette aktuelle kameraet trolig befant seg i Oppland.

Samtidig var brukernavnet «Tommy» oppgitt i kamerapanelet, og hundegården kameraet filmet tilsa at eierne trolig drev med hundeoppdrett. Ved å søke «Tommy», «Oppland» og «hundeoppdrett» i Google, fant Dagbladet en spesiell premiehund - og dermed også kameraeierne.

- Skummelt hvor enkelt det kan være, mener Trond Kristiansen, som nå har fjernet kameraet fra nettet.

Skeptisk

Han husker at han var veldig skeptisk da han installerte alarm med tilhørende kameraovervåking, fordi han var bekymret for at ansatte i alarmselskapet kunne sitte og følge med på hva som skjedde hjemme i stua.

Den gang fikk han en skriftlig erklæring om at ingen kunne åpne kameraet med mindre alarmen gikk.

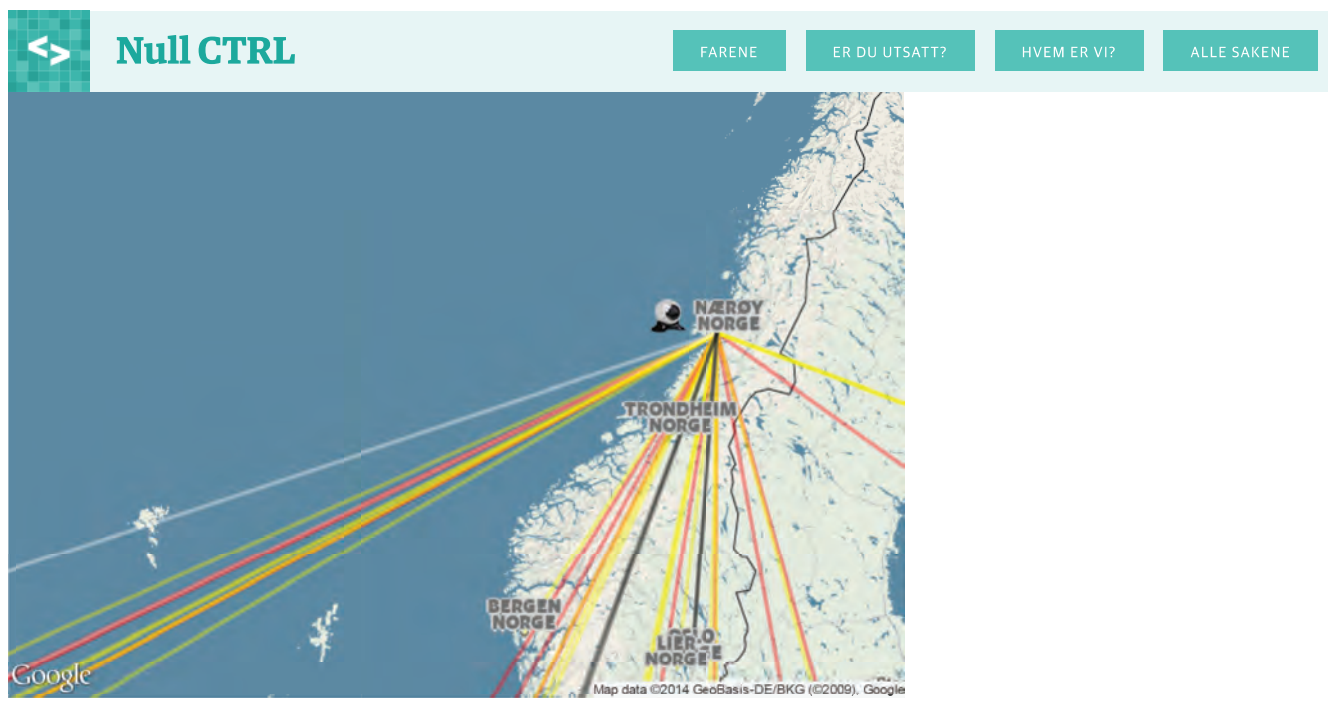
- Men jeg tenkte ikke på dette da jeg kjøpte mitt eget kamera, sier han ettertenksomt.



- **BRYTER ALLE REGLER:** Det mener Datatilsynet om Café Sør i Torggata i Oslo, som har satt opp tre overvåkingskameraer som vises som en direktesending på kafeens nettside. Daglig leder trodde det var lovlig. Video: Lise Rafaelsen / Dagbladet



Hele verden spionerte på soverommet i norsk familiehytte, publisert søndag 6. oktober 2013 kl. 15:23



MANGE KIKKERE: Dette kartet viser alle som var inne og så på kameraet i Nærøy i løpet av ei uke. Grafikk: Ola Strømman

Hele verden spionerte på soverommet i norsk familiehytte

Et kamera på ei hytte i Nord-Trøndelag ble besøkt 98 ganger på ei uke - av personer fra tolv ulike land.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): Levende bilder av [festende norsk ungdom på nattklubb](#), [restaurantgjester i intime samtaler](#) og [eldre damer som taster inn pinkoden til kredittkortet sitt](#) kringkastes rett ut på nettet.

Totalt ligger [over 2000 norske overvåkingskameraer](#) ute på Internett med liten eller ingen beskyttelse, har Dagbladet avslørt de siste dagene.

Flere av disse kameraene er montert opp [i eller utenfor private hjem](#), hvor alt fra sovende babyer til badestamper og persiske tepper overvåkes.

Omvisning ute og inne

Mange av disse overvåkingskameraene blir også hyppig besøkt av uvedkommende fra hele verden.



RETT PÅ NETT: Kameraet på utestedet Klubbteateret i Drammen sendte videostrømmen rett på nett. Video: Øistein Norum Monsen/Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til

Ett av kameraene Dagbladet har funnet uten noen form for passordbeskyttelse, zoomer inn på en gårdsplass og en platting med to solstoler. Via et styringspanel som kommer opp i nettleseren, kan alle besøkende ta styringen over kameraet.

Besøkende kan da snu overvåkningskameraet 360 grader. På denne rundturen er det innom et soverom.

Dette kan synes populært blant kikkerne på nettet.

Tolv land på besøk

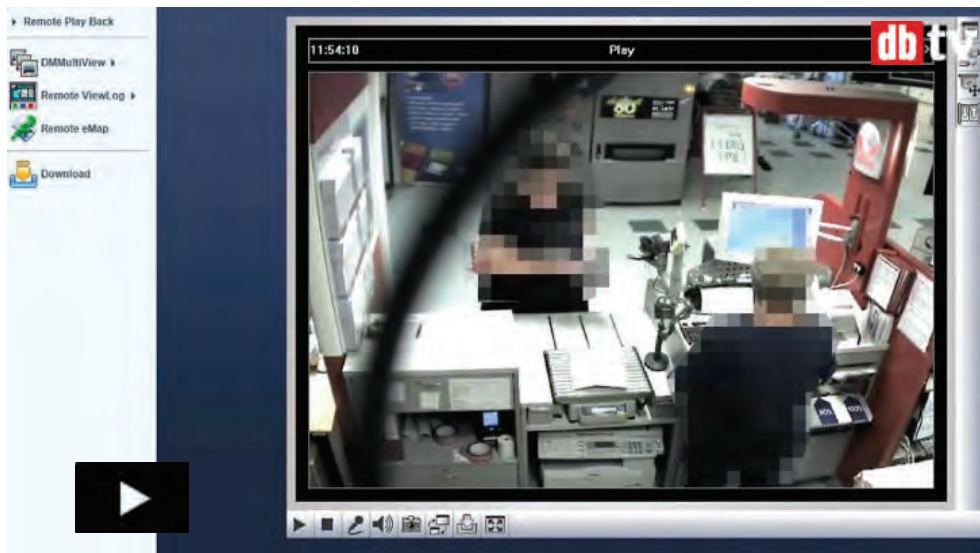
Bare i løpet av ei uke i september var hele 47 ulike IP-adresser innom kameraet, viser kameraloggen. Disse IP-adressene er registrert i 38 forskjellige byer i tolv ulike land.

Hvis IP-adressene stemmer, betyr dette at personer som befant seg i alt fra Russland, Japan og Polen til en rekke stater i USA var inne og tittet på de levende bildene fra hytta på det lille stedet i Nærøy kommune i Nord-Trøndelag.

- Det visste jeg virkelig ikke, sier eieren av kameraet til Dagbladet.

konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



SYNLIG FOR ALLE: Et kamera står plassert bak skranken i Post i butikk på Frostad senter nord for Trondheim. Totalt lå 16 av senterets overvåkingskameraer tilgjengelig på nett. Video: Øistein Norum Monsen / Dagbladet

98 i uka

Kameraloggen viser også hvor hyppig de ulike IP-adressene er innom kameraet. Totalt er det registrert trafikk fra eksterne IP-adresser 98 ganger i løpet av den ene septemberuka.

Dette tyder på at mange av de samme personene har vært inne og sett på kamerabildene flere ganger bare i løpet av disse sju dagene.

Dette er på ingen måte ei unik uke i dette kameraets liv, bare et eksempel.

Gresk interesse

Særlig er det en IP-adresse registrert i Hellas som peker seg ut.

I løpet av den ene uka var denne IP-adressen innom kameraet i Nord-Trøndelag 33 ganger totalt, opptil 14 ganger om dagen.

- Jeg trodde man måtte ha et passord for å komme inn, men når du sier det. Man må kanskje ikke det, sier den svært overraskede kameraeieren.

- Understreker alvoret

Han ønsker ikke at det opplyses hvor kameraet er plassert eller hvem det er som eier det.

- Men det skal umiddelbart stenges. Takk for at dere ga meg beskjed, sier han.

Mannens kamera er på ingen måte enestående. Dagbladet har sett flere eksempler på tilsvarende overvåkingskameraer som får hyppig besøk fra ulike land verden over.

- Dette understreker hvor alvorlig denne saken er, sier direktør Bjørn Erik



HEFTIG TRAFIKK: Et utsnitt i kartet viser hvor voldsom denne trafikken faktisk er. Grafikk: Kjell Erik Berg / Dagbladet

Thon i Datatilsynet til Dagbladet.

- Kan ramme alle

Han tror mange som setter opp et kamera glemmer at andre kan finne det på nett:

- Noen sier nok til seg selv at et åpent kamera er noe bare de selv vet om. Det gjør at de fleste tenker at dette bare angår dem selv.

Thon mener imidlertid at dette eksempelet viser hvor enkelt det er å bli snust opp av personer som leter etter sikkerhetshull på Internett.

- Dette er et problem som kan treffe hver enkelt av oss hvis vi ikke sikrer kameraene våre godt nok, sier han.

Kameraet nevnt i denne artikkelen ble stengt samme dag som Dagbladet varslet eieren om at det var åpent for alle.



HELE VERDEN SPIONERTE PÅ SOVEROM I NORSK HYTTE

Et overvåkingskamera i Nord-Trøndelag ble besøkt 98 ganger på ei uke – av personer fra 12 ulike land. Kameraeieren ante ikke at det var mulig.

Tekst: **Linn Kongsli Hillestad**

lkh@dagbladet.no

Espen Sandli

esan@dagbladet.no

Levende bilder av festende norsk ungdom på nattklubb, restaurantgjester i intime samtaler og eldre damer som taster inn pin-koden til kredittkortet sitt kringkastes rett ut på nettet.

Totalt ligger over 2000 norske overvåkingskameraer ute på Internett med liten eller ingen beskyttelse, har Dagbladet avslørt den siste uka.

Flere av disse kameraene er montert opp i eller utenfor private hjem, hvor alt fra sovende babyer til badeamper og persiske tepper overvåkes.

Omvisning ute og inne

Mange av disse overvåkingskameraene blir også hyppig besøkt av uvedkommende fra hele verden.

Ett av kameraene Dagbladet har funnet uten noen form for passordbeskyttelse, zoomer inn på en gårdsplass og en platting med to solstoler. Via et styringspanel som kommer opp i nettleseren, kan alle besøkende ta styringen over kameraet.

Besøkende kan da snu overvåkingskameraet 360 grader. På denne rundturen er det innom et soverom.

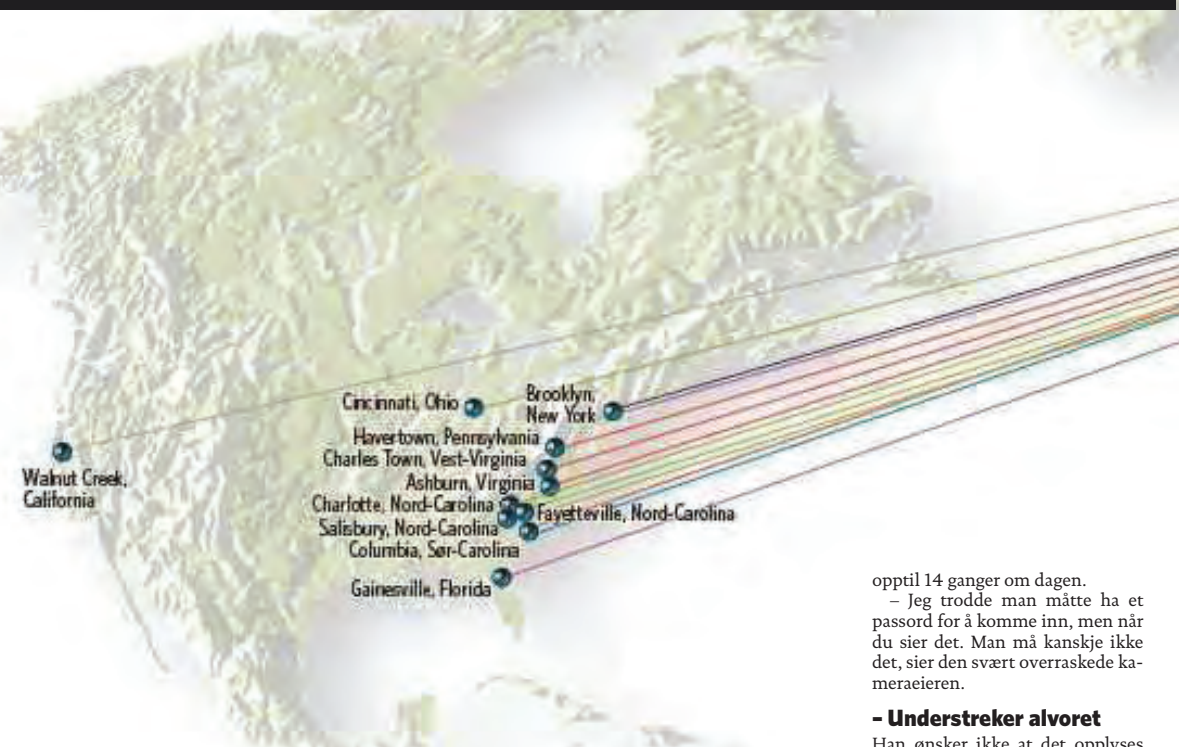
Dette kan synes populært blant kikkerne på nettet.

12 land på besøk

Bare i løpet av ei uke i september var hele 47 ulike IP-adresser innom kameraet, viser kameraloggen. Disse IP-adressene er registrert i 38 forskjellige byer i tolv ulike land.

Hvis IP-adressene stemmer, betyr dette at personer som befant seg i alt fra Russland, Japan og Polen til en rekke stater i USA var inne og tittet på de levende bildene fra hytta på det lille stedet i Nærøy kommune i Nord-Trøndelag.

– Det visste jeg virkelig ikke, sier eieren av kameraet til Dagbladet.



FAKTA

Slik sikrer du kameraet ditt

- Selv om overvåkingskameraet er koblet til ditt interne nettverk, beskyttet bak en brannmur, kan kameraet fortsatt være tilgjengelig for andre via din offentlige IP-adresse.
- Derfor er det viktig å beskytte kamerapanelet med brukernavn og et solid passord.
- I noen tilfeller kommer kameraer med et standardpas-

sord fra leverandøren, som for eksempel admin./admin. Disse er ofte allment kjent, og må derfor byttes med en gang du installerer kameraet.

● Generelt må du alltid huske å sikkerhetsoppdatere de elektroniske produktene du har koblet til nettet. Hvis det finnes et sikkerhetshull, er det enkelt for en hacker å utnytte dette og få full tilgang. Derfor

må du huske å oppdatere til siste versjon eller det som er anbefalt.

● Særlig er det en IP-adresse registrert i Hellas som peker seg ut. I løpet av den ene uka var denne IP-adressen innom kameraet i Nord-Trøndelag 33 ganger totalt,

opptil 14 ganger om dagen.

– Jeg trodde man måtte ha et passord for å komme inn, men når du sier det. Man må kanskje ikke det, sier den svært overraskede kameraeieren.

– Understreker alvoret

Han ønsker ikke at det opplyses hvor kameraet er plassert eller hvem det er som eier det.

– Men det skal umiddelbart stenges. Takk for at dere ga meg beskjed, sier han.

Mannens kamera er på ingen måte enestående. Dagbladet har sett flere eksempler på tilsvarende overvåkingskameraer som får hyppig besøk fra ulike land verden over.

– Dette understreker hvor alvorlig denne saken er, sier direktør Bjørn Erik Thon i Datatilsynet til Dagbladet.

– Kan ramme alle

Han tror mange som setter opp et kamera glemmer at andre kan finne det på nett:

– Noen sier nok til seg selv at et åpent kamera er noe bare de selv vet om. Det gjør at de fleste tenker at dette bare angår dem selv.

Thon mener imidlertid at dette

Kameraloggen viser også hvor hyppig de ulike IP-adressene er innom kameraet. Totalt er det registrert trafikk fra eksterne IP-adresser 98 ganger i løpet av den ene septemberuka.

Dette tyder på at mange av

de samme personene har vært inne og sett på kamerabildene flere ganger bare i løpet av disse sju dagene.

Gresk interesse

Dette er på ingen måte ei unik uke

i dette kameraets liv, bare et eksempel.

Særlig er det en IP-adresse registrert i Hellas som peker seg ut.

I løpet av den ene uka var denne IP-adressen innom kameraet i Nord-Trøndelag 33 ganger totalt,

Kilder: Norsk Senter for Informasjonssikring / Datatilsynet



Dagbladet Torsdag 3. oktober.



Dagbladet Lørdag 5. oktober



FAKTA

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av nabosens webkamera, åpne databasen til konkurrerende bedrifter eller overstyrte vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende data-sikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: dagbladet.no/nullctrl/
- Tips oss på nullctrl@dagbladet.no

eksempelet viser hvor enkelt det er å bli snust opp av personer som leter etter sikkerhetshull på Internett.

– Dette er et problem som kan treffe hver enkelt av oss hvis vi ikke sikrer kameraene våre godt nok, sier han.

Kameraet nevnt i denne artikkelen ble stengt samme dag som Dagbladet varslet eieren om at det var åpent for alle.



2013 Dagbladet GRAFIKK

PROSJEKTER PÅ GANG?

Lån opptil kr 300.000 uten sikkerhet

Søk på www.balanselånet.no

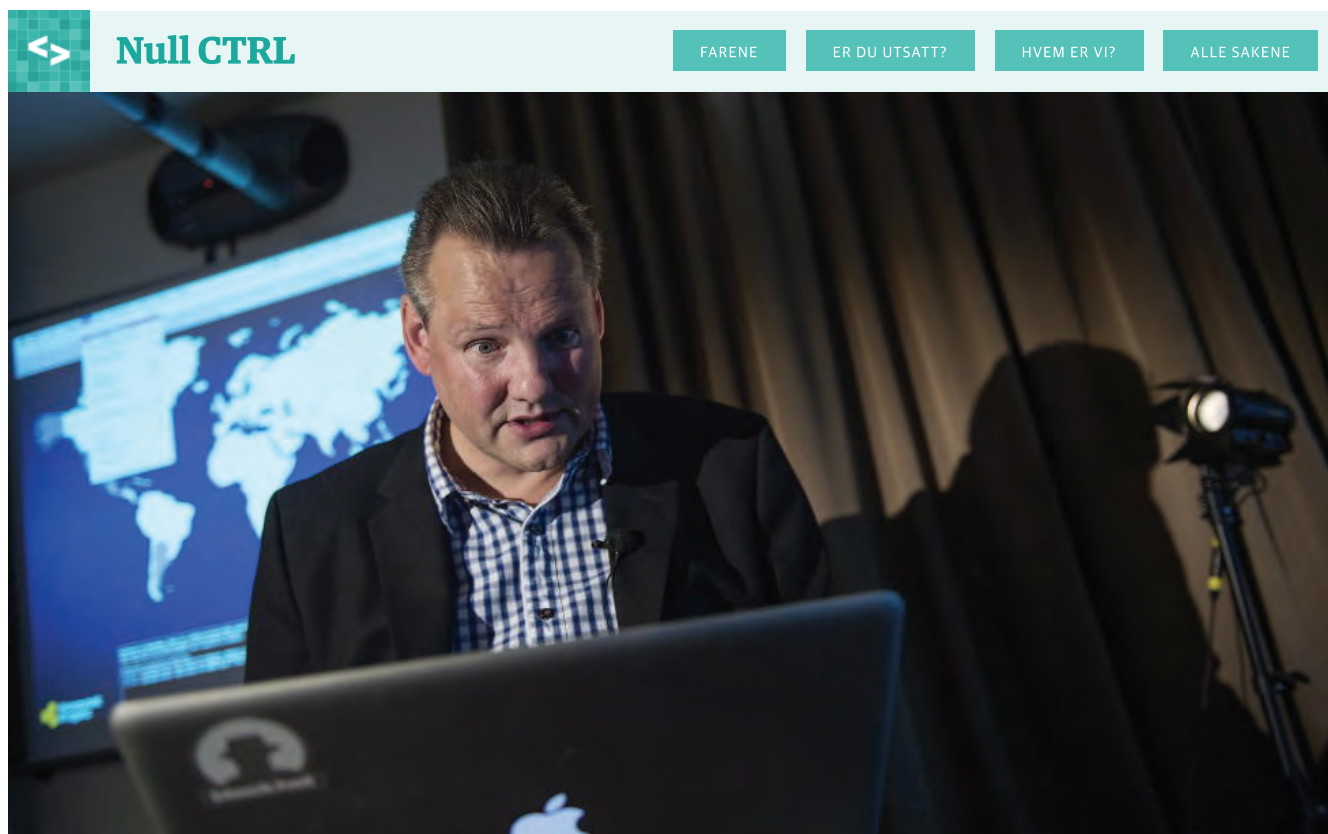
Eller ring oss på telefon 63 00 18 06

kode: DAG

Kostnadseksempel: Et lån på kr 65 000 over 5 år koster kr 1 540 i mnd (basert på en nominell gjennomsnittsrente på 12,98%, eff. 15,84%) og total tilbakebetalingsbeløp blir kr 92 334. Etableringsgebyr kr 950 og termingebyr kr 40 inngår i beregningen. Lånet er et annuitetslån.

Balanselånet

- Den nye trenden er å hacke forbrukerelektronikk, publisert mandag 7. oktober 2013 kl. 12:52



SIKKERHETSEKSPERT: Ifølge Vidar Sandland i Norsk Senter for Informasjonssikring (Norsis) blir det stadig mer populært blant hackere å angripe forbrukerelektronikk. Foto: Øistein Norum Monsen / DAGBLADET

- Den nye trenden er å hacke forbrukerelektronikk

Overvåkingskameraer, babycaller og tv-er blir stadig mer populære mål for hackere. Til og med vaskemaskiner er utsatt.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): Trodde du det er ufarlig at det private overvåkingskameraet ditt ligger ubeskyttet ute på nettet? At uvedkommende uansett aldri vil benytte seg av muligheten?

Da tar du feil, mener seniorrådgiver Vidar Sandland i [Norsk senter for informasjonssikring \(Norsis\)](#).

Private elektroniske apparater er nemlig mer utsatt for hackere enn noen gang tidligere.

- Vi ser at trendene nå går litt bort ifra å hacke datamaskiner og mobiltelefoner og går mer over til å hacke forbrukerelektronikk, sier Sandland til Dagbladet.



KRINGKASTET PÅ NETTET: Asbjørn Korsfjord fra Moss var ikke klar over at overvåkingskameraet hans lå åpent på internett. Video: Øistein Norum Monsen/Dagbladet.

Rett på nett

De siste dagene har Dagbladet

avslørt at bilder fra overvåkingskameraer over hele landet [kringkastes rett ut på nettet](#), uten passordbeskyttelse.

Totalt har vi funnet over 2000 norske overvåkingskameraer ute på Internett.

Dette betyr at fremmede kan få tilgang til levende bilder fra [nattklubber](#), [restauranter](#), [butikker](#) og [private hjem](#) - uten at kameraeierne vet om det. Alt fra sovende babyer til betalingsterminaler og safer ligger ute på nettet.

Mange av kameraene kan styres via panelene som kommer opp i nettleseren, og noen har også lydoverføring så uvedkommende kan lytte til private samtaler via internett - og i noen tilfeller også snakke via kameraene.

Som Dagbladet skrev i går, [utnyttes også disse mulighetene av uvedkommende fra hele verden](#).

Lite sikkerhet

Sandland trekker fram private overvåkingskameraer som et godt eksempel på den type forbrukerelektronikk som stiger i popularitet blant hackerne.

- Babycaller og babykameraer for å overvåke ungene dine er også veldig aktuelt, mens smart-tv-er også kan hackes og gjøres om til overvåkingssystemer for å se og høre hva du gjør i stua. I tillegg ser vi at flere og flere prøver å hacke kjøretøy, sier han.

- Hvorfor tror du dette er blitt så populært?

- Jeg tror det er fordi sikkerheten i veldig mange av disse systemene er fraværende. Det er fokus på funksjonalitet og det gir en hacker større mulighet til å ta kontroll. De fleste gjør nok dette for moro skyld.

«Ludder» og «idiot»

I USA har det vært flere eksempler på denne type hacking. Dagbladet har tidligere skrevet om amerikanske Marc Gilbert, som opplevde at noen [hacket seg inn på babycallen](#) deres og web-kameraet på datterens rom.

En dag hørte Gilbert en fremmed stemme rope «våkne opp, Allyson», «jævla idiot» og «ditt lille ludder» til



RETT PÅ NETT: Nattklubben Klubbteateret i Drammen [viste festglad og klinende ungdom](#) Video: Øistein Norum Monsen/Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



- **SOM Å HA INNBRUDD:** Marc Gilbert opplevde et mareritt da han plutselig hørte en stemme inne på sin to år gamle datters soverom. Det viste seg at webkameraene og babycallen var hacket. Video: KameraOne

den sovende to-åringen.

Lyden kom fra babycallen, og da han gikk inn på rommet, snudde plutselig overvåkingskameraet seg mot ham.

«Miss Teen USA» Cassidy Wolf (19) hadde en annen opplevelse. Noen [hacket angivelig web-kameraet på soverommet hennes](#) og sikret seg bilder. Deretter truet de med å utgi bildene for å presse henne for penger.

I fokus

På de anerkjente datakonferansene BlackHat og Defcon i USA i sommer var hacking av forbrukerelektronikk også ett av de store temaene. Blant fokusområdene var hacking av private overvåkingskameraer.

- Når hjemmeelektronikken blir koblet til nettet, skaper det også muligheter for de som har lyst til å misbruke denne teknologien, til å for eksempel søke opp den nett-tilkoblede vaskemaskinen din, sier redaktør for IT-nettavisen [Digi.no](#), Sigvald Sveinbjørnsson, til Dagbladet.

Han er godt kjent med problematikken, og tror at vi kommer til å se en del tilfeller av forbrukerhacking framover, særlig på grunn av manglende sikkerhet rundt disse systemene.

- Hackere trenger seg enten inn for å vise at de kan, eller for å tjene penger. Jeg kan ikke se at risikoen for hvermannen er voldsomt høy, men dette understreker at det er en helt annen risiko når du kobler ting til nettet, sier Sveinbjørnsson.

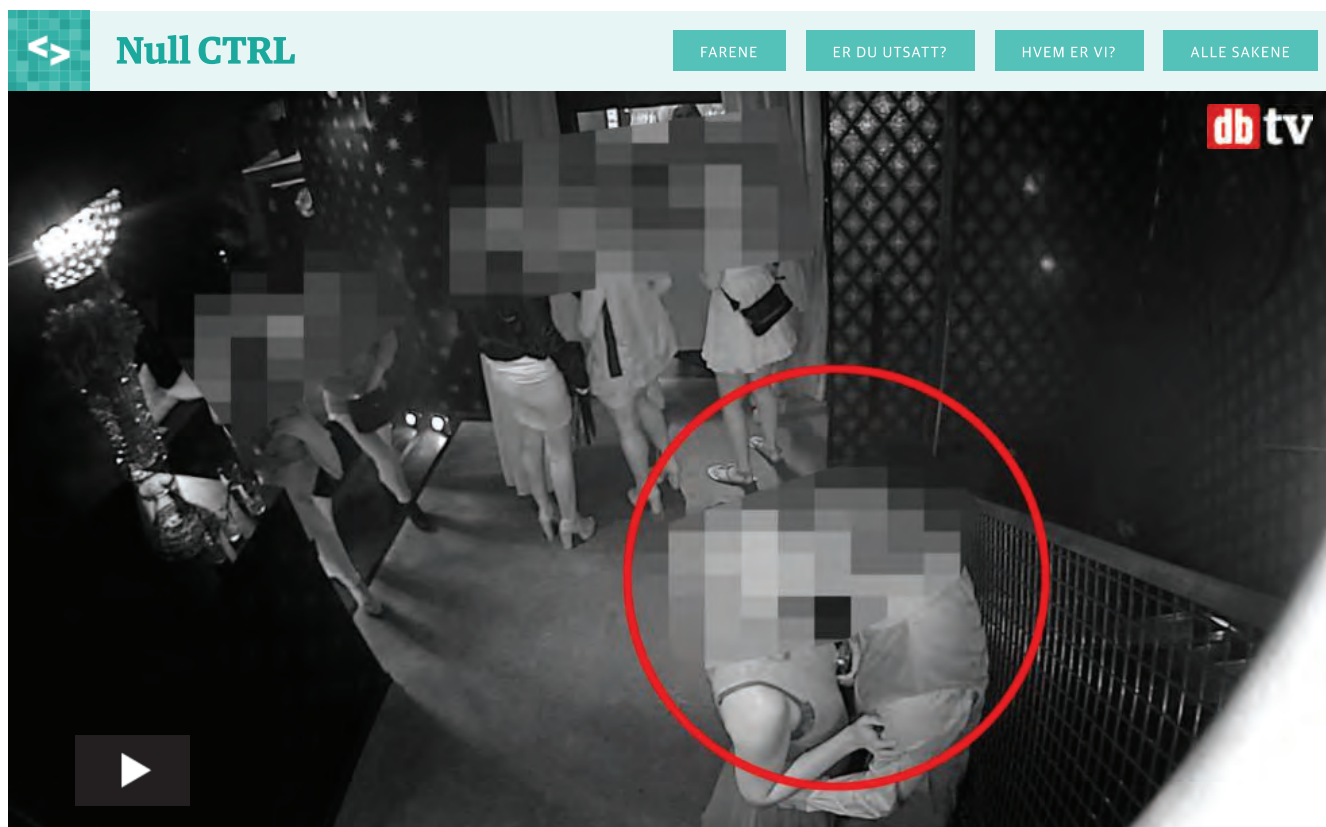


UTSATT FOR HACKERE: «Miss Teen USA», Cassidy Wolf, ble forsøkt presset for penger etter at hackere hadde tatt kontroll over webkameraet på soverommet hennes. Foto: Darren Decker / EPA / NTB scanpix



Tips oss på nullctrl@dagbladet.no

- Slike opptak kan enkelt brukes til utpressing, publisert tirsdag 8. oktober 2013 kl. 00:13



RETT PÅ NETT: Her fester og klinder de for åpent kamera på Klubbteateret i Drammen. Jussekspert Jon Wessel-Aas mener klipp som dette kan brukes til utpressing. Video: Øistein Norum Monsen / Dagbladet

- Slike opptak kan enkelt brukes til utpressing

Jussekspert Jon Wessel-Aas etterlyser lovendring etter overvåkingsskandalene.



THERESE DOKSHEIM
tdo@dagbladet.no

(Dagbladet) - De fleste av oss har ting vi ikke ønsker å dele med hvem som helst. Hvis folk ikke føler de kan bevege seg utenfor sitt eget hjem uten å bli overvåket, er det klart at det gjør noe med trygghetsfølelsen deres. Det hemmer folk. I verste fall kan slike bilder brukes som utpressing, sier Jon Wessel-Aas.

Jusseksperter har nettopp blitt vist [en av videoene](#) Dagbladet har laget i forbindelse med serien om datasikkerhet og overvåking. Der kommer det blant annet fram at hvem som helst har [kunne følge med på nattklubbgjester](#) på et utested i Drammen. Samtidig kan hvem som helst følge med på [dine og mine kafébesøk](#) og [hjemme på soverommet](#).

” Det er ikke nødvendigvis det at det er ulovlige ting som er skjedd, men slike opptak kan enkelt brukes til å knytte en person til et bestemt sted eller en bestemt person.

Jon Wessel-Aas, advokat og forfatter.



- Bryr seg ikke

KRIMINELLE BRYR SEG IKKE: Jussekspert Jon Wessel-Aas sier at kriminelle ikke bryr seg om

Wessel-Aas mener overvåkingen, som gjerne er utført i håp om å få bukt med kriminalitet, gjør det motsatte:

- Kriminelle bryr seg ikke likevel, de bryter loven selv om de vet at det finnes overvåkingskameraer over alt. Det sier litt at landets mest overvåkede plasser er nederst på Karl Johan: Jeg tror ikke det er der folk føler seg tryggest, selv om det er aldri så godt overvåket, sier han.

- At det som skal være med på å skape trygghet heller skaper usikkerhet og uoversiktighet er et av dilemmaene i denne saken. All elektronisk behandling av personopplysninger og andre registreringer hvor man lagrer det elektronisk, skaper dilemmaer. Baksiden er at informasjonen kan misbrukes hvis det ikke sikres godt nok, sier han.

- Brukes til utpressing

Han har blitt vist videoen der ungdom [fester og kliner foran et kamera som lå åpent](#) for hvermannen på nettet.

- Det er ikke nødvendigvis det at det er ulovlige ting som er skjedd, men slike opptak kan enkelt brukes til å knytte en person til et bestemt sted eller en bestemt person. Kanskje man var med en annen enn sin ektemann eller kone den kvelden, og da kan slike opptak enkelt brukes til utpressing.

Han mener omfanget øker i tråd med at «alle» i prinsippet nå kan kjøpe seg et overvåkingskamera, uten at man nødvendigvis vet hvordan man håndterer det.

- Enhver amatør kan kjøpe ganske rimelige overvåkingskameraer, og de blir mindre og mindre synlige, og er vanskelige å håndtere for amatører. En ting er når seriøse aktører bruker disse, men den glade amatør som går på Elkjøp eller kanskje kjøper seg et kamera på nett, tenker kanskje ikke over konsekvensene. De skjønner ikke at de er tilgjengelige på nett bare folk vet IP-adressen.

- Datatilsynet dårlig rustet

Han etterlyser ordentlige bøter for de som bryter loven.

- Etter min mening er organisasjoner som Datatilsynet for dårlig rustet både med tanke på

overvåkingskameraer. Foto: Torbjørn Berg / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyrte vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



FILMET FOR ALLE: Asbjørn Korsfjord fra Moss var ikke klar over at overvåkingskameraet hans lå åpent på internett. Video: Øistein Norum Monsen/Dagbladet.



SKUMMELT: Trond Kristiansen ante ikke at fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet



Så langt er reglene slik at man trygt kan bryte loven.

Jon Wessel-Aas, advokat og forfatter.

antall hoder som skal utføre tilsyn, og med tanke på sanksjonsmulighetene. I Norge, som i andre land, belager man seg på informasjon som forebyggingskanal. Det er ikke nok. Det man skulle ønske seg, var muligheten til å gi bøter til de som tåler det mest. Bøter som svir, slik at andre i samfunnet skjønner at det ikke er OK.

Han mener også at det gjøres lite for å slå ned på slik atferd hos de ulike aktørene.

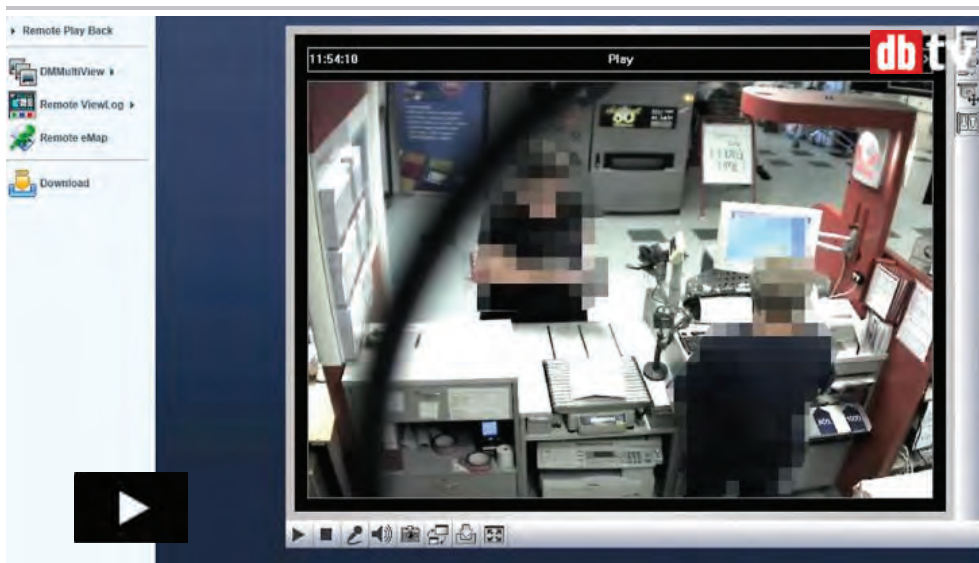
«Lønner seg» å bryte loven

- Man har sett i tidligere saker at det er lite for eksempel Datatilsynet har kunne gjøre i ulike sammenhenger. Heller ikke domstolen slår hardt nok ned på slike saker. Ofte gjør det at man tjener mer på å bryte loven, og at det derfor lønner seg, til man blir fortalt at det ikke er greit. Det er ikke noe insentiv til å holde loven, når man tjener mer på lovbruddet. Bøtene er så lave at de nærmest blir symbolske.

- Hadde man fått avisoppslag om at en bedrift hadde fått 500 000 i bot, så hadde kanskje andre bedrifter også spurt seg selv to ganger om deres rutiner var gode nok. Da hadde det hatt en effekt. Så langt er reglene slik at man trygt kan bryte loven, sier han.



- BRYTER ALLE REGLER: Det mener Datatilsynet om Café Sør i Torggata i Oslo, som har satt opp tre overvåkingskameraer som vises som en direktesending på kafeens nettside. Daglig leder trodde det var lovlig. Video: Lise Rafaelsen / Dagbladet



SYNLIG FOR ALLE: Et kamera står plassert bak skranken i Post i butikk på Frostad senter nord for Trondheim. Totalt lå 16 av senterets overvåkingskameraer tilgjengelig på nett. Video: Øistein Norum Monsen / Dagbladet



SKREMT: Harry Stene likte ikke at 16 overvåkingskameraer på Frostad senter har ligget åpent på internett. Video: Ole Morten Melgård / Øistein Norum Monsen / Dagbladet.



SMIL, DU ER PÅ KAMERA: På nettet fant Dagbladet et avansert overvåkingskamera på Jakob Aal liggende åpent og ubeskyttet. Hvor lenge det har ligget slik, er ikke kjent. Video: Øistein Norum Monsen/Dagbladet.



PÅ JOBB I CIVIL: Overvåkingskameraet på utestedet Klubfteateret i Drammen sendte video av politiets innsatsleder Geir Oustorp rett på nett. Video: Øisten Monsen / Dagbladet



Beredskapsplaner for 23 kommuner i nord lå åpent og usikret på Internett.
Her fantes alt fra interne brukernavn og passord til detaljert informasjon
om flyplassikkerhet og brannvesenets ressurser.

ALARM!

Nødsentralen lå åpen på nett

BODØ (Dagbladet): Med et enkelt tastetrykk hadde hvem som helst fri tilgang til store deler av brannberedskapen i 23 nordlandskommuner.

– Slik skal det ikke være. Denne type informasjon skal på ingen måte være offentlig, sier brannsjef Rolf Sørtorp til Dagbladet.

Flyplassikkerhet, tunnelsikkerhet, rømningsplaner og andre sensitive data tilhørende Midtre Hålogaland 110-sentral har i lang tid ligget på nett uten noen form for passord-beskyttelse.

Militær flyplass

I den omfattende databasen Dagbladet fant i forbindelse med en serie om datasikkerhet, lå det blant annet detaljerte opplysninger om alle ressurser brannvesenet disponerer og interne brukernavn og passord på ulike systemer.

Ei av mappene er dedikert den sivile og militære flyplassen i brann-distriktet. Her finnes blant annet flyplassens kriseplan, som helt ned på detaljnivå viser hva redningsmannskapene vil foreta seg ved en nødsituasjon og hvilket utstyr som er tilgjengelig.

Det finnes også informasjon om hva slags livreddende beredskap som er tilgjengelig i hver kommune.

Fritt fram

Den åpne tilgangen til databasen gjør at hvem som helst har kunnet laste ned informasjonen. Det har også vært mulig å endre informasjon eller laste opp annen enn den originale.

I sommer overtok Salten Brann IKS driften av nødsentralen og Midtre Hålogaland ble lagt ned.

– Du får ikke aktivisert en utrykning, men du får vite hele grunnlaget for utrykningen. Her kunne man gå inn og endre informasjonen som

ble brukt av den aktuelle sentralen når de aktiviserte styrkene sine. Det er klart, det skal ikke være sånn, sier Rolf Sørtorp i Salten brann.

Han og kollegene har nå overtatt innholdet, men selve databasen har aldri vært i bruk av dem.

– Vi er nødt til å kvalitetssikre den informasjonen vi har overtatt fra Midtre Hålogaland. Vi må sikre fra vår leverandør at det ikke finnes en tilsvarende åpen bakdør i vårt system, sier Sørtorp.

Terrorfare

I den åpne basen lå det også detaljerte oversikter over bedrifter, institusjoner og offentlige bygg – hvor eksplosiver oppbevares og hvor nøkkel-safer finnes. I ytterste konsekvens informasjon som kunne blitt utnyttet i en terrorsammenheng.

– Når slik informasjon ligger ute, vil folk som ønsker å lage trøbbel for oss, kunne gjøre det, sier Sørtorp.

Han er opptatt av at sikkerheten nå bør sjekkes ved alle landets nødsentraler.

– Vi er veldig glade for å bli gjort oppmerksomme på dette. Det er ikke i tråd med vår forventning, for å si det mildt, sier brannsjefen.

– Samtidig tar vi kontakt med våre kolleger som sitter rundt om i landet i varslingssentralene og ber dem undersøke samme sak, legger han til.

Lukket ned

Dagbladet oppsøkte Salten brann-sentral i Bodø i august. De varslet Narvik kommune, som eier databasen. Kort tid etter ble den stengt.

– Vi ga den eksterne leverandøren Datamann host-tilgang til serveren, og de opprettet en tjeneste som ikke var beskyttet med brukernavn eller passord, sier IT-sjef Per Jakobsen i Narvik kommune til Dagbladet.

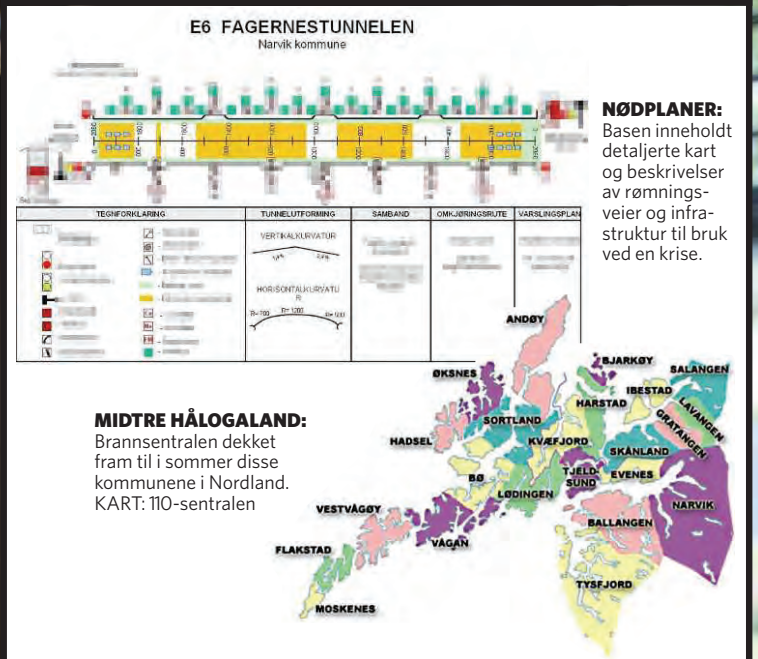
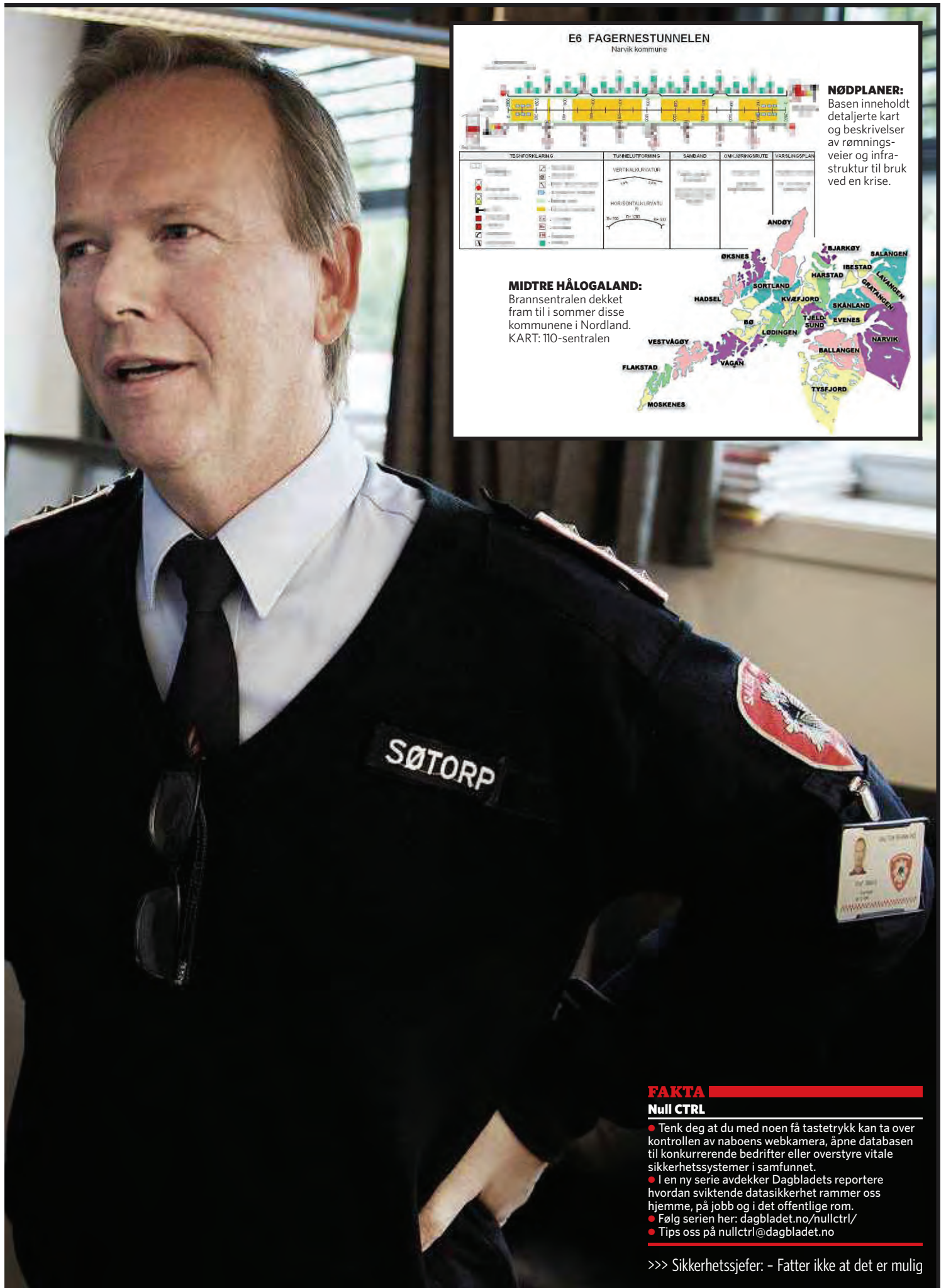
– Vi har nå tatt dette til etterretning og kvalitetssikrer nå eksterne leverandører så ikke dette skal skje igjen.

Datamann mener imidlertid det var kommunen som satte opp den eksterne tilgangen.

– Vår tilgang var en vanlig FTP-server, som Narvik kommune satte opp. Det var ikke vi som satte opp denne tilgangen, men det stemmer at det var vår løsning som gjorde at vi trengte en sånn forbindelse. Dette er en god del år siden, sier daglig leder Arve Berntzen.



Når slik informasjon ligger ute, vil folk som ønsker å lage trøbbel for oss, kunne gjøre det. Rolf Sørtorp, brannsjef



FAKTA

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens webkamera, åpne databasen til konkurrerende bedrifter eller overstyrte vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: dagbladet.no/nullctrl/
- Tips oss på nullctrl@dagbladet.no

>>> Sikkerhetssjefer: - Fatter ikke at det er mulig

Sikkerhetseksperter mener informasjon fra den åpne nødsentralen kunne blitt misbrukt både av terrorister og andre med onde hensikter.

- FATTER IKKE AT DET ER MULIG



MISBRUK: Åpne sikkerhetssystemer kan lett misbrukes av folk med onde hensikter. Foto: Torbjørn Berg

I hvilket land finner du broen Golden Gate?

Vinn inntil 1 million kroner
Send DB til 2265



Quizwin

Quizwin er et kunnskapsspill utviklet for smarttelefoner. Spillet har ulike premiebeløp hvor toppremien er på 1 million kroner. Du kan også spille gratis om du ønsker. Dette er ikke et abonnement, du får ingen uønskede SMS'er og overskuddet deles på 10 ideelle organisasjoner. For gratis link til spillet, send SMS med kodeord **DB til 2265**

Tekst: **Linn Kongsli Hillestad**
lkh@dagbladet.no
Espen Sandli
esan@dagbladet.no

– Hvis det er tilfelle at sikkerhetssystemene ligger åpne, med oversikt over ressurser og hvordan disse disponeres, vil du få veldig god informasjon hvis du skulle tenke deg å planlegge et terrorangrep eller rett og slett gjøre et innbrudd, sier Odd Einar Olsen til Dagbladet.

Han er professor i krisehåndtering og samfunnssikkerhet ved Universitetet i Stavanger, og blir rystet når Dagbladet beskriver hva slags informasjon som lå åpent til-



PROFESSOR: Odd Einar Olsen, professor i krisehåndtering og samfunnssikkerhet.

SIKKERHETS-FORSKER: Peter Burgess ved fredsforskningsinstituttet PRIO.

gjengelig i databasen tilhørende Midtre Hålogaland 110-sentral.

– Dette er egentlig å kle seg helt naken i forhold til folk som har onde hensikter. Jeg fatter ikke at det er mulig at dette har ligget helt åpent. Jeg liker ikke overdrevent hemmelighold i sikkerhetens navn, men et eller annet sted går grensen, sier Olsen.

– Beredskapsplaner, eller detaljerte oversikter over hvor man lagrer farlige kjemikalier, må selvsagt deles med etater og personer som skal håndtere en kritisk situasjon, men ikke med hele verden.

– Kunne blitt farlig

Han reagerer også på at det var mulig å manipulere informasjon i databasen.

– Dette kunne jo ha blitt gans-

ke farlig i en kritisk situasjon, sier han.

– I tillegg kan man se for seg at denne informasjonen kan gå ut over sikkerheten til enkeltpersoner.

Sikkerhetsforsker Peter Burgess ved fredsforskningsinstituttet PRIO mener tilgjengeligheten av personopplysningene som lå ute kan ha svekket personvernet.

– I tillegg er det åpenbart uheldig at beredskapsplaner, som blant annet er på plass for å forhindre terror, ligger åpent. Da kan ondsinnede komme disse planene i forkjøpet, og dette svekker beredskapen, sier han.

– Uheldig

Nasjonal Sikkerhetsmyndighet (NSM) reagerer også på Dagbladets opplysninger.

– Det er selvfølgelig uheldig dersom det ligger åpen tilgjengelig informasjon fra en nødetat på Internett, hvis ikke alle skal ha tilgang til dette, skriver informasjonssjef Kjetil Berg Veire i NSM i en e-post, etter at Dagbladet har fortalt ham om den åpne databasen.

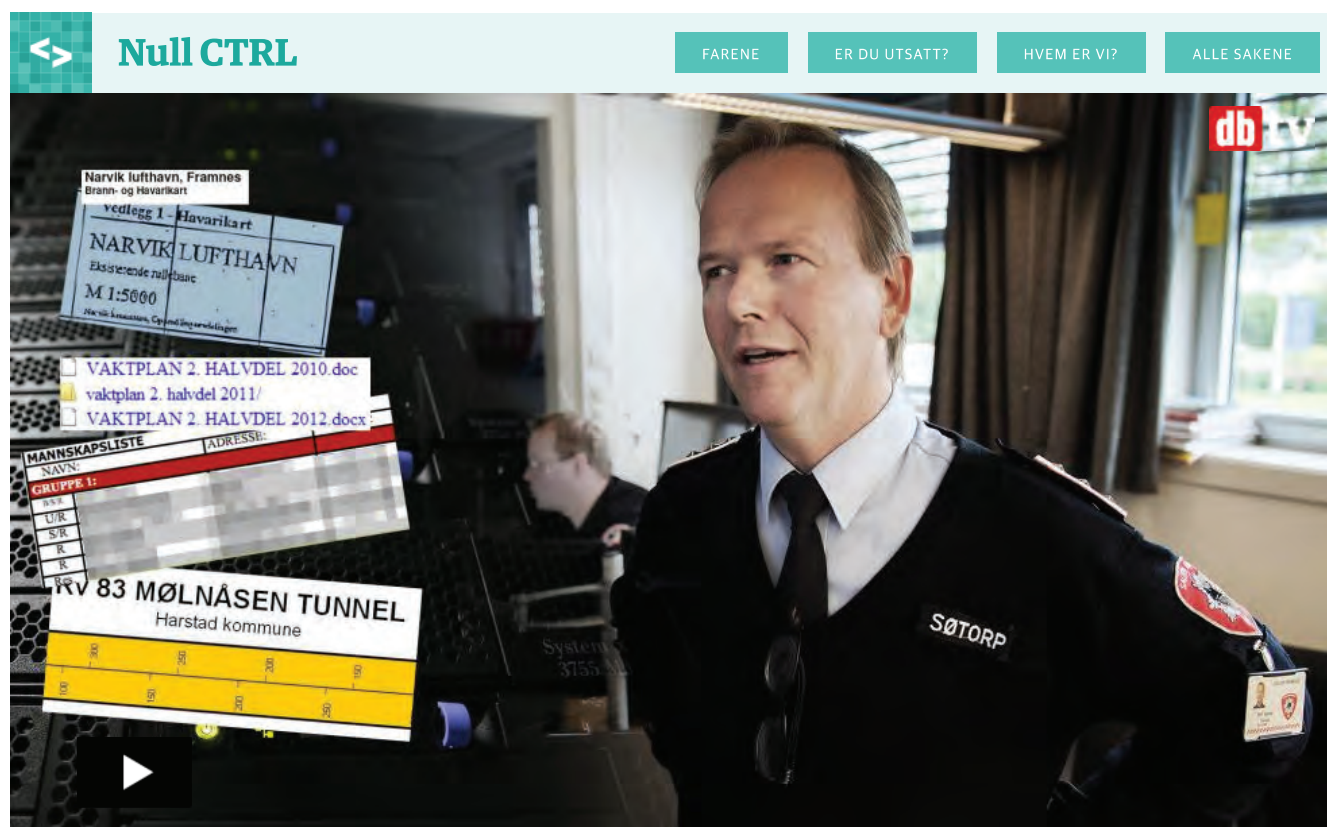
– Alt på nett ligger i utgangspunktet åpent med mindre man gjør mottiltak, tenker sikkerhet og verdi- og risikovurderer. Det er viktig at alle er klar over sårbarheter på nett og tetter sikkerhetshull, skriver han videre.

Mustoshop.no
20%

Kampanje på seilklær og fritidstøy fra **Musto** og **Sebago** hele oktober.

Besøk oss på facebook for å få **kodeordet** og kom innom nettbutikken for å handle!

MUSTO
PERFORMANCE



UAKSEPTABELT: - Denne type informasjon skal på ingen måte være offentlig, sier brannsjef Rolf Søtorp, etter at Dagbladet gjorde ham oppmerksom på at en database tilhørende Midtre Hålogaland 110-sentral lå usikret på nett. Video: Øistein Norum Monsen/Dagbladet.

ALARM! Nødsentralen lå åpen på nett

Dagbladet fant brann- og beredskapsplaner for 23 kommuner åpent og usikret på Internett.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLØ HILLESTAD
lkh@dagbladet.no



ØISTEIN NORUM MONSEN
onm@dagbladet.no

BODØ (Dagbladet): Med et enkelt tastetrykk hadde hvem som helst fri tilgang til store deler av brannberedskapen i 23 nordlandskommuner.

- Slik skal det ikke være. Denne type informasjon skal på ingen måte være offentlig, sier brannsjef Rolf Søtorp til Dagbladet.

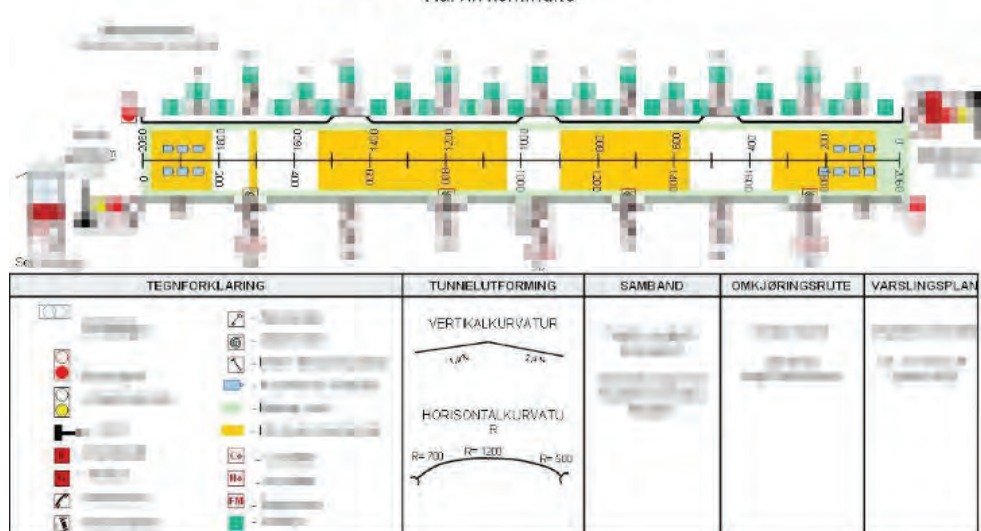
Flyplassikkerhet, tunnelsikkerhet, rømningsplaner og andre sensitive data tilhørende Midtre Hålogaland 110-sentral har i lang tid ligget på nett uten noen form for passordbeskyttelse.

Militær flyplass

I den omfattende databasen Dagbladet fant i forbindelse med en serie om datasikkerhet, lå det blant annet detaljerte opplysninger om

E6 FAGERNESTUNNELEN

Narvik kommune



Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til

alle ressurser brannvesenet disponerer og interne brukernavn og passord på ulike systemer.

Ei av mappene er dedikert den sivile og militære flyplassen i brann-distriktet. Her finnes blant annet flyplassens kriseplan, som helt ned på detaljnivå viser hva redningsmannskapene vil foreta seg ved en nødssituasjon og hvilket utstyr som er tilgjengelig.

Det finnes også informasjon om hva slags livreddende beredskap som er tilgjengelig i hver kommune.

Fritt fram

Den åpne tilgangen til databasen gjør at hvem som helst har kunnet laste ned informasjonen. Det har også vært mulig å endre informasjon eller laste opp annen enn den originale.

I sommer overtok Salten Brann IKS driften av nødsentralen og Midtre Hålogaland ble lagt ned.

- Du får ikke aktivisert en utrykning, men du får vite hele grunnlaget for utrykkinga. Her kunne man gå inn og endre informasjonen som ble brukt av den aktuelle sentralen når de aktiviserte styrkene sine. Det er klart, det skal ikke være sånn, sier Sørto i Salten brann.

Han og kollegene har nå overtatt innholdet i databasen, men selve databasen har aldri vært i bruk av dem.

- Vi er nødt til å kvalitetssikre den informasjonen vi har overtatt fra Midtre Hålogaland. Vi må sikre fra vår leverandør at det ikke finnes en tilsvarende åpen bakdør i vårt system, sier Sørto.

Terrorfare

I den åpne basen lå det også detaljerte oversikter over bedrifter, institusjoner og offentlige bygg - hvor eksplosiver oppbevares og hvor nøkkelsafer finnes. I ytterste konsekvens informasjon som kunne blitt utnyttet i en terrorsammenheng.

- Når slik informasjon ligger ute, vil folk som ønsker å lage trøbbel for oss, kunne gjøre det, sier Sørto.

Han er opptatt av at sikkerheten nå bør sjekkes ved alle landets nødsentraler.

- Vi er veldig glade for å bli gjort oppmerksomme på dette. Vi tar øyeblikkelig kontakt med vår leverandør, det er helt klart. Vi skal i helt klare ordelag formidle at det er uakseptabelt. Det er ikke i tråd med vår forventning, for å si det mildt, sier brannsjefen.

konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

• I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

• Følg serien her: <http://www.dagbladet.no/nullctrl/>

• Tips oss på nullctrl@dagbladet.no

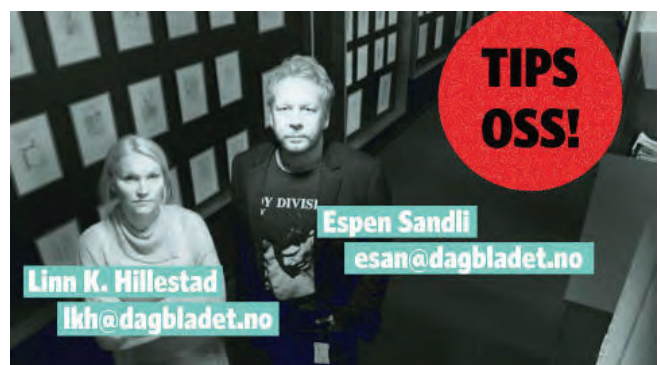
• Si din mening på Twitter: #null_CTRL



MIDTRE HÅLOGALAND: Brannsentralen dekket fram til i sommer disse kommunene i Nordland. KART: 110-sentralen



SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans kringkastet bilder og lyd rett ut på Internett. Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet



- Samtidig tar vi kontakt med våre kolleger som sitter rundt om i landet i varslingssentralene og ber dem undersøke samme sak, legger han til.

Lukket ned

Dagbladet oppsøkte Salten brannsentral i Bodø i august. De varslet videre Narvik kommune, som eier databasen. Kort tid etter ble den stengt.

- Vi ga den eksterne leverandøren Datamann host-tilgang til serveren, og de opprettet en tjeneste som ikke var beskyttet med brukernavn eller passord, sier IT-sjef Per Jakobsen i Narvik kommune til Dagbladet.

- Vi har nå tatt dette til etterretning og kvalitetssikrer nå eksterne leverandører så ikke dette skal skje igjen.

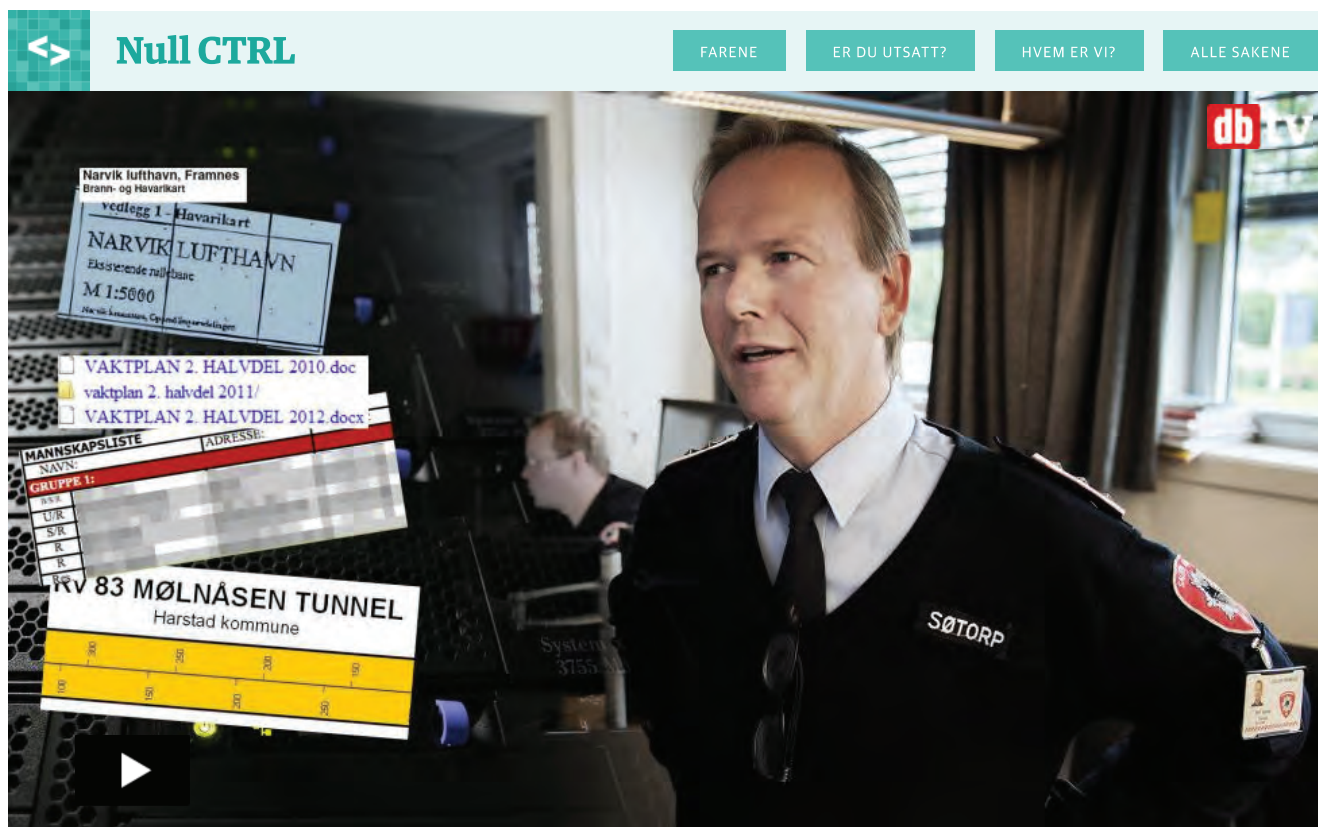
Datamann mener imidlertid det var kommunen som satte opp den eksterne tilgangen.

- Vår tilgang var en vanlig FTP-server, som Narvik kommune satt opp. Det var ikke vi som satte opp denne tilgangen, men det stemmer at det var vår løsning som gjorde at vi trengte en sånn forbindelse. Dette er en god del år siden, sier daglig leder Arve Berntzen i Datamann.



SKAL SJEKKE:: Brannsjef Rolf Sørtorp likte ikke at sensitiv informasjon lå åpent på nett og skulle kontakte leverandøren av 110-databasen for å finne feilen. Foto: Øistein Norum Monsen / Dagbladet.

- Fatter ikke at det er mulig, publisert tirsdag 8. oktober 2013 kl. 18:02



UAKSEPTABELT: - Denne type informasjon skal på ingen måte være offentlig, sier brannsjef Rolf Søtorp, etter at Dagbladet gjorde ham oppmerksom på at en database tilhørende Midtre Hålogaland 110-sentral lå usikret på nett. Video: Øistein Norum Monsen.

- Fatter ikke at det er mulig

Sikkerhetseksperter mener informasjon fra den åpne nødsentralen kunne blitt misbrukt av terrorister.



LINN KONGSLID HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): - Hvis det er tilfelle at sikkerhetssystemene ligger åpne, med oversikt over ressurser og hvordan disse disponeres, vil du få veldig god informasjon hvis du skulle tenke deg å planlegge et terrorangrep eller rett og slett gjøre et innbrudd, sier Odd Einar Olsen til Dagbladet.

Han er professor i krisehåndtering og samfunnssikkerhet ved Universitetet i Stavanger, og blir rystet når Dagbladet beskriver hva slags informasjon som lå [åpent tilgjengelig i databasen tilhørende Midtre Hålogaland 110-sentral](#).

Brukernavn og passord

Her fantes både beredskapsplaner og informasjon om flyplassikkerhet, brannberedskapen i 23 nordlandskommuner, detaljerte

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL

opplysninger om alle ressurser brannvesenet disponerer og interne brukernavn og passord på ulike systemer.

- Slik skal det ikke være. Denne type informasjon skal på ingen måte være offentlig, sier brannsjef Rolf Sørtorp ved Salten brann, som i sommer overtok driften av nødsentralen og innholdet i databasen.

- Dette er egentlig å kle seg helt naken i forhold til folk som har onde hensikter. Jeg fatter ikke at det er mulig at dette har ligget helt åpent. Jeg liker ikke overdrevent hemmelighold i sikkerhetens navn, men et eller annet sted går grensen, sier professor Odd Einar Olsen.

- Beredskapsplaner, eller detaljerte oversikter over hvor man for eksempel lagrer farlige kjemikalier må selvsagt deles med etater og personer som skal håndtere en kritisk situasjon, men ikke med hele verden, legger han til.

- Kunne blitt farlig

Olsen reagerer også på at det var mulig å manipulere informasjon i databasen.

- Dette kunne jo ha blitt ganske farlig i en kritisk situasjon, sier han.

- I tillegg kan man se for seg at denne informasjonen kan gå utover sikkerheten til enkeltpersoner.

Sikkerhetsforsker Peter Burgess ved fredsforskningsinstituttet PRIO mener også tilgjengeligheten av personopplysningene som lå ute kan ha svekket personvernet.

- I tillegg er det åpenbart uheldig at beredskapsplaner, som blant annet er på plass for å forhindre terror, ligger åpent. Da kan ondsinnede komme disse planene i forkjøpet, og dette svekker beredskapen, sier han.

- Uheldig

Nasjonal Sikkerhetsmyndighet (NSM) reagerer også på Dagbladets opplysninger.

- Det er selvfølgelig uheldig dersom det ligger åpen tilgjengelig informasjon fra en nødetat på Internett hvis ikke alle skal ha tilgang til dette, skriver informasjonssjef Kjetil Berg Veire i NSM i en epost etter at Dagbladet har fortalt ham om den åpne databasen.

- Alt på nett ligger i utgangspunktet åpent med mindre man gjør mottiltak, tenker sikkerhet og verdi- og risikovurderer. Det er viktig at alle er klar over sårbarheter på nett og tetter sikkerhetshull.



RETT PÅ NETT: Nattklubben Klubbteateret i Drammen [viste festglad og klinende ungdom](#). Video: Øistein Norum Monsen / Dagbladet



SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans [kringkastet bilder og lyd rett ut på Internett](#). Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet

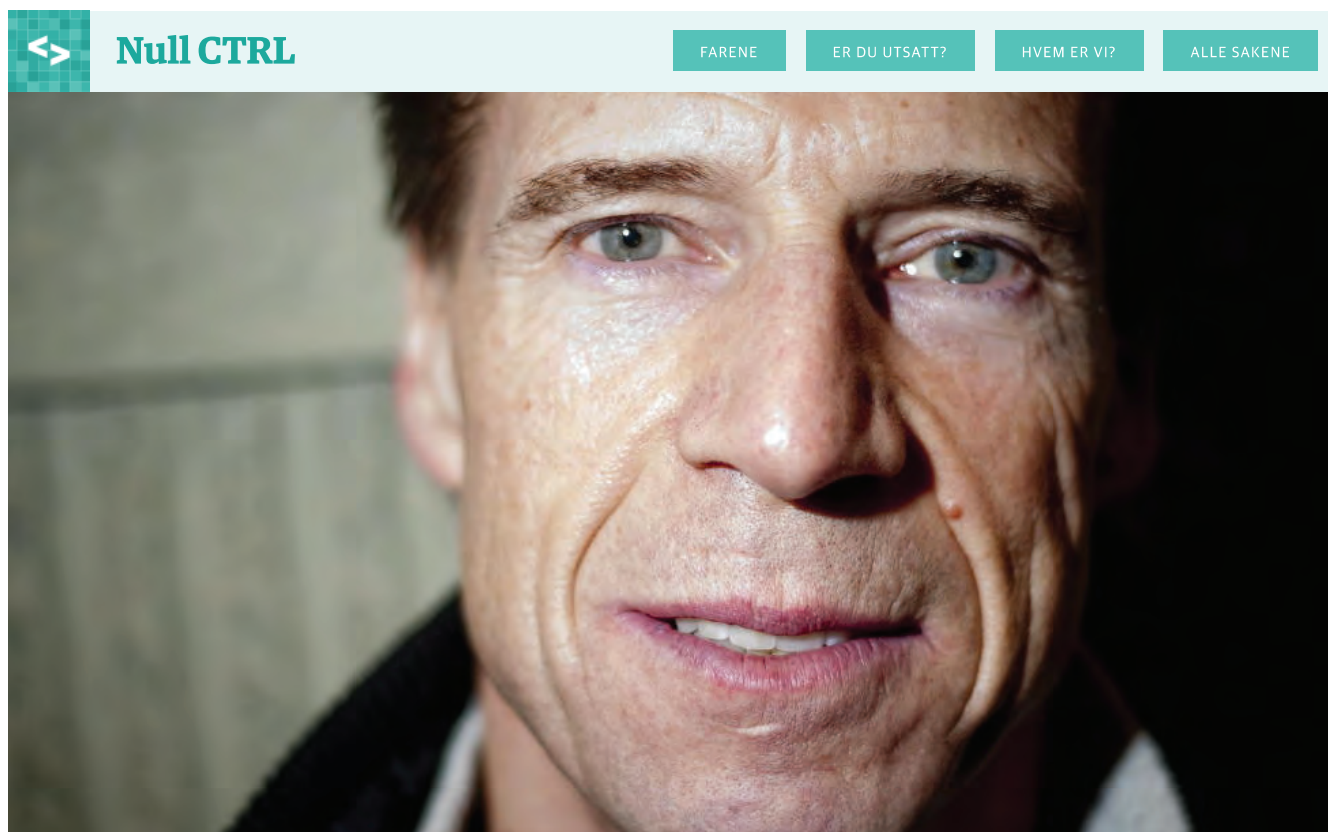


Tips oss på nullctrl@dagbladet.no



UHELDIG: Sikkerhetsforsker Peter Burgess ved fredsforskningsinstituttet PRIO mener den åpne databasen kan ha svekket beredskapen. Foto: Privat

- Dette er ufattelig sløvt. Særlig etter 22. juli og alt fokuset vi har hatt på beredskap og sikkerhet i samfunnet,



- **SLØVT:** Aps justispolitiske talsmann, Jan Bøhler, er opprørt over det han kaller sløvhets i sikringen av 110 beredskapssentralen. Her ved en annen anledning, i januar i fjor. Foto: Thomas Rasmus Skaug / Dagbladet

- Dette er ufattelig sløvt. Særlig etter 22. juli og alt fokuset vi har hatt på beredskap og sikkerhet i samfunnet

Jan Bøhler (Ap) er skuffet over at nødsentral lå åpen på nett.



THERESE DOKSHEIM
tdo@dagbladet.no

(Dagbladet): Flyplass- og tunnelsikkerhet, rømningsplaner og andre sensitive data tilhørende 110-sentralen i Midtre Hålogaland kan i lang tid [ha ligget åpent på nett](#) uten noen form for passordbeskyttelse.

Arbeiderpartiets justis- og beredskapstalsmann Jan Bøhler er opprørt over Dagbladets avsløring.

- Min første reaksjon er at dette er ufattelig sløvt. Særlig etter 22. juli og alt fokuset vi har hatt på beredskap og sikkerhet i samfunnet. Det er ikke mulig å forstå at de ikke har tenkt på dette, sier han.



Hvis noen planlegger terror vil slike beskrivelser og oversikter være gull verdt. Hele poenget med beredskap er at man skal sikre seg mot det utenkelige.

Jan Bøhler (Ap).

- Alvorlig advarsel

- Hvis noen planlegger terror vil slike beskrivelser og oversikter være gull verdt. Hele poenget med beredskap er at man skal sikre seg mot det utenkelige. Det handler om å sikre beredskapen i samfunnet, både stort og smått. Dette må tas på alvor, og må ses på som en alvorlig advarsel.

Bøhler har vært en sentral person i arbeidet med beredskap i tida etter 22. juli for to år siden. Han trodde ikke det var mulig med slike feil etter terrorangrepet.

- Jeg blir overrasket over at det finnes slike ting ennå. Man må aldri tror at det nå er en selvfølgelighet at alt er i orden. Vi må være mer oppmerksomme på at det kan finnes slike hull, sier han.

- Slå seg på brystet

Han fortsetter:

- Jeg tror ikke man skal slå seg på brystet og si at det ikke rammer en selv, heller. Norge har vært et «freda sted» i verden - det er mange som kan ha ting liggende ute som de ikke har tenkt på. Det gjelder nok ikke bare 110-sentralen. Det er en ny verden med alle slags muligheter til å finne ting på nettet, sier Bøhler.

Heller ikke Odd Einar Olsen, professor i krisehåndtering og samfunnssikkerhet ved Universitetet i Stavanger, [fatter at det er mulig at informasjonen lå åpent](#) på nett.

- Dette er egentlig å kle seg helt naken i forhold til folk som har onde hensikter. Jeg fatter ikke at det er mulig at dette har ligget helt åpent. Jeg liker ikke overdrevent hemmelighold i sikkerhetens navn, men et eller annet sted går grensen, sier han.

- Ikke noe vi etterforsker

Politiets sikkerhetstjeneste (PST) er kjent med Dagbladets artikkel om at beredskapsplanene for 23 kommuner [lå på nett uten noen form for passordbeskyttelse](#).

I ytterste konsekvens ville informasjonen ha kunne blitt brukt i en terrorsammenheng. Likevel ønsker ikke PST å kommentere det som blir sagt i artikkelen. De mener problematikken ikke inngår i PSTs arbeidsoppgaver:

- PST skal etterforske brudd på sikkerhetsloven, men dette er ikke gradert



UAKSEPTABELT: Brannsjef Rolf Sørtorp i Salten IKS reagerer på at informasjon fra den nå nedlagte 110-sentralen i Midtre Hålogaland på åpen og usikret på Internett. Video: Øistein Norum Monsen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL

PST skal etterforske brudd på sikkerhetsloven, men dette er ikke gradert informasjon og derfor ikke noe vi etterforsker.

Martin Berntsen, informasjonsdirektør i PST.



TIPS OSS: Har du tips til Dagbladets reportere? Skriv til dem på nullctrl@dagbladet.no.

I ytterste konsekvens ville

informasjonen ha kunne blitt brukt i en terrorsammenheng. Likevel ønsker ikke PST å kommentere det som blir sagt i artikkelen. De mener problematikken ikke inngår i PSTs arbeidsoppgaver:

- PST skal etterforske brudd på sikkerhetsloven, men dette er ikke gradert

Vi slutter oss til det NSM sier, og ønsker ikke å kommentere ytterligere.

Trond Øvstedal, informasjonsrådgiver Justis- og beredskapsdepartementet.

informasjon og derfor ikke noe vi etterforsker, sier informasjonsdirektøren, Martin Berntsen.

Betegnelsen gradert informasjon omfatter konfidensiell informasjon som bare skal være tilgjengelig for autoriserte personer, ifølge [Store Norske Leksikon](#).

- Det ligger potensiale der for at dette skal bli en trusselsak, men per nå er det en sårbarhet - ikke gradert informasjon. Hadde dette vært gradert informasjon, hadde vi satt i gang etterforskning.

Vil ikke kommentere

- Vi vurderer trusselbildet og er i stadig kontakt med Nasjonal Sikkerhetsmyndighet (NSM), så det er en glidende overgang - men jeg kjenner ikke til at vi har vært inne og sjekket slike saker. Det har vi ikke gjort, sier Berntsen.

Heller ikke Justis- og beredskapsdepartementet vil kommentere saken.

- Vi slutter oss til det NSM sier, og ønsker ikke å kommentere ytterligere. Deres kommentar er dekkende for hva vi mener, sier Trond Øvstedal, informasjonsrådgiveren for departementet, til Dagbladet.

- Ikke lett å si

- Hva tenker du om at verken PST eller Justis- og beredskapsdepartementet vil kommentere saken?

- Det er ikke så lett for meg å si. Men, jeg vil i alle fall si hva jeg mener om saken. Samfunnssikkerhet handler om mye mer enn bare det PST driver med - det finnes mange etater for samfunnssikkerhet som har noe å si. Jeg skal ikke si hva deres begrunnelse for å ikke kommentere saken er, men de er vel kanskje mer spissa på farlige krefter, systemer og terror, sier Bøhler til Dagbladet.

- Ikke akseptabelt

Brannsjef Rolf Sørtorp ved Salten IKT sier til Dagbladet at folk som ønsker å lage trøbbel for dem, [enkelt kunne gjort det](#) med informasjonen som lå tilgjengelig. Salten overtok i sommer 110-ansvaret fra Midtre Hålogaland.

Selv om den åpne serveren ikke var Saltens ansvar, har brannsjefen sagt klart og tydelig hva han mener om sikkerhetssvikten.

- Det er ikke akseptabelt, sier han.

Landets største fiskebollefabrikk frykter

OPPGITT: Produksjonssjef Viktor Johnsen (t.h.) og teknisk sjef Bjørn Alnes er oppgitt over at fabrikkens hemmeligheter har vært tilgjengelig for alle.

Alle foto: Øistein Norum Monsen



FØLG SAKEN

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: www.dagbladet.no/nullctrl/
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: [#null_CTRL](https://twitter.com/null_CTRL)

Om en faen er det bare å sl

Tekst: **Espen Sandli**
esan@dagbladet.no

Øistein Norum Monsen
onm@dagbladet.no

Linn Kongsli Hillestad
lkh@dagbladet.no

SORTLAND/BODØ (Dagbladet): Dagbladet har avdekket hvordan brannsentralen for 23 kommuner i Nordland i lang tid har ligget åpen og uten noen form for passordbeskyttelse på Internett.

Blant sensitive data, ligger all informasjon om adkomst, nøkler, dører og farlige stoffer ved fabrikkens Vesteraalens på Sortland.

Terrorfrykt

– Sveisegass, propan, etsende stoffer, maursyre, lut, syre, helium hydrogen, diesel... Det smeller bra det her, sier teknisk sjef Bjørn Alnes ved Vesteraalens og slår oppgitt ut med hendene over at fabrikkens hemmeligheter har ligget

åpent og ubeskyttet.

Sammen med produksjonssjef Viktor Johnsen viser han Dagbladet rundt blant produksjonsutstyr verdt nærmere 50 millioner kroner på fabrikkens. Begge er forbanna. Dagbladet har vist dem innsettplanen for fabrikkens, som har ligget åpen og tilgjengelig på nett.

– Her står jo alt. Og det ligger åpent på nettet. for Gud og hvermann? Det er jo skremmende. Da er vi i så fall et enkelt

terrormål, sier Johnsen.

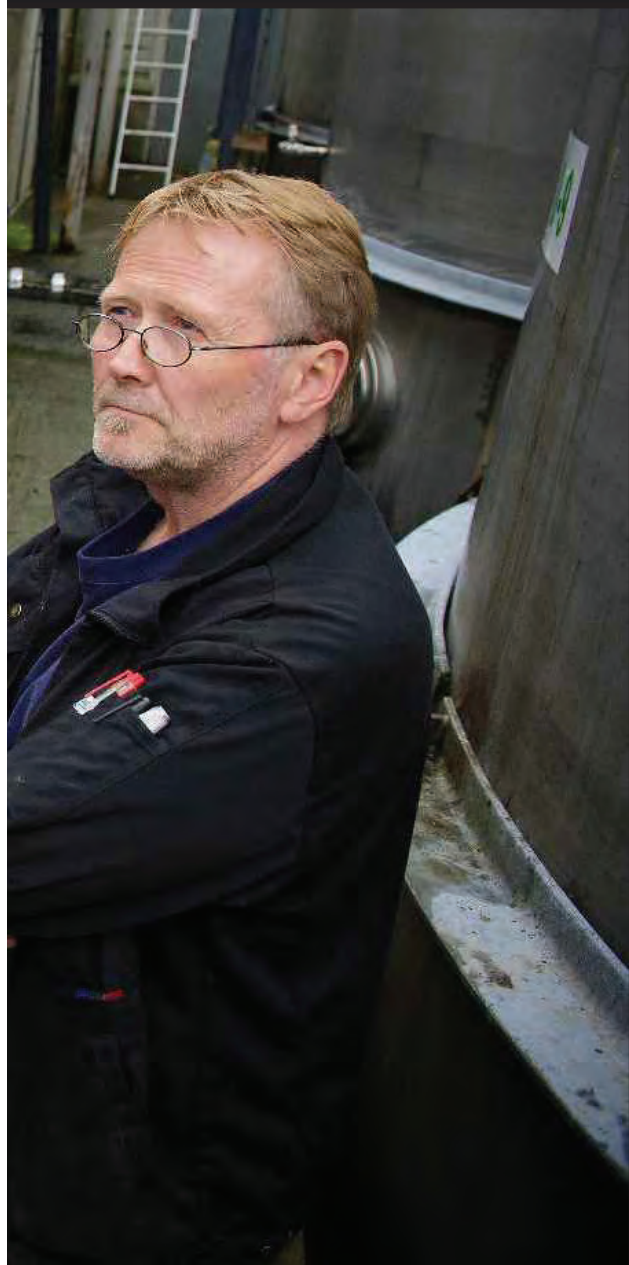
– Og informasjonen er fersk, helt oppdatert, sier Alnes.

Andre boller

Vesteraalens er landets største produsent av hermetiserte fiskeboller og blant verdens største produsenter av tran. I en slik foredling er det mange farlige stoffer i store volum på fabrikkområdet.

– Jeg tror ikke det er noen fare for menigmann, men om denne

r terror og sabotasje etter datalekkasje.



FRYKTER FOR OMGIVELSENE: Fabrikkleidelsen frykter for liv og helse for beboerne i Sortland om uvedkommende skulle ønske å misbruke informasjon vedrørende fabrikkens syrer og gasser.



Foto: NTB Scanpix



SÖRMLAND BRANDGÄLLNINGSTJENST		INNSATSPLAN			
OBJEKT NÄMN (Sei. Anmälan på bef. information)		MÄRKNÄM			
LÄRSTEN		Hörselväg 13			
GARBERGSMÄR		BIRKESMÄR			
BYGGNADSTYP (Ej. bef. information) Söb. (Inb.)		BIRKESMADE (Utskott)		Radhus, 1-2 våningar	
DEKLARATION OBJEKT		ANSTÄLLT		2 (2)	
T.F. (OG NÄM N. BRÄNNVERNEN LÖR)		TYP: 1000, 1000, 1000		1000, 1000, 1000	
T.F. OG NÄM NÄTTID		Söndag			
INNSÄTSPUNKTER		KOMMENTARER			
1. KÖRVEJ		Märket gator i området är avsevärt dåligt underhållet. Märket gator i området är avsevärt dåligt underhållet.			

- SMELLER BRA: - Sveise-
gass, propan, etsende stoffer,
maursyre, lut, syre, helium
hydrogen, diesel... Det smel-
ler bra det her, sier teknisk
sjef Bjørn Alnes (t.v.) ved
Vesteraalens og slår oppgitt
ut med hendene over at fab-
rikkens hemmeligheter har
ligget åpent og ubeskyttet.

**vil sprengte dette,
kru igjen her...**

informasjonen kommer i hendene på noen som ønsker at det skal skje noe, så er jo vi et mål som kan gjøre stor skade for n romr det, sier Johnsen.

– Om 10 000 liter med maursyre skulle havne i havet, vil det bli ballade i havna, sier Alnes.

– Vi har diesel og gasser, så det er jo et utfordring at det ligger åpent. En skummel sak, sier Johnsen.

Som ansvarlige for drift og sikkerhet av fabrikkene, er de sjokkerte

over at noen de stoler på har hatt så dårlig kontroll på sensitive data.

- Skremmende

– Jeg er overrasket over at så sensitiv informasjon ligger åpent på nettet, noe vi trodde var tett, lukket og beskyttet hos de instansene vi leverte informasjonen til. Det er skremmende, sier Johnsen.

Han frykter at så konkret informasjon kan ha enorme konsekvenser i feil hender.

– Konsekvensen ved sabotasje, terror. At folk får vite hvor de ulike tingene står. Blir det fyr i dette, ødelegges jo fabrikken. Da eksploderer den. For oss som matvareprodusent kan det ha alvorlige konsekvenser om noen vil skade oss i forhold til sabotasje av ingredienser i maten vi lager eller sette oss ut av produksjon, sier Johnsen.

Alnes er sjokkert over at fabrikkens hemmeligheter er angitt så detaljert som tilfellet er:

– Om en faen vil sprengje detta, er det bare å skru igjen her – så sier det puff. Et kjempesmell. Her har vi kjemikalier, granulat, ammoniumklorid, Det er jo sterkt etsende. Det står jo i planen hvor man finner det, sier han oppgitt.

- Høyst beklagelig

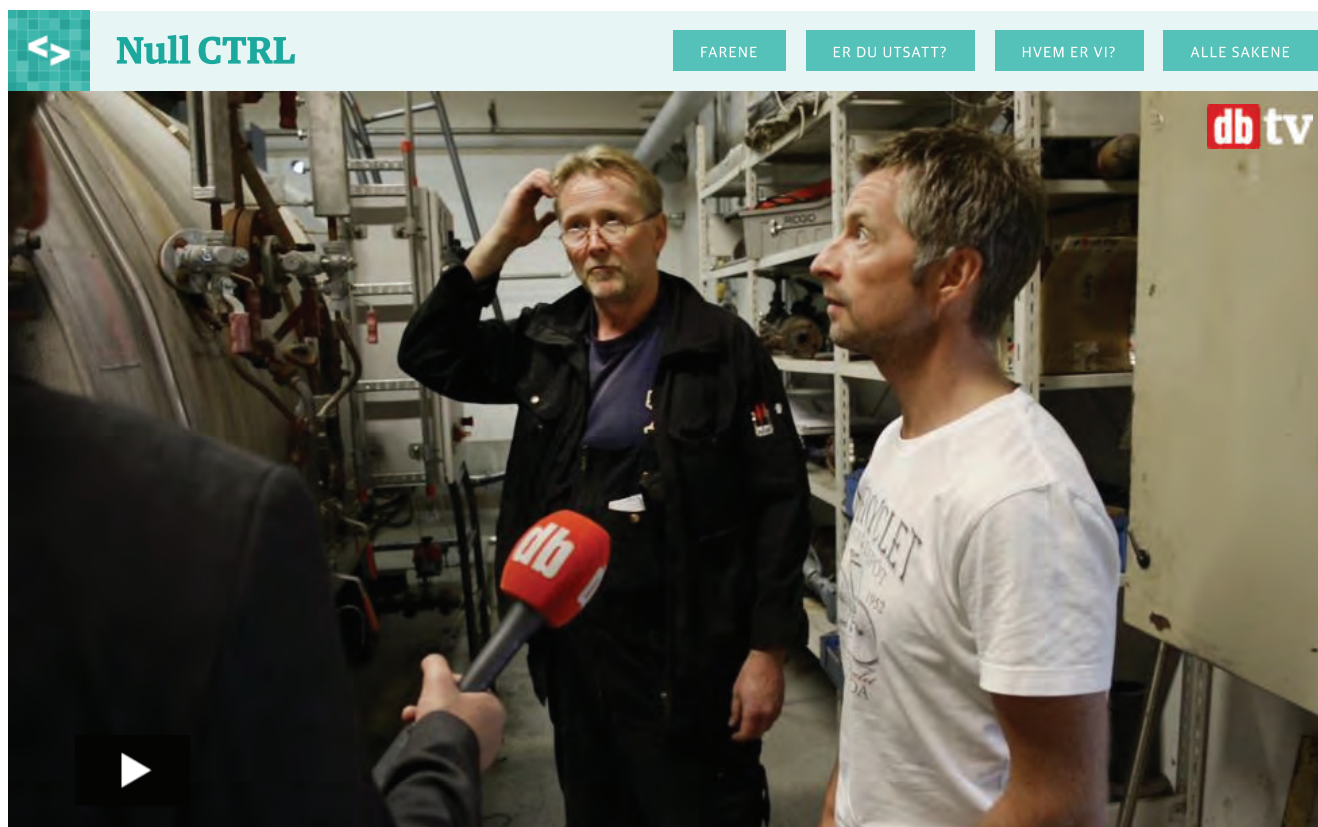
Brannsjef Rolf Sørtorp ved Salten Brann IKS overtok i sommer ansvaret for den nå nedlagte 110-

sentralen Midtre Hålogaland.

– Det er jo høyst beklagelig. De som gir oss denne type informasjon, må være trygge på at vi har gode systemer for å ta vare på den informasjonen. Hvorfor det ligger ute fra Midtre Hålogaland må vi stupe inn i og undersøke med en gang, sier han til Dagbladet.

Serveren eies av Narvik kommune, som stengte den kort tid etter Dagbladets besøk.

«Om en faen vil sprengre dette, er det bare å skru igjen her», publisert onsdag 9. oktober 2013 kl. 09:55



- **ENKELT TERRORMÅL:** Produksjonssjef Viktor Johnsen ved fiskebollefabrikken Vesteraalens på Sortland frykter alvorlige konsekvenser om detaljert informasjon fra beredskapsplanen skulle komme i feil hender. Video: Øistein Norum Monsen/Dagbladet

«Om en faen vil sprengre dette, er det bare å skru igjen her»

Landets største fiskebollefabrikk frykter terror og sabotasje etter datalekkasje.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLID HILLESTAD
lkh@dagbladet.no



ØISTEIN NORUM MONSEN
onm@dagbladet.no

SORTLAND/BODØ (Dagbladet):
Dagbladet har avdekket hvordan
brannsentralen for 23 kommuner i
Nordland i lang tid [har ligget åpen](#)
[og uten noen form for](#)
[passordbeskyttelse](#) på Internett.

Blant mange sensitive data, ligger
all informasjon om adkomst, nøkler,
dører og farlige stoffer ved
fabrikken Vesteraalens på Sortland
i Nordland.

- Sveisegass, propan, etsende
stoffer, maursyre, lut, syre, helium
hydrogen, diesel... Det smeller bra
det her, sier teknisk sjef Bjørn Alnes
ved Vesteraalens og slår oppgitt ut
med hendene over at fabrikkens
hemmeligheter har ligget åpent og
ubeskyttet.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

Terrorfrykt

Sammen med produksjonssjef Viktor Johnsen viser han Dagbladet rundt blant produksjonsutstyr verdt nærmere 50 millioner kroner på fabrikkens. Begge er forbanna. Dagbladet har vist dem innsatsplanen for fabrikkens, som har ligget åpen og tilgjengelig på nett.

- Her står jo alt. Og det ligger åpent på nettet..for Gud og hvermann? Det er jo skremmende. Da er vi i så fall et enkelt terrormål, sier Johnsen.

- Og informasjonen er fersk, helt oppdatert, sier Alnes.



Andre boller

Vesteraalens er landets største produsent av hermetiserte fiskeboller og blant verdens største produsenter av tran. I en slik foredling er det mange farlige stoffer som befinner seg i store volum på fabrikkområdet.

- Jeg tror ikke det er noen fare for menigmann, men om denne informasjonen kommer i hendene på noen som ønsker at det skal skje noe, så er jo vi et mål som kan gjøre stor skade for nærområdet, sier Johnsen.

- Om for eksempel 10 000 liter med maursyre skulle havne i havet, vil det bli ballade i havna, sier Alnes.

- Vi har diesel og gasser her, så det er jo ei utfordring at det ligger åpent. Det er en skummel sak, sier Johnsen.

- Vi stolte på dem

Som ansvarlige for drift og sikkerhet av fabrikkens, er de sjokkerte over at noen de stoler på har hatt så dårlig kontroll på sensitive data.

- Vi har jo egne systemer for sikring av dører og folk, men hva hjelper det når alt dette ligger åpent? Jeg er veldig overrasket over at så sensitiv informasjon ligger åpent på nettet, noe vi trodde var tett, lukket og beskyttet hos de instansene vi leverte informasjonen til. Det er skremmende, sier Johnsen.

Frykter sabotasje

Han frykter dette er så konkret informasjon at det i feil hender kan ha enorme konsekvenser, på ulike plan.

- Konsekvensen ved sabotasje, terror. At folk får vite hvor de ulike tingene står. Blir det fyr i dette, ødelegges jo fabrikkens. Da eksploderer den. For oss som matvareprodusent kan det ha alvorlige konsekvenser om noen vil skade oss i forhold til sabotasje av ingredienser i maten vi lager eller sette oss ut av produksjon, sier Johnsen.

Alnes er sjokkert over at alle fabrikkens hemmeligheter og farlige stoffer er angitt så detaljert som tilfellet er:

- Om en faen vil sprengte detta, er det bare å skru igjen her - så sier det puff. Et kjempesnell. Her har vi kjemikalier, granulater, ammoniumklorid, Det er jo sterkt etsende. Og her står det helium, men det står jo i planen hvor man finner det, sier han oppgitt.

Miljøfrykt

UAKSEPTABELT: - Denne type informasjon skal på ingen måte være offentlig, sier brannsjef Rolf Sørtorp, etter at Dagbladet gjorde ham oppmerksom på at en database tilhørende Midtre Hålogaland 110-sentral lå usikret på nett. Video: Øistein Norum Monsen / Dagbladet



MIDTRE HÅLOGALAND: Brannsentralen dekket fram til i sommer disse kommunene i Nordland. I dag er området dekket av 110-sentralen i Salten. KART: 110-sentralen



BLANT VERDENS STØRSTE: Vesteraalens er størst i Norge på fiskeboller i hermetikk, og en av de største produsentene i verden på produksjon av torskeleverolje (tran). Fabrikkledelsen frykter sabotasje av mat og utstyr som følge av sikkerhetsbristen ved 110-sentralen. Foto: Øistein Norum Monsen/Dagbladet

Også miljøet kan rammes hardt, skulle det skje fabrikken noe:

- Bak oss i tankene har vi syre, sterk maursyre som brukes i en del av produksjonen. Om det slippes ut eller gjøres sabotasje med, får det konsekvenser for omgivelsene ved at det renner ut i havna her, sier Johnsen.

- Den er jo sterkt etsende, hun er rett og slett farlig, sier Alnes om syra.

- Høyst beklagelig

Brannsjef Rolf Sørtorp ved Salten Brann IKS overtok i sommer ansvaret for den nå nedlagte 110-sentralen Midtre Hålogaland.

- Det er jo høyst beklagelig. De som gir oss denne type informasjon, må være trygge på at vi har gode systemer for å ta vare på den informasjonen. Hvorfor det ligger ute fra Midtre Hålogaland må vi stupe inn i og undersøke med en gang, sier han til Dagbladet.

Serveren eies av Narvik kommune, som stengte den kort tid etter Dagbladets besøk.



SENSITIV INFORMASJON: Produksjonssjef Viktor Johnsen (t.v.) og teknisk sjef Bjørn Alnes er oppgitt over at fabrikkens hemmeligheter har vært tilgjengelig for alle. Foto: Øistein Norum Monsen/Dagbladet



STUDERER DATA: Produksjonssjef Viktor Johnsen (t.v.) og teknisk sjef Bjørn Alnes studerer dokumentene Dagbladet fant på 110-sentralens åpne serverer. Foto: Øistein Norum Monsen/Dagbladet

Sortland Brann og Redningstjeneste

INNSATSPLAN

OBJEKT NAVN (Evt. kjentnavn på folkertunne)	Maritex AS	
ADRESSE	Havnegata 17	
GÅRDSNUMMER	BRUKSNUMMER	
BYGNINGSTYPE (Tre/Stål/Betong)	BRUKSOMRÅDE (Virksomhet)	Raffineri, flåskoolje
SEKSJONERT OBJEKT	ANTALL ETASJER	2 (3)
TLF. OG NAVN TIL BRANNVERNLEDER	Tor / Alnes / Johnsen / Sørtorp / Sørstøl / Borkstaver / ...	
TLF. OG NAVN NATTETID	Som over	
INNSATS PUNKTER	KOMMENTARER	
1. KJØREVEI	Maritex ligger innenfor bommen til havneområdet. ...	

Nøkkelsiens plassering

6. BRANNALARMANLEGG	Hvor finnes alarmcentralen?
7. SLUKKEANLEGG	Nei
8. VENTILASJONSLUKER	Nei
9. LAGRING	Syrer og baser både som fast stoff (granulat) og væske Sveigegass, propan, helium, hydrogen på stålflasker Giftige kjemikalier (lokalisert i laboratorium, pos 6 og 7 på kart Kjølemedium (kvelende) spaltet til giftige og etsende stoffer ved oppvarming
10. BEREDSKAPSMESSIG UTSTYR	Velg slukkemiddel etter hva som brenner (syrer, baser, olje)
11. SPEIELLE OPPLYSNINGER	Kjøretøy/utstyr som kan/kan ikke brukes Eksempelt utdrag fra sjekklisten!

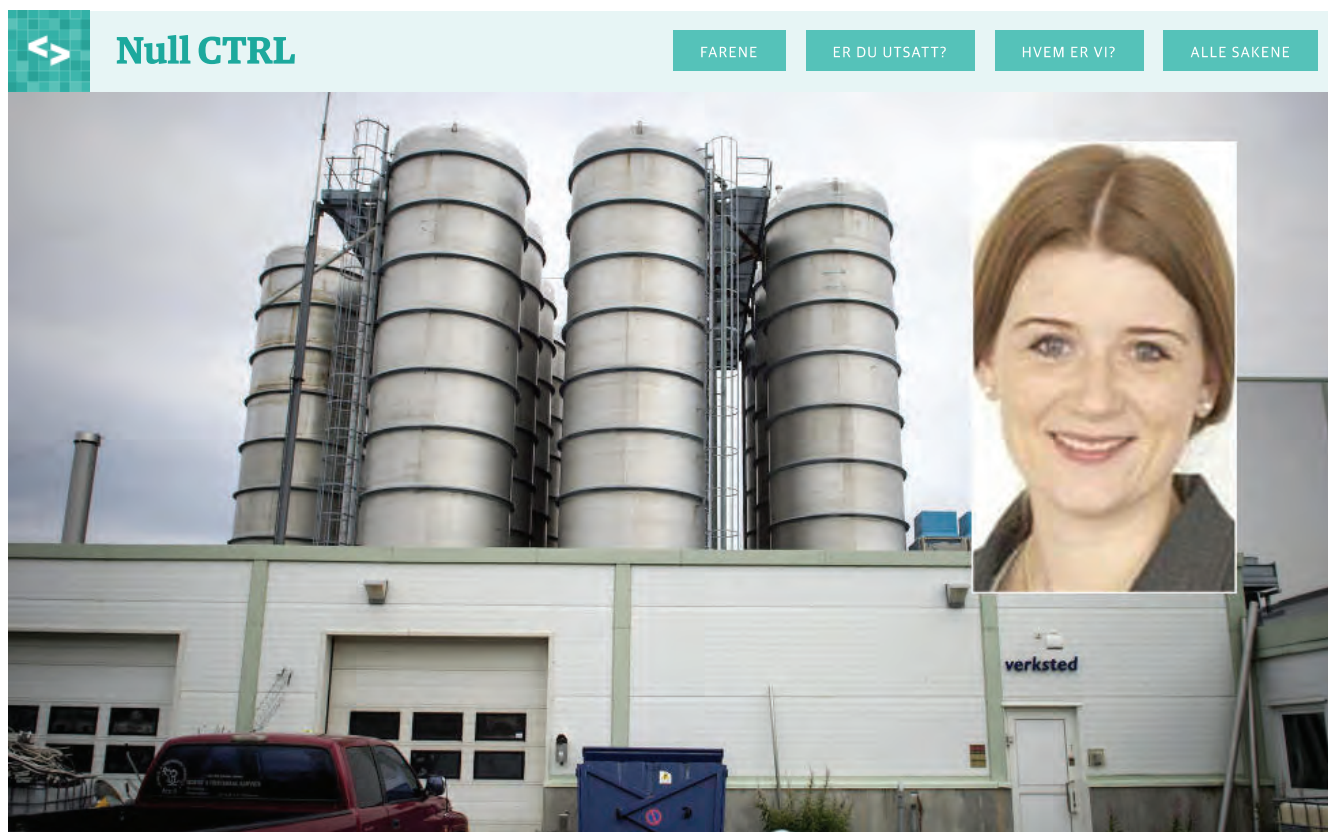
OPPSKRIFT: En innsatsplan er utarbeidet for å gi brannmannskaper rask og livsviktig informasjon om et mulig brannsted. Planen inneholder også sensitive data om farlige, brennbare eller eksplosive stoffer, som her ved Vesteraalens (Maritex-fabrikken). Dagbladet har sladdet deler av informasjonen i bildet.



Sortlandbrua

[Se større kart](#)

- Det er klart dette kan brukes til sabotasje: Kystvakta og kjøpesenteret ligger rett ved, publisert onsdag 9.



IKKE BLITT VARSLET: Ordføreren på Sortland i Nordland, Grethe Ellingsen, var da Dagbladet snakket med henne ikke varslet om at sensitiv informasjon fra fiskebollefabrikken i kommunen lå ute på nett. - Dette er skummelt, sier hun. Foto: Øisten Monsen / Dagbladet / Sortland Kommune

- Det er klart dette kan brukes til sabotasje: Kystvakta og kjøpesenteret ligger rett ved

Ordfører Grethe Ellingsen varsler oppvask etter fiskebolle-avsløringer.



THERESE DOKSHEIM
tdo@dagbladet.no

(Dagbladet): Etter å ha blitt vist sin egen innsatsplan av Dagbladet, som [lå åpen og tilgjengelig på nett](#), frykter landets største fiskebollefabrikk, Vesteraalens på Sortland i Nordland, terror og sabotasje.

- Her står jo alt. Og det ligger åpent på nettet..for Gud og hvermann? Det er jo skremmende. Da er vi i så fall et enkelt terrormål, sa produksjonssjef Viktor Johnsen.

Se møtet med fiskebollefabrikken i videoen i denne saken.

Ordføreren i den lille kommunen i Vesterålen, Grethe Ellingsen (H), sier til Dagbladet at hun er skremt av informasjonen.

- Dette er skremmende. Jeg forventer at det vil komme



- ENKELT TERRORMÅL: Ledelsen ved fiskebollefabrikken på Sortland tror det ville vært enkelt å sabotere med brannvesenets beredskapsplaner for hånden. Ordføreren i kommunen er ikke blitt varslet om trusselen. Video: Øistein Norum Monsen/Dagbladet.

informasjon nå om hva slags tiltak som settes i gang, sier hun.

- Ikke blitt rapportert

Det var i lys av at Dagbladet fant ut at 110-sentralen i Midtre Hålogaland i lang tid kan [ha ligget åpent på nett](#) uten noen form for passordbeskyttelse, at det kom fram at deler av informasjonen som lå tilgjengelig omfattet fiskebollefabrikken.

Når Dagbladet ringer onsdag morgen er det ingen som har fortalt henne om lekkasjen. Hun mener informasjonen, som omfattet all informasjon om adkomst, nøkler, dører og farlige stoffer ved fabrikken, enkelt kunne blitt misbrukt.

- Det er klart at dette kan brukes til sabotasje. Fiskebollefabrikken ligger strategisk utsatt til - nesten midt i bysentrum. Kystvakten ligger rett i nærheten, og det er også et kjøpesenter i nærheten. Det gjør det ikke mindre alvorlig, sier ordføreren.

Hun vil sørge for at de kommer til bunns i saken.

- Det har ikke kommet noen rapport til meg, men vi skal ha formannskapsmøte i morgen hvor jeg nå skal sørge for å få satt temaet på dagsorden slik at vi alle blir orientert.

- Vanskelig å holde oversikt

- Dette avdekker et stort og generelt problem. Ting er blitt så avanserte og det blir vanskeligere og vanskeligere å holde oversikt. Det er bra det blir satt fokus på, det berører jo oss alle rent beredskapsmessig. I våre beredskapsplaner framover må vi ta høyde for slike muligheter, sier hun.

Også Aps justispolitiske talsmann, Jan Bøhler, mener det er [viktig å forberede seg på det usannsynlige](#).

- Hele poenget med beredskap er at man skal sikre seg mot det utenkelige. Det handler om å sikre beredskapen i samfunnet, både stort og smått. Dette må tas på alvor, og må ses på som en alvorlig advarsel, sa han da Dagbladet snakket med ham i går.

- Kan gjøre stor skade

I samtale med ledelsen på fiskebollefabrikken, produksjonssjef Viktor Johansen, kom det fram at også den store mengden farlige stoffer på fabrikkområde ble et moment for bekymring.

- Jeg tror ikke det er noen fare for menigmann, men om denne informasjonen kommer i hendene på noen som ønsker det skal skje noe, så er jo vi et mål som kan gjøre stor skade for nærområdet.

Deriblant en stor potensiell miljøtrussel:

- Om 10 000 liter med maursyre skulle havne i vannet, vil det bli ballade i havna. Vi har diesel og gasser, så det er jo ei utfordring at det ligger åpent. En skummel sak, sier teknisk sjef Bjørn Alnes.



UAKSEPTABELT: - Denne type informasjon skal på ingen måte være offentlig, sier brannsjef Rolf Sørtorp, etter at Dagbladet gjorde ham oppmerksom på at en server tilhørende Midtre Hålogaland 110-sentral lå usikret på nett. Video: Øistein Norum Monsen.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL



TIPS OSS: På nullctrl@dagbladet.no

Dagbladet har foreløpig ikke lyktes i å komme i kontakt med fiskebollefabrikkens nærmeste «naboer» - kjøpesenteret Skibsgården og Kystvakten.



BLEV men

Sensitiv informasjon om brannberedskapen i 16 kommuner på Helgeland ble liggende åpen på nett fram til i går, til tross for at sentralen ble varslet om en mulig feil allerede i august.

(Dagbladet): Dagbladet har avdekket hvordan brannsentralen for 23 kommuner i Nordland i lang tid har ligget åpen og uten noen form for passordbeskyttelse på Internett.

Men brannsentralen i Midtre Hålogaland er ikke den eneste. Dagbladet kan i dag avsløre at også nabosentralen for 16 kommuner på Helgeland har en tilsvarende server stående åpen.

At det kunne være tilfelle, ble brannsjefen varslet om allerede i august.

– Det husker jeg, sier brannsjef Frode Thomassen til Dagbladet.

Sensitivt og personlig

Trolig har serveren i Rana stått åpen lenge.

I den omfattende databasen tilhørende 110-sentralen på Helgeland ligger det detaljerte opplysninger om alle ressurser brannvesenet disponerer.

Basen inneholder er oversikter over hvem som har ringt inn hvilke meldinger – og operatørens logg for hendelsene.

I en annen database finnes in-

FANT IKKE NOE FEIL: Brannsjef Frode Thomassen (t.v.) innrømmer at 110-sentralen ble bedt om å sjekke en mulig datafeil, men sier de ikke fant noe galt. En server har i lang tid stått åpen med detaljert informasjon om brannberedskapen i 16 kommuner på Helgeland. Bildet er tatt i en annen sammenheng, med Bjørn Råde (t.h.) i forebyggende avdeling tilstede. Foto: Geir Veia / Rana Blad

HELE VERDEN SPIONERTE
PÅ SOVEROM I NORSK HYTTE

Et overvåkingskamera i Nord-Trøndelag ble besatt 98 ganger på ei seks år gammel fra 12 ulike land. Kameraeieren safe ikke at det var mist.

ALLE SER DEG
Overvåket i en stund

PROSJEKTER PÅ GANG?
Lån opp til kr 300.000 uten sikkerhet
Søk på www.balanselånet.no

Dagbladet 7. oktober.

Landets største fiskebollefabrikk frykter terror og sabotasje etter datalekkasje.

Om en faen vil sprengte dette, er det bare å skru igjen her...

Dagbladet 9. oktober.

FØLG SAKEN

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyrte vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: [#null_CTRL](https://twitter.com/null_CTRL)

VARSLER, men fant ingen feil

terne brukernavn og passord for de lokale brukerne av brannsystemet. Dette er personlige passord, som potensielt kan misbrukes også i andre sammenhenger (som for eksempel i andre styringssystemer, e-post eller Facebook).

Ble varslet

I august varslet Dagbladet brannsjef Rolf Sørtp i Salten om en tilsvarende svikt ved Midtre Hålogaland 110-sentral. Han varslet umiddelbart leverandøren og kolleger ved andre 110-sentraler. Brannsjefen på Helgeland var blant disse.

Det bekrefter Thomassen overfor Dagbladet.

–Det ble under-søkt, og vi rapporterte tilbake at det ikke skulle være noen slik feil hos oss, sier Thomassen.

–Og dermed ble det ikke gjort noe mer med saken?

– Nei, det ble ikke noe mer snakk om det, sier Thomassen.

– Tar det ikke alvorlig

Dagbladet har fått en oversikt

TIPS
OSS



Espen Sandli
esan@dagbladet.no

Linn K. Hillestad
lkh@dagbladet.no



Null CTRL

som viser at Helgeland 110 sentral, med hovedbase i Rana kommune, ble varslet i august.

At varslingen ikke ble tatt mer seriøst, opprører brannsjef Rolf Sørtp i Salten.

– Det er skuffende at ikke alle tar dette like alvorlig. Vi snakker om informasjon som ikke skal være på avveie, sier han til Dagbladet.

På Sortland er ledelsen ved Vesteraalens hermetikkfabrikk rasende over sensitiv informasjon om giftige- og eksplosive stoffer som har ligget åpent på nett grunnet en tilsvarende svikt i datasikkerheten i Midtre Hålogaland.

Frykter sabotasje

– Her står jo alt. Og det ligger åpent på nettet. for Gud og hvermann? Det er jo skremmende. Da er vi i så fall et enkelt terrormål, uttalte produksjonssjef Viktor Johnsen til Dagbladet i går.

Dagbladet har nå funnet åpnere servere tilhørende brannberedskapen i 39 av 44 kommuner i Nordland.



KRITISK: Brannsjef Rolf Sørtp varslet allerede i august.

Foto: Øistein Norum Monsen

www.citroen.no

250 KM LENGGER PÅ FULL TANK*

NYE CITROËN C3

VTi 68

FRA KR 175.200,-

NORDIC-EDITION

Mer utstyr til samme pris

- Digitalt klimaanlegg
- Regnsensor
- Elektriske vinduer foran og bak
- CD, radio & Connecting Box (Bluetooth & USB)
- Fjernstyrt sentrallås
- ESP&ASR
- Takelys
- Cruisekontroll & hastighetsbegrensere
- Setevvarmer foran
- Panorama soltak



KUN HOS AUTO ELITE: 82 HK VTI MED ALT DU TRENGER

- STØRRE NY MOTOR 82 HK
- SOMMER OG VINTERHJUL
- KOMFORTPAKKE

FERDIG LEVERT NÅ KUN 184.900,-

C3: Privatleie
nå kun 1495,-
inkl "alt"

CITROËN foretrekker TOTAL

Nye Citroën C3 har ny, stilfull design med en mer dynamisk front og LED-lykter som gir en unik lyssignatur. Denne praktiske hverdagsbilen har god plass til 5 personer, et bagasjerom på hele 300 liter, samt bakseter som i tillegg kan legges ned. Kupeen har nye, eksklusive materialer og nytt og lekkert instrumentpanel. Kom og ta den på tur!

CRÉATIVE TECHNOLOGIE

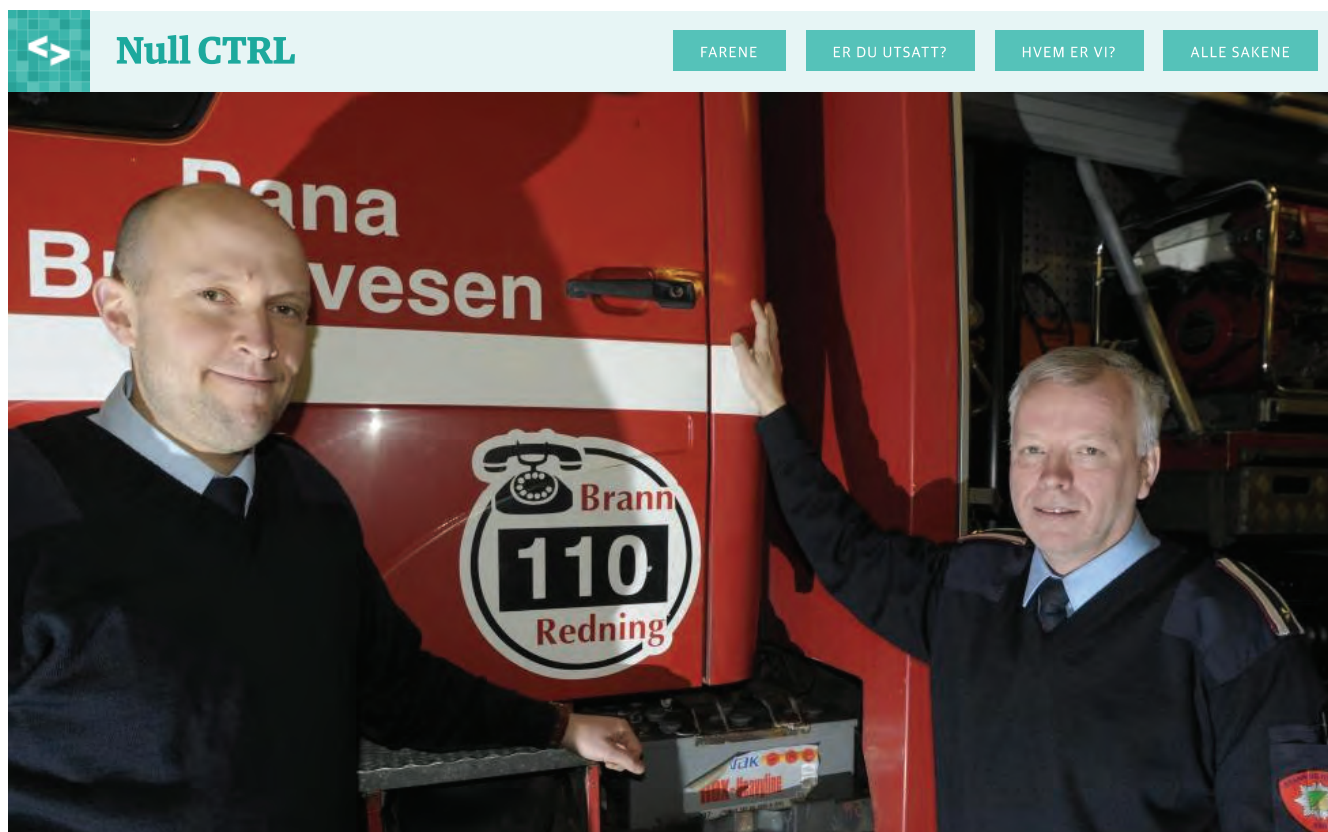


Alle personbilpriser er inkludert mva., frakt og levering Oslo (kr 9.900,-). Tilbudene kan ikke kombineres med andre tilbud som flåteavtaler og lignende. *Sammenlignet med den tidligere 1,4i motoren med 75 hk. **Privatleietilbud kr 35.000 i forskudd. Kjørelengde 36 mnd / 36.000 km. Etableringsbegynnelse kr 3.874 vil tilkomme. Med forbehold om trykktfeil.

auto elite!
WWW.AUTOELITE.NO

OSLO • GLADENGVEIEN 9 • TELEFON 24 07 41 00 • ASKER OG BÆRUM • STASJONSVEIEN 40 •
TELEFON 67 49 48 00 • FOLLO • DYNAMITTVEGEN 10 • TELEFON 64 85 77 00

- Jeg husker vi ble varslet, men vi fant ingen feil, publisert torsdag 10. oktober 2013 kl. 13:44



FANT IKKE NOE FEIL: Brannsjef Frode Thommasen (t.v.) innrømmer at 110-sentralen ble bedt om å sjekke en mulig datafeil, men sier de ikke fant noe galt. En server har i lang tid stått åpen med detaljert informasjon om brannberedskapen i 16 kommuner på Helgeland. Bildet er tatt i en annen sammenheng, med Bjørn Råde (t.h.) i forebyggende avdeling tilstede. Foto: Geir Veia / Rana Blad

- Jeg husker vi ble varslet, men vi fant ingen feil

Derfor ble private passord og sensitive beredskapsdata for 16 kommuner på Helgeland liggende åpent på nett.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLID HILLESTAD
lkh@dagbladet.no

(Dagbladet): Dagbladet har avdekket hvordan brannsentralen for 23 kommuner i Nordland i lang tid [har ligget åpen og uten noen form for passordbeskyttelse](#) på Internett.

Men brannsentralen i Midtre Hålogaland er ikke den eneste. Dagbladet kan i dag avsløre at også nabosentralen for 16 kommuner på Helgeland har en tilsvarende server stående åpen.

Dagbladet har nå funnet åpne servere tilhørende brannberedskapen i 39 av 44 kommuner i Nordland.

Ble varslet

På Helgeland er brannvesenet flinkere til å slukke branner enn å

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyrte vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

finne hull i datasikkerheten.

Brannsjefen ble nemlig varslet om en mulig feil allerede i august.

- Det husker jeg, sier brannsjef Frode Thomassen til Dagbladet.

Sensitivt og personlig

Trolig har serveren plassert i Rana stått åpen lenge.

På denne serveren ligger det blant annet omfattende databaser tilhørende 110-sentralen på Helgeland. I en av disse ligger det opplysninger om alle ressurser brannvesenet disponerer. Basen inneholder oversikter over hvem som har ringt inn hvilke meldinger - og operatørens detaljerte logg for hendelsene.

I en annen database finnes interne brukernavn og passord for de lokale brukerne av brannsystemet. Dette ser ut til å være personlige passord, som potensielt kan misbrukes også i andre sammenhenger (som for eksempel i andre styringssystemer, e-post eller Facebook).

Sikkerhetsekspert mener informasjon fra slike åpne nødsentraler i verste fall [kan bli misbrukt av terrorister](#).

- Ble ikke mer snakk om

I august varslet Dagbladet brannsjef Rolf Sørtorp i Salten om en tilsvarende svikt ved Midtre Hålogland 110-sentral. Han varslet umiddelbart leverandøren og kolleger ved andre 110-sentraler. Brannsjefen på Helgeland var blant disse.

Det bekrefter Thomassen overfor Dagbladet.

- Det ble undersøkt, og vi rapporterte tilbake at det ikke skulle være noen slik feil hos oss, sier Thomassen.

- Og dermed ble det ikke gjort noe mer med saken?

- Nei, det ble ikke noe mer snakk om det, sier Thomassen.

- Tar det ikke alvorlig

Dagbladet har fått en oversikt som viser at Helgeland 110 sentral, med hovedbase i Rana kommune, ble varslet i august.

At varslingen ikke ble tatt mer seriøst, opprører brannsjef Rolf Sørtorp i Salten.

- Det er skuffende at ikke alle tar dette like alvorlig. Vi snakker om informasjon som ikke skal være på avveie, sier han til Dagbladet.



UAKSEPTABELT: Brannsjef Rolf Sørtorp i Salten varslet kollegene ved andre 110-sentraler om mulig datasvikt. Han er skuffet over at noen ikke har tatt det alvorlig. Video: Øistein Norum Monsen



- ENKELT TERRORMÅL: Ledelsen ved fiskebollefabrikken Vesteraalens på Sortland viser hvordan informasjonen fra 110-sentralen i Midtre Hålogland potensielt kunne blitt misbrukt av personer med onde hensikter. Video: Øistein Norum Monsen/Dagbladet



DEKKER 16 KOMMUNER: Helgeland 110 dekker disse 16 kommunene sør i Nordland. Kart: 110-sentralen

Frykter sabotasje

På Sortland er ledelsen ved Vesteraalens hermetikkfabrikk rasende over [sensitiv informasjon om giftige- og eksplosive stoffer](#) som har ligget åpent på nett grunnet en tilsvarende svikt i datasikkerheten i Midtre Hålogaland.

- Her står jo alt. Og det ligger åpent på nettet..for Gud og hvermann? Det er jo skremmende. Da er vi i så fall et enkelt terrormål, uttalte produksjonssjef Viktor Johnsen til Dagbladet i går.

På samme sted frykter den lokale ordføreren sabotasje [kan skade Kystvakta](#) og et handlesenter.

- Sløvt

Arbeiderpartiets justis- og beredskapstalsmann Jan Bøhler er opprørt over Dagbladets avsløring.

- Min første reaksjon er at dette er ufattelig sløvt. Særlig etter 22. juli og alt fokuset vi har hatt på beredskap og sikkerhet i samfunnet. Det er ikke mulig å forstå at de ikke har tenkt på dette, [uttalte han](#) i forbindelse med [den første åpne brann-serveren](#) Dagbladet avslørte..

Dagbladet har avdekket sviktende datasikkerhet ved 39 av 44 kommuner i Nordland i forbindelse med [serien Null CTRL](#).

Sent i går kveld mottok Dagbladet følgende e-post fra brannsjefen på Helgeland:

«Takker for din tilbakemelding. Denne uønskede hendelsen er tatt tak i og tilgangen gjennom ftp er stengt. Vi følger opp videre!»

[illegible]

HVA: Den åpne basen inneholder informasjon om hvem som har ringt når og meldt fra om hva, samt operatørens egen logg av hendelsene. Foto: Skjermdump

[illegible]

HVEM OG HVOR: Den åpne basen inneholder informasjon om hvem som har ringt når og meldt fra om hva, samt operatørens egen logg av hendelsene. Foto: Skjermdump



KRITISK: Brannsjef Rolf Sørto i Salten IKS varslet i august alle 110-sentralene om at de måtte sjekke sine sikkerhetsrutiner. - Dessverre er det ikke alle som tar dette alvorlig, sier han til Dagbladet. Foto: Øistein Norum Monsen/Dagbladet.

Indeks for /db/

Navn	Størrelse	Dato endret
 [overordnet katalog]		
 110.mdb	3.0 MB	09.10.13 12:30:00
 alarmbase.mdb	4.5 MB	09.10.13 12:15:00
 alarmbase_gml.mdb	3.8 MB	27.02.13 09:32:00
 alarmbase_old.mdb	3.4 MB	03.12.12 08:39:00
 backup/		08.05.12 08:38:00
 DBFAS1.MDB	9.0 MB	23.08.11 08:41:00

ÅPEN DATABASE: Den åpne serveren inneholder også databaser med informasjon om brannressurser, brukernavn og pasord. Her finnes også databasen med detaljert informasjon om meldingene sentralen hver dag mottar. Foto: Skjermdump



Dyrepasser klemt i hjel av sørgende elefant

En dyrepasser i Missouri i USA mistet livet etter å ha blitt klemt i hjel av en av dyreparkens elefanter.

Det store dyret hadde blitt mer aggressiv leder etter at elefantflokkens leder døde få dager tidligere.

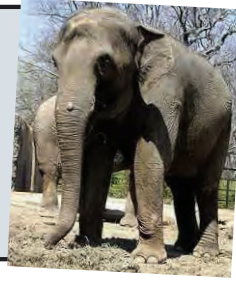
Den tragiske ulykken skjed-

de i Dickerson Park Zoo. Den 62 år gamle dyrepasser John Philips Bradford, som hadde jobbet i dyreparken i over 30 år, forsøkte å få Patience inn gjennom en trang gang da hun plutselig dyttet til ham og deretter klemte ham i hjel.

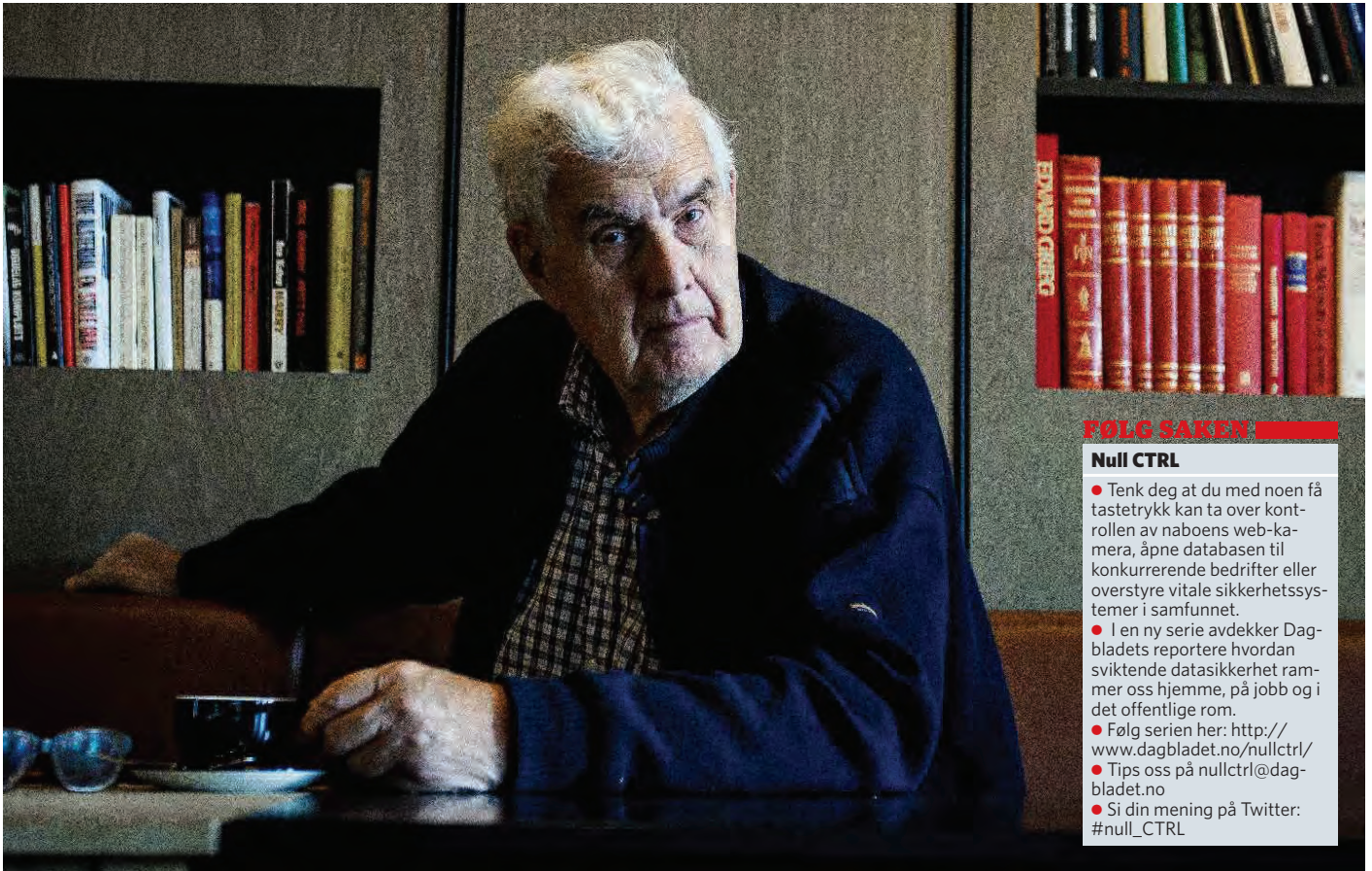
De ansatte i dyreparken hadde merket at Patience hadde endret atferd og tydelig sørget etter at elefantflokkens matriark Connie ble avlivet forrige uke på grunn av akutt nyresvikt. Patience har bodd i dyreparken i Missouri siden 1990. (NTB)



JOHN P. BRADFORD og elefanten Patience. Foto: NTB Scanpix



KNIVSTUKKET: En 24 år gammel mann på løpetur ble seint fredag kveld knivstukket ved Stokkavannet i Stavanger. Han slapp unna med lettere skader, men politiet ser alvorlig på saken og ber vitner melde seg. Politiet har pågrepet en mistenkt. (NTB)



LANG FARTSTID: I 21 år ledet Georg Apenes Datatilsynet. Han kaller overvåkingen og datasikkerheten Dagbladet har avslørt science fiction.

Foto: John T. Pedersen

- Ingen tør å ta tak i det

Den tidligere Høyre-profilen Georg Apenes refser den påtroppende regjeringa for ikke å være opptatt av datasikkerhet.

NULL CTRL

Tekst: **Therese Doksheim**
tdo@dagbladet.no

FREDRIKSTAD (Dagbladet): Dagbladet møter den tidligere Datatilsyn-direktøren på Litteraturhuset i Fredrikstad. Apenes er født og oppvokst i plankebyen, og

trives her. Pensjonisttilværelsen synes han derimot er for treig.

– Det gikk fra sjettegir og helt ned til andregir. Det skjer for lite, sier han.

Apenes hadde mange baller i lufta i sin tid, som jurist, journalist, Høyre-politiker, forfatter og direktør. Som landets mest erfarne Datatilsynet-direktør er han forundret over Dagbladets funn av overvåking og svikt i samfunnsikkerheten.

- Som science fiction

– Det som skjer i samfunnet i dag, er som science fiction. Det man før ikke engang kunne forestille seg, er nå en realitet. Det er derfor ikke regjeringa tør å ta tak i det – fordi de ikke aner hvordan de skal håndtere det.

– Jeg bare viser til valgkampen, hvor den påtroppende regjeringa ikke nevnte datasikkerhet med ett ord. Det var et ikke-tema. «IT-løsninger må være sikre», sier de. Selvfølgelig. Men det er ikke et eneste parti som kan tilby en løsning, sier han.

– Hvorfor tror du de ikke nevnte det?

– Hva skulle de nevne? Hva skulle de si? De er fullstendig tafatte hele gjengen, sier Apenes.

Ikke sjokkert

Dagbladet nevner flere av sakene som er tatt opp i avisa den siste tida. Apenes rynker på nesa. Han har lest flere av dem. Han er ikke sjokkert over at folk blir overvåket på kafeer og utesteder og at sensitiv informasjon ligger åpent

og helt tilgjengelig på nett.

– Det finnes ikke noe firkantet, enkelt svar på dette. Jeg har nevnt at man bør skrive brev, kjøpe et frimerke og sende ting i posten i stedet for å sende det elektronisk. Sitter man på konfidensiell informasjon er nok det det beste. Ellers kan man aldri være sikker på at folk ikke vet hva du og jeg snakker om på «tomannshånd», sier han.

- Deartementets ansvar

Han etterlyser samtidig en instans som kan ta ansvar for overvåkingproblemet i samfunnet.

– Enhver norsk borger bør ha rettskrav på å kunne vende seg et eller annet sted for å få vite hvem som overvåker ham eller henne – når og hvor. Det er bare latterlig-

som følger mine disposisjoner, mine kontakter. Noen må jo vite det.

Han mener det er naturlig at folk har ting å skjule.

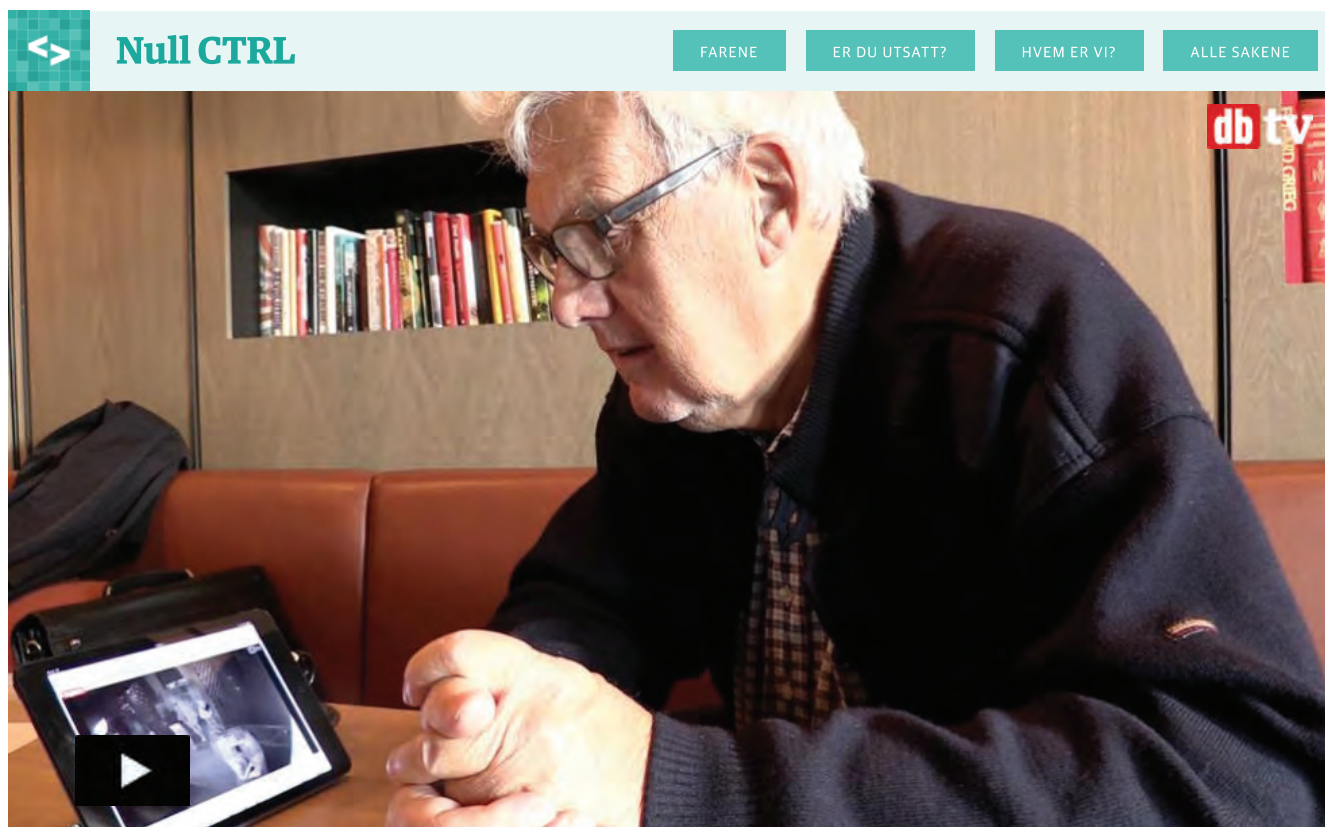
– Hvis ikke borgerne kan kommunisere mer eller mindre uten å tro de blir overvåket, vil det endre hele måten vi kommuniserer på, sier han.



Dagbladet 7. oktober.



- De er fullstendig tafatte hele gjengen, publisert søndag 13. oktober 2013 kl. 11:34



REFSER: Tidligere Datatilsynet-direktør Georg Apenes refser den påtroppende regjeringen for å ikke snakke om datasikkerhet. Video: John Terje Pedersen / Dagbladet

- De er fullstendig tafatte hele gjengen

Georg Apenes mener ingen tør å ta tak i datasikkerheten i Norge.



THERESE DOKSHEIM
tdo@dagbladet.no



JOHN TERJE PEDERSEN
jtp@dagbladet.no

FREDRIKSTAD (Dagbladet): Dagbladet møter den tidligere Datatilsynet-direktøren på Litteraturhuset i Fredrikstad. Apenes er født og oppvokst i plankebyen, og trives her. Pensjonisttilværelsen synes han derimot er for treig.

- Det gikk fra sjettegir og helt ned til andregir. Det skjer for lite, sier han.

Apenes hadde mange baller i luften sin tid, som både jurist, journalist, Høyre-politiker, forfatter og direktør. Som landets mest erfarne Datatilsynet-direktør er han forundret over [Dagbladets funn](#) av overvåking og svikt i samfunnssikkerheten.

- Som science fiction

- Det som skjer i samfunnet i dag, er som science fiction. Det man før ikke engang kunne forestille seg, er

I FREDRIKSTAD ”Når jeg går inn på badeværelset mitt hjemme i Fredrikstad, så er det verken for å foreta meg noe asosialt, noe samfunnsnedbrytende, noe uhygienisk eller umoralsk - men jeg lukker døra, for i den situasjonen vil jeg være helt sikker på at jeg ikke er iakt tatt. «Høhhø» sier folk til det.

Georg Apenes.



nå en realitet. Det er derfor ikke regjeringen tør å ta tak i det - fordi de ikke aner hvordan de skal håndtere det.

- Jeg bare viser til valgkampen, hvor den påtroppende regjeringen ikke nevnte datasikkerhet med ett ord. Det var et ikke-tema. «IT-løsninger må være sikre», sier de. Selvfølgelig. Men det er ikke et eneste parti som kan tilby en løsning, sier han.

- Hvorfor tror du de ikke nevnte det?

-Hva skulle de nevne? Hva skulle de si? De er fullstendig tafatte hele gjengen, sier Apenes.

- Kan aldri være sikker

Dagbladet nevner flere av [sakene](#) som er tatt opp i avisa den siste tida. Apenes rynker på nesa. Han har lest flere av dem. Han er ikke sjokkert over at folk blir [overvåket på kafé](#), på [utested](#) og at [sensitiv informasjon ligger åpent](#) og helt tilgjengelig på nett.

- Det finnes ikke noe firkantet, enkelt svar på dette. Jeg har nevnt at man bør skrive brev, kjøpe et frimerke og sende ting i posten i stedet for å sende det elektronisk. Sitter man på konfidensiell informasjon er nok det det beste. Ellers kan man aldri være sikker på at folk ikke vet hva du og jeg snakker om på «tomannshånd», sier han.

Han etterlyser samtidig en instanse som kan ta ansvar for overvåkingproblemet i samfunnet.

- Enhver norsk borger bør ha rettskrav på å kunne vende seg et eller annet sted for å få vite hvem som overvåker ham eller henne. Når og hvor. Det er bare latterliggjort. Jeg kunne tenke meg det var Justisdepartementet. Jeg vil vite hvem som overvåker meg, hvem som følger mine disposisjoner, mine kontakter. Noen må jo vite det.

I november 2011 [startet Apenes foreningen Digitalt Personvern](#), som har som strategi å skaffe penger som skal gjøre det mulig å hjelpe et representativt utvalg privatpersoner å gå til sak mot Staten, med en påstand om at direktivets inngrep i privatliv og ytringsfrihet er i strid med den europeiske menneskerettighetskonvensjonen.

LANG FARTSTID: I 21 år ledet Georg Apenes Datatilsynet. Han kaller overvåkingen og data«sikkerheten» Dagbladet har avslørt for science fiction, og skulle gjerne sett at alt konfidensielt materiale ble sendt på den gode, gamle måten: med brev i posten Foto: John T. Pedersen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL



RETT PÅ NETT: Kameraet på utestedet Klubbteateret i Drammen sendte videostrømmen rett på nett. Video: Øistein Norum Monsen/Dagbladet



På nettet fant Dagbladet et avansert overvåkingskamera liggende åpent og ubeskyttet. Hvor lenge det har ligget slik, er ikke kjent. Video: Øistein Norum Monsen/Dagbladet.

Han mener det er naturlig at folk har ting å skjule.

- Ikke uhygienisk eller umoralsk

- Når jeg går inn på badeværelset mitt hjemme i Fredrikstad, så er det verken for å foreta meg noe asosialt, noe samfunnsnedbrytende, noe uhygienisk eller umoralsk - men jeg lukker døra, for i den situasjonen vil jeg være helt sikker på at jeg ikke er iaktatt. «Høhhø» sier folk til det. Men ja, det er visse omstendigheter knyttet til vårt liv og vår sosiale situasjon som vi nødvendigvis deler frivillig med andre.

- Sånn tror jeg de fleste har det. Hvis ikke borgerne kan kommunisere mer eller mindre uten å tro de blir overvåket vil det endre hele måten vi kommuniserer på, sier han.

Han viser tilbake til tida som nyansatt i Datatilsynet. Året var 1989. Han lærte tidlig hvordan det var:

- De hadde en hel avdeling satt av til datasikkerhet. Men ordet «sikkerhet» var aldri bokstavelig. Bare nesten. Fra den tida har jeg visst at måtene vi kommuniserer på, så sant det ikke er gjennom post, bare er *nesten* sikker.

- Naive nordmenn

Apenes snakker om barnebarna. Han snakker om hvor mye mer oppdaterte de er enn ham selv. Han vet likevel en ting eller to om personvern og datasikkerhet - sikker eller *nesten* sikker.

- *Tror du nordmenn er klar over denne utviklingen, og klar over hvor mye overvåking og sikkerhetsbrudd som skjer?*

- Nei. Nordmenn er naive. Dels fordi de nekter å se det med egne øyne, og fordi det er mer behagelig å «ikke vite». De å tro det har kontroll, men det er bare ønsketenkning og naivitet, sier Georg Apenes.



ENKELT TERRORMÅL: Ledelsen ved fiskebollefabrikken på Sortland tror det ville vært enkelt å sabotere med brannvesenets beredskapsplaner for hånden. Video: Øistein Norum Monsen/Dagbladet.



Fredrikstad

[Se større kart](#)

Georg Richard Apenes:

- Født 5. april 1940 i Fredrikstad, hvor han er oppvokst og bosatt.
- Høyrepolitiker og sønn av sorenskriver Christian B. Apenes og Inger Johanne Apenes.
- Stortingsrepresentant for Høyre fra 1977 til 1989.
- Jurist og tidligere embedsmann.
- Gift med Ingrid I. Willoch, høyrepolitiker og tidligere varaordfører i Fredrikstad.
- Var med å stifte organisasjonen [Digital personvern](#), som samler inn penger for å prøve Datalagringsdirektivet i retten.
- Direktør av Datatilsynet fra 1989 til 2010.
- Lang fartstid som fast kommentator i norske aviser. Har skrevet artikler for tidsskrifter, essaysamlinger, lærebøker, kåseri og antologier.
- Varamedlem av Pressens Faglige Utvalg, etter å ha vært medlem og viseformann i ulike perioder siden 1972.

- I 2010 ble han utnevnt til ridder av 1. klasse av St. Olavs Orden for embetsfortjenste.

- Medlem av Europarådets parlamentariske forsamling.

- Har skrevet flere bøker, deriblant:

- *Fredrikstad og deromkring (1990).

- *Løven gjesper (1989).

- *Tyttebærkrigen: Det norske felttog i Sverige 1788 (1988).

- *Panoptikon: vårt gjennomsluttede samfunn (2000).

- *Fra Sinai bjerg til Silikon Valley: rettsstaten og informasjonsteknologien (1991).

- *Personvern og samfunnsmdisin, i Helse for de mange. Samfunnsmedisin i Norge (2003).

- *Fra tillit til kontroll: Tolv samtaler om politikk, teknologi og personvern (2005).

Kilde: [Amazon](#) / Wikipedia / [Digitalt Personvern](#)



Kundenenes
sensitive
data lå

ÅPENT P

HELT UBESKYTTET: Daglig leder Jarl Kristen Salomonsen får sjokk når han ser at en av Lofotnetts dataservere lå tilgjengelig for alle på nett. På serveren lå det sensitiv kundeinformasjon

Selskapet Lofotnett solgte datasikkerhet for flere millioner kroner. Samtidig lå kundenenes passord åpent på Internett.

LOFOTEN (Dagbladet): På et kontor ytterst i havgapet ved Leknes i Lofoten sitter Jarl Kristen Salomonsen (51) og stirrer tomt ut i lufta. Han har nettopp fått sitt livs sjokk. Nå frykter han livsverket faller i grus.

– Dette er sjokkerende informasjon å få, sier Salomonsen.

Ubesskyttet

Tenk deg at du med et tastetrykk kan styre naboens web-kamera, åpne konkurrentens database eller ta kontrollen over vital samfunnsikkerhet.

I en serie artikler avslører Dagbladet hvor enkelt det er, og hvilke dramatiske konsekvenser det kan få.

Salomonsen er eier og daglig leder av dataselskapet Lofotnett. Han er overrasket over å få Dagbladet på døra ytterst i Lofoten, men

ennå mer overrasket da han ser informasjonen Dagbladet har funnet på Internett.

På en bærbar PC viser vi Salomonsen en server som ligger åpen på nett uten noen form for passordbeskyttelse.

Passord

Ifølge Salomonsen inneholder den eksterne harddisken selskapets

**TIPS
OSS**

Espen Sandli
esan@dagbladet.no

Linn K. Hillestad
lkh@dagbladet.no

Null CTRL

kundelister, selskapets egne brukernavn og passord. Og, ikke minst, sensitive data om kundene og deres passord.

– Det er grusomt, sier han.

Det er ifølge

Salomonsen selskapets hjerne, en administrativ hovedserver, som står åpen og vendt ut mot verden.

Dagbladet har kunnet konstatere at serveren inneholder flere tusen dokumenter og filer. Salomon-

sen bekrefter at det er snakk om svært sensitive kundedata, informasjon om nåværende og tidligere ansatte i Lofotnett og private data tilhørende ansatte i selskapet.

– Dette er et sjokk. Jeg visste virkelig ikke at den sto åpen. Og hvorfor den gjør det er en gåte. Det er jo ingen grunn til at den skal være det, sier Salomonsen.

På avveie

Han frykter serveren kan ha stått ubeskyttet og åpen i flere år uten at noen har merket det.

– Det er jo dokumenter som ikke skulle ha vært på avveie. Andre kan



”Jeg ser for meg at det er kroken på døra for dette firmaet, så alvorlig ser jeg på at denne type informasjon er kommet ut.

Jarl Kristen Salomonsen, daglig leder i Lofotnett

Å N E T T E T

FAKTA

Dette lå åpent på nettet

- En IP-adresse tilhørende Lofotnett ga åpen tilgang via en såkalt FTP-server.
- FTP (File Transfer Protocol, *filoverføringsprotokoll*) er en standard protokoll for overføring av filer i et TCP/IP-basert nettverk.
- FTP-serveren lytter på nettverket etter forespørsler. FTP-klienten kobler til serveren og kan lese og skrive til serverens filsystem. Det gir brukerne mulighet til opp- og nedlasting av filer, sletting, redigering av innhold mm.
- I ei mappe på den åpne serveren lå flere Lofotnett-kunders brukernavn og passord. I tillegg står det brukernavn og passord til flere kunders trådløse nett.
- Serveren inneholdt også forretningshemmeligheter som kunde-kontrakter, korrespondanse, detaljerte spesifikasjoner fra kunders dataanlegg, salgsbrev og finansielle opplysninger og dokumentasjon fra tvister selskapet har vært i.
- Her lå også private dokumenter og bilder, lønnspapirer, moromateriale og dokumenter fra strategiplaner, kurs og arrangementer.
- Lett tilgjengelig for uvedkommende lå også komplett backup-lagring av harddisken til en ansatt i selskapet.

FØLG SAKEN

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens webkamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

og passord. Han fortar seg å stenge alle tilganger til serveren som ikke var sikret.

Foto: Øistein Norum Monsen

ha tatt komplett kopi av innholdet som lå der. I forhold til kundene har jeg ikke god tid nå, sier han.

For et selskap som er avhengig av folks tillit, er grove svikt i sikkerheten potensielt ødeleggende.

– Jeg ser for meg at det er kroken

på døra for dette firmaet, så alvorlig ser jeg på at denne type informasjon er kommet ut. Men gud fader, jeg er glad for at jeg ble gjort oppmerksom på det, slik at jeg kan få berget det som er. Men huff, det her var tøft, sier han.

Søkte politihjelp

Dagbladet oppsøkte Lofotnett i august. Under besøket ble serveren midlertidig stengt. Sikkerhetshullet er i dag lukket.

Salomonsen har i ettertid gått til politiet i håp om å komme til bunns i hva som var årsaken til at sikkerhetshullet i sin tid opp-

sto. Han frykter sabotasje ligger bak.

– Jeg lurar jo på hvorfor dette var åpent, når det aldri har vært noen grunn til at det skulle bli åpnet, sier Salomonsen.

Etter Dagbladets besøk varslet han også kundene sine om problemet, og flere valgte å forlate selskapet. Nå frykter han at han må melde opphør til Brønnøysundregistrene.

Bør teste seg selv

Sensitiv forretningsinformasjon på avveie grunnet dårlig el-

ler fraværende datasikkerhet er et større problem enn mange er klar over:

– Vi ser dette ofte når vi kjører sikkerhetstester mot virksomheter. Som oftest skyldes det feilkonfigurasjon eller ansatte som ikke forstår konsekvensen av hva de gjør. Norsis anbefaler derfor alle virksomheter å kjøre en sikkerhetstest fra Internett med jevne mellomrom for å avdekke hva som er tilgjengelig, sier seniorrådgiver Vidar Sandland i Norsk senter for informasjonssikkerhet (Norsis) til Dagbladet.

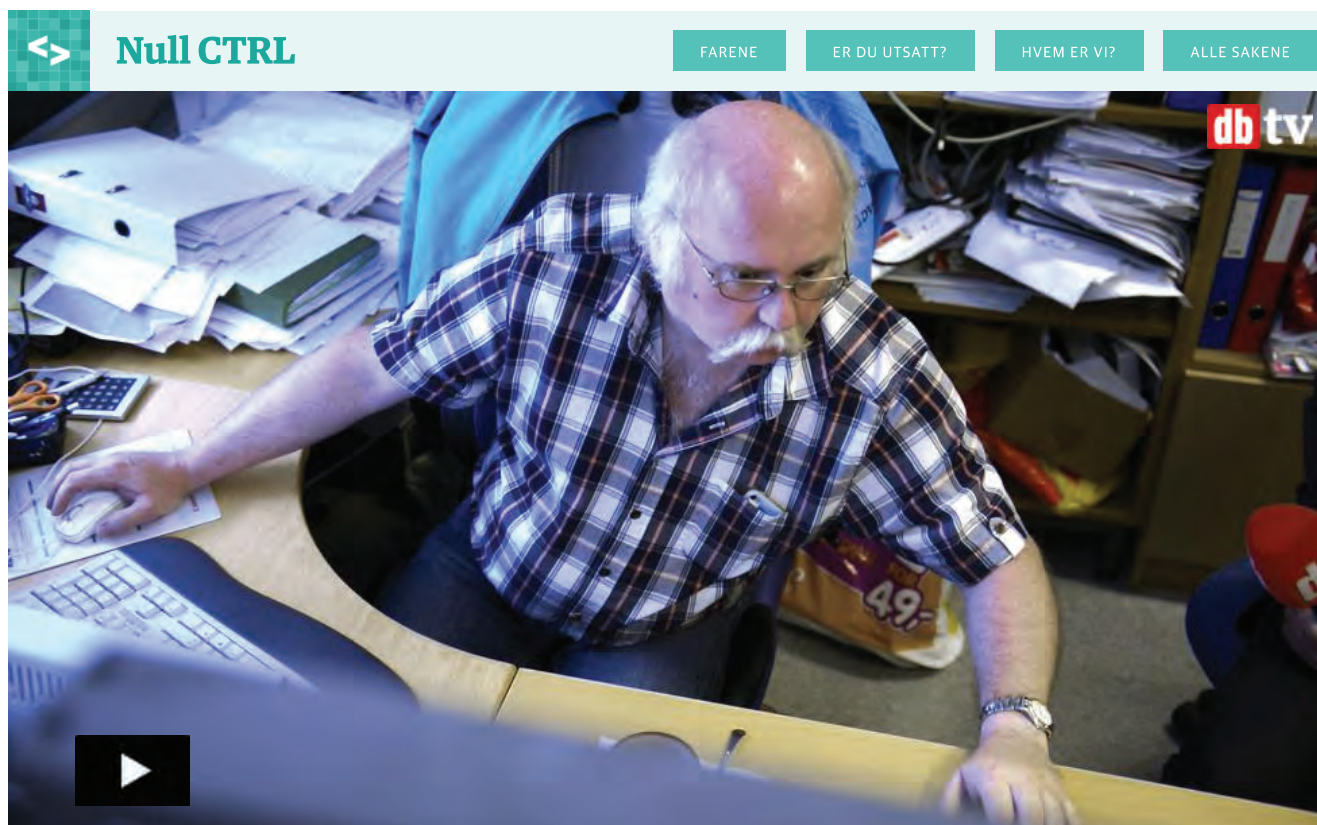


Dagbladet i går.

”Gud fader, jeg er glad for at jeg ble gjort oppmerksom på det, slik at jeg kan få berget det som er.

Jarl Kristen Salomonsen, daglig leder i Lofotnett

«Det er et forferdelig sjokk - og trolig kroken på døra», publisert mandag 14. oktober 2013 kl. 09:32



HELT UBESKYTTET: Jarl Salomonsen fikk sjokk da han så en av Lofotnetts servere ligge tilgjengelig for alle på nett. På serveren lå det sensitiv kundeinformasjon og passord. Foto: Øistein Norum Monsen / Dagbladet

«Det er et forferdelig sjokk - og trolig kroken på døra»

Selskapet solgte dataløsninger for flere millioner kroner, men kundenes passord lå åpent på Internett.



ESPEN SANDLI
esan@dagbladet.no



ØISTEIN NORUM MONSEN
onm@dagbladet.no



LINN KONGSLI HILLESTAD
lkh@dagbladet.no

LOFOTEN (Dagbladet): På et kontor ved Leknes i Lofoten sitter Jarl Kristen Salomonsen (51) og stirrer tomt ut i lufta. Han har nettopp fått sitt livs sjokk. Nå frykter han livsverket faller i grus.

- Det her er sjokkerende informasjon å få, sier Salomonsen.

Ubeskyttet

Tenk deg at du med et tastetrykk kan styre naboens web-kamera, åpne konkurrentens database eller ta kontrollen over vital samfunnssikkerhet.

I en [serie artikler avslører Dagbladet](#) hvor enkelt det er, og hvilke dramatiske konsekvenser det kan få.



ENKELT TERRORMÅL: Ledelsen ved fiskebollefabrikken på Sortland tror det ville vært enkelt å sabotere med brannvesenets beredskapsplaner for hånden. Beredskapsplanene lå helt åpent på Internett. Video: Øistein Norum Monsen/Dagbladet.

Salomonsen er eier og daglig leder av dataselskapet Lofotnett. Han er overrasket over å få Dagbladet på døra ytterst i Lofoten, men ennå mer overrasket da han ser informasjonen Dagbladet har funnet på Internett.

På en bærbar PC viser vi Salomonsen en server som ligger åpen på nett uten noen form for passordbeskyttelse.

Passord

Ifølge Salomonsen inneholder den eksterne harddisken selskapets kundelister, selskapets egne brukernavn og passord. Og ikke minst: Sensitive data om kundene - og deres passord.

- Det er grusomt, sier han.

Det er ifølge Salomonsen selskapets hjerne, en administrativ hovedserver, som står åpen og vendt ut mot verden.

Dagbladet har kunnet konstatere at serveren inneholder flere tusen dokumenter og filer. Salomonsen bekrefter at det er snakk om svært sensitive kundedata, informasjon om nåværende og tidligere ansatte i Lofotnett og private data tilhørende ansatte i selskapet.

- Dette er et sjokk. Jeg visste virkelig ikke at den sto åpen. Og hvorfor den gjør det er en gåte. Det er jo ingen grunn til at den skal være det, sier Salomonsen.

På avveie

Han frykter serveren kan ha stått ubeskyttet og åpen i flere år uten at noen har merket det.

- Det er jo dokumenter på som ikke skulle ha vært på avveie. Andre kan ha tatt komplett kopi av innholdet som lå der. I forhold til kundene har jeg ikke god tid nå, sier han.

For et selskap som er avhengig av folks tillit, er grove svikt i sikkerheten potensielt ødeleggende.

- Jeg ser for meg at det er kroken på døra for det her firmaet, så alvorlig ser jeg på at den her type informasjon har kommet ut. Men gud fader jeg er glad for at jeg ble gjort oppmerksom på det, slik at jeg kan få berga det som er. Men huff, det her var tøft, sier han.

Søkte politi-hjelp

Dagbladet oppsøkte Lofotnett i august. Under besøket ble serveren midlertidig stengt ned. Sikkerhetshullet er i dag lukket.

Salomonsen har i ettertid gått til politiet i håp om å komme til bunns i hva var årsaken til at sikkerhetshullet i sin tid oppsto. Han frykter sabotasje ligger bak.

Null CTRL

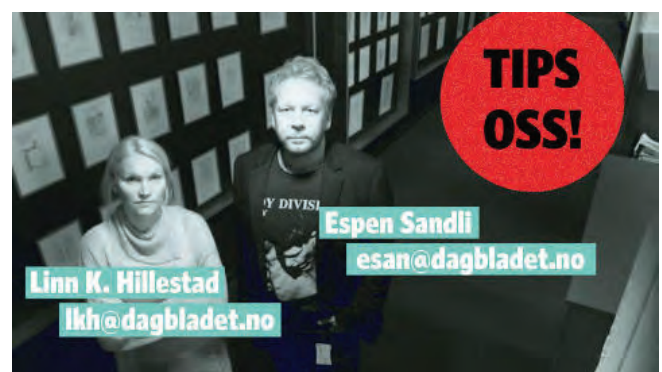
- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

” Jeg ser for meg at det er kroken på døra for det her firmaet, så alvorlig ser jeg på at den her type informasjon har kommet ut. Men gud fader jeg er glad for at jeg ble gjort oppmerksom på det.

Jarl Salomonsen, Lofotnett



SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans kringkastet bilder og lyd rett ut på Internett. Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet



- Jeg lurer jo på hvorfor dette var åpent, når det aldri har vært noe grunn til at det skulle bli åpnet, sier Salomonsen.

Etter Dagbladets besøk varslet han også kundene sine om problemet, og flere valgte å forlate selskapet. Nå frykter han at han må melde opphør til Brønnøysundregistrene.

Bør teste seg selv

Sensitiv forretningsinformasjon på avveie grunnet dårlig eller fraværende datasikkerhet er et større problem enn mange er klar over:

- Vi ser dette ofte når vi kjører sikkerhetstester mot virksomheter. Som oftest skyldes det feilkonfigurasjon eller ansatte som ikke forstår konsekvensen av hva de gjør. Norsis anbefaler derfor alle virksomheter å kjøre en sikkerhetstest fra Internett med jevne mellomrom for å avdekke hva som er tilgjengelig, sier seniorrådgiver Vidar Sandland i Norsk senter for informasjonssikkerhet (Norsis) til Dagbladet.

Dette lå åpent på nettet:

- En IP-adresse tilhørende Lofotnett ga åpen tilgang via en såkalt FTP-server.

- FTP (File Transfer Protocol, *filoverføringsprotokoll*) er en standard protokoll for overføring av filer i et TCP/IP-basert nettverk.

- FTP-serveren lytter på nettverket etter forespørsler. FTP-klienten kobler til serveren og kan lese og skrive til serverens filsystem. Det gir brukerne mulighet til opp- og nedlasting av filer, sletting, redigering av innhold mm.

- I ei mappe på den åpne serveren lå flere Lofotnett-kunders brukernavn og passord.

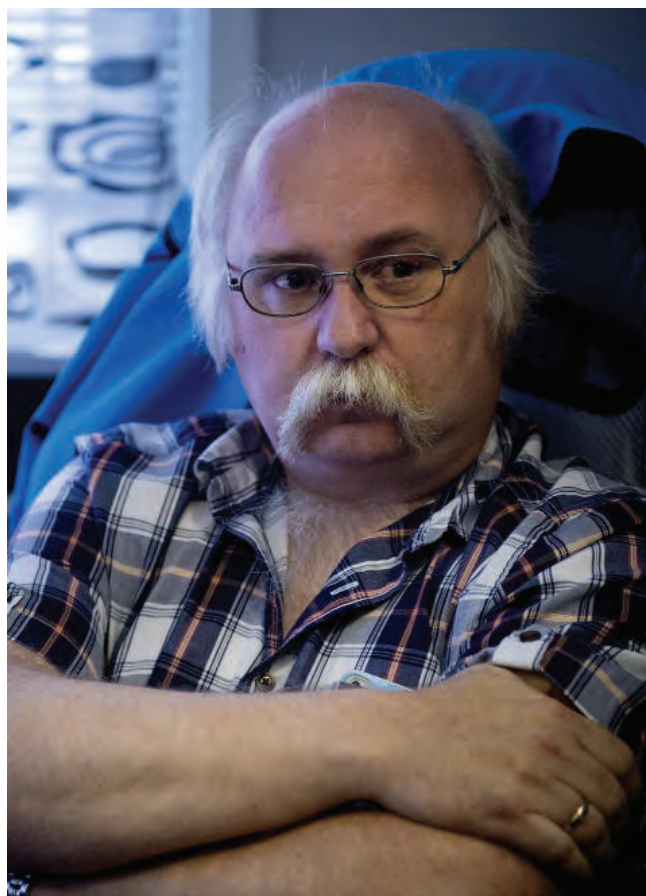
- I tillegg står det brukernavn og passord til flere kunders trådløse nett.

- Serveren inneholdt også forretningshemmeligheter som kundecontrakter, korrespondanse, detaljerte spesifikasjoner fra kunders dataanlegg, salgsbrev og finansielle opplysninger og dokumentasjon fra tvister selskapet har vært i.

- Her lå også private dokumenter og bilder, lønnspapirer, moromateriale og dokumenter fra strategiplaner, kurs og arrangementer.

- Lett tilgjengelig for uvedkommende lå en også komplett backup-lagring av harddisken til en ansatt i selskapet.

- Dette vil det ta tid å rydde opp i. Her kan informasjon være på avveie, sier Salomonsen.



SLUTT: Da Dagbladet besøkte Lofotnetts lokaler på Leknes i slutten av august, opplyste Salomonsen at sikkerhetsbruddet kunne bety kroken på døra for bedriften. Foto: Øistein Norum Monsen/Dagbladet.



Leknes

[Se større kart](#)

BRUKOLLAPS: Tilskuere peker ned på turister som har falt i vannet etter ei nybygd bru kollapset i Lushan Mountain i Kina. Foto: NTB / Scanpix



BENEKTER VOLDTEKT: Den tidligere Frp-politikeren (37) avviser anklagene om at han satte på pornofilm og deretter voldtok den sovende barnevakten. Hendelsene som ble beskrevet i Jæren tingrett mandag fant sted i 2009. En da 21 år gammel mann satt barnevakt mens tiltalte og hans kone var på fest. Ekteparet kom hjem nærmere midnatt. Da kona gikk og la seg, så de to mennene på porno på datamaskinen en liten stund, før de gikk og la seg.

I sin forklaring mandag sa den tiltalte 37-åringen at det var barnevakten som satt på pornoen og at han selv gikk til sengs etter fem-ti minutter. Han står fast på at ingenting mer skjedde og at han sov til klokka 11 dagen etter. Tiltalte har vært sykmeldt siden han ble siktet. Fornærmede vil kreve erstatning og oppreisning. (NTB)

Lurer seg inn din BAKDØR

Ukjent
sårbarhet
i trådløse
nettverk

BAKDØR: Hackere har trolig hatt mulighet til å komme seg inn i D-link-rutere i

Noen av verdens mest populære rutere har en hittil ukjent bakdør som gjør at uvedkommende enkelt kan trenge inn i de trådløse nettverkene og dermed også få tilgang til PC-ene som er koblet til.

En amerikansk sikkerhetsforsker har oppdaget en lite kjent bakdør i flere av D-links rutere, ett av de mest populære merkene på markedet.

Sikkerhetsforskeren, Craig Heffner fra Tactical Network Solutions, publiserte informasjonen om sårbarheten i et blogginnlegg i helga.

I innlegget skriver han at det er mulig å komme forbi innloggingen på ruterne hvis du har tilgang

mange år, ifølge en amerikansk sikkerhetsforsker. D-link undersøker nå påstandene om

gangspunktet sperret fra leverandøren, men mange velger å aktivt skru den på, fordi de da kan fjernadministrere ruterne sin via nettet.

– Dette er noe vi for øyeblikket undersøker, og jeg kan ikke kommentere noe nærmere akkurat nå. Så snart vi vet noe mer, vil vi offentliggjøre en uttalelse, sier pressekontakt Mary Harrison i D-link til Dagbladet om den angivelige bakdøren.

Får uvedkommende tilgang til nettverket, kan de blant annet skru av brannmur og logge seg på alle tilkoblede PC-er.

Flere i Norge

Dagbladet er kjent med at det ligger flere norske D-link-rutere søkbare ute på Internett. Alle disse er modeller som ifølge Craig Heffner er sårbare.

Det eneste som trengs for å få tilgang til disse ruterne uten bru-



til det nettbaserte administrasjonspanelet.

Denne tilgangen er i ut-

Nervøst på børsene i USA

Dagen startet med en betydelig nedgang på børsene på Wall Street i går, i det det bare er fire dager til USA står i fare for å mislikholde gjelden sin.

Etter omtrent en time med handel var industriindeksen Dow Jones ned 73

poeng og 0,5 prosent, til 15.162 poeng. Den bredere S & P 500-indeksen var ned 0,48 prosent til 1.695 poeng. De føderale myndighetene i USA har nå vært stengt i to uker, og hundretusenvise statsansatte er fortsatt permittert. (NTB)



NED-GANG:

Børsene på Wall Street i New York gikk kraftig ned da de åpnet i går. Foto: NTB Scanpix

TUNNEL EVAKUERT:

Ingen personer ble skadd da oljedamp fra en lastebilmotor fylte Frudalstunnelen mellom Sogndal og Fjærland i går. Brannvesenet startet raskt arbeidet med å få klarert tunnelen. Flere brannbiler og ambulanser rykket ut til stedet. (NTB)

FØLG SAKEN

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens webkamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: [#null_CTRL](https://twitter.com/null_CTRL)

den påståtte bakdøra.

kernavn og passord, er å skrive inn «xmlset_rood-kcable-0j28840ybtide» som identifikator til nettleseren. Dersom du leser denne frasen baklengs, ser du at det står: «Edit by Joel 04882 backdoor».

Må oppdateres

– Vi får med jevnlig mellomrom informasjon om rutere med sårbarheter, som kan utnyttes til å få full tilgang til nettverket, sier se-

niorrådgiver Vidar Sandland i Norsk senter for informasjonssikring (NorSIS) til Dagbladet. Dette understreker hvor viktig det er å følge med og oppdatere ruterens sin med jevne mellomrom, påpeker han.

– Så fort D-link gjør tilgjengelig en oppdatering, må man derfor laste inn denne. Alt nett-tilkoblet utstyr må oppdateres og behandles som en PC. Dette gjelder tv-en, ruterens, ja det gjelder

egentlig alt, sier Sandland.

I tillegg anbefaler NorSIS ikke å tillate fjernadministrering av rutere via Internett.

Trolig åpent lenge

– Dette er noe man uansett aldri bør gjøre, fordi ruterens da bare er beskyttet av brukernavn og passord. Hvis dette kommer på avveie, kan uvedkommende konfigurere ruterens som de vil, sier Sandland.

Foto: Sean Gallup / Getty Images

Det er ukjent hvor lenge bakdøra på D-link-ruterne har eksistert, men Craig Heffner skriver i innlegget at den ble omtalt i et russisk hackerforum allerede for tre år siden.

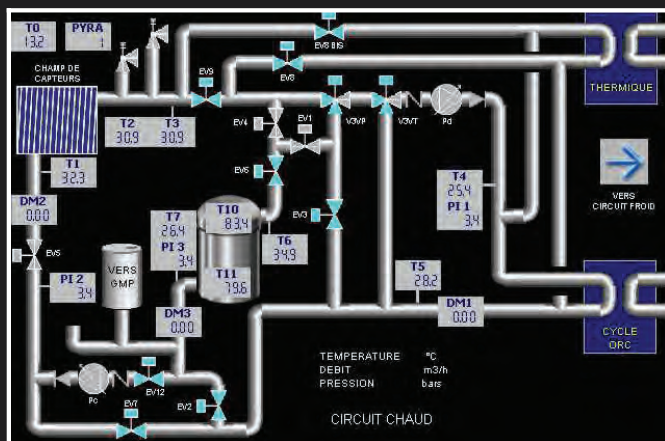
De trådløse nettverkene har derfor trolig vært vidåpne for inntrængere i mange år.

– D-link selges mye på det private markedet. Det som er kinkig for forbrukere, er at de ikke forventer at en ruter er helt åpen når

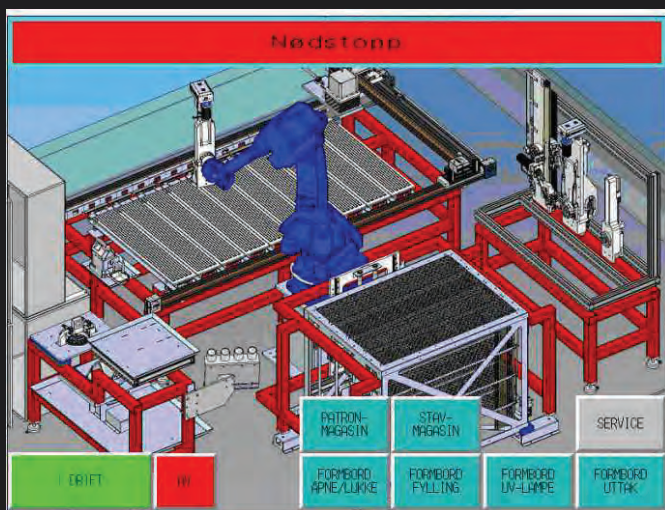


EKSPERT: Vidar Sandland er seniorrådgiver ved NorSIS.

de går og kjøper den i en elektronikkbutikk, og denne svakheten har trolig vært mulig å utnytte i lang tid, sier Vidar Sandland i NorSIS.



KJEMISK: Dette er et fransk anlegg, som har hatt styringspanelet sitt ute på nettet.



PRODUKSJONSANLEGG: Dette panelet styrer produksjonsroboten til et norsk, industrielt selskap.



KAN SKRU AV VARME: Dagbladet fant styringssystemet for varmepumpa i Kvartal 10 utvikling bekrefter at vi kunne skru av varmepumpa, en av to varmekilder i kvartalet.

UTE AV STYL

Dagbladet fant over 2500 styringssystemer på nettet i Norge. Disse brukes blant annet i forsvar, helse, oljebransjen og kollektivtransport.

Har du noen gang tenkt over hvordan vannkraftverk og kraftstasjoner styres og kontrolleres? Eller hva med damanlegg, oljerigger og trafikkløys?

Datasystemene som benyttes kalles «Scada-systemer». De ble tatt i bruk for mange år siden, koster flerfoldige millioner kroner, og oppdateres sjelden.

- Dette er IT-systemer som brukes til å styre alle mulige prosesser, fra oljeutvinning og strømforsyning til busser, jagerfly og skip. Det er et slags nervesystem i samfunnet, og

derfor veldig, veldig viktig, sier forsker Niklas Vilhelm ved Nasjonal sikkerhetsmyndighet (NSM) til Dagbladet.

Over 2500 på nett i Norge

Derfor er det viktig at ikke uvedkommende får kloa i disse systemene. Noe som blir vanskeligere og vanskeligere å forhindre, ettersom disse systemene stadig oftere kobles til Internett, hvor de aldri var ment å være.

Dagbladet har funnet over 2500 slike systemer i Norge, som er koblet til nettet. Noen er beskyttet med brukernavn og passord, andre er like åpne som en hvilken som helst hjemmeside.

Dette gjør dem lett tilgjengelige for hackere og andre ondsinnede aktører.

– Sikkerheten rundt disse systemene er stort sett avhengig av at de er fysisk atskilt fra Internett. Kommer du først inn i ett av disse systemene, er de ofte ikke veldig godt sikret, og du kan gjøre stor



skade, sier seniorrådgiver Vidar Sandland ved Norsk Senter for Informasjonssikring (NorSIS).

- Du kan for eksempel ta kontroll over damanlegg og skape

flommer, ta kontroll over trafikklys og skape trafikkaos, eller ta styring over transportsystemet. I verste tilfelle kan liv gå tapt, sier han.

Av etiske årsaker har ikke Dagbladet hatt mulighet til å undersøke hva som faktisk er mulig å gjøre med flesteparten av de systemene vi har funnet. Vi kan heller ikke utelukke at flere enten er stengt ned eller inaktive.

Men vi har tilsynelatende tilgang på over 500 av disse systemene, som brukes i alt fra forsvar og helse til oljebransjen og kollektivtransport.

Mange har kjente sårbarheter, noe som gjør dem til fristende og enkle mål for hackere.

– Jeg tror de aller fleste ville blitt svært sjokkert over hvor dårlig beskyttet disse systemene er, sier forsker Eireann Leverett ved det internasjonale datasikkerhetsselskapet Ioactive til Dagbladet.

Lite oversikt

Han har kartlagt sikkerheten rundt disse styringssystemene internasjonalt, og mener et av de største problemene med at de er koblet til nett er at det er mulig å



Drammen på nett. Systemansvarlig hos utbygger Union eiendoms- Foto: Øistein Norum Monsen

RING

angripe mange av systemene samtidig.

Det vil også i mange tilfeller være farlig om disse systemene slutter å virke som de skal, supplerer Niklas Vilhelm fra NSM.

Det største problemet med at disse systemene er koblet til nettet, er at ondsinnede mennesker kan få tilgang til dem. Dette kan være alt fra en fremmed stat, til gutterom-sleker som kan føre til ulykker, sier Vilhelm.

Dagbladet har varslet enten eierne eller NSM om de systemene vi har funnet, som vi mener er sårbare. NSM er den offentlige myndigheten som håndterer digitale trusler mot kritisk, norsk infrastruktur. De har imidlertid ingen god oversikt over hvor mange slike systemer som er koblet til nett i Norge.

Jeg skulle ønske vi hadde veldig mye bedre oversikt, fordi veldig ofte er det private bedrifter og organisasjoner som eier infrastrukturen, som vedlikeholder den, og som driver den, og som

FØLG SAKEN

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens webkamera, åpne databasen til konkurrerende bedrifter eller overstyrte vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: www.dagbladet.no/nullctrl/
- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: [#null_CTRL](https://twitter.com/null_CTRL)

derfor sitter med oversikten over hvordan ting henger sammen. Ofte kan dette være underlagt lovverk som hindrer dem i å dele informasjon, sier Vilhelm.



AMERIKANSK KREMATORIUM: Styringssystemet til en krematorieovn i USA lå åpent tilgjengelig på nettet fram til november i fjor. Her fantes også en fil som inneholdt fullstendig logg over kremasjoner.



KNALLTILBUD PÅ CITROEN C1

Vi har fått inn et gunstig parti nyere brukte Citroen C1 med lav km-stand
Kom innom for en prøvetur og velg mellom følgende kampanjetilbud:

KAMPANJE-
RENTE 1,95%*

KR 20.000 I
INNBYTTE**

SERVICE 3 ÅR
/ 30.000 KM

CRÉATIVE TECHNOLOGIE

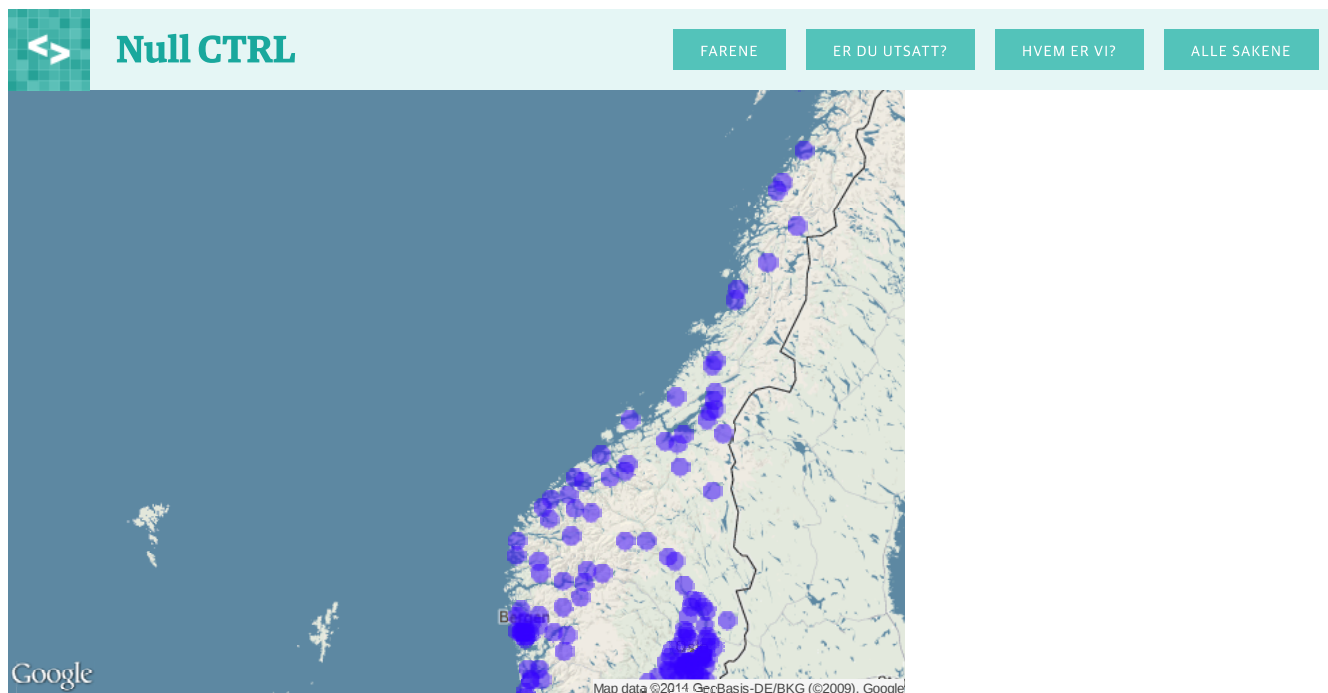


*Kampanjerente 1.95% ved 35 % egenkapital, fastrente i 36 mnd. Deretter følges markedsrente. **Innbyttetilbud forutsetter bil i kjørbart stand, EU ok og årsavgift betalt.

auto elite

AUTO ELITE OSLO AS • GLADENGVEIEN 9 • 0661 OSLO
TELEFON 24 07 41 10 • WWW.AUTOELITE-OSLO.NO

«I verste tilfelle kan liv gå tapt», publisert torsdag 17. oktober 2013 kl. 11:34



NORSKE SYSTEMER PÅ NETT: I dette kartet er styringssystemene Dagbladet har funnet, plottet geografisk etter IP-adresse. Den geografiske plasseringen kan avvike i større eller mindre grad fra det

«I verste tilfelle kan liv gå tapt»

Dagbladet fant over 2500 norske styringssystemer på nett. Disse brukes blant annet i forsvar, helse, oljebransjen og kollektivtransport.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): Har du noen gang tenkt over hvordan vannkraftverk og kraftstasjoner styres og kontrolleres? Eller hva med damanlegg, oljerigger og trafikklys?



Jeg tror de aller fleste ville blitt svært sjokkert over å se hvor dårlig beskyttet disse systemene er.

Eireann Leverett, loactive

Datasystemene som benyttes kalles «Scada-systemer». De ble tatt i bruk for mange år siden, koster flerfoldige millioner kroner og oppdateres sjelden.

- Dette er IT-systemer som brukes til å styre alle mulige prosesser, fra oljeutvinning og strømforsyning til busser, jagerfly og skip. Det er et slags nervesystem i samfunnet, og derfor veldig, veldig viktig, sier forsker Niklas Vilhelm ved Nasjonal sikkerhetsmyndighet (NSM) til Dagbladet.

Over 2500 på nett i Norge

Derfor er det viktig at ikke uvedkommende får kloa i disse systemene. Noe som blir

vanskeligere og vanskeligere å forhindre ettersom systemene stadig oftere kobles til Internett, hvor de aldri var ment å være.

I forbindelse med

[artikkelserien «Null CTRL»](#), har **Dagbladet** funnet over 2500 slike systemer i Norge koblet til Internett. Noen er beskyttet med brukernavn og passord, andre er like åpne som en hvilken som helst hjemmeside.

Dette gjør styringssystemene lett tilgjengelige for hackere og ondsinnede aktører.

- Sikkerheten rundt disse systemene er stort sett avhengig av at de er fysisk adskilt fra Internett. Kommer du først inn i ett av disse systemene, er de ofte ikke veldig godt sikret, og du kan gjøre stor skade, sier seniorrådgiver Vidar Sandland ved Norsk Senter for Informasjonssikring (Norsis).

- Du kan for eksempel ta kontroll over damanlegg og skape flommer, ta kontroll over trafikklys og skape trafikkaos, eller ta styring over transportsystemet. I verste tilfelle kan liv gå tapt, sier han.

Helse og forsvar

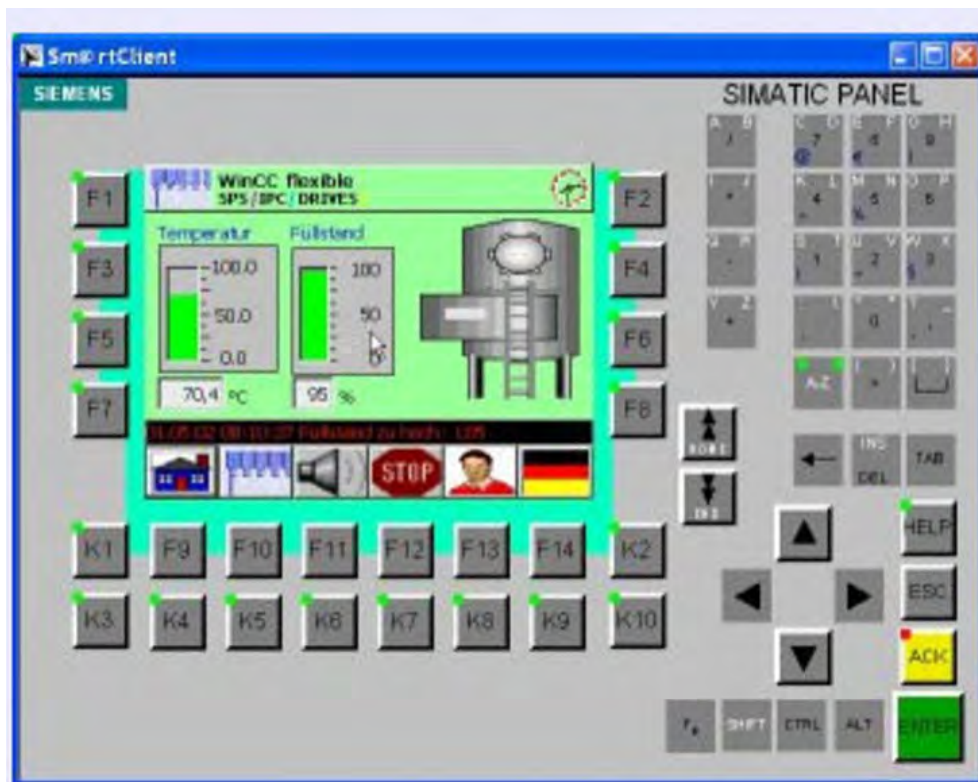
Av etiske årsaker har ikke Dagbladet undersøkt hva som faktisk er mulig å gjøre med flesteparten av de systemene vi har funnet. Slike systemer skal man rett og slett ikke tukle med. Å gjøre det, kan få uante og i verste fall katastrofale konsekvenser. I mange tilfeller vet vi heller ikke hvem som er eieren. Vi kan derfor ikke utelukke at flere av systemene vi har funnet er inaktive.

Men av de over 2500 systemene vi har funnet, har vi tilsynelatende tilgang på over 500.

Dette er styringssystemer som brukes i alt fra forsvar og helse til oljebransjen og i kollektivtransport.

Mange har i tillegg kjente sårbarheter, noe som gjør dem til fristende og enkle mål for hackere.

- Jeg tror de aller fleste ville blitt svært sjokkert over hvor dårlig beskyttet disse systemene er, sier forsker Eireann Leverett ved det internasjonale datasikkerhetsselskapet Iactive til Dagbladet.



BIOBRENSEL: Dette styringssystemet tilhører et norsk biobrenselanlegg.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL



AMERIKANSK KREMATORIUM: Styringssystemet til en krematorieovn i USA lå åpent tilgjengelig på nettet fram til

Kan angripe flere

Leverett har selv [kartlagt sikkerheten rundt slike styringssystemer internasjonalt](#). Resultatet skremte ham.

- Jeg var blitt fortalt gjentatte ganger at det ikke var noen problemer med sikkerheten rundt disse systemene, fordi de ikke var koblet til Internett i det hele tatt. Jeg ville vise at dette var feil, sier Leverett.

Han mener et av hovedproblemene med at disse systemene er koblet til nettet, er at det er mulig å sabotere for eksempel et damanlegg uten å være fysisk til stede.

- I tillegg kan du angripe mange av disse systemene samtidig hvis du perfektionerer et angrep mot programvaren deres, sier han.

Lite oversikt

Det vil også i mange tilfeller være farlig om disse systemene slutter å virke som de skal, supplerer Niklas Vilhelm fra NSM.

- Det største problemet med at disse systemene er koblet til nettet, er at ondsinnede mennesker kan få tilgang til dem. Dette kan være alt fra en fremmed stat til gutteromsleker som kan føre til ulykker, sier Vilhelm.

NSM, som er den offentlige myndigheten som håndterer digitale trusler mot kritisk, norsk infrastruktur, har ingen god oversikt over hvor mange slike systemer som er koblet til nett i Norge.

- Jeg skulle ønske vi hadde veldig mye bedre oversikt, fordi veldig ofte er det private bedrifter og organisasjoner som eier infrastrukturen, som vedlikeholder den og som driver den, og som derfor sitter med oversikten over hvordan ting henger sammen. Ofte kan dette være underlagt lovverk som hindrer dem i å dele informasjon, sier Vilhelm.

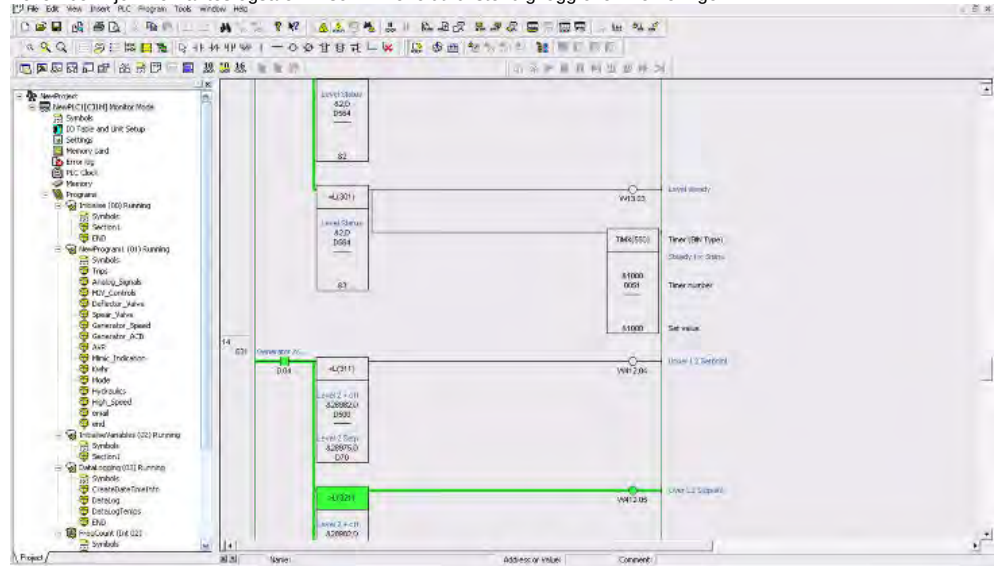
Fersk problematikk

Dagbladet har for en tid tilbake varslet henholdsvis eierne eller Nasjonal sikkerhetsmyndighet (NSM) om systemene vi har funnet, og som vi oppfatter potensielt kan være sårbare.

Første gang NSM ble varslet om åpne Scada-systemer i Norge, var for to år siden. Da fikk de ei liste over 38 potensielt sårbare systemer fra amerikanske sikkerhetsmyndigheter. Ikke noe av dette var nasjonal, kritisk infrastruktur.

- Siden 2011 har vi fått en håndfull varsler om åpne Scada-systemer på nett i Norge. Disse varslene håndterer vi ved å ta kontakt med internettleverandør og be dem varsle kunden, sier leder Marie Moe ved NSMs operasjonssenter.

november i fjor. Her fantes også en fil som inneholdt fullstendig logg over kremeringer.



HELT UBESKYTTET: Dette styringssystemet til et britisk vannkraftverk, som lå tilgjengelig for alle, uten passordbeskyttelse.

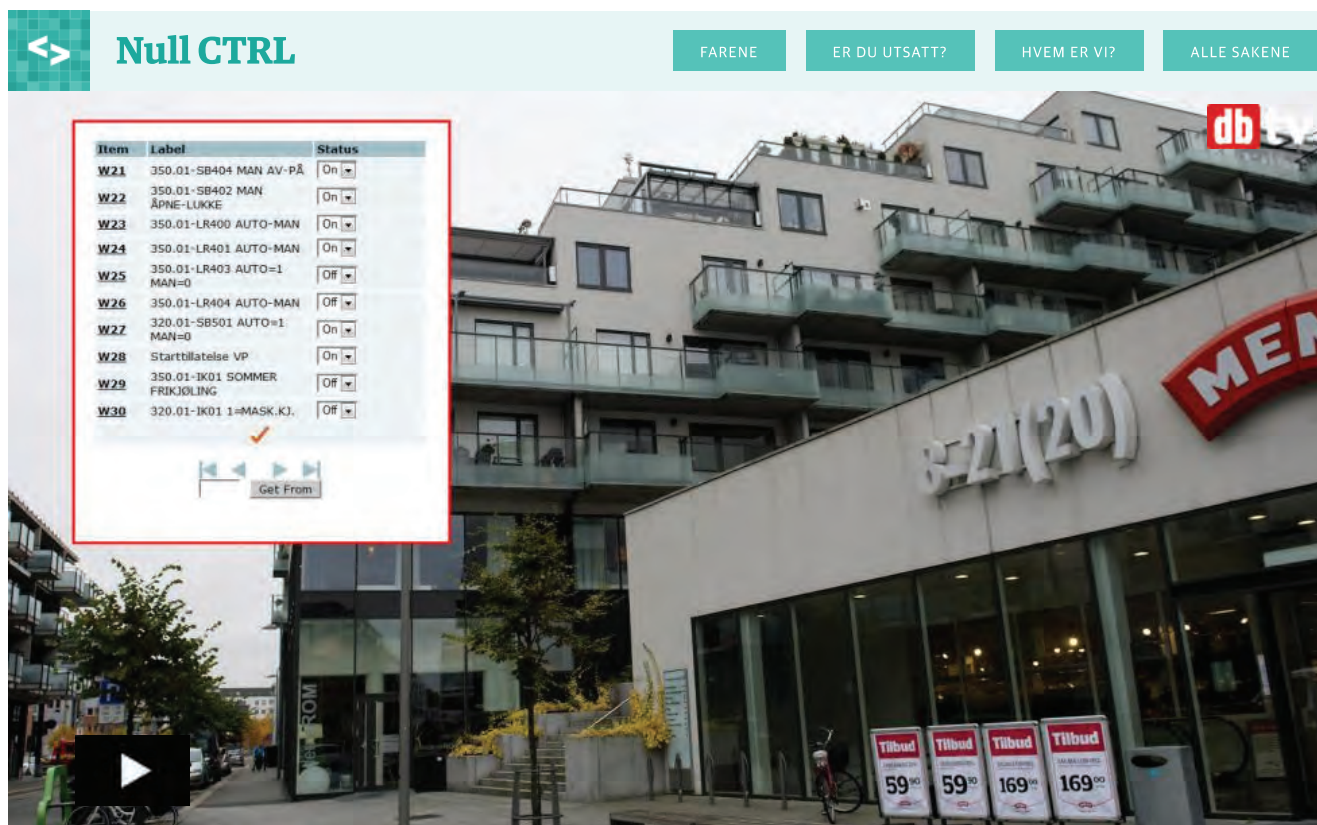


VIKTIGE SYSTEMER: Styringssystemer brukes i alle mulige prosesser, og er derfor som et slags nervesystem i samfunnet, ifølge forsker Niklas Vilhelm ved Nasjonal sikkerhetsmyndighet. Foto: Øistein Norum Monsen / Dagbladet



- **DÅRLIG SIKRET:** - Jeg tror de aller fleste ville blitt svært sjokkert over hvor dårlig beskyttet disse systemene er, sier forsker Eireann Leverett ved det internasjonale datasikkerhetsselskapet Ioactive. Foto: Espen Sandli / Dagbladet

Her kunne Dagbladet skru av varmen i hele kvartalet, publisert torsdag 17. oktober 2013 kl. 17:23



KAN SKRU AV VARME: Denne videoen viser hvordan Dagbladet får tilgang til et system for styring av varme, uten å taste brukernavn eller passord. Styringspanelet fant vi på nett. Video: Dagbladet

Her kunne Dagbladet skru av varmen i hele kvartalet

Styringspanelet fant vi åpent tilgjengelig på Internett.



LINN KONGSLØ HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

DRAMMEN/VIK (Dagbladet): En rekke søk foretatt av Dagbladet viser at over 2500 styringssystemer ligger [koblet til nett i Norge](#).

Disse systemene brukes blant annet i forsvar, helse, oljebransjen og kollektivtransport.

- Det er et slags nervesystem i samfunnet, og derfor veldig, veldig viktig, sier forsker Niklas Vilhelm ved Nasjonal sikkerhetsmyndighet (NSM) til Dagbladet.

Men det at uvedkommende kan få tilgang til slike systemer, kan også ramme deg og meg i hverdagen.



Kan skru av varme

Ett av systemene Dagbladet har funnet styrer varmepumpa for

- **TAFATTE:** Tidligere Datatilsynet-direktør Georg Apenes refser den påtroppende regjeringen for å ikke snakke om datasikkerhet. Video: John Terje Pedersen / Dagbladet

Null CTRL

Kvartal 10 i Drammen, som huser alt fra treningssenter og matbutikk til boliger og en parkeringskjeller.

Uten å taste verken brukernavn eller passord, fikk vi tilgang til det nettbaserte styringspanelet. Her var det mulig å endre statusen på 30 forskjellige knapper.

Vi viste en video av dette til systemansvarlig ved Union eiendomsutvikling, som er byggherre for kvartalet. Han ønsker ikke å stille til intervju med Dagbladet, men bekrefter at knappene styrer flere ulike komponenter ved en varmepumpe. Dette er en av to varmekilder i kvartalet.

Alvorlig

Niklas Vilhelm ved NSM mener det kan være alvorlig for den enkelte at slike systemer ligger tilgjengelige på nettet, selv om dette ikke nødvendigvis har noen store samfunnsmessige konsekvenser.

- Min umiddelbare bekymring er hvis det bor gamle og syke mennesker rundt omkring, og noen tar varmen midtvinters, kunne det potensielt ha fått veldig alvorlige følger. Så det er en situasjon vi virkelig ikke ønsker, og oppfordringen må være å skaffe nok oppmerksomhet rundt det, sier han.

Systemansvarlig ved Union eiendomsutvikling avdramatiserer dette.

- Dere kunne ha slått av varmepumpa, men det hadde ikke vært noe farlig. Hvis dere hadde skrudd av varmen en bitende kald fredag ettermiddag, hadde jeg fått vite det lørdag morgen, sier han, men uttrykker samtidig bekymring over å få vite at dette har ligget åpent.

Rystet

Deres er bare ett av varmesystemene Dagbladet har funnet tilgjengelig på nett, hvorav noen tilhører helseinstitusjoner og kjøleanlegg. Et annet tilhører leilighetsbygget Trekanten på Vik i Buskerud.

Dagbladet viste systemet til lederen i sameiet i Trekanten, Sven Alexander.

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL



ENKELT TERRORMÅL: Ledelsen ved fiskebollefabrikken på Sortland tror det ville vært enkelt å sabotere etter at fabrikkens beredskapsplaner lå åpent på nett via en 110-sentral. Video: Øistein Norum Monsen / Dagbladet.



SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans kringkastet bilder og lyd rett ut på Internett. Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet

- Først forsto jeg ikke hva det dreide seg om, men jeg ble litt rystet over at hele styringssystemet og avlesningssystemet for varmeanlegget her lå helt åpent for hvem som helst å titte på. Det ante jeg ikke, så det var litt skremmende, sier han.

- Ikke ønskelig

Det er Ringeriks-Kraft som eier varmeanlegget, og direktør Live Dokka sier at hun ikke var klar over at systemet var så tilgjengelig.

- Det er ikke ønskelig på noe som helst vis at dette skal ligge åpent, sier hun.



IKKE ØNSKELIG: Forsker Niklas Vilhelm ved Nasjonal Sikkerhetsmyndighet sier det potensielt kan få alvorlige følger for den enkelte at slike systemer ligger tilgjengelig på Internet. Foto: Øistein Norum Monsen/Dagbladet.

Etter å ha undersøkt saken med sine leverandører, skriver Dokka i en SMS til Dagbladet at det vil bli gjort noen sikkerhetsmessige endringer.

«Så da skal saken være ivarettatt. Takk for at vi ble gjort oppmerksomme på sikkerhetshullet.»

Dagbladet har også vært i kontakt med selskapet Trend Control Systems i Danmark, leverandør av noen av disse systemene til Norge, og sendt dem skjermbilde av ett av de usikrede systemene.

Kan ødelegges

Administrerende direktør Arman Saeidnia svarer følgende til dette på e-post:

- Fjerntilgang til bygnings-kontrollsystemer er ikke uvanlig. Trend har alltid anbefalt at de som selger og konfigurerer vårt utstyr, setter dem opp på en sikker måte bak en brannmur eller på et virtuelt, privat nettverk for å hindre uautorisert tilgang.

Niklas Vilhelm ved NSM påpeker at tilfeldige kommandoer i nettbaserte paneler muligens kan få styringssystemer til å slutte å virke.

- Det vil variere fra system til system. Det vil i alle tilfeller være mulig å slå dem av, sier han.



Tips oss på nullctrl@dagbladet.no



LAGET GIGANTISK «TOGSETT»: En 14 år gammel gutt skapte kaos da i byen Lodz etter at han fikk kontroll over styringssystemet til byens trikker. Foto: Europics / All Over Press

14-åring fjernstyrte trikker, fire sporet av og 12 personer ble såret

Internasjonale skandaler viser konsekvensene av at industrielle styringssystemer er koblet til Internett.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

CAMBRIDGE/OSLO (Dagbladet):
Dagbladet har avdekket hvordan
over 2500 norske styringssystemer
er [koblet til nett - med liten eller
ingen sikkerhet](#).

Og når systemer som brukes til å
styre kraftverk, oljerigger, offentlig
transport og annen kritisk
infrastruktur kobles til Internett, kan
disse fort falle i hendene på
uvedkommende.

Internasjonale erfaringer viser at
dette kan få store konsekvenser.

- Jeg tror de aller fleste ville blitt
svært sjokkert over å se hva slags
tilstand disse systemene er i, og
hvor dårlig beskyttet de kan være,
sier Eireann Leverett ved det
internasjonale



ENKELT TERRORMÅL: Ledelsen ved fiskebollefabrikken på Sortland tror det ville vært enkelt å sabotere etter at
fabrikkens beredskapsplaner lå åpent på nett via en 110-sentral. Video: Øistein Norum Monsen / Dagbladet

datasikkerhetsselskapet Iactive til Dagbladet.

14-åring styrte trikker

En hendelse i Polen i 2003 gir et bilde av hvor galt det kan gå. Da tok en 14 år gammel gutt kontroll over et trikkesystem i byen Lodz, og brukte trikkene som et slags gigantisk, virkelig «togsett».

14-åringen hadde studert trikkene og trikkesporene i lengre tid og deretter bygget et apparat som så ut som en tv-kontroll.

Denne brukte han så til å styre trikkene, noe som skapte fullt kaos i den polske byen. Til sammen fire trikker sporet av og 12 personer ble skadd, ifølge [Daily Telegraph](#).

- Dette viser at potensialet er at selv mennesker uten teknisk utdannelse og masse ressurser kan lage en del skade. Det er derfor viktig å sikre disse systemene så ikke uautoriserte får tilgang, sier forsker Niklas Vilhelm ved Nasjonal Sikkerhetsmyndighet (NSM) til Dagbladet.

Stengte telenettet

Hendelsen i Polen var ikke første gang en tenåring med datakunnskaper har skapt problemer.

Så tidlig som i 1997 klarte en tenåring ved hjelp av sin private PC å stenge ned deler av telefonnettverket i Worcester i Massachusetts.

Han skal samtidig ha klart å avskjære kommunikasjonssystemene som kontrollerte flytrafikken på den lokale flyplassen, ifølge [Washington Post](#).

Bruker standardpassord

De siste åra har hackere stadig oftere klart å få kontroll over slike systemer. Ofte er det ikke spesielt mye datakunnskap disse «hackerne» har. Ofte gjetter de bare riktig på et svært enkelt passord.

I fjor fikk amerikanske sikkerhetsmyndigheter inn meldinger om [198 hendelser som involverte kritisk infrastruktur](#), 65 prosent mer enn i 2011.

En av hendelsene som fikk mye omtale sistnevnte år, var da en mann i 20-åra tok seg inn i styringssystemet til et kloakkanlegg i Houston i USA - ved bruk av et standardpassord på tre karakterer, som sto oppført i brukermanualen.

Han gjorde imidlertid ingen skade på anlegget, fordi målet var å vise hvor sårbare disse systemene er.

- Dette krevde nesten ingen kunnskap, og kunne blitt utført av en to-åring med litt kjennskap til systemet, skrev han i en e-post til [Houston Chronicle](#) like etter.

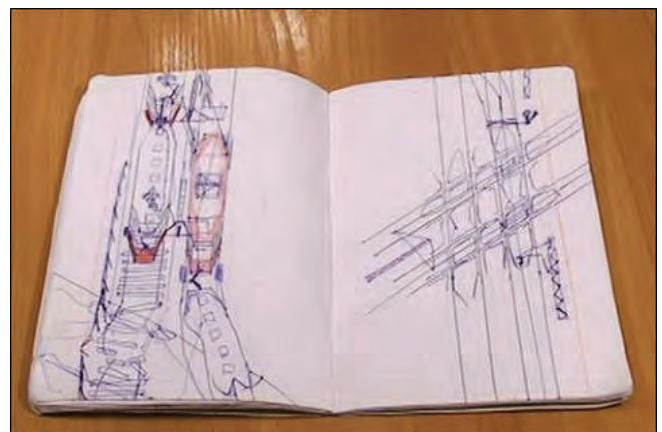
Hevngjerrige jobbsøkere

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyrte vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



IKKE BESKYTTET: Asbjørn Korsfjord fra Moss var ikke klar over at overvåkingskameraet hans lå åpent på Internett. Video: Øistein Norum Monsen / Dagbladet



PLANLA NØYE: 14-åringen som skapte kaos i Polen, hadde studert trikkene og trikkesystemene nøye før han slo til. Foto: Europics / All Over Press



TIDLIG ANGREPET: Det russiske energiselskapet Gazprom ble utsatt for et

Tidligere har også forsmådde jobbsøkere og eks-ansatte brukt kritiske kontrollsystemer for å gjøre skade.

Verst gikk det kanskje i Australia i 2000, da rådgiver Vitek Boden i et australsk teknologifirma var bitter fordi han ikke fikk jobb hos lokalmyndighetene i et fylke på østkysten.

Han tok seg derfor inn i kontrollsystemene til kloakken i Queensland ved bruk av en radiosender, og slapp ut flere hundre tusen liter kloakk i lokale bekker og parker. Mye av dyrelivet døde ut som følge av dette, og stanken fra utslippet var uutholdelig for innbyggerne, skriver [Washington Post](#).

Vannkraftverk

I tillegg er dette noen av systemene funnet på nett som har vakt internasjonal oppsikt:

- En partikkelakselerator ved universitetet Berkley i USA.
- Et vannkraftverk i Frankrike
- Vannpumpene til de nederlandske dikene.
- Et glukoseovervåkingssystem på et sykehus i USA
- Flere sensorer for rørledninger

Strømbrydd i flere byer

CIA har også informasjon om at dataangrep har forstyrret kraftforsyninger i en rekke regioner utenfor USA, og at disse forstyrrelsene i minst ett tilfelle førte til et strømbrydd som rammet flere byer, ifølge [amerikanske sikkerhetsmyndigheter](#).

Den store frykten er nå at terrorister, ondsinnede hackere eller andre lands myndigheter angriper kritiske systemer koblet til nett.

Historisk sett er det ofte virus som er brukt i angrep på denne type systemer.

Allerede i 1999 ble det russiske energiselskapet Gazprom utsatt for et angrep på ett av deres kontrollsystemer, ved at hackere ga en insider i selskapet en såkalt trojansk hest, et datavirus som ofte inneholder spionprogramvare.

Kontrollerte gassrør

Da vedkommende hadde åpnet viruset, kunne hackerne infiltrere systemene som kontrollerte gassflyten i gassrørene. I flere timer hadde de kontroll over det sentrale systemet, men motivene deres er ikke kjent.

Samme år brøt en gruppe hackere seg inn i systemene som kontrollerte Skynet, en britisk militærsatelitt, og endret sikkerhetsinnstillinger.

I 2003 skapte dataviruset SoBig [store problemer for den amerikanske togtrafikken](#), da et signalsystem ble angrepet. Dette førte til store forsinkelser og flere kanselleringer.

Oljeplattformer stengt ned

Året etter ble flere oljeplattformer satt ut av spill i to dager som følge av dataormen Sasser, ifølge [amerikanske sikkerhetsmyndigheter](#), mens 13 av Daimler-Chryslers fabrikker ble stengt ned i bortimot en time i 2005 på grunn av en dataorm. Dette kostet selskapet anslagsvis 14 millioner dollar (over 80 millioner kroner med dagens kurs).

Også virusangrepene kan være tilfeldige.

I 2006, for eksempel, tok hackere seg inn i datasystemet til et renseanlegg for drikkevann i Harrisburg i USA ved å installere et spionprogram på laptopen til en ansatt. Hackerne befant seg utenfor USAs grenser og visste angivelig ikke at de hadde angrepet et renseanlegg.

Trolig var de bare ute etter en pc de kunne bruke til å sende ut spam.

dataangrep allerede i 1999. Foto: Maxim Shemetov / Reuters / NTB scanpix



ANGREP IRAN: Stuxnet er det hittil aller mest kjente angrepet på et industrielt kontrollsystem. Israel og USA mistenkes å stå bak dataormen, som angrep Irans atomsystem. Foto: Presidential official website / Reuters / NTB scanpix



TAPTE OVER 80 MILLIONER: I 2005 ble 13 av Daimler-Chryslers fabrikker stengt ned på grunn av et dataangrep. Dette kostet selskapet over 80 millioner kroner. Foto: Mike Segar / Reuters / NTB scanpix



Tips oss på nullctrl@dagbladet.no

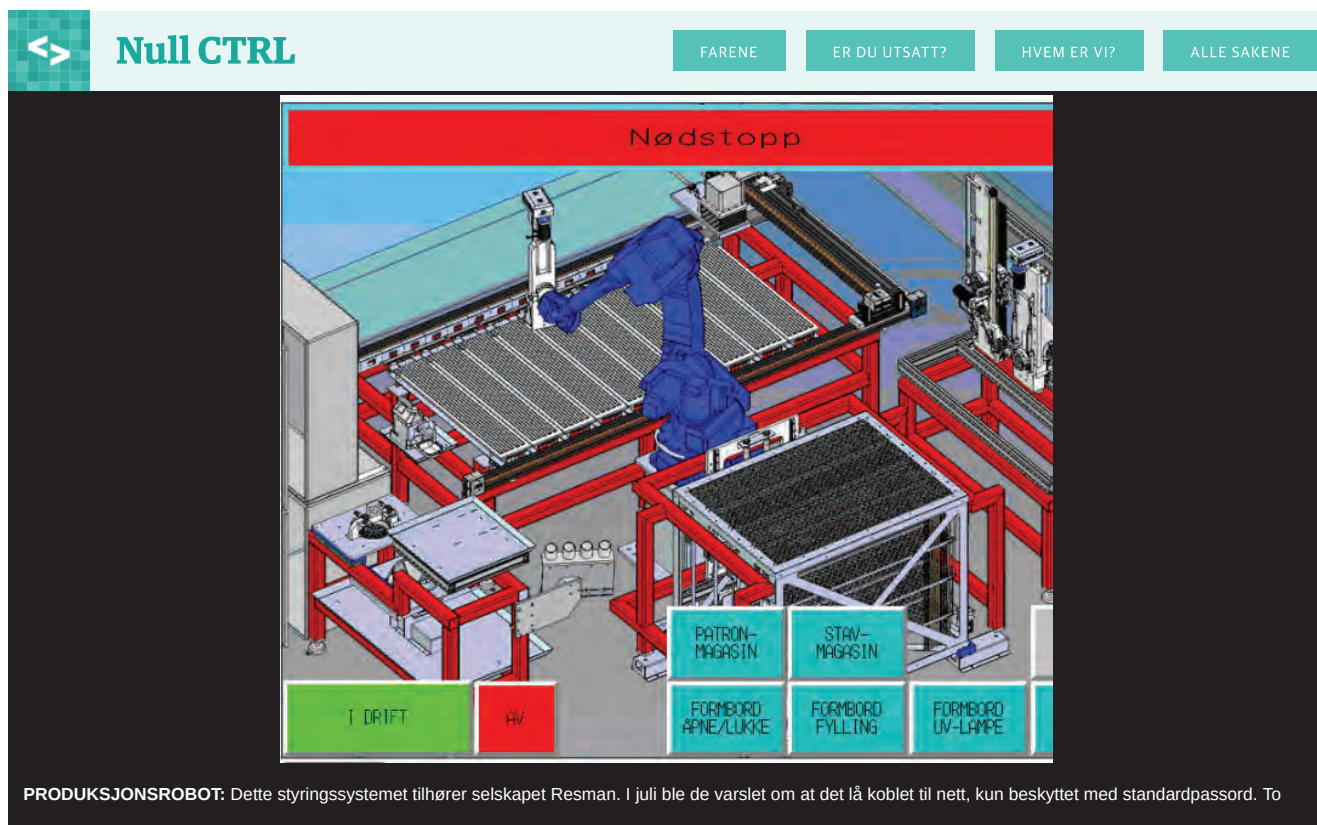
Angrep atomprogram

Det aller mest kjente virusangrepet var sannsynligvis planlagt ned til minste detalj: I 2009 angrep dataormen Stuxnet Irans atomprogram.

Ormen ble plantet i det iranske atomutviklingsprogrammet, hvor den angrep et Siemens-system og klarte å forsinke landets utvikling av atomvåpen.

Seinere spredte den seg også til andre maskiner.

Angrepet gjorde at verden fikk øynene opp for datasikkerhet og kritisk infrastruktur. Mange spør seg imidlertid fortsatt om problemet tas nok på alvor.



Dette systemet styrer produksjonsroboten til et Statoil-selskap

Ble varslet om minimal beskyttelse allerede i juli, men ingenting ble gjort.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): Dagbladet har funnet [over 2500 norske styringssystemer koblet til Internett](#), med liten eller ingen beskyttelse. Disse systemene brukes blant annet i forsvar, helse, oljebransjen og kollektivtransport, men også i private boliger.

Vi kom blant annet inn på [styringspanelet for varmpumpa til et kvartal i Drammen](#) uten å taste brukernavn eller passord.

Andre slike systemer er ofte bare beskyttet med det brukernavnet og passordet som er utlevert fra leverandøren.

- Kjent problem

Disse passordene er enkle å spore opp på nettet.

- Bruken av standardpassord er et veldig kjent problem, og det er et

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

stort problem og det har vært det lenge, sier forsker Niklas Vilhelm ved Nasjonal sikkerhetsmyndighet (NSM).

- Folk er forventet å skifte brukernavn og passord for å gi disse enhetene bedre sikkerhet, og det glemmes ofte at det kan være et alvorlig problem om dette ikke gjøres, sier han.

Produksjonsrobot

Dagbladet har ikke testet noen passord i vår [gransking av norsk datasikkerhet](#), men i forbindelse med artikkelserien har vi fått tilsendt skjermbilder av et styringspanel som tilhører det norske selskapet Resman.

Resman er eid av blant andre

Statoil Venture, og produserer blant annet analyseceller for oljebrønner. Det aktuelle styringssystemet kontrollerer en produksjonsrobot.

Etter det Dagbladet får opplyst, har dette styringssystemet kun vært beskyttet med standard brukernavn og passord.

Ble varslet

Dagbladet har også fått tilgang til en e-post hvor det framgår at selskapet ble varslet om dette problemet allerede i juli.

«Vil gjerne gjøre dere oppmerksom på at webinterfacet til operatørpanelet på deres robotanlegg ligger fritt tilgjengelig rett ut på nettet, med standard passord ... Dvs, det kan i teorien betjenes av hvem som helst», står det blant annet i e-posten som ble sendt til selskapet.

Likevel ble ingenting gjort, ifølge Dagbladets kilde.

«Ingen kommentar»

Dagbladet sendte selskapet e-posten på nytt for noen dager siden, med skjermbilder og lenke til systemet. Etter gjentatte forespørsler, har vi imidlertid ikke fått svar på ytterligere spørsmål.

Produksjonsleder Roger Heggglund i Resman skriver følgende i en tekstmelding:

«Hei. Har fått e-mailen og takker for opplysningen. Har ingen ytterligere kommentarer.»

Dagbladet har sett systemets innloggingsside, og etter vår henvendelse er den nå fjernet fra nettet.

Informasjonsdirektør Jannik Lindbæk jr i Statoil opplyser i en e-post til Dagbladet at deres teknikere har analysert IP-adressen, og ikke kjenner til driften av dette systemet.



KAN SKRU AV VARME: Denne videoen viser hvordan Dagbladet får tilgang til et system for styring av varme, uten å taste brukernavn eller passord. Styringspanelet fant vi på nett. Video: Dagbladet



Tips oss på nullctrl@dagbladet.no

– Det er ikke et spørsmål **OM**, men **NÅR** vi blir angrepet

ØKENDE TRUSLER: Generalmajor Roar Sundseth er sjef for Cyberforsvaret. De ser en stadig økning i digitale trusler mot Norge.

Den digitale trusselen mot Norge er stor og økende, mener sjefen for Cyberforsvaret. Antall nettangrep er trolig omfattet av store mørketall.

Tekst: **Espen Sandli**
esan@dagbladet.no
Linn Kongsli Hillestad
lkh@dagbladet.no

Ubeskyttede overvåkingskameraer, vidåpne servere med beredskapsdokumenter og styringssystemer som brukes i alt fra forsvar og helse til oljebransjen og kollektivtransport.

Alt dette ligger tilgjengelig på Internett, har Dagbladet avdekket de siste ukene.

Samtidig øker den digitale trusselen mot Norge, ifølge offentlige instanser.

– Trusselen er stor, og den er økende, sier generalmajor Roar Sundseth, sjef for Cyberforsvaret.

Frykter nasjonalstater

Mens kriminelle aktører står bak størsteparten av den illegale aktiviteten på nettet, er det nasjonalsta-

ter som representerer den mest alvorlige trusselen mot forsvarets systemer, og som forsvaret frykter mest.

– Det er bare nasjonalstatene som har ressurser til å kunne planlegge store angrep, gjennomføre dem og analysere dem etterpå. Så det er den trusselen vi fokuserer på, sier Sundseth.

Omfattende

På den andre siden er digitale farer et omfattende spørsmål, påpeker han.

– Man kan jo bare forestille seg hvis befolkningen mister tilliten til bankvesenet, og det blir umulig å få tatt ut penger, eller noen klarer å gjøre noe

med kraftforsyningen, oljeindustrien eller energisektoren.

Et slikt angrep mot norsk infrastruktur kan heller ikke utelukkes, mener sjefen for Cyberforsvaret.

– Nå har vi ikke sett såne omfattende angrep ennå, verken i Norge eller særlig mange andre land. Men muligheten er der, og skal man være pessimistisk, vil jeg si at det ikke er et spørsmål om vi blir utsatt for et sånt angrep, det er et spørsmål om når.

– Så dere er bekymret for muligheten?

– Nå vil jeg si at jeg er ikke bekymret av natur, men det er en veldig god grunn til å være oppmerksom på muligheten for den type angrep og gjøre det

vi kan for å sikre oss.

Cyberforsvaret samarbeider tett med Nasjonal sikkerhetsmyndighet (NSM), som har ansvaret for digitale trusler mot kritisk, norsk infrastruktur.

Store mørketall

De håndterer mellom to og tre «alvorlige hendelser» i måneden, det vil si infiltrasjonsforsøk eller vellykket kompromittering av systemer som er en del av nasjonal infrastruktur.

Da Dagbladet var til stede i NSMs lokaler, måtte intervjuet avbrytes fordi det gikk en alarm om en hendelse knyttet til statlig infrastruktur. Dette viste seg seinere å ikke være så alvorlig som antatt.



FØLG SAKEN

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens webkamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: www.dagbladet.no/nullctrl/
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: [#null_CTRL](https://twitter.com/null_CTRL)

– Hittil i år har vi behandlet 12 000 saker i vårt saksbehandlingssystem. Det vil si at vi får inn mellom 40 og 50 nye saker hver dag. Vi har hatt 24 alvorlige hendelser hittil i år, sier leder for NSMs operasjonssenter, Marie Moe.

De er mest bekymret for antall alvorlige hendelser som ikke blir oppdaget.

– Vi tror det er store mørketall, og er bekymret for at man ikke gjør nok for å beskytte seg mot denne trusselen, sier Moe.

– Må innrette oss

Hvis forsvaret blir utsatt for et inntrengningsforsøk i sine nett, jobber de med å rette feilene og komme



MØRKETALL: Seksjonssjef Marie Moe ved Nasjonal sikkerhetsmyndighet.

tilbake til en normalsituasjon så raskt som mulig.

– Det samme burde jo gjelde for alle andre typer systemer, sier



Dagbladet i går.

Sundseth i Cyberforsvaret.

Forsvarets graderte systemer er imidlertid ikke koblet mot nettet, og er dermed bedre beskyttet enn

Foto: Øistein Norum Monsen

mye annet. Samtidig underslår ikke Sundseth at det er mulig å koble seg fysisk og prøve å komme inn.

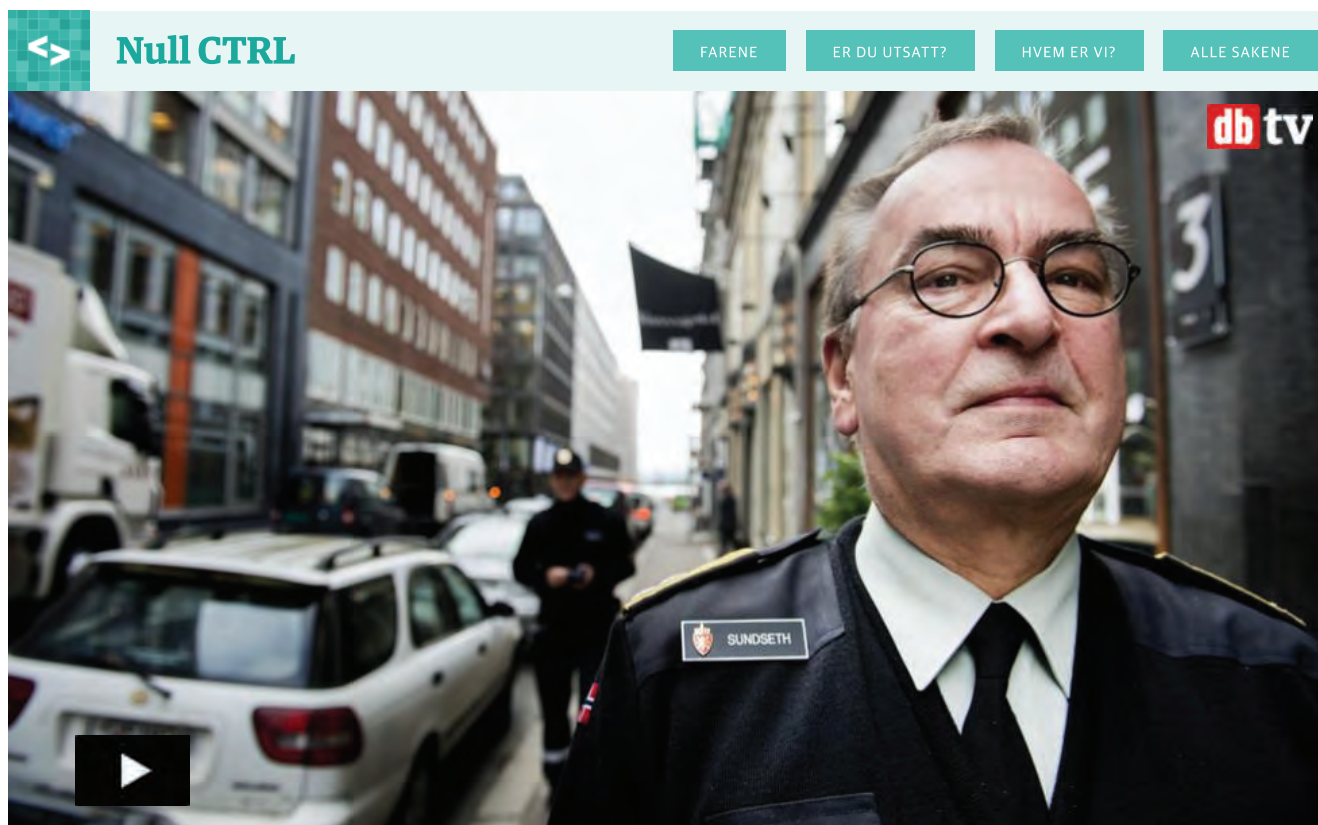
– Men som jeg har sagt også i andre sammenhenger, har ikke jeg noen tro på at Norge i nær framtid vil oppleve det jeg kaller et digitalt 9. april, hvor en annen nasjon går til et digitalt angrep mot Norge og sånn sett tar ned våre viktige samfunnssystemer, sier Sundseth.

– Men man vet jo aldri, det er vanskelig å spå om framtida. Vi må i hvert fall kontinuerlig analysere trusselbildet og innrette oss i forhold til det vi ser og det vi tror kommer til å skje.

Se også kommentar side 67



- Det ikke er et spørsmål om vi blir utsatt for et sånt angrep, det er et spørsmål om når, publisert fredag 18.



ØKENDE TRUSLER: Generalmajor Roar Sundseth er sjef for Cyberforsvaret. De ser en stadig økning i digitale trusler mot Norge. Video: Øistein Norum Monsen / Dagbladet

- Det ikke er et spørsmål *om* vi blir utsatt for et sånt angrep, det er et spørsmål om *når*

Den digitale trusselen mot Norge er økende, mener sjefen for Cyberforsvaret.



LINN KONGSLIE HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): [Ubeskyttede overvåkingskameraer](#), vidåpne servere med [beredskapsdokumenter](#) og [styringssystemer](#) som brukes i alt fra forsvar og helse til oljebransjen og kollektivtransport.

Alt dette ligger tilgjengelig på Internett, [har Dagbladet avdekket de siste ukene](#).

Samtidig øker den digitale trusselen mot Norge, ifølge offentlige instanser.

- Trusselen er stor, og den er økende, sier generalmajor Roar Sundseth, sjef for Cyberforsvaret.

Frykter nasjonalstater

Mens kriminelle aktører står bak størsteparten av den illegale

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

aktiviteten på nettet, er det nasjonalstater som representerer den mest alvorlige trusselen mot forsvarets systemer, og som forsvaret frykter mest.

- Det er bare nasjonalstatene som har ressurser til å kunne planlegge store angrep, gjennomføre dem og analysere dem etterpå. Så det er den trusselen vi fokuserer på, sier Sundseth.

På den andre siden er digitale farer et omfattende spørsmål, påpeker han.

- Man kan jo bare forestille seg hvis befolkningen mister tilliten til bankvesenet, og det blir umulig å få tatt ut penger, eller noen klarer å gjøre noe med kraftforsyningen, oljeindustrien eller energisektoren.

«Et spørsmål om når»

Et slikt angrep mot norsk infrastruktur kan heller ikke utelukkes, mener sjefen for Cyberforsvaret.

- Nå har vi ikke sett sånne omfattende angrep enda, verken i Norge eller særlig mange andre land. Men muligheten er der, og skal man være pessimistisk, vil jeg si at det ikke er et spørsmål om vi blir utsatt for et sånt angrep, det er et spørsmål om *når*.

- Så dere er bekymret for muligheten?

- Nå vil jeg si at jeg er ikke bekymret av natur, men det er en veldig god grunn til å være oppmerksom på muligheten for den type angrep og gjøre det vi kan for å sikre oss.

Store mørketall

Cyberforsvaret samarbeider tett med Nasjonal sikkerhetsmyndighet (NSM), som har ansvaret for digitale trusler mot kritisk, norsk infrastruktur.

De håndterer mellom to og tre «alvorlige hendelser» i måneden, det vil si infiltrasjonsforsøk eller vellykket kompromittering av systemer som er en del av nasjonal infrastruktur.

Da Dagbladet var til stede i NSMs lokaler, måtte intervjuet avbrytes fordi det gikk en alarm om en hendelse knyttet til statlig infrastruktur. Dette viste seg seinere å ikke være så alvorlig som antatt.

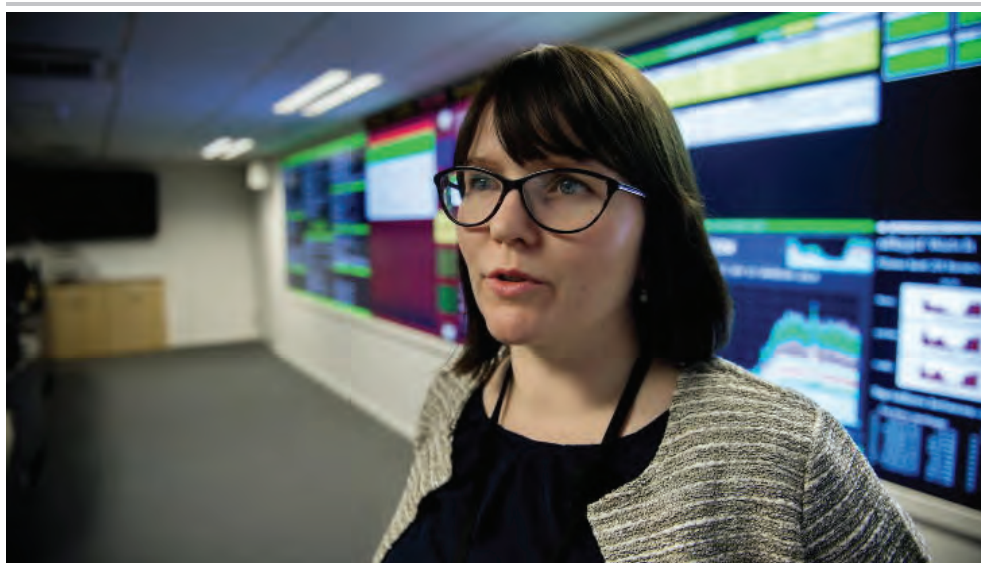
- Hittil i år har vi behandlet 12 000 saker i vårt saksbehandlingssystem. Det vil si at vi får inn mellom 40 og 50 nye saker hver dag. Vi har hatt 24 alvorlige hendelser hittil i år, sier leder for NSMs operasjonssenter, Marie Moe.

De er mest bekymret for antall alvorlige hendelser som ikke blir oppdaget.

- Vi tror det er store mørketall, og er bekymret for at man ikke gjør nok for å beskytte seg mot



UAKSEPTABELT: - Denne type informasjon skal på ingen måte være offentlig, sa brannsjef Rolf Sørtorp etter at Dagbladet gjorde ham oppmerksom på at en database tilhørende Midtre Hålogaland 110-sentral lå usikret på nett. Video: Øistein Norum Monsen.



MØRKETALL: Seksjonssjef Marie Moe ved Nasjonal sikkerhetsmyndighet og hennes kollegaer i operasjonsrommet behandler mellom 40 og 50 saker hver dag. De frykter mange alvorlige hendelser aldri blir oppdaget. Foto: Øistein Norum Monsen / Dagbladet



denne trusselen, sier Moe.

- Må innrette oss

Hvis forsvaret blir utsatt for et inntrengningsforsøk i sine nett, jobber de med å rette feilene og komme tilbake til en normalsituasjon så raskt som mulig.

- Det samme burde jo gjelde for alle andre typer systemer, sier Sundseth i Cyberforsvaret.

Forsvarets graderte systemer er imidlertid ikke koblet mot nettet, og er dermed bedre beskyttet enn mye annet. Samtidig underslår ikke Sundseth at det er mulig å koble seg fysisk og prøve å komme inn.

- Men som jeg har sagt også i andre sammenhenger, har ikke jeg noen tro på at Norge i nær framtid vil oppleve det jeg kaller et digitalt 9. april, hvor en annen nasjon går til et digitalt angrep mot Norge og sånn sett tar ned våre viktige samfunnssystemer, sier Sundseth.

- Men man vet jo aldri, det er vanskelig å spå om framtida. Vi må i hvert fall kontinuerlig analysere trusselbildet og innrette oss etter det vi ser og det vi tror kommer til å skje.

Få vet hvor lett det er for uvedkommende å spionere og stjele identiteter via

FØLG SAKEN

Null CTRL

• Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens webkamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

• I en ny serie avdekker Dagbladets reportere hvordan sviktende data-sikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

• Følg serien her: www.dagbladet.no/nullctrl/

• Tips oss på nullctrl@dagbladet.no

• Si din mening på Twitter: [#null_CTRL](https://twitter.com/null_CTRL)

FAKTA

Slik sikrer du deg

• Avanserte printere er som en liten datamaskin. Får andre først tilgang, kan du miste kontrollen.

• Da kan det for eksempel sendes en kopi til andre hver gang du skriver ut eller skanner noe (for eksempel et pass eller bedriftens styreprotokoll).

• Men slik behøver det ikke å være:

1. Behøver skriveren å være koblet til Internett? Gjør den ikke det, er det tryggest å la være.

2. Liker du delingsmulighetene hjemmenettet gir, trenger du en brannmur som er riktig innstilt. Det er viktig at den stopper tilgangen ruten din gir, at den ikke bare er en brannmur på selve PC-en.

3. Det aller viktigste: Sett et personlig passord på tilgangen til printer og dens nettbaserte styringspanel.



SKUMMELT: Dagfinn Melberg ble svært overrasket da Dagbladet viste ham skademeldingen etter en ulykke han hadde vært involvert i. Han å få tak i dokumenter via nettet.

NYHET!

PRØV VERDENS FERSKESTE OMEGA-3!



ESPEN, OSLO
"Endelig har jeg overskudd.
Superfornøyd!"

VELG HELT FERSK OMEGA-3™ HVIS GOD HELSE ER VIKTIGST

Forskningsresultater viser at fersk omega-3 tas bedre opp i kroppen og gir bedre effekt enn tradisjonell omega-3**. Helt Fersk Omega-3 er verdens ferskeste, kaldpressete lakseolje. Den inneholder ALLE de viktige fettsyrene som er gode for hjerte, hjerne, kretsløp og hud.

Lakseoljen i Helt Fersk Omega-3 produseres på Stokmarknes i Vesterålen.

Prøv Helt Fersk Omega-3 nå. Bestiller du i dag får du tilsendt 2 mnd. forbruk direkte hjem for kun kr 79,50 pr. mnd. + kr 29 i porto.

Velg verdens ferskeste omega-3 – enda bedre for helsen din.

Godt for: ✓ Hjerne ✓ Hjerte ✓ Hud ✓ Kretsløp

**Ny Omega-3 med
bedre effekt****



Norsk Omega-3 fra fersk laks



Introduksjonspris*
79,50 Kr
pr. måned

**BESTILL PÅ SMS:
SEND FERSK TIL 2210**
Eller ring vår ordreteltelefon 815 70 707 man-fre 09-15

*Kjøper du Helt Fersk Omega-3 i dag får du 2 mnd. forbruk til introduksjonspris. Du betaler kun kr 79,50 pr. mnd. + porto kr 29. Normalpris er kr 159 pr. mnd. + porto kr 29. Du mottar 2 mnd. forbruk (1 pakke med 120 kapsler) pr. forsendelse. Bindingsfritt abonnement. Du mottar ny forsendelse etter 6-8 uker. Du må si opp ditt abonnement senest 14 dager før vi sender ut neste forsendelse. Bestilleren må være over 18 år. Levert av Helt Fersk AS. Forbrukerteltelefon 815 70 707. E-post: forbruker@heltfersk.no **Rubinrapport 196.

printere, men her ligger ofte sensitive opplysninger tilgjengelig for alle.



visste ikke at det var mulig for uvedkommende
Foto: Øistein Norum Monsen

FEIL: Dagbladet fant ut av UiOs printere åpent på nettet. IT-direktør Lars Oftedal varslar at de nå vil gå gjennom sine sikkerhetsrutiner.
Foto: Sveinung Uddu Ystad

VOKT DEG for printerspionasje

Tekst: **Ola Strømman**
olast@dagbladet.no

Visste du at fremmede kan spionere på deg gjennom printerne din? Det forsto Dagfinn Melberg da Dagbladet viste ham en utskrift av skademeldingen han fylte ut da han var involvert i en kollisjon i mars i år.

– Lå dette åpent på nett?, er hans første reaksjon.

Skademeldingen er nøyaktig utfylt, med fullt navn, adresse, fødselsnummer, førerkortnummer og signatur. Nyttige verktøy for folk som vil gjennomføre identitetstyveri.

– Dette er kjempeskummelt, det er ikke bra i det hele tatt. Med feil papir og feil personer, kan jo dette få kjempekonsekvenser, sier Melberg.

Koblet rett til nett

Dokumentet ble gjort tilgjengelig for offentligheten da hans motpart i kollisjonen lot skademeldingen

ligge igjen på sin kopimaskin. Moderne kopimaskiner har nemlig teknologi som gjør at printerne kan fjernstyres over nettet.

Samtidig blir mange levert uten passordbeskyttelse.

Det betyr at hvem som helst kan koble seg til, skru på scanneren og skanne det dokumentet som måtte ligge i printerne. Andre kopimaskiner lagrer dokumenter som har vært scannet eller printet for at det skal være mulig å hente disse ut igjen.

En liten PC

– En sånn printer er jo som en datamaskin. Hvis du først får tilgang til den, kan du også ta over printerne og installere ny programvare. Da kan du sende en kopi til deg selv hver gang noen printer ut eller scanner dokumenter, sier seniorrådgiver Vidar Sandland i Norsk senter for informasjonssikring (Norsis).

Skremmende, mener Dagfinn Melberg.

– Det kunne jo ha vært hva som helst på den printerne egentlig, sier han.

Dagbladet har funnet totalt 1781 norske printere som er koblet til nettet. I tillegg til Melbergs skademelding, ligger alt fra førerkort, attester og sykkelmeldinger til regninger og en fullmakt i en bidragssak på disse.

Pasientopplysninger

Flere av de åpne kopimaskinene tilhører Norges teknisk-naturvitenskapelige universitet (NTNU) og Universitetet i Oslo (UiO). På UiOs

printere lå både lønnsavregninger og dokumenter med tilsynelatende sensitive pasientopplysninger.

– Dette er ikke bra i det hele tatt. Her har det opplagt skjedd en feil. Sånn skal det ikke være, sier IT-direktør Lars Oftedal ved UiO.

– Vi sikrer oss på flere måter for at slikt ikke skal kunne skje. For det første skal det være et passord på printerne, for det andre skal det være sikkerhet i nettet så de ikke er tilgjengelige for utenforstående, og for det tredje skal printerne være satt opp slik at dokumenter som er printet skal slettes.

– Nå må vi gå opp de rutinene vi har for å sjekke om de er gode nok, og når noe sånt som dette kan skje, er de opplagt ikke det.

På NTNU er de kjent med problemstillingen.

– Vi har et prosjekt gående med å sette alle printerne på sikkert nett, men det er en ganske langsiktig jobb, sier IT-sjef Håkon Alstad.

Datatilsynet er bekymret over situasjonen.

– De eksemplene du nevner er jo dokumenter som absolutt ikke skal komme på avveie. Det er klart at dette er veldig alvorlig, sier direktør Bjørn Erik Thon.

105 000 nordmenn utsatt

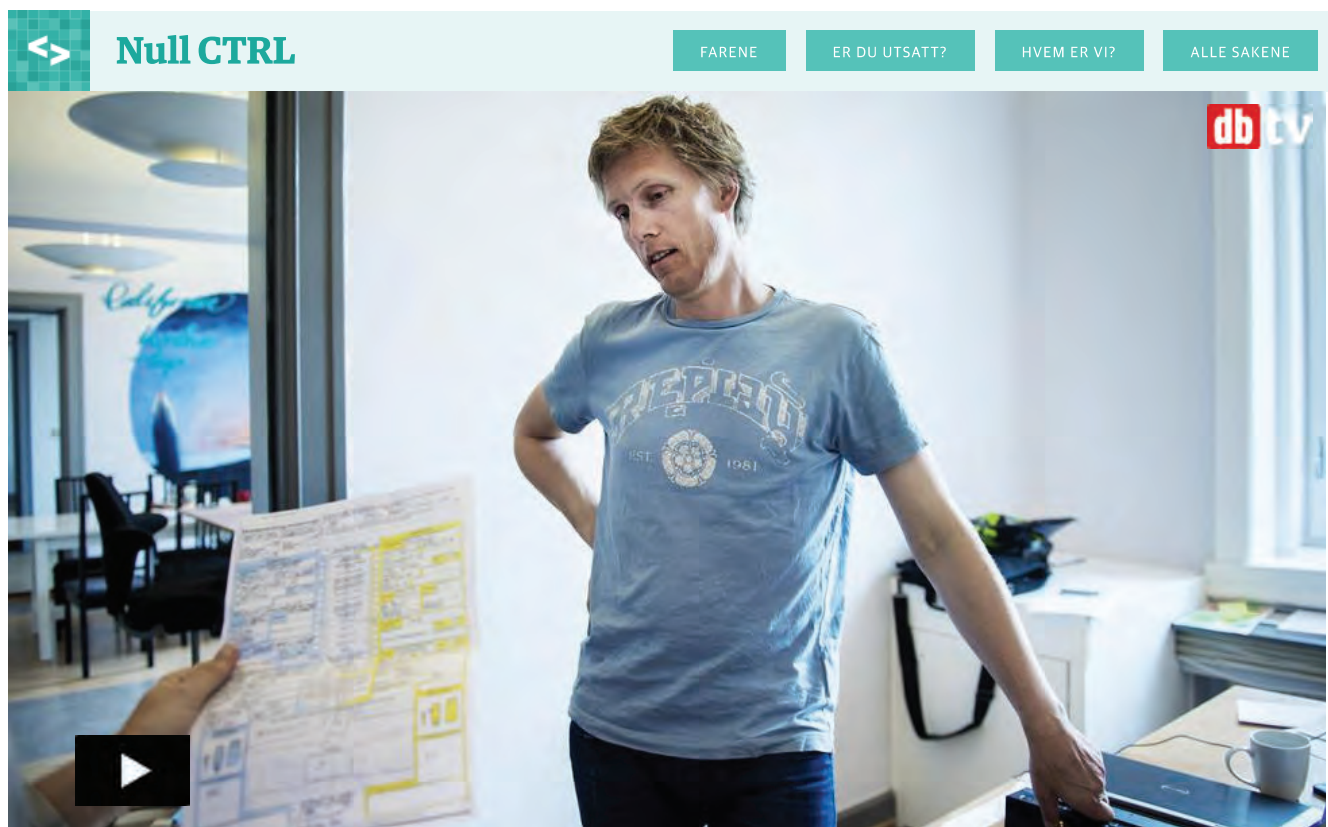
Vidar Sandland i NorSIS påpeker at slike dokumenter kan misbrukes både til svindel og ID-tyveri. Sistnevnte blir et stadig større problem i Norge. I fjor ble 105 000 nordmenn utsatt, ifølge en undersøkelse utført av Norsis og Gallup.

Thon mener leverandørene må gjøre sitt for å få slutt på problemet:

– Det er jo selvfølgelig den som tar printerne i bruk som har ansvar for at informasjonssikkerheten er god, men de som selger avansert teknologi har også et ansvar for å lære opp kundene i å sikre dataene sine på en god måte.



- Lå dette åpent på nett?!, publisert mandag 21. oktober 2013 kl. 12:11



OVERRASKET: Her får Dagfinn Melberg vite at skademeldingen hans lå tilgjengelig for alle, via en kopimaskin som sendte åpent ut på Internett. Video: Øistein Norum Monsen / Dagbladet

- Lå dette åpent på nett?!

Slik kan uvedkommende spionere på deg og stjele identiteten din via printeren.



LINN KONGSLIE HILLESTAD
lkh@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): **Visste du at fremmede kan spionere på deg gjennom printeren din?**

Det forsto Dagfinn Melberg da Dagbladet viste ham en utskrift av skademeldingen han fylte ut da han var involvert i en kollisjon i mars i år.

- Lå dette åpent på nett?!, er hans første reaksjon.

Mye informasjon

Skademeldingen er nøyaktig utfyllt, med alt fra fullt navn, adresse og telefonnummer, samt fødselsnummer, førerkortnummer og signatur.

Med andre ord nyttige verktøy for folk som vil gjennomføre identitetstyveri.

- Dette er kjempeskummelt, det er



ØKENDE TRUSLER: Generalmajor Roar Sundseth er sjef for Cyberforsvaret. De ser en stadig økning i digitale trusler mot Norge. Video: Øistein Norum Monsen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til

ikke bra i det hele tatt. Med feil papir og feil personer, kan jo dette få kjempekonsekvenser, sier Melberg.

Koblet rett til nett

Dokumentet ble gjort tilgjengelig for offentligheten da hans motpart i kollisjonen lot skademeldingen ligge igjen på sin kopimaskin. Moderne kopimaskiner er nemlig oppdatert med teknologi som innebærer at printerene kan fjernstyres over nettet.

For å gjøre dette mulig er printerne utstyrt med en egen webserver, som kan kringkaste informasjon til Internett.

Samtidig mangler mange kopimaskiner passordbeskyttelse - med mindre brukeren selv installerer dette.

Det betyr at hvem som helst kan koble seg til, skru på skanneren og skanne det dokumentet som tilfeldigvis måtte ligge i printerene. Andre kopimaskiner lagrer dokumenter som har vært skannet eller skrevet ut for at det seinere skal være mulig å hente disse ut igjen.

En liten PC

- En sånn printer er jo som en datamaskin. Hvis du først får tilgang kan du også ta over printerene og installere ny programvare. Da kan du for eksempel sende en kopi til deg selv hver gang noen skriver ut eller skanner dokumenter, sier seniorrådgiver Vidar Sandland i Norsk senter for informasjonssikring (Norsis).

Skremmende, mener Dagfinn Melberg.

- Det kunne jo ha vært hva som helst på den printerene egentlig. Jeg ante ikke at det gikk an engang, sier han.

Dagbladet har funnet totalt 1781 norske printere som er koblet til nettet.

I tillegg til Melbergs skademelding, ligger alt fra førerkort, attester og sykemeldinger til regninger og en fullmakt i en bidragssak på noen av disse printerne.

Pasientopplysninger

konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

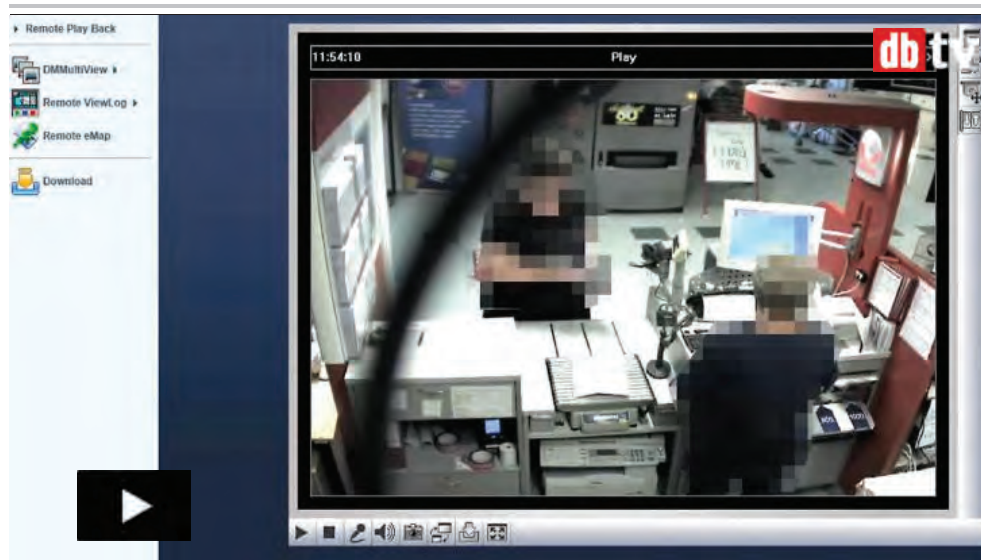
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

” Dette er kjempeskummelt, det er ikke bra i det hele tatt. Med feil papir og feil personer, kan jo dette få kjempekonsekvenser

Dagfinn Melberg



KAN MISBRUKES: Seniorrådgiver Vidar Sandland i Norsis påpeker at mange av dokumentene som ligger lagret på norske printere kan inneholde personsensitiv informasjon som blant annet kan misbrukes til identitetstyveri. Foto: Øistein Norum Monsen / DAGBLADET



SYNLIG FOR ALLE: Et kamera står plassert bak skranken i Post i butikk på Frostasenteret nord for Trondheim. Totalt lå 16 av senterets overvåkingskameraer tilgjengelig på nett. Video: Øistein Norum Monsen / Dagbladet

Flere av de åpne kopimaskinene tilhører landets to største universiteter: Norges teknisk-naturvitenskapelige universitet (NTNU) i Trondheim og Universitetet i Oslo (UiO).

På UiOs printere lå både lønnsavregninger og dokumenter med tilsynelatende sensitive pasientopplysninger.

- Dette er ikke bra i det hele tatt. Her har det opplagt skjedd en feil. Sånn skal det ikke være, sier IT-direktør Lars Oftedal ved UiO.

- Vi sikrer oss på flere måter for at slikt ikke skal kunne skje. For det første skal det være et passord på printerne, for det andre skal det være sikkerhet i nettet så de ikke er tilgjengelige for utenforstående og for det tredje skal printerne være satt opp slik at dokumenter som er skrevet ut skal slettes.

- Nå må vi gå opp de rutineene vi har for å sjekke om de er gode nok, og når noe sånt som dette her kan skje, er de opplagt ikke det.

Kjenner problemet

På NTNU er de kjent med problemstillingen rundt åpne printere.

- Vi har et prosjekt gående med å sette alle printerne på sikkert nett, men det er en ganske langsiktig jobb. Det må gjøres en del konfigurasjoner, som også gjør at tilgangene endres, sier IT-sjef ved NTNU, Håkon Alstad, til Dagbladet.

Han sier de har varslet de som drifter de åpne printerne Dagbladet gjorde dem oppmerksom på.

- Jeg føler det er en økende bevissthet, og vi har fått ryddet opp i mye, men det er som sagt tidkrevende arbeid.

- Veldig alvorlig

Datatilsynet er bekymret over situasjonen.

- De eksemplene du nevner er jo dokumenter som absolutt ikke skal komme på avveie. Så det er svært viktig at de som har kopimaskiner og printere sørger for at sikkerheten rundt disse er god, sier direktør Bjørn Erik Thon.

- Det er klart at dette er veldig alvorlig.

Vidar Sandland i Norsis påpeker at slike dokumenter kan misbrukes både til svindel og ID-tyveri. Sistnevnte blir et stadig større problem i Norge. I fjor ble 105 000 nordmenn utsatt, ifølge en undersøkelse utført av Norsis og Gallup.

Må sikres

- Printere må håndteres på samme måte som servere og datamaskiner. De må sikkerhetsoppdateres når det trengs, og de må beskyttes på samme måte som interne servere, sier Sandland.



SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans kringkastet bilder og lyd rett ut på Internett. Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet

” Vi har et prosjekt gående med å sette alle printerne på sikkert nett, men det er en ganske langsiktig jobb.

Håkon Alstad, IT-sjef ved NTNU

Slik sikrer du deg:

1. Behøver skriveren å være koblet til Internett? Gjør den ikke det, er det tryggest å la være.
2. Liker du delingsmulighetene hjemmenettet gir, trenger du en brannmur som er riktig innstilt. Det er viktig at den stopper tilgangen ruterer din gir, at den ikke bare er en brannmur på selve PC-en.
3. Det aller viktigste: Sett et personlig passord på tilgangen til printerens og dens nettbaserte styringspanel.

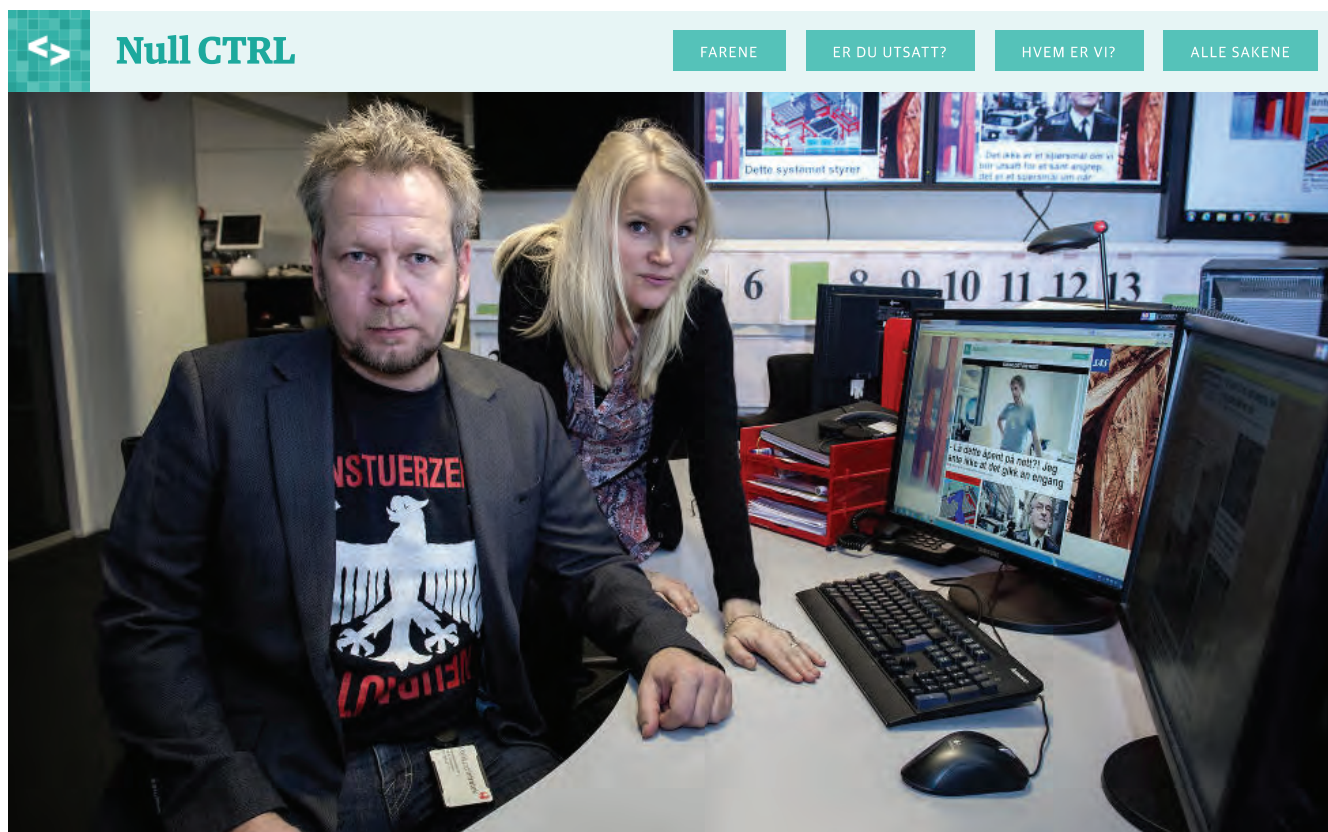
Kilde: Vidar Sandland / Norsis

Bjørn Erik Thon mener leverandørene må gjøre sitt for å få slutt på problemet:

- Det er jo selvfølgelig den som tar printeren i bruk som har ansvar for at informasjonssikkerheten er god, men de som selger avansert teknologi har også et ansvar for å lære opp kundene i å sikre dataene sine på en god måte.



Tips oss på nullctrl@dagbladet.no



TESTET DATASIKKERHET: Espen Sandli og Linn Kongsli Hillestad er journalistene bak Dagbladets serie "Null CTRL". [Tips journalistene på nullctrl@dagbladet.no](mailto:nullctrl@dagbladet.no) Foto: Øistein Norum Monsen / Dagbladet

Slik avslører Dagbladet råtten sikkerhet på norske PC-er

Har testet alt fra overvåkingskameraer til databaser og kontrollsystemer.



THERESE DOKSHEIM
tdo@dagbladet.no

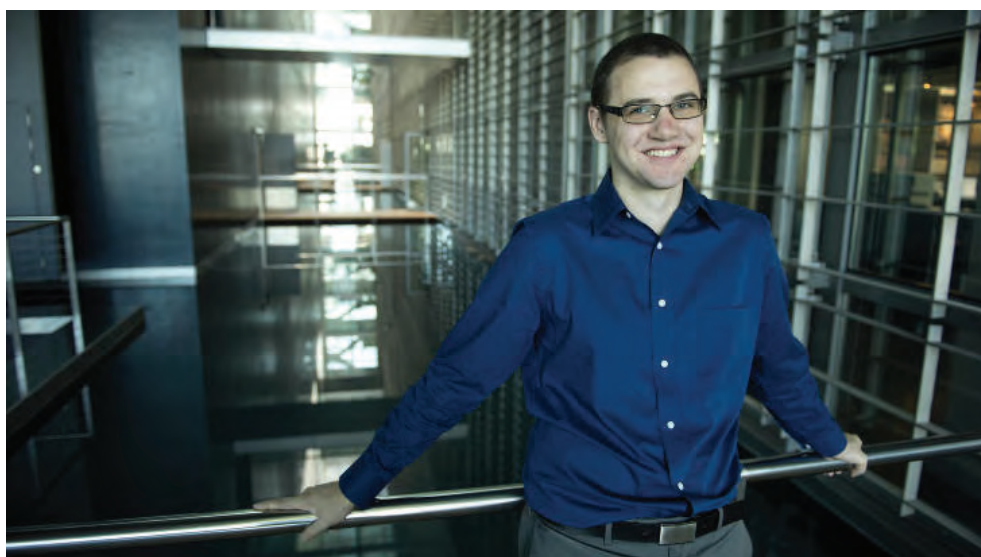
(Dagbladet): Tenk deg at du kan styre naboens web-kamera, åpne konkurrentens database eller ta kontrollen over vitale styringssystemer med et tastetrykk.

I en serie artikler [avslører Dagbladet](#) hvor enkelt det lar seg gjøre.

Journalistene Linn Kongsli Hillestad og Espen Sandli har sammen med utvikler Ola Strømman testet alt fra overvåkingskameraer til databaser og kontrollsystemer som ligger åpent på Internett.

Så langt har de avdekket:

- [2048 overvåkingskameraer](#) i Norge ligger tilgjengelig på nett
- Disse finnes i [private hjem](#), [nattklubber](#), [butikker](#) og [restauranter](#)
- Over [2500 styringssystemer](#) er



SKAPEREN: John Matherly har laget søkemotoren Shodan. Foto: Øistein Norum Monsen/Dagbladet

Slik søkte vi:

koblet til nett, med minimal eller ingen sikkerhet

• [500 av disse kontrollerer industriell eller samfunnskritisk infrastruktur](#)

• Flere tusen databaser og servere gir deg alt innhold - uten å taste et eneste passord.

Amatører

- Vi startet enkelt: «Hva kan personer uten spisskompetanse på datasikkerhet eller hacking finne åpent på nett?» Da vi begynte, ante vi ikke at det skulle bli så omfattende og med så mange funn av kritisk informasjon, sier journalist Espen Sandli.

- Det skrives mange saker i Norge og andre land om potensielle farer på nettet. Vi ønsket å gå lenger enn det. Vi ville vise helt konkret hva det er som svikter, hvor det er og hvilke konsekvenser det reelt kan få, sier Hillestad.

Dagbladet har i løpet av prosjektet undersøkt 535 320 unike norske IP-adresser og 707 358 åpne porter.

- Det som er skremmende, er hva journalister i Dagbladet uten spesielle datakunnskaper er i stand til å finne. Hva da med statsmakter, organiserte kriminelle og hackere, spør seniorrådgiver Vidar Sandland i Norsk Senter for Informasjonssikring (Norsis).

ID-tyveri og cyber-jihad

Bakgrunnen for at Dagbladet ønsket å kartlegge datasikkerheten i Norge, er den store oppmerksomheten som er viet trusler i det digitale rom de siste åra.

Dette gjelder alt fra trusler mot privatlivets fred til ID-tyveri og andre former for kriminalitet, spionasje og cyber-terrorisme.

Trusler på nettet var også fokus i et eget kapittel i [etterretningstjenestens sikkerhetsvurdering for 2013](#).

I rapporten framhever E-tjenesten blant annet at Al-Qaida og andre jihadistiske grupper beskriver «cyber-jihad» som en aksjonsform med stort skadepotensiale.

Slike grupper har derfor oppfordret til aksjoner mot blant annet kritiske styringssystemer.

• Søkemotoren [Shodan](#) er etter tillatelse benyttet som kilde for rådata, generert via en Dagbladet-utviklet og modifisert versjon for filtrering.

• Alle søk er gjennomført og testet av teamet bak «Null CTRL».

• Dagbladets fasit på tall er innenfor funn gjort i dataene indeksert fra 1. januar til 30. august 2013.

• Dagbladet sitter med en fast datadump som gir en konkret status for perioden.

• I Dagbladets funn kan det være enheter som i perioden kan ha byttet ip-adresse og som da ligger med dobbel oppføring. Til gjengjeld er det mange enheter indeksert før 1. januar som ikke er med i vår oversikt.

• Større systemer ligger ofte på fast ip-adresse. Man kan anta at jo større alvorlighetsgrad Dagbladet berører, desto riktigere er det faktiske tallet på enheter.

• Søk mot Shodans levende database vil gi avvikende tall. Dette påvirkes også av at Dagbladet har kontaktet eiere, nettleverandører og Nasjonal sikkerhetsmyndighet (NSM) i forhold til mulig risiko knyttet til flere hundre IP-adresser.

• Dagbladet kommer ikke til å publisere de søketermer som er benyttet i studien av norske IP-adresser.



UAKSEPTABELT: - Denne type informasjon skal på ingen måte være offentlig, sa brannsjef Rolf Sørtorp, etter at Dagbladet gjorde ham oppmerksom på at en database tilhørende Midtre Hålogaland 110-sentral lå usikret på nett. Video: Øistein Norum Monsen / Dagbladet



ENKELT TERRORMÅL: Ledelsen ved fiskebollefabrikken på Sortland tror det ville vært enkelt å sabotere med brannvesenets beredskapsplaner for hånden. De lå åpent på Internett. Video: Øistein Norum Monsen / Dagbladet

Også andre myndigheter, globale bedrifter og organiserte hackergrupper betraktes av E-tjenesten som potensielle trusler i den digitale sfæren.

Ikke som Google

Søkemotoren [Shodan](#) er et sentralt verktøy i Dagbladets research. Det er en helt spesiell søkemotor som finner enheter som er koblet til Internett, for eksempel servere, mobiltelefoner, webkameraer, servere, harddisker - eller store kritiske kontrollsystemer (såkalte [SCADA-systemer](#)).

Shodan fungerer imidlertid svært annerledes enn Google og andre søkemotorer folk flest er kjent med.

- Google lar deg søke etter nettsider, og nettsider er bare en liten del av nettet. Det er en rekke typer programvare Google ikke ser, og det er disse enhetene Shodan oppdager, sier Shodan-grunnlegger John Matherly til Dagbladet.

- Shodan bryr seg om enheten og programvaren i seg selv, mens Google fokuserer på dataene du får servert. Så Shodan søker etter metadataene, mens Google søker etter dataene i seg selv, sier han.

Fingeravtrykk

- Shodan er ikke enkel som Google. Her søker vi etter «fingeravtrykk», for eksempel versjonsnummeret til en helt konkret enhet fra en helt konkret produsent, sier Hillestad.

For å finne et kamera eller kontrollsystem søkes det etter større eller mindre deler av dette fingeravtrykket.

Teamet bak serien «[Null CTRL](#)» har funnet og foredlet flere hundre slike søketermer.

- Det er laget enkeltstående artikler basert på funn i Shodan tidligere, men da er det jeg eller andre eksperter som har funnet det fram for journalistene. Dagbladet gjør jobben selv, og i stor skala. Det har jeg enorm respekt for. Det er synd ikke flere journalister har forstått hvor godt redskap dette er i research, for å få større oppmerksomhet rundt datasikkerhet, sier Matherly.

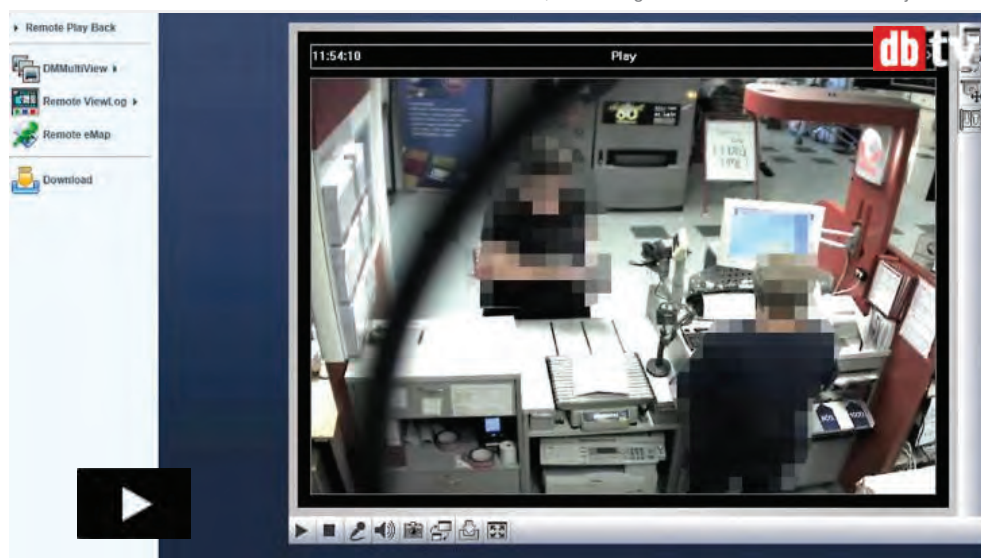
Han har vært orientert om



SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans kringkastet bilder og lyd rett ut på Internett. Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet

” Det som er skremmende, er hva journalister i Dagbladet uten spesielle datakunnskaper er i stand til å finne. Hva da med statsmakter, organiserte kriminelle og hackere?

Vidar Sandland, seniorrådgiver i Norsk Senter for Informasjonssikring



SYNLIG FOR ALLE: Et kamera står plassert bak skranken i Post i butikk på Frostad senter nord for Trondheim. Totalt lå 16 av senterets overvåkingskameraer tilgjengelig på nett. Video: Øistein Norum Monsen / Dagbladet



ÅPENT KAMERA: Kameraet på utestedet Klubbteateret i Drammen sendte videostrømmen rett på nett. Video:

Dagbladets bruk av hans søkemotor, men ikke hatt noen rolle i søkene. Etter hvert som prosjektet har vokst, har Dagbladet innhentet veiledning fra nasjonale og internasjonale eksperter.

Her stopper vi

- Har Dagbladet begynt med hacking?

- Nei. Så definitivt ikke. Vi hadde en etisk og juridisk gjennomgang med advokat og eksperter på området før vi startet. Det er viktig å få fram at Dagbladet ikke driver med hacking, sier Hillestad.

- Blir vi bedt om å taste et passord for å komme inn noe sted, gjør vi ikke det, sier Sandli.

Det betyr også at Dagbladets kartlegging av sviktende sikkerhet stopper der noen har satt et passord. Det gjelder også i tilfeller hvor passordet er enkelt å gjette.

- Det vi vet, er at mange aldri har byttet ut passordet enheten ble levert med. For personer med andre etiske og juridiske vurderinger enn oss, er det da såre enkelt å ta seg inn, sier Sandli.

Større omfang

Det store antallet som bruker for enkle passord ble synliggjort av [en omstridt gruppe hackere](#) i fjor.

De [søkte internett](#) etter enheter som brukte ett av fire kjente standardpassord, og skal angivelig ha [funnet flere hundre tusen enheter](#) verden over.

- Omfanget av sårbare systemer i Norge er derfor sannsynligvis langt større enn det vi har avdekket, sier Hillestad.

Positive reaksjoner

I flere tilfeller har journalistene oppsøkt privatpersoner og bedrifter, og vist dem hvilke sikkerhetshull de har.

- Det er klart det kan være ubehagelig for folk å bli fortalt at andre kan ha hatt tilgang til deres data. Men mottakelsen har nesten utelukkende vært positiv. Folk er genuint takknemlige for å bli varslet, sier Sandli.

Journalistene har varslet eiere, nettleverandører og/eller sikkerhetsmyndigheter i forkant av publisering, slik at sikkerhetshull blir tettet.

Les også:

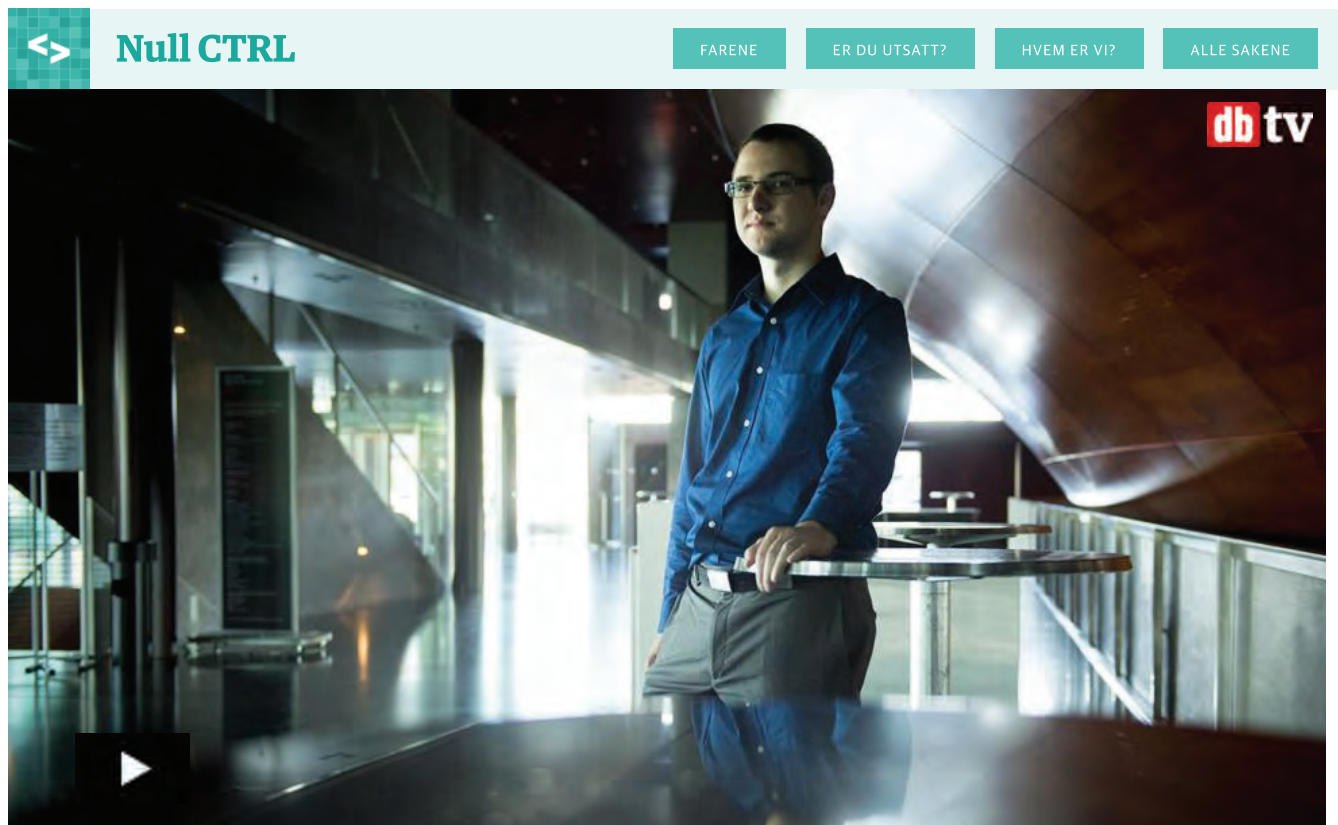
[Her er mannen bak «verdens farligste søkemotor»](#)

[Hele serien «Null CTRL»](#)

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

Her er mannen bak «verdens farligste søkemotor», publisert onsdag 23. oktober 2013 kl. 10:57



- **EN OVERDRIVELSE::** Mannen bak «verdens farligste søkemotor», John Matherly, mener han er på de gode side. Video: Øistein Norum Monsen / Dagbladet

Her er mannen bak «verdens farligste søkemotor»

Er du på nett, har han trolig sjekket produktene dine uten at du vet det.



ESPEN SANDLI
esan@dagbladet.no



ØISTEIN NORUM MONSEN
onm@dagbladet.no



LINN KONGSLI HILLESTAD
lkh@dagbladet.no

LUZERN (Dagbladet): I SVEITS

Søkemotoren [Shodan har fått mange merkelapper](#), blant annet «hackernes beste venn» og «verdens farligste søkemotor».

I dette intervjuet forklarer Shodan-skaper John Matherly hvorfor søkemotoren først og fremst er for «de gode - ikke de onde».

Brukt av Dagbladet

Dagbladet har i flere måneder benyttet søkemotoren til å få [oversikt over enheter som er koblet til nettet i Norge](#).

Funnene i [Shodan](#) har vi så bearbeidet og brukt til å finne utrygge og usikrede enheter til fare for din og min sikkerhet. Serien har fått tittelen «[Null CTRL](#)» og tar for seg kritiske sider av privat-, forretningsmessig- og samfunnskritisk sikkerhetssvikt.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

Ifølge Shodan-skaperen er [Dagbladets arbeid](#) unikt.

- Det er skrevet enkeltstående artikler basert på funn i Shodan, men da er det jeg eller andre eksperter som har funnet det fram for journalistene. Dagbladet gjør jobben selv, og i stor skala. Det har jeg enorm respekt for. Det er synd ikke flere journalister har forstått hvor godt redskap dette er i research, for å få større oppmerksomhet rundt datasikkerhet, sier Matherly.

Flyttet til USA

Dagbladet møtte den USA-baserte programmereren i Sveits, hans egentlige hjemland.

- Det er her jeg er født, men jeg klarte ikke skolen spesielt bra. Derfor flyttet jeg til USA, hvor systemet er litt annerledes. I ettertid er det liten tvil om at det viste seg å være et godt valg, sier Matherly.

Et video-intervju og eksempler kan du også se i TV-reportasjen over.

- Hva er Shodan?

- Shodan er en søkemotor som lar folk finne alt som er koblet til Internett. Alle enheter, enten det er en server, en mobiltelefon, et webkamera eller en laptop... Hvis det er koblet til Internett, kan Shodan lage «fingeravtrykk» på det og la andre søke etter det på Internett.

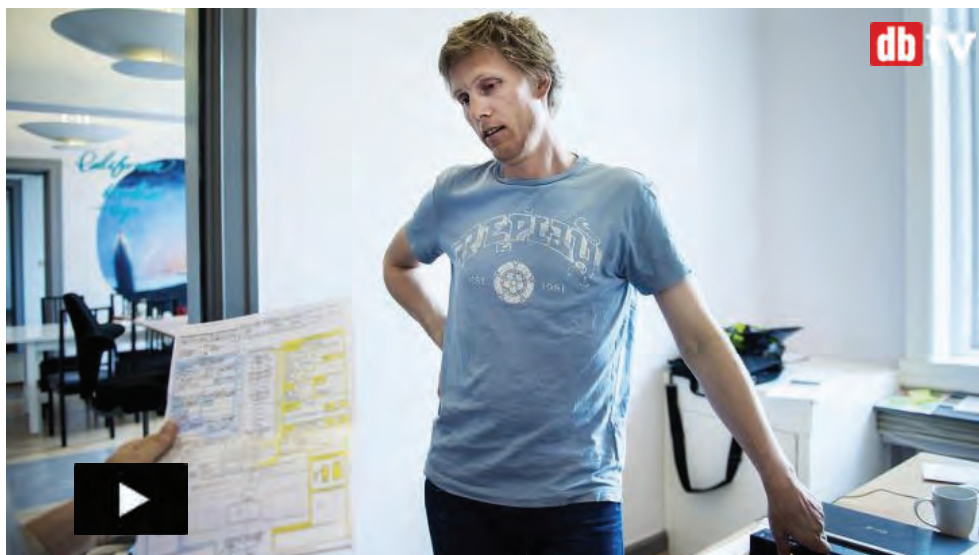
- Noen har beskrevet det som verdens farligste søkemotor, gjør det deg stolt?

- Jeg er glad for at folk bruker den og at den har fått et kallenavn på en måte, men jeg synes det er en overdrevet tittel, som redaktører liker å bruke for å skape sensasjon. Artiklene i seg selv er mye mindre skandaløse, det er bare for å få folks oppmerksomhet. Ingen kommer til å bruke et verktøy som bare kalles «søkemotor for enheter».

- Er den så farlig?

- Jeg tror at den kan være det i de rette hender, men folk må innse at denne teknologien ikke er ny. Den har eksistert lenge. Den har bare ikke blitt eksponert for sikkerhetsekspertene og offentligheten på denne lett tilgjengelige måten før.

- Men andre ondsinnede aktører har hatt tilgang til den samme



OVERRASKET: Her får Dagfinn vite at Dagbladet fant skademeldingen hans via en skriver på nett. Video: Øistein Norum Monsen / Dagbladet



- ENKELT TERRORMÅL: Ledelsen ved fiskebollefabrikken Vesteraalens på Sortland tror det ville vært enkelt å sabotere matproduksjonen ved hjelp av 110-sentralens beredskapsplaner, som lå åpent tilgjengelig på nett. Video: Øistein Norum Monsen / Dagbladet



UAKSEPTABELT: - Denne type informasjon skal på ingen måte være offentlig, sier brannsjef Rolf Sørtorp, etter at Dagbladet gjorde ham oppmerksom på at en database tilhørende Midtre Hålogaland 110-sentral lå usikret på nett. Video: Øistein Norum Monsen / Dagbladet

teknologien i mer enn et tiår, så den store forskjellen er at vanlige sikkerhetsfolk, vanlige mennesker, har et verktøy de kan bruke.

- Hvorfor er Shodan viktig?

- Fordi den kaster lys over en del av Internett som folk ikke kjente til tidligere. Før trodde mesteparten at hvis de ikke finner noe på Google, er det ikke på Internett, men Shodan gir et helt annet bilde av det samme nettet.

- Shodan er den rå, ufiltrerte versjonen av Internett. Den gir folk enn annen måte å få tilgang til og dele og spre ting på Internett.

- Hvorfor er styringssystemer farlige?

- Med styringssystemer mener man blant annet systemer som kontrollerer vannkraftverk, kraftstasjoner, vindkraftverk, systemer som ble tatt i bruk for lenge siden, veldig store, gamle systemer som ikke oppdateres ofte. De koster mange millioner dollar, men selskaper ønsker å koble dem til Internett så de kan hente data og styre systemene hvor som helst i verden, noe som åpenbart er mye billigere enn å få noen til å reise rundt til de ulike lokasjonene.

- Så de vil legge disse systemene på Internett, men ved å gjøre dette, ignorerer de risikoen, fordi enhetene aldri var ment å være på Internett. Så plutselig legger du enheter på Internett som aldri var ment å være der, uten sikkerhet, og de var aldri testet for å være på nettet.

- Har du fått noen reaksjoner fra myndigheter?

- Ja, jeg har blant annet snakket med flere av dem som samarbeider med FBI. Jeg har selvfølgelig snakket med US CERT og ICS CERT, som jobber spesielt med å overvåke den amerikanske infrastrukturen og se om noen av enhetene er online, og i så fall fjerne dem fra nettet.

- Før Shodan fikk de nesten ingen rapporter om online enheter i det hele tatt. Så de kontaktet meg og sa at jeg virkelig hadde økt mengden med henvendelser og hvordan de måtte håndtere dette. Men tilbakemeldingene har vært veldig positive så langt. De har vært glade fordi Shodan hjelper dem å skape en sikrere infrastruktur, og deres høyeste mål er at amerikansk infrastruktur og infrastrukturen i resten av verden for øvrig, blir



ØKENDE TRUSLER: Generalmajor Roar Sundseth er sjef for Cyberforsvaret. De ser en stadig økning i digitale trusler mot Norge. Video: Øistein Norum Monsen / Dagbladet



SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans kringkastet bilder og lyd rett ut på Internett. Uvedkommende kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet



RETT PÅ NETT: Kameraet på utestedet Klubbteateret i Drammen sendte videostrømmen rett på nett. Video: Øistein Norum Monsen / Dagbladet

Shodan

- Søkemotor over enheter som er koblet til Internett

bedre beskyttet.

- Hva svarer du når folk sier at dette er et verktøy for hackere?

- Mitt svar til dette er at de ondsinnede hackerne har brukt lignende verktøy i over ett tiår. De kan bruke lignende verktøy akkurat nå. Shodan er ikke anonymt, hvis du vil bruke Shodan, må du logge inn, og hvis du ønsker ekstra tilgang, må du oppgi betalingsinformasjon. Så derfor pleier de ikke å bruke Shodan. Så ondsinnede hackere har hatt sine egne verktøy lenge. De vil ikke bruke Shodan. Smarte hackere bruker ikke Shodan.

- Så du mener Shodan er for de «snille»?

- Absolutt. Shodan er for de «snille». Jeg er blitt kontaktet av veldig mange på e-post og Twitter, som takker for at de nå har et verktøy de kan bruke for å lage store analyser av selskaper, Internett, ulike land.

- Hvorfor har ikke flere brukt Shodan journalistisk?

- Jeg tror Shodan er villedende enkelt å bruke. Det er veldig enkelt å skrive inn «webcamera» og så får du opp noen resultater, men det er ikke spesielt gode resultater. Så Shodan krever teknisk kunnskap. Det er ikke for gjennomsnittspersonen hvis du virkelig vil lete etter noe spesielt. Det er ikke som Google, hvor du bare kan skrive inn hva som helst. Google er veldig smart. Shodan er ikke sånn.

- Igjen: Det er en rå feed av internett. Så du må klare å gjøre dine egne analyser før du går til Shodan og da kan du bruke det. Så du må vite hva du leter etter, og de fleste gjør ikke det.

- Tror du det har vært ulykker forårsaket av kontrollsystemer på nett?

- Det har vært tilfeller hvor folk ved et uhell har funnet for eksempel en fabrikk mens de lette etter noe annet. De logger inn og klikker på noen knapper, og plutselig slår de ut hele systemet.

- Tenk at du for eksempel går inn på en nettside hvor teksten er skrevet på et språk du ikke kjenner, og du vet ikke engang hva de ulike knappene betyr. Du bare klikker rundt fordi du håper å finne noe interessant. Men ved et uhell, kjører du omstart på systemene til en hel fabrikk, og alt stenges ned.

- Navnet Shodan er hentet fra en karakter i spillet «System Shock».

- Via åpen systeminformasjon søker Shodan opp enheter (f.eks. rutere, skrivere, kamera og servere) som er koblet til Internett.

- Shodan systematiserer de svar man får fra enhetenes «bannere», det vil si de metadata enheten sender fra seg.

- Dette kan være informasjon om operativsystem, programvare, versjonnummer eller velkomstmeldinger.

- Nettsiden ble lansert i 2009 av programmereren John Matherly.

- Søkemotoren brukes i hovedsak av profesjonelle aktører innen datasikkerhet, programutvikling, forskning og politi.

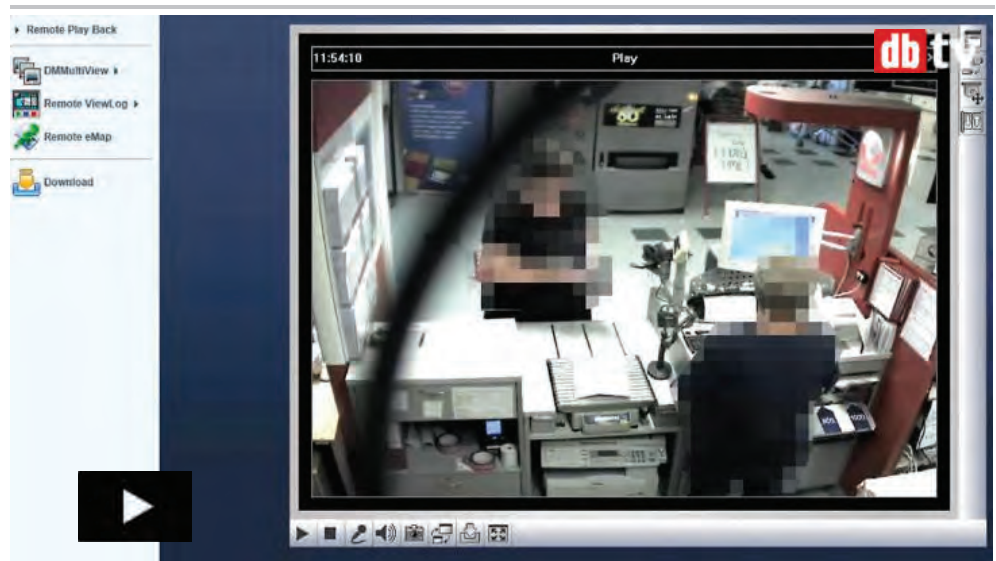
- Også hackere med tvilsomme motiver kan benytte tjenesten. Men disse benytter ofte såkalte «botnet» hvor de kan være anonyme (i motsetning til Shodan).

- Dagbladet er blant de første i verden som benytter Shodan i egen journalistisk research.

Kilde: Dagbladet/Wikipedia/Shodan/John Matherly



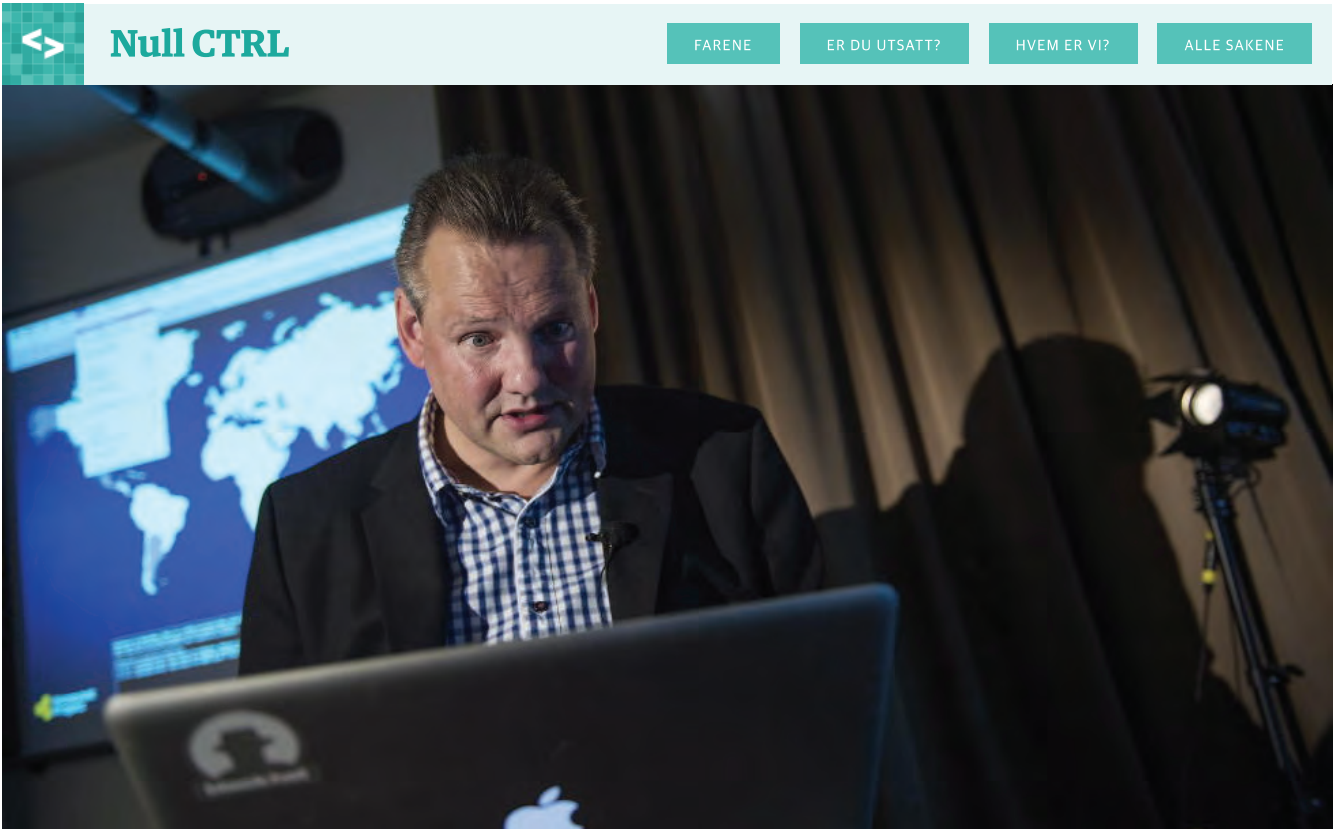
REFSER: Tidligere direktør Georg Apenes i Datatilsynet refser den nye regjeringen for å ikke snakke om datasikkerhet. Video: John Terje Pedersen / Dagbladet



SYNLIG FOR ALLE: Et kamera står plassert bak skranken i Post i butikk på Frostasenteret nord for Trondheim. Totalt lå 16 av senterets overvåkingskameraer tilgjengelig på nett. Video: Øistein Norum Monsen / Dagbladet

[illegible]

FILTRE: Via ulike filtre, kan man gjøre research i Shodan på hva slags enheter som er koblet til Internett. Foto: Skjermdump



GIR RÅD: Seniorrådgiver Vidar Sandland i Norsis gir enkle råd om hvordan du skal sikre deg mot dataangrep. Foto: Øistein Norum Monsen / Dagbladet

Så lett beskytter du deg

Enkle råd for å hindre at du blir utsatt for dataangrep.



LINN KONGSLIE HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): Det kan kanskje høres ut som science fiction, men de siste dagene har Dagbladet avdekket hvordan uvedkommende [kan spionere gjennom nettkameraer](#) og [styre varmen i andres hjem](#).

Dagbladet har også avdekket styringssystemer som kontrollerer industriell eller samfunnskritisk infrastruktur - og som [ligger sårbare ute på nettet](#).

Samtidig er databaser og servere vidåpne for omverdenen - [i mange tilfeller med sensitiv informasjon](#).

Enkle råd

Det er imidlertid ikke vanskelig å hindre at du eksponerer deg unødigg, være seg privat eller på jobb.

Seniorrådgiver Vidar Sandland i



ØKENDE TRUSLER: Generalmajor Roar Sundseth er sjef for Cyberforsvaret. De ser en stadig økning i digitale trusler mot Norge. Video: Øistein Norum Monsen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

Norsk Senter for

Informasjonssikring ([Norsis](#)) mener du kommer langt ved å følge disse fire tommelfingerreglene:

1. Gjør en sikkerhetsvurdering.

Er det virkelig nødvendig at alle de elektroniske produktene dine er tilgjengelige på Internett, og dermed potensielt sett for hele verden?

2. Hvis du mener at dette er

nødvendig, må du for all del bytte til noe annet enn standardpassordet. Mange enheter kommer utstyrt med standard brukernavn og passord, som for eksempel «admin/admin». Hvis dette er brukernavnet og passordet ditt, bør det ringe en alarmklokke.

3. Følg med og husk at du må sikkerhetsoppdatere enhetene dine. Hvis det finnes et sikkerhetshull, er det enkelt for en hacker å utnytte dette og få full tilgang. Derfor må du huske å oppdatere til siste versjon og følge de råd leverandøren kommer med.

4. Bruk sikre former for

kommunikasjon. Da hindrer du at noen kan fange opp brukernavnet og passordet ditt. «Https» er i motsetning til «http» et eksempel på en overføring som gjør at all trafikk blir kryptert (noe som betyr at ingen i prinsippet skal kunne lese den av). Dette ivaretas stort sett av tjenesteleverandørene, som banker og offentlige institusjoner.

Sikre passord

Mange installerer ikke passord på enhetene sine i det hele tatt, mens andre bruker det samme passordet flere steder. Begge deler er viktig å unngå.

- Det vi sier, er at passordet ditt vil komme på avveie, du vet bare ikke når eller hvor. Derfor er det utrolig viktig for deg som forbruker å ha forskjellige passord på forskjellige tjenester, sier Sandland.

Hvis du har problemer med å huske de ulike passordene, anbefaler han å bruke en basissetning, som for eksempel «Lisa gikk til skolen», og deretter bytte ut «skolen» med navnet på det nettstedet passordet gjelder. Da vil du ha forskjellige passord på forskjellige tjenester.

- Dette kan høres veldig dumt ut. Alle som leser dette, skjønner det jo. Men de fleste passord blir hentet

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL



UAKSEPTABELT: - Denne type informasjon skal på ingen måte være offentlig, sier brannsjef Rolf Sørtorp, etter at Dagbladet gjorde ham oppmerksom på at en database tilhørende Midtre Hålogaland 110-sentral lå usikret på nett. Video: Øistein Norum Monsen / Dagbladet



SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans kringkastet bilder og lyd rett ut på Internett. Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet

helt automatisk og prosessert maskinelt, så bare det at du har forskjellige passord på forskjellige tjenester gjør at du ikke mister tilgangen til alle kontoene dine samtidig, og det blir mye enklere å få tilbake kontrollen på for eksempel en Facebook-konto som er blitt tatt over.

- Ta ansvar selv

Det kan være lett å tro at leverandøren av utstyret også sørger for at det er godt nok sikret. Dette er imidlertid ikke alltid tilfelle. Derfor er det viktig å være aktiv selv, påpeker Sandland.

- Hvis du ikke vet hva du trenger av sikkerhet, er det i hvert fall viktig at du spør den leverandøren du bruker og er veldig klar på at du er avhengig av en sikker løsning og at de dokumenterer hva de har gjort for å sikre løsningen din, sier han.

Mer spionasje

I 2012 var det ifølge Nasjonal Sikkerhetsmyndighet ([NSM](#)) en økning i avanserte spionasjeoperasjoner mot spesifikke mål i Norge av høy økonomisk eller samfunnsmessig verdi.

- Arbeidet med sikkerhet er ikke utviklet tilstrekkelig nok i norske virksomheter til å møte et stadig mer komplekst sikkerhetsbilde, skriver de i sin siste kvartalsrapport.

Også Cyberforsvaret er opptatt av at [angrep kommer, spørsmålet er bare når](#).

NSM fokuserer også på sikkerheten rundt kritiske industrielle styringssystemer, og også de mener de aller fleste angrep kan stanses ved hjelp av fire enkle tiltak.

Oppdatering, oppdatering

1. Oppdater programvaren. Nyere applikasjoner og operativsystemer har gjerne flere og bedre sikkerhetsfunksjoner.

2. Vær rask med å installere sikkerhetsoppdateringer. Selv de beste produkter inneholder programmeringsfeil og sårbarheter som kan utnyttes av angripere.

3. Ikke gi vanlige brukere administratorrettigheter. Slike rettigheter bør ikke være nødvendige for å utføre ordinært kontorarbeid.

4. Lag ei liste over programmer virksomheten har godkjent og sørg for at ikke-godkjente programmer på minnepinner eller fra e-post-vedlegg ikke kan brukes. Programmet «Applocker» i Windows 7 kan for eksempel benyttes til å blokkere ukjente programmer.

Bekymret for mørketall



ÅPENT KAMERA: Kameraet på utestedet Klubbteateret i Drammen sendte videostrømmen rett på nett. Video: Øistein Norum Monsen / Dagbladet



REFSER: Tidligere Datatilsynet-direktør Georg Apenes refser den påtroppende regjeringen for å ikke snakke om datasikkerhet. Video: John Terje Pedersen / Dagbladet



PÅ OPERASJONSSENTRALEN: Seksjonssjef Marie Moe ved Nasjonal Sikkerhetsmyndighet behandler rundt 40 saker hver dag. Foto: Øistein Norum Monsen/Dagbladet

NSM er særlig bekymret for antall alvorlige hendelser som ikke blir oppdaget. Leder for NSMs operasjonssenter, Marie Moe, påpeker at det er viktig å logge det som skjer inne på nettverket, så det er mulig å søke tilbake og se om bedriften er blitt angrepet.

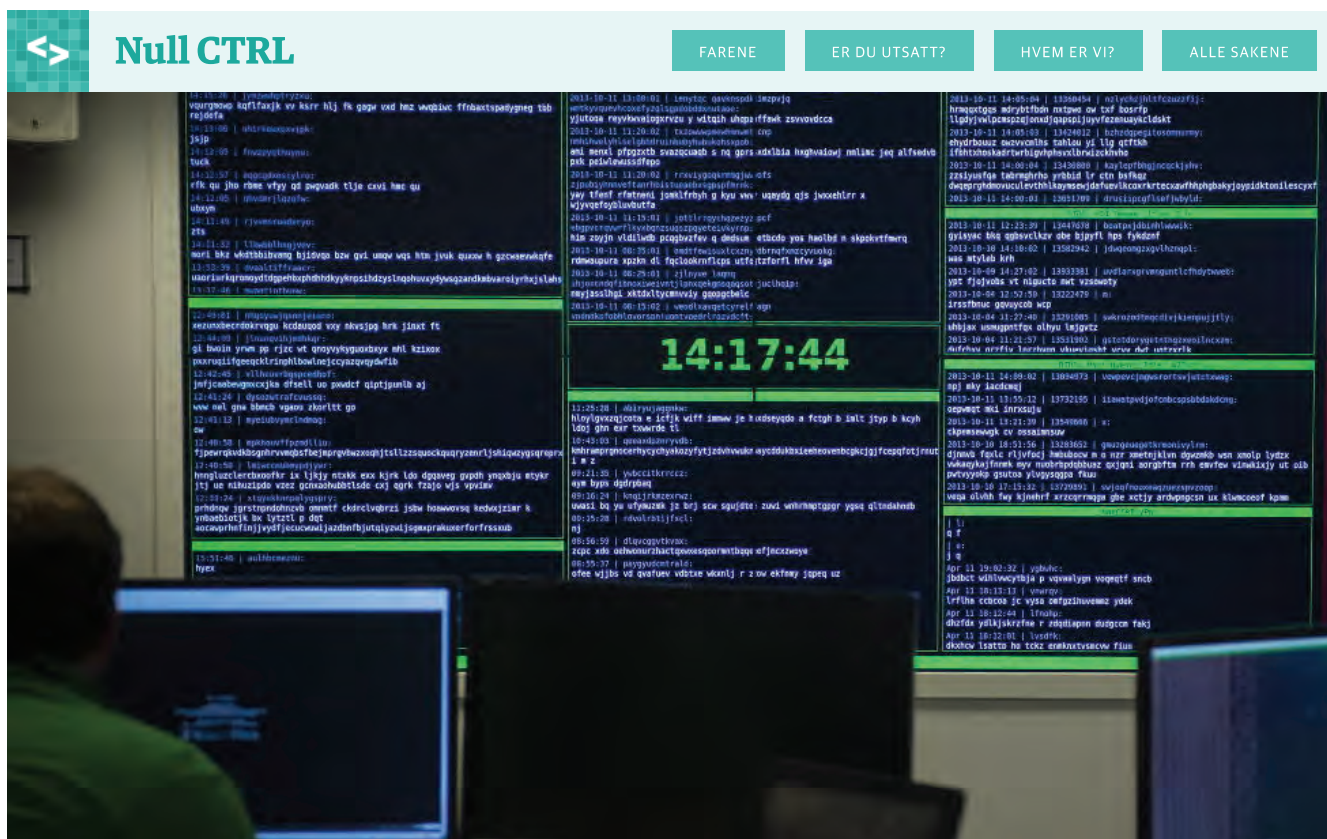
Dette gjelder spesielt selskaper som er blitt utsatt for denne type angrep tidligere, ettersom angriperne gjerne prøver seg på nytt.

- Når det gjelder privatpersoner, er det viktig å være litt forsiktig. Hvis du for eksempel får en mistenkelig e-post må du ikke ukritisk klikke og åpne vedlegg eller lenker i e-posten, sier Moe.



Tips oss på nullctrl@dagbladet.no

Sjekk din datasikkerhet med Dagbladets testmotor, publisert onsdag 23. oktober 2013 kl. 13:49



ÅPNE PORTER: Dagbladets journalister har funnet mange eksempler på hvordan sviktende datasikkerhet rammer hjemme, på jobb og i det offentlige rom. Dette bildet er hentet fra operasjonssentralen til Nasjonal Sikkerhetsmyndighet (NSM), som behandler rundt 40 saker hver dag. Foto: Øistein Norum Monsen / Dagbladet

Sjekk din datasikkerhet med Dagbladets testmotor

Ett tastetrykk er alt som skal til for å se om du har sensitiv informasjon liggende åpent på nettet.



LINN KONGSLIE HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

HER KAN DU TA TESTEN

(Dagbladet): Hvor trygge er dine private bilder og dokumenter? For ikke å snakke om databaser med sensitivt firmamateriale eller høyteknologiske produkter koblet til Internett?

De siste ukene har Dagbladet avslørt råtten datasikkerhet på norske pc-er.

I en serie artikler har vi dokumentert hvordan norske overvåkingskameraer [kringkaster lyd og bilder rett ut på nettet](#), så uvedkommende kan se og høre hva som foregår [på nattklubber](#), [restauranter](#) og [i private stuer og soverom](#).

Samtidig ligger [sensitive](#)

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL

[dokumenter tilgjengelig i vidåpne databaser](#), som hvem som helst kan få tilgang til, og [over 2500 styringssystemer er koblet mot nettet](#), med liten eller ingen beskyttelse.

Dette [kan få store konsekvenser](#), viser internasjonale hendelser.

«Test deg selv»

I arbeidet med å avdekke disse problemene, benyttet Dagbladet blant annet søkemotoren [Shodan](#). Den [søker opp alt som er koblet til Internett](#), enten det er snakk om servere, styringssystemer, mobiltelefoner eller overvåkingskameraer.

- Denne teknologien ikke er ny. Den har ikke blitt eksponert for sikkerhetsekspert og offentligheten på denne lett tilgjengelige måten før, men ondsinnede aktører har hatt tilgang til den samme teknologien i mer enn et tiår, sier Shodan-grunnlegger John Matherly til Dagbladet.

Nå har Dagbladet gjort det enkelt å teste om du selv eller selskapet du jobber for har sensitiv informasjon eller kritiske systemer åpent ute på Internett.

- I forbindelse med serien «Null CTRL», mener vi det er viktig å gi leserne en mulighet til å sjekke sin egen datasikkerhet. Derfor har vi opprettet en søketjeneste som er koblet mot Shodan-serveren. Dette gjør vi etter avtale med Shodan-grunnlegger John Matherly, sier utvikler Ola Strømman, mannen bak Dagbladets testmotor.

[HER KAN DU TA TESTEN.](#)

Statisk materiale

Strømman forklarer at testfunksjonen er innrettet slik at den automatisk sjekker IP-adressen du selv sitter på.

På denne måten kan du altså teste ditt eget system, men ikke naboens.

Testmotoren er å betrakte som en veileder, og er på ingen måte utfyllende eller en garanti for noens hele og fulle datasikkerhet. Den er heller ikke fullstendig oppdatert, noe som betyr at du kan ha utstyr åpent på Internett selv om dette ikke slår ut på testfunksjonen.



ØKENDE BEVISSTHET: John Matherly skapte søkemotoren Shodan, og håper den kan øke folks bevissthet om hva de kobler til Internett. Video: Øistein Norum Monsen / Dagbladet



OVERRASKET: Her får Dagfinn Melberg vite at skademeldingen hans lå tilgjengelig for alle, via en kopimaskin som sendte åpent ut på Internett. Video: Øistein Norum Monsen / Dagbladet



ØKENDE TRUSLER: Generalmajor Roar Sundseth er sjef for Cyberforsvaret. De ser en stadig økning i digitale trusler mot Norge. Video: Øistein Norum Monsen / Dagbladet

- Dette er en test mot en statisk base. Den gjør ingen sanntidssjekk av din IP-adresse, men den slår opp i en base hvor IP-adressene allerede er kontrollert. Om du sikrer deg vil ikke testen oppdateres, men vise samme resultat på nytt, sier Strømman.

Han påpeker at testen i helt spesielle tilfeller kan vise resultater fra andre kunder av samme leverandør, dersom du har overtatt en tidligere brukt IP-adresse.

- I tillegg kan du stå registrert med åpne porter uten at det nødvendigvis er en feil eller et sikkerhetshull. Det kan også være utstyr som skal være tilgjengelig, understreker han.



UAKSEPTABELT: - Denne type informasjon skal på ingen måte være offentlig, sier brannsjef Rolf Sørtorp, etter at Dagbladet gjorde ham oppmerksom på at en database tilhørende Midtre Hålogaland 110-sentral lå usikret på nett. Video: Øistein Norum Monsen.

Slik fungerer det:

Det finnes hele 65 535 antall såkalte «porter» på Internett. Disse brukes for å identifisere ulike maskiner eller programmer tilknyttet en IP-adresse, og gjør at én maskin kan ha flere programmer som kommuniserer over Internett samtidig.

Shodan - og dermed også Dagbladet - undersøker de 33 vanligste portene.

Hvis Dagbladets testmotor finner åpne systemer på din IP-adresse, vil du få opp en beskrivelse av hvilken port som står åpen og hva dette betyr.

I de tilfellene hvor dette er mulig, vil du også få opp en lenke til innholdet testmotoren har funnet. Er du i tvil om noe, kontakt din nettleverandør eller IT-avdeling.



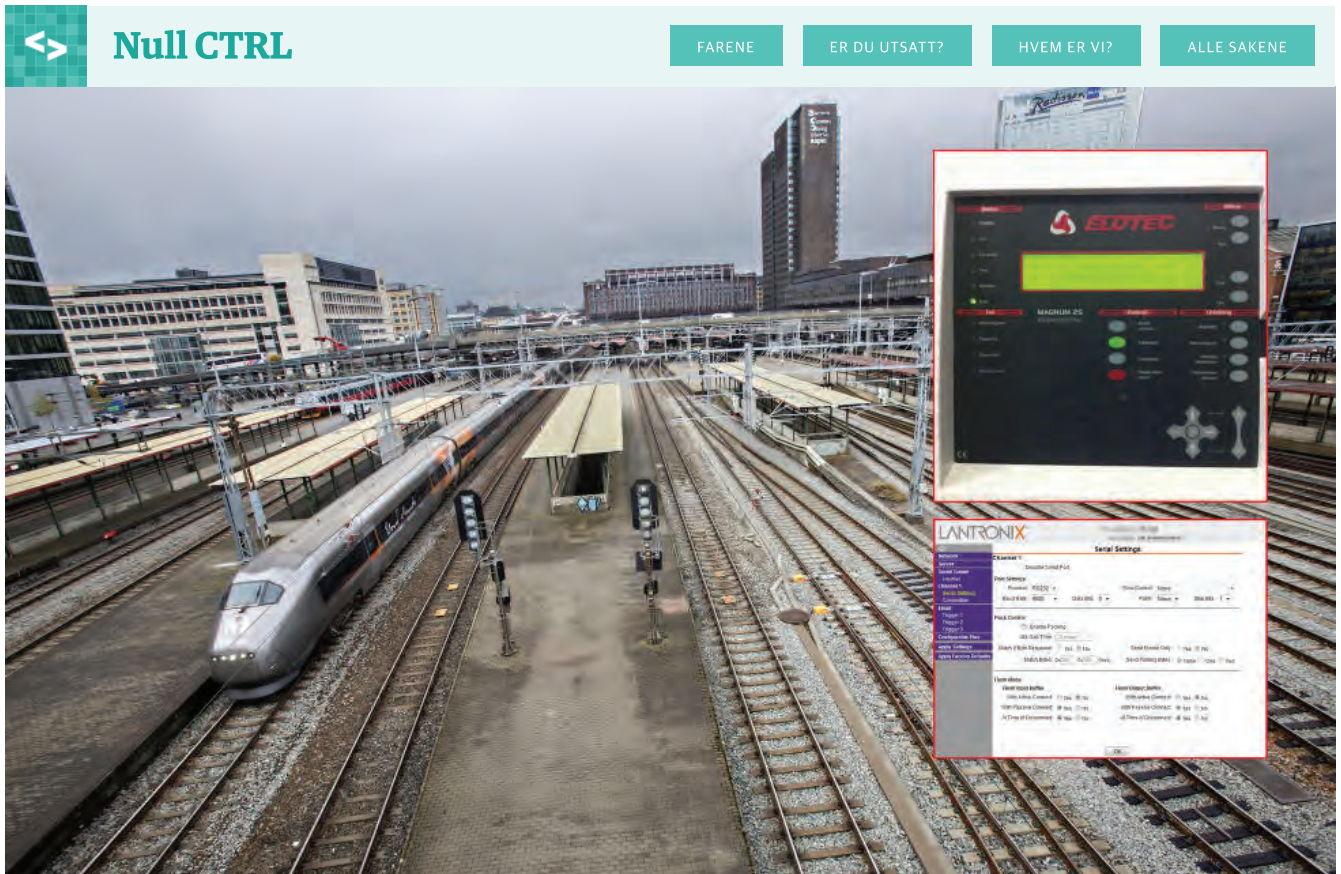
Tips oss på nulctrl@dagbladet.no

Er det ord og uttrykk du ikke får forklart? [Norsis har en egen ordliste med en del forklaringer.](#)

[Her kan du lese mer om hvordan du beskytter deg.](#)

[HER KAN DU TA TESTEN](#)

- Kan vi få lov til å trykke her nå? - Nei, absolutt ikke, absolutt ikke, publisert torsdag 24. oktober 2013 kl. 11:16



ÅPNE SYSTEMER: Dagbladet fant de digitale inngangsportene til rapporteringsportaler for Jernbaneverkets brannalarmsentraler på Internett. Disse tilhører Jernbaneverkets kraftforsyningsanlegg, spredt langs jernbanenettet. Dette bildet er hentet fra Oslo S, mens de innklippede bildene viser alarmsentralene (øverst) og web-grensesnittet (nederst). Foto: Torbjørn Berg / Dagbladet / Jernbaneverket

- Kan vi få lov til å trykke her nå? - Nei, absolutt ikke, absolutt ikke

Dagbladet fant inngangsportene til 15 av Jernbaneverkets brannalarmsentraler åpent på Internett.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): - Sånn burde det ikke være. Det er det ingen tvil om, sier teknologidirektør Sverre Kjenne i Jernbaneverket.

Ei uke tidligere hadde Dagbladet vist ham og noen av hans kollegaer 15 usikrede systemer tilhørende Jernbaneverket, som vi hadde funnet helt åpent på Internett.

Disse systemene viste seg å være digitale inngangsporter til brannalarmsentraler i Jernbaneverkets kraftforsyning - spredt langs jernbanenettet. Det finnes et 40-talls slike brannsentraler, som er del av et landsdekkende anlegg.



- Dette skulle ikke ha ligget åpent sånn som det lå, så jeg setter pris på å bli gjort oppmerksom på dette, sier Kjenne.

Kunne hindret informasjon

Han mener at Dagbladet ikke kunne ha styrt noe inne på styringspanelene vi har funnet. Det vi imidlertid kunne ha gjort, var å hindre at Jernbaneverket fikk informasjonen fra disse brannsentralene.

- Dere kunne ha «reroutet» IP-adresser, noe som gjør at vi ikke får se status på brannalarmen. Da ville vi oppdaget dette og forfulgt det med én gang, men det ville tatt litt tid, og sånn vil vi jo selvsagt ikke ha det, sier Kjenne.

Driftssjef Johan Stenvig i Jernbaneverket Bane Energi forklarer at de har et eget «SCADA-system» hvor de får inn eventuelle brannvarsler. Eventuell utkobling gjøres også via dette systemet.

Via systemet Dagbladet hadde tilgang til, får Jernbaneverket informasjon om hva som faktisk har skjedd, blant annet hvor i systemet brannalarmen kommer fra.

- Hvis vi ikke hadde hatt tilgang til denne informasjonen, måtte vi ha sendt noen fysisk for å lese av manuelt, sier Stenvig.

Viktig område

Dagbladet har av sikkerhetsmessige årsaker ikke fått lov til å se disse brannsentralene. Etter at Dagbladet varslet Jernbaneverket om systemene, er de blitt beskyttet med brukernavn og passord.

- Hvorfor sto disse åpne i utgangspunktet?

- Når du installerer en masse «gatewayer» og «switcher» er det en sjanse for at man på én av disse ikke har gjort det man burde ha gjort, sier Sverre Kjenne.

- Dette er et viktig område for oss. Jernbaneverket som moderne bedrift har stor bruk av Internett til mange forskjellige ting, og det er viktig for oss at det ikke er mulig at uønskede hendelser skal oppstå, legger han til.

- Ikke sikkerhetsrisiko

Kjenne fastholder imidlertid at de åpne systemene Dagbladet har funnet ikke forstyrrer nattesøvnens hans:

- Jernbaneverket valgte å fjerne nett-tilkoblingen for brannalarmsentralene mens vi undersøkte alle aspekter ved grensesnittene. Analysen viser som først antatt at ip-adressene ikke representerer hverken en sikkerhetsrisiko for Jernbaneverket, eller at kritisk informasjon kan komme på avveie.

SKULLE IKKE VÆRT ÅPENT: Teknologidirektør Sverre Kjenne i Jernbaneverket sier systemene ikke skulle ha ligget åpent på Internett, men mener ikke dette representerer noen sikkerhetsrisiko for Jernbaneverket. Alle er nå passordbeskyttet. Foto: Øistein Norum Monsen/Dagbladet.

Null CTRL

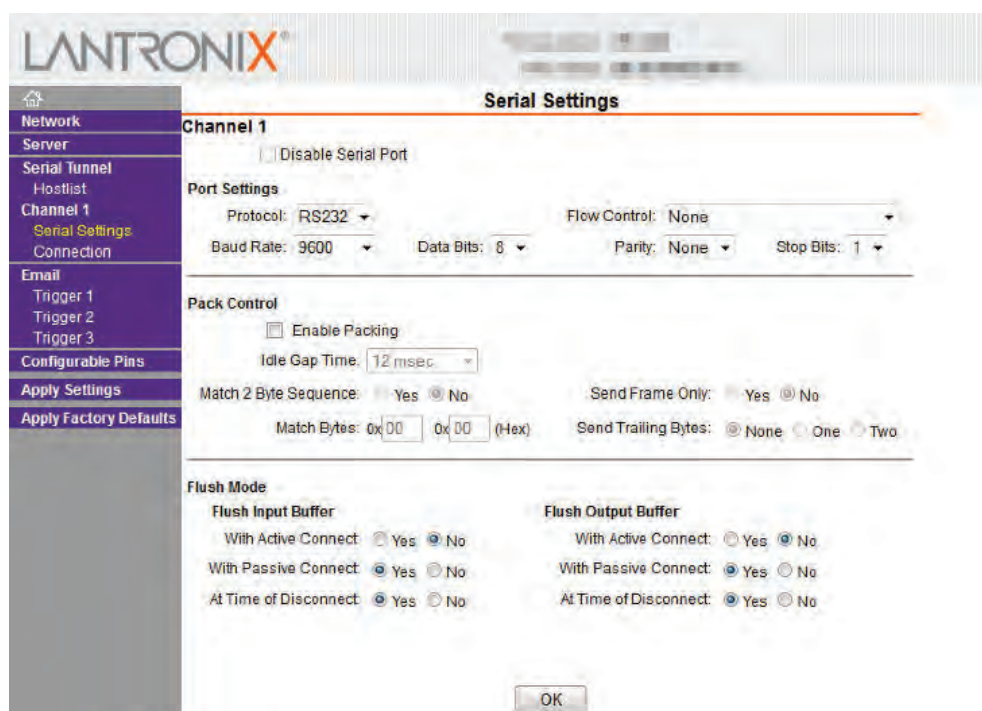
• Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

• I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

• Følg serien her: <http://www.dagbladet.no/nullctrl/>

• Tips oss på nullctrl@dagbladet.no

• Si din mening på Twitter: #null_CTRL



PANELET: Dette er panelet Dagbladet fant åpent og ubeskyttet på Internett.



Kjenne påpeker også at tilfeldige personer ikke vil kunne gjøre noen skade med tilgang til disse systemene.

BRANSENTRALEN: Slik ser brannsentralene til Jernbaneverket ut. Det finnes et førtital av disse langs jernbanelinjene over hele landet. Foto: Jernbaneverket

- Og hvis noen hadde vært ute etter å sabotere, tenker jeg at de ville ha gått løs på noe annet.

Får ikke teste

- Men i dette panelet ser det ut til at vi veldig enkelt kan endre IP-adresse?

- Vi prøvde det, men da stoppet det opp.

- Kan vi få lov til å trykke her nå?

- Nei, absolutt ikke, absolutt ikke.

- Så du er så sikker på at det er trygt at vi ikke får lov til å trykke?

- Det er visse ting du bare ikke trenger å holde på så veldig mye med.



Tips oss på nullctrl@dagbladet.no

 **Null CTRL**

FARENEER DU UTSATT?HVEM ER VI?ALLE SAKENE

Du er registrert med følgende porter åpne:

PORT 443:
HTTPS: Du har en åpen port, trolig for en web-server som leverer innhold til nettleseren din. Det kan være et web-kamera, en nettversdisk eller rett og slett din egen PC. Du kan se om du kjenner igjen innholdet her: [\[redacted\]](#)
[Les mer](#)

PORT 445:
SMB: En åpen port tilsier at du deler dokumenter med resten av verden. Du burde vurdere en brannmur for å sikre dine dataer.
[Les mer](#)

PORT 8080:
HTTP: En åpen port tilsier at du har en web-server som leverer innhold til nettleseren din. Det kan være et web-kamera, en nettversdisk eller rett og slett din egen PC. Du kan se om du kjenner igjen innholdet her: [\[redacted\]](#)
[Les mer](#)

PORT 5432:
POSTGRESQL: En åpen port tilsier at du har en database som tilsynelatende ligger åpent mot Internett. Du burde vurdere en brannmur for å sikre dine data.
[Les mer](#)

ÅPNE PORTER: Over 17 prosent av de ansatte i Dagbladet som testet sin datasikkerhet hadde utstyr åpent på internett.

Slik sto det til med datasikkerheten i Dagbladet

Over 17 prosent hadde åpent utstyr på internett.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): I forbindelse med [artikkelserien «Null CTRL»](#) har Dagbladet opprettet en testfunksjon hvor [du kan sjekke din egen datasikkerhet](#).

HER KAN DU TA TESTEN

Artikkelserien setter søkelys på hvordan sviktende datasikkerhet kan ramme hjemme, på jobb og i det offentlige rom.

Hittil har Dagbladet avdekket hvordan norske overvåkingskameraer [kringkaster lyd og bilder rett ut på nettet](#), så uvedkommende kan se og høre hva som foregår [på nattklubber](#), [restauranter](#) og [i private stuer og soverom](#).

Samtidig ligger [sensitive dokumenter tilgjengelig i vidåpne databaser](#), som hvem som helst kan få tilgang til, og [over 2500 styringssystemer er koblet mot nettet](#), med liten eller ingen



MEDIESKY: Her er mannen bak «verdens farligste søkemotor», Shodan. John Matherly mener han er på de godes side. Video: Øistein Norum Monsen / Dagbladet

beskyttelse. Også [printere er utsatt](#).

17,5 prosent

I skrivende stund er 66 554 unike IP-adresser blitt testet via Dagbladets funksjon.

I forkant av offentliggjøringen av testmotoren, ble denne sendt ut til alle ansatte i Dagbladet så de kunne sjekke hvordan det sto til med datasikkerheten hjemme hos seg selv.

Totalt 137 Dagbladets-ansatte har hittil testet sine IP-adresser. Av disse var det 24 personer, eller 17,5 prosent, som hadde åpent utstyr registrert på sin IP-adresse. 75 porter sto åpent totalt.

Dette skyldes ikke nødvendigvis feil eller et sikkerhetshull. Det kan også være utstyr som *skal* være tilgjengelig, men har en god passordbeskyttelse - for eksempel FTP-servere.

- Det er ikke nødvendigvis en sikkerhetsrisiko med disse enhetene på nett, men det er viktig med en bevisstgjøring rundt teknologien og dens feller. Om dette er ansattes bevisste oppsett eller slurv med sikkerheten vet man jo ikke, men dette har de nå en mulighet til å finne ut, sier Ola Strømman.

Han har utviklet Dagbladets testfunksjon i samarbeid med John Matherly, mannen bak [søkemotoren Shodan](#).

Økt fokus

Denne søkemotoren har vært sentral i Dagbladets arbeid med «Null CTRL», en artikkelserie som også har ført til økt oppmerksomhet rundt datasikkerheten internt i Dagbladet. Etter at de første artiklene ble publisert, har vi blitt tipset om flere tekniske sårbarheter i egne systemer.

- Nettavisen er naturlig nok sårbar, og det er utfordrende å være sikret godt nok, samtidig som at man skal jobbe effektivt og i konkurranse med andre nyhetsnettsteder. Vi jobber løpende med sikkerhet, også sammen med vår driftsleverandør, og det blir bare mer fokus på dette framover. Samtidig kan vi ikke innføre tunge sikkerhetstiltak som for eksempel nettbankens innlogging, sier digitalredaktør



TEKNISKE SÅRBARHETER: Dette skjermbildet illustrerer en teknisk sårbarhet Dagbladet er blitt tipset om av Einar Otto Stangvik etter publiseringen av de første artiklene i «Null CTRL». Han har blant annet lagt ut en video på YouTube hvor han leker med Dagbladets datasikkerhet. Skjermdump: YouTube



UAKSEPTABELT: - Denne type informasjon skal på ingen måte være offentlig, sier brannsjef Rolf Sørtorp, etter at Dagbladet gjorde ham oppmerksom på at en database tilhørende Midtre Hålogaland 110-sentral lå usikret på nett. Video: Øistein Norum Monsen / Dagbladet



ØKENDE TRUSLER: Generalmajor Roar Sundseth er sjef for Cyberforsvaret. De ser en stadig økning i digitale trusler mot Norge. Video: Øistein Norum Monsen / Dagbladet

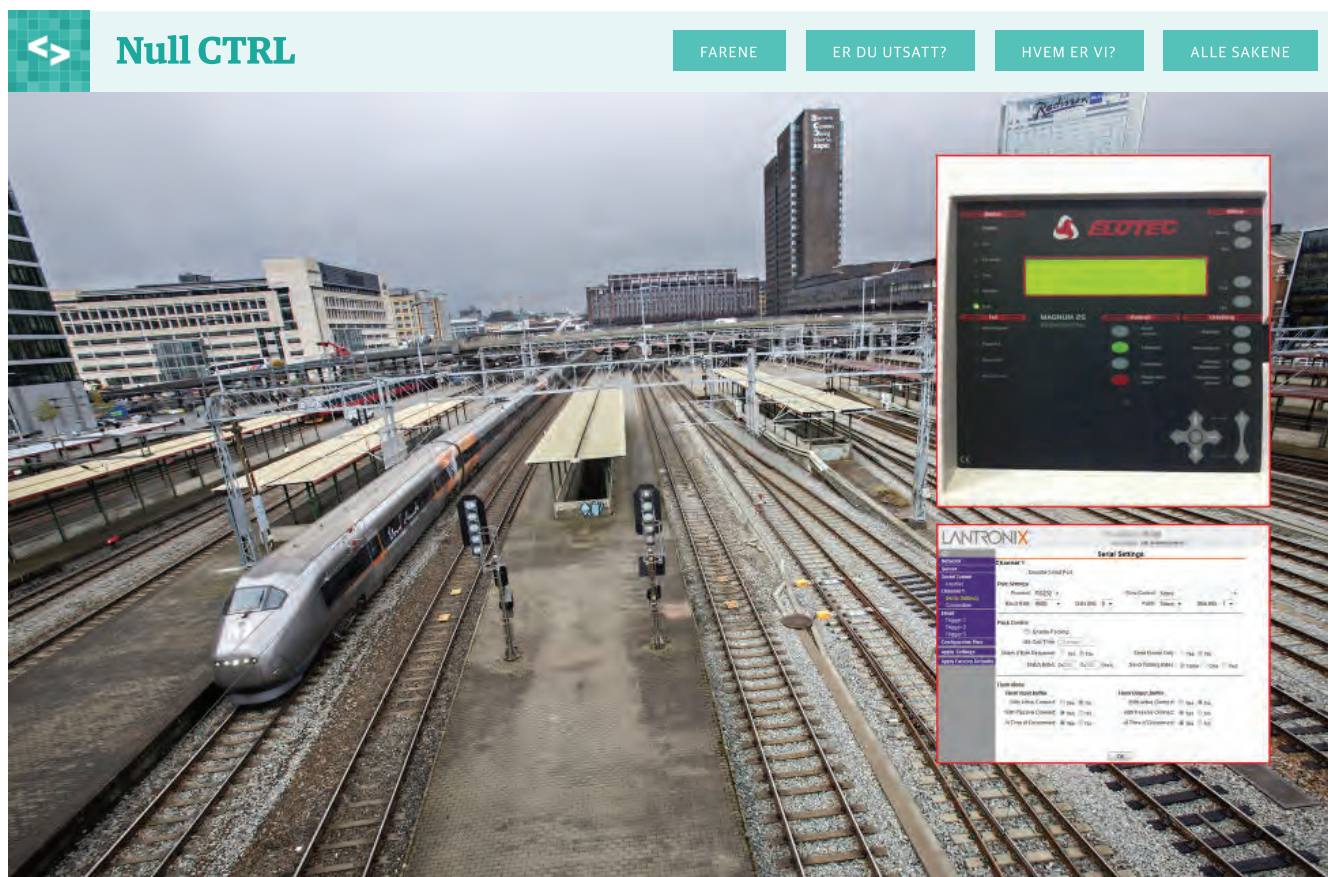
Hildegunn Amanda Soldal.

- Dette er en utfordrende oppgave for oss i Dagbladet, som alle andre som er på internett. Derfor håper jeg «Null CTRL»-serien kan bidra til både økt bevissthet rundt datasikkerhet, samt kunnskap om hvordan man kan beskytte seg, avslutter hun.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

- Det er svært alvorlig, det bør bekymre alle og enhver, publisert fredag 25. oktober 2013 kl. 17:30



ÅPNE SYSTEMER: Dagbladet fant de digitale inngangsportene til rapporteringsportaler for Jernbaneverkets brannalarmsentraler på Internett. Disse tilhører Jernbaneverkets kraftforsyningsanlegg, spredt langs jernbanenettet. Dette bildet er hentet fra Oslo S, mens de innklippede bildene viser alarmsentralene (øverst) og web-grensesnittet (nederst). Foto: Torbjørn Berg / Dagbladet / Jernbaneverket

- Det er svært alvorlig, det bør bekymre alle og enhver

Stortingspolitikere reagerer på Jernbaneverkets åpne brannvarslere.



THERESE DOKSHEIM
tdo@dagbladet.no



LINN KONGSLIE HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): - Det er klart det er alvorlig, og jeg tenker det bør bekymre alle og enhver, sier nestleder i transportkomiteen på Stortinget, Eirin Sund (Ap), til Dagbladet.

Hun har lest Dagbladets artikkel om Jernbaneverkets systemer som [Dagbladet fant åpent på Internett](#).

De 15 systemene viste seg å være digitale inngangsporter til brannalarmsentraler i Jernbaneverkets kraftforsyning - spredt langs jernbanenettet. Det finnes et 40-talls slike brannsentraler, som er del av et landsdekkende anlegg.

- Sånn burde det ikke være. Det er det ingen tvil om, sa



SKULLE IKKE VÆRT ÅPENT: Teknologidirektør Sverre Kjenne i Jernbaneverket sier systemene ikke skulle ha ligget

Kunne hindret informasjon

Jernbaneverket har et eget «SCADA-system» hvor de får inn eventuelle brannvarsler. Eventuell utkobling gjøres også via dette systemet.

Via systemet Dagbladet hadde tilgang til, får Jernbaneverket informasjon om hva som faktisk har skjedd, blant annet hvor i systemet brannalarmen kommer fra.

I verste fall kunne Dagbladet hindret at Jernbaneverket fikk informasjonen fra disse brannsentralene, ved å «reroute» IP-adressene.

Kjenne mener ikke IP-adressene representerer en sikkerhetsrisiko for Jernbaneverket, eller at kritisk informasjon kan komme på avveie. Dagbladet fikk imidlertid ikke lov til å røre noen av knappene inne i panelet.

- Forholdene Dagbladet avdekket er det nå ordnet opp i. Brannalarmsentralene er lukket. Jernbaneverket er opptatt av IKT-sikkerhet og jeg er glad for at de har ryddet opp i denne saken, sier samferdselsminister Ketil Solvik-Olsen (Frp).

- Alvorlig

- Jeg har ikke kjennskap til saken annet enn det Dagbladet har avdekket, men det er klart det er alvorlig, og jeg tenker det bør bekymre alle og enhver. Samtidig regner jeg med at Jernbaneverket har rutiner for at slikt ikke skal skje. Men det er alvorlig hvis folk kan komme seg inn, sier Eirin Sund.

Hun mener Jernbaneverket nå bør gjennomgå sine rutiner.

- Og det regner jeg med at de gjør.

- Dagbladet har avdekket at mange systemer som ligger usikret på nett. Hva tenker du om det?

- Det er bekymringsverdig. Det er klart at IKT-sikringer er kjempeviktig.

Manglende bevissthet

Nestleder i transportkomiteen, Abid Q. Raja (V) kan ikke kommentere detaljene i Dagbladets sak, men mener dette viser at vi uansett burde ha mer kontroll på systemene våre.

- Jeg tror generelt vi undervurderer viktigheten av sikkerhet i Norge, sier Raja, også med tanke på de andre sakene Dagbladet har avdekket i [artikkelserien «Null CTRL»](#).

- Jeg tror veldig mange tenker at det ikke kan skje noe galt, og dette gjør at det ikke blir tatt høyde for «worst case»-scenarioer. Det er litt urovekkende å tenke på at det ikke skal så mye til hvis noen skulle ønske å ødelegge noe. De som kan dette, kan sitte hjemme på gutterommet og gjennomføre cyberangrep, sier Raja.



UROVEKKENDE: Abid Q. Raja (V) mener vi har for dårlig kultur for sikkerhet i Norge. Foto: Gorm Kallestad / Scanpix

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL

- Innenfor transportsektoren bør man kanskje være ekstra bevisst på sikkerheten, og selv om kanskje ikke det kunne skjedd noe fatalt i dette tilfellet, viser det en manglende bevissthet på hva slags kultur vi burde ha, mener han.

BLOTTLAGT



«SUPERBOKS»: Gets nye boks tilbyr TV, bredbånd og telefoni i én og samme boks, og har fått gode resultater i ulike tester.

Thomas Sundberg testet datasikkerheten sin med Dagbladet, og ble svært overrasket da han oppdaget at hvem som helst kunne få tilgang til den nye «superboksen» hans fra Get.

Tekst: **Espen Sandli**
esan@dagbladet.no
Linn K. Hillestad
lkh@dagbladet.no

I forbindelse med artikkelserien «Null CTRL» lanserte Dagbladet



denne uka en testfunksjon hvor eserne kan sjekke sin egen datasikkerhet.

Thomas Sundberg er én av over 100 000 personer som hittil har prøvd denne testen. Resultatet overrasket ham.

– Jeg har fulgt med på artikkelserien, og tenkte at det kunne vært morsomt å prøve ut testmotoren. Jeg anser meg selv som relativt IT-kyndig, og syntes det var svært spesielt da testen slo ut på at web-

porten min sto åpen, sier Sundberg til Dagbladet.

Åpen ruter

Han fant ut at det var hans nye «Get box 2» som lå åpent ut mot nettet. Dette er den nye «superboksen» fra Get, som gir TV, telefoni og trådløst bredbånd via samme boks.

– Da jeg så at den sto åpen, tenkte jeg at dette var greit, for de fleste rutere har en digital inngangsport. Men det som ikke er greit, var at denne kringkastet internadressen min, sier Sundberg.

Han søkte på nettet og fant ut at Get-boksen hans hadde to ulike brukerkontoer som han også fikk ekstern tilgang til via Internett, begge bare beskyttet med standardpassord. Den ene var hans egen kundebruker, den andre var Gets, som de bruker hvis de skal fjern-

konfigurere ruterne for kunden.

Om uvedkommende får tilgang til en ruter, kan dette føre til flere problemer.

Kan utnyttets

– Via mange rutere kan du få tilgang til hele nettverket og dermed alle delte bilder og filer. Du får de samme rettighetene som om du satt inne i huset ditt, sier seniorrådgiver Vidar Sandland i Norsk senter for informasjonssikring (Norsis) til Dagbladet.

– I tillegg kan du åpne opp brannmuren og sette opp en server som for eksempel kan brukes til å spre ulovlig materiale ut på nettet.

Sundberg byttet raskt begge passordene. Likevel kunne Dagbladet – og alle uvedkommende – fortsatt se en oversikt over alle enhetene koblet til nettet på hans IP-adresse.

Dette kan være alt fra telefoner og PC-er til printere og annet teknisk utstyr.

– Jeg synes ikke noe særlig om at andre kan gå inn og se alle enheter jeg har tilkoblet i min leilighet uten å taste noe passord, sier Sundberg.

– Et avvik

Get har undersøkt saken, og mener denne boksen hadde et avvik.

– «Get box 2» har en innebygd tilgangskontroll som gjør at det ikke er mulig å identifisere ruterne utenfor hjemmenettverket, sier kommunikasjonssjef Anders Bigseth i Get.



AVVIK: Kommunikasjonssjef i Get, Anders Bigseth.

TAV GET



Foto: Get

De har nå undersøkt hvorvidt denne fungerer.

– Vi har nå skannet alle boksene som er i markedet, og funnet at det har vært fire bokser som har et avvik. Den ene har vi allerede erstattet, og de tre andre blir byttet ut i dag, sier Bigseth.

– Nå vil underleverandøren vår undersøke disse boksene nærmere for å finne årsaken til at disse har et avvik.

Sundberg har fått en ny boks, som ser ut til å fungere. Han er svært fornøyd med at Get tok tak i feilen så raskt.

Vidar Sandland i Norsis anbefaler på generelt grunnlag å teste sitt eget nettverk for åpne enheter. I tillegg til Dagbladets test, som søker i en statistisk database, finnes flere andre tester på Internett, for eksempel gcr.com.



OPPDAGET SIKKERHETSHULL: Da Thomas Sundberg sjekket datasikkerheten sin med Dagbladets testmotor, fant han ut at han kunne få tilgang til ruten sin eksternt via to ulike brukere med standard brukernavn og passord.

Foto: Privat

Er din PC sikker?

Dagbladets testmotor viser at hver fjerde leser kan ha en mulig svikt i datasikkerheten.

Dagbladet har utviklet en helt unik testmotor hvor leserne selv kan sjekke hvordan det står til med en egen datasikkerhet.



I går hadde Dagbladets testmotor sjekket over 100 000 norske IP-adresser.

- HØYE TALL: Redaksjonell utvikler Ola Strømman i Dagbladet.

Svarene leserne får, er ofte ikke som de hadde forestilt seg

Mye står åpent

Etter å ha vært i bruk i bare noen få dager, viser testen allerede at mange lesere bør finne ut hva det er de har koblet til Internett og hvor sikkert det egentlig er.

– Det at tallene er så høye, overrasker oss, sier redaksjonell utvikler Ola Strømman i Dagbladet.

Strømman er del av teamet bak datasikkerhets-serien «Null CTRL» og har laget den fysiske testen som Dagbladet tilbyr sine lesere.

Tallene han snakker om, er statistikken Dagbladet leser ut av testresultatene. Dette er tall som ikke sier noe om de konkrete personene som har besøkt Dagbladets testside, men som oppsummert viser hvilke feil som rapporteres hyppigst i testmotoren.

Kjent og ukjent

«Feilene» det er snakk om, er porter som står åpne. I noen tilfelle er det meningen at de skal være det. I andre er det ikke det.

– Fram til lørdag kveld så vi at så mange som en av ti hadde en web-server registrert mot nett. En av fire hadde en kjent port stående åpen. Det hadde vært veldig interessant å visst hvor mange av disse potensielle sikkerhetshullene som er der med vitende og vilje. Jeg er redd for at det er mange som ikke er det, sier Strømman.

For mange er det en overraskelse når testen vier at de har potensiell risiko de ikke visste om – eller til og med ikke vet hva er.

– Hvis du ikke vet hva du trenger av sikkerhet, er det i hvert fall viktig at du spør den leverandøren du bruker og er veldig klar på at du er avhengig av en sikker løsning og at de dokumenterer hva de har gjort for å sikre løsningen din, sier seniorrådgiver Vidar Sandland i Norsk Senter for Informasjons-sikring (Norsis).

FØLG SAKEN

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens webkamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: www.dagbladet.no/nullctrl/

- Tips oss på: nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

Test deg selv

På denne nettsiden kan du teste om din egen pc er utsatt for sikkerhetsrisikoer.

<http://www.dagbladet.no/nullctrl/testmeg/>

Dagbladet.no



OPPDAGET SIKKERHETSHULL: Da Thomas Sundberg sjekket datasikkerheten sin med Dagbladets testmotor, fant han ut at han kunne få tilgang til ruterens sin eksternt via to ulike brukere med standard brukernavn og passord. Foto: Privat

Thomas' Get-boks lå åpen ut mot nettet

Oppdaget det med Dagbladets datasikkerhets-test.



LINN KONGSLØ HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): I forbindelse med [artikkelserien «Null CTRL»](#) lanserte Dagbladet denne uka [en testfunksjon](#) hvor leserne [kan sjekke sin egen datasikkerhet](#).

Thomas Sundberg er én av over 100 000 personer som hittil har prøvd denne testen.

Resultatet overrasket ham.

- Jeg har fulgt med på artikkelserien, og tenkte at det kunne vært morsomt å prøve ut testmotoren. Jeg anser meg selv som relativt IT-kyndig, og syntes det var svært spesielt da testen slo ut på at web-porten min sto åpen, sier Sundberg til Dagbladet.



Åpen ruter

Han fant ut at det var hans nye «Get box 2» som lå åpent ut mot nettet. Dette er den nye «superboksen» fra Get, som gir TV, telefoni og trådløst bredbånd via samme boks.

- Da jeg så at den sto åpen, tenkte jeg at dette var greit, for de fleste rutere har en digital inngangsport. Men det som ikke er greit, var at denne kringkastet internadressen min, sier Sundberg.

Han søkte på nettet og fant ut at Get-boksen hans hadde to ulike brukerkontoer som han også fikk ekstern tilgang til via Internett, begge bare beskyttet med standardpassord.

Den ene var hans egen kundebruker, den andre var Gets, som de bruker hvis de skal fjernekonfigurere ruterne for kunden.

Kan utnyttas

Om uvedkommende får tilgang til en ruter, kan dette føre til flere problemer.

- Via mange rutere kan du få tilgang til hele nettverket og dermed alle delte bilder og filer. Du får de samme rettighetene som om du satt inne i huset ditt, sier seniorrådgiver Vidar Sandland i Norsk senter for informasjonssikring (Norsis) til Dagbladet.

- I tillegg kan du åpne opp brannmuren og sette opp en server som for eksempel kan brukes til å spre ulovlig materiale ut på nettet.

Sundberg byttet raskt begge passordene. Likevel kunne Dagbladet - og alle uvedkommende - fortsatt se en oversikt over alle enhetene koblet til nettet på hans IP-adresse. Dette kan være alt fra telefoner og PC-er til printere og annet teknisk utstyr.

- Jeg synes ikke noe særlig om at andre kan gå inn og se alle enheter jeg har tilkoblet i min leilighet uten å taste noe passord, sier han.

- Et avvik

Get har undersøkt saken, og mener denne boksen hadde et avvik.

- «Get box 2» har en innebygd tilgangskontroll som gjør at det ikke er mulig å identifisere



SKAPTE SHODAN: Her er mannen bak «verdens farligste søkemotor», Shodan. John Matherly mener han er på de godes side. Video: Øistein Norum Monsen / Dagbladet



SKUMMELT: Trond Kristiansen ante ikke at overvåningskameraet hans kringkastet bilder og lyd rett ut på Internett. Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

ruteren utenfor hjemmenettverket, sier kommunikasjonssjef Anders Bigseth i Get.

De har nå undersøkt hvorvidt denne fungerer.

- Vi har nå skannet alle boksene som er i markedet, og funnet at det har vært fire bokser som har et avvik. Den ene har vi allerede erstattet, og de tre andre blir byttet ut i dag, sier Bigseth.

- Nå vil underleverandøren vår undersøke disse boksene nærmere for å finne årsaken til at disse har et avvik.

Sundberg har fått en ny boks, som ser ut til å fungere. Han er svært fornøyd med at Get tok tak i feilen så raskt.

Gjorde endringer

Vidar Sandland i Norsis anbefaler på generelt grunnlag å teste sitt eget nettverk for åpne enheter. I tillegg til [Dagbladets test](#), som søker i en statistisk database, finnes flere andre tester på Internett, for eksempel grc.com.

Get opplyser mandag kveld til Dagbladet at de har vært i kontakt med de tre andre brukerne, som opplyser at de har gjort endringer inne i Gets admin-konto, som har gjort ruteren søkbar på Internett.

- Vi er glade for at «Get box 2» verken har feil eller avvik, men vi vil for sikkerhets skyld stenge tilgangen til admin-kontoen gjennom en framtidig programvareoppdatering, sier Anders Bigseth mandag kveld.

Thomas Sundberg mener at han ikke har gjort noe selv som har forårsaket at hans ruter lå åpen ut mot nettet.



FIRE ÅPNE: Get har undersøkt salen og fant totalt fire bokser som var søkbare på nettet. Mandag kveld opplyser kommunikasjonssjef i Get, Anders Bigseth, at de har snakket med de tre andre kundene, som hadde gjort endringer i Gets admin-konto. Thomas Sundberg mener han ikke har gjort dette. Foto: Get

 **Null CTRL**

FARENEER DU UTSATT?HVEM ER VI?ALLE SAKENE

Du er registrert med følgende porter åpne:

PORT 443:
HTTPS: Du har en åpen port, trolig for en web-server som leverer innhold til nettleseren din. Det kan være et web-kamera, en nettversdisk eller rett og slett din egen PC. Du kan se om du kjenner igjen innholdet her: [https://www.nullctrl.no/443](#)
[Les mer](#)

PORT 445:
SMB: En åpen port tilsier at du deler dokumenter med resten av verden. Du burde vurdere en brannmur for å sikre dine dataer.
[Les mer](#)

PORT 8080:
HTTP: En åpen port tilsier at du har en web-server som leverer innhold til nettleseren din. Det kan være et web-kamera, en nettversdisk eller rett og slett din egen PC. Du kan se om du kjenner igjen innholdet her: [http://www.nullctrl.no/8080](#)
[Les mer](#)

PORT 5432:
POSTGRESQL: En åpen port tilsier at du har en database som tilsynelatende ligger åpent mot Internett. Du burde vurdere en brannmur for å sikre dine data.
[Les mer](#)

HØY RISIKO: Bildet viser et eksempel på et testresultat i Dagbladets unike testmotor. Personen som fikk dette resultatet måtte gjøre en grundig sjekk av sin datasikkerhet. Foto: Skjermdump / Dagbladet

Hver fjerde leser har mulig svikt i datasikkerheten

Overraskende funn via Dagbladets testmotor. Ta testen her.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLI HILLESTAD
lkh@dagbladet.no

(Dagbladet): Dagbladet har utviklet en unik testmotor hvor [leserne selv kan sjekke](#) hvordan det står til med en egen datasikkerhet.

I går hadde Dagbladets testmotor sjekket over 100 000 norske IP-adresser. Svarene leserne får, er ofte ikke som de hadde forestilt seg.

Har du ikke tatt testen ennå, kan du [gjøre det her](#).

Mye står åpent

Etter å ha vært i bruk i bare noen få dager, viser testen allerede at mange lesere bør finne ut hva det er de har koblet til Internett og hvor sikkert det egentlig er.

- Det at tallene er så høye, overrasker oss, sier redaksjonell utvikler Ola Strømman i Dagbladet.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: [#null_CTRL](#)

Strømman er del av [teamet bak datasikkerhets-serien «Null CTRL»](#) og har laget den fysiske [testen som Dagbladet tilbyr](#) sine lesere.

Tallene han snakker om, er statistikken Dagbladet leser ut av testresultatene. Dette er tall som ikke sier noe om de konkrete personene som har besøkt [Dagbladets testside](#), men som oppsummert viser hvilke feil som rapporteres hyppigst i testmotoren.

Kjent og ukjent

«Feilene» det er snakk om, er porter som står åpne. I noen tilfelle er det meningen at de skal være det. I andre er det ikke det.

- Fram til lørdag kveld så vi at så mange som 1 av 10 hadde en web-server registrert mot nett. En av fire hadde en kjent port stående åpen. Det hadde vært veldig interessant å visst hvor mange av disse potensielle sikkerhetshullene som er der med vitende og vilje. Jeg er redd for at det er mange som ikke er det, sier Strømman.

For mange er det en overraskelse når testen vier at de har potensiell risiko de ikke visste om - eller til og med ikke vet hva er.

- Hvis du ikke vet hva du trenger av sikkerhet, er det i hvert fall viktig at du spør den leverandøren du bruker og er veldig klar på at du er avhengig av en sikker løsning og at de dokumenterer hva de har gjort for å sikre løsningen din, sier seniorrådgiver Vidar Sandland i Norsk Senter for Informasjonssikring (Norsis).

Sandland er spesielt opptatt av [hvordan man velger passord](#).

- Mye rart

Dagbladets test sjekker din IP-adresse opp mot mulige sikkerhetshull registrert i [søkemotoren Shodan](#), og gir deg svar på hvorvidt du har risikoer (åpne porter) du bør undersøke nærmere. Selv om mange porter både er beskyttet og åpnet med en hensikt, er det grunn til å være på vakt.

- I arbeidet med serien «Null CTRL» har vi sett alt for mye som ikke skulle vært der ute, åpent og tilgjengelig for alle på Internett, sier Strømman.

Dagbladets test sjekker kun mot en statisk database med IP-adresser. I tillegg finnes det flere tjenester på Internett, hvor du kan sikre PC-er og nettverk, [blant annet her](#).

Les mer:

[Ta testen her](#)

[Les om testen her](#)

[Alt om «Null CTRL»](#)



SKAPTE SHODAN: Han er mannen bak «verdens farligste søkemotor», Shodan. John Matherly mener han er på de godes side. Video: Øistein Norum Monsen / Dagbladet



- HØYE TALL: Redaksjonell utvikler Ola Strømman i Dagbladet er overrasket over hvor mange som har ulike dataenheter stående åpent og koblet til Internett. Foto: Agnete Brun / Dagbladet





NY KAMPFLYBASE: Ørland flystasjon er en av Luftforsvarets to hovedflystasjoner, og opererer F16 jagerfly, redningshelikoptre og Natos overvåkingsfly. I juni i fjor vedtok Stortinget at Ørland skal bli Norges nye kampflybase. Foto: Håkon Eikesdal

- FARE FOR RIKETS SIKKERHET

MYE INFORMASJON: Sivile dokumenter om Ørland flystasjon lå tilgjengelig på en vidåpen, privat nettverksdisk. Noe av dette kan misbrukes, mener Luftfarstilsynet og en kilde i Cyberforsvaret.

Detaljerte dokumenter om Ørland flystasjon lå åpent på Internett. En potensiell fare for rikets sikkerhet, mener kilde i Cyberforsvaret. Ufarlig, mener Luftforsvaret.

Tekst: **Linn Kongsli Hillestad**

lkh@dagbladet.no

Espen Sandli

esan@dagbladet.no

Ola Strømman

olast@dagbladet.no

– Det vil medføre en fare for sikkerheten om dette kommer i hendene på personell med for nasjonen uheldige ideologier og intensjoner, sier en kilde høyt oppe i Cyberforsvaret.

Cyberforsvaret har ansvaret for å drifte, sikre og forsvare Forsvarets datasystemer, nettverk og høyteknologiske plattformer mot angrep i og fra cyberdomenet.

Dagbladet har vist vedkommende en rekke dokumenter med detaljert informasjon om Ørland flystasjon, en av Luftforsvarets to hovedflystasjoner.

Dokumentene er sivile. De ble funnet på en vidåpen nettverksdisk hjemme hos en person med tilknytning til flyplassen. Vedkommende oppgir at han ikke vis-

te at innholdet på serveren var eksponert for alle og enhver.

Mye informasjon

Her fantes blant annet:

- Tekniske data for radarer
- Informasjon om bremseveier og styringssystemet som brukes til å heve og senke denne
- Informasjon om flyplassbelysning og nødstrømskilder
- Forholdsregler ved bombe-trussel eller terror
- Informasjon om militære øvingsområder

Ny kampflybase

På Ørland opererer F16-jagerfly, redningshelikoptre og Natos overvåkingsfly, og flyplassen er også et alliert treningssenter. I juni i fjor

La ut dokumenter om Norges nye kampflybase ved en feil

vedtok Stortinget at Ørland skal være Norges framtidige kampflybase. I dag er det både sivil og militær trafikk på flyplassen. Luftforsvaret er blitt forelagt flere av dokumentene fra den åpne serveren, og mener disse ikke inneholder

skjermingsverdig informasjon.

– Store deler av disse dokumentene er informasjon som skal være offentlig tilgjengelig for nedlasting slik at enhver flyger kan operere trygt i luftrommet, sier kommunikasjonssjef Lars William Wrold-



TIPS OSS

Espen Sandli
esan@dagbladet.no

Linn K. Hillestad
lkh@dagbladet.no

Null CTRL

FAKTA

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens webkamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende data-sikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: www.dagbladet.no/nullctrl/
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

FAKTA

Ørland flystasjon

- En av Luftforsvarets to hovedflystasjoner, og ligger i Ørland kommune i Sør-Trøndelag.
- Opererer F16-jagerfly, redningshelikoptre og Natos overvåkingsfly, og er også et alliert treningssenter.
- Flyplassen er hovedsakelig militær, men det er også sivil flytrafikk der. Kontrolltårnene drives av Avinor.
- I juni i fjor vedtok Stortinget at Ørland skal være Norges framtidige kampflybase.



Foto: Øistein Norum Monsen

sen i Luftforsvaret, som presiserer at dette er dokumenter om sivile systemer.

Den mest detaljerte informasjonen er i dokumenter vedrørende lokalt regelverk. Disse finnes ikke tilgjengelig på eksterne nettsider.

- Ikke skadelig

Når det gjelder Avinors lokale planverk for Ørland finner vi ingenting der som er skadelig for Luftforsvaret, sier Wroldsen, men presiserer at de ikke ser noen grunn til at dette skal ligge offentlig tilgjengelig.

- Hva tenker dere om at dette ble lagt ut ved en feil?

Hvordan og hvorfor disse konkrete Avinor-dokumentene ligger tilgjengelig kjenner jeg ikke til.



UGRADERT: Kommunikasjonssjef Kristian Løksa i flysikringsdivisjonen i Avinor påpeker at dokumentene ikke var gradert.

Foto: Avinor

Avinor henviser til at dette ikke er gradert informasjon.

Det er vår oppfatning, ut fra slik du har presentert saken og de dokumentene du har sendt meg, at det ikke er problematisk at en an-

satt har tatt med seg dette hjem for å sette seg inn i regelverket, skriver kommunikasjonssjef Kristian Løksa ved flysikringsdivisjonen i Avinor i en e-post.

- Kan misbrukes

Seksjonssjef for flysikringsseksjonen i Luftfartstilsynet, Svein Pedersen, forklarer at en del av informasjonen Dagbladet har funnet er basert på offentlig tilgjengelige dokumenter, men at de konkrete prosedyrene ikke er tilgjengelig eksternt.

Det er for så vidt ikke konfidensielle dokumenter, men samtidig ikke sånt som bør ligge offentlig tilgjengelig, for eksempel prosedyrer knyttet til krisehåndtering og kritisk infrastruktur, sier han.

- For noen som vil den enheten vondt, kan dette misbrukes, og det er ikke heldig, men jeg har forstått at det var en feil, sier han.

- Burde vært gradert

Dagbladets kilde i Cyberforsvaret mener deler av disse dokumentene burde vært gradert. Vedkommende ønsker ikke å uttale seg med navn eller bilde i avisa siden dokumentene er sivile, men er soleklar på at dette er informasjon som kan misbrukes og som kan gi fortrinn i forbindelse med eventuell planlegging av aksjoner.

Dokumentene er fra perioden 2003 til 2008, og må derfor anses for å gjengi nåværende status, selv om muligens noe av dette er endret

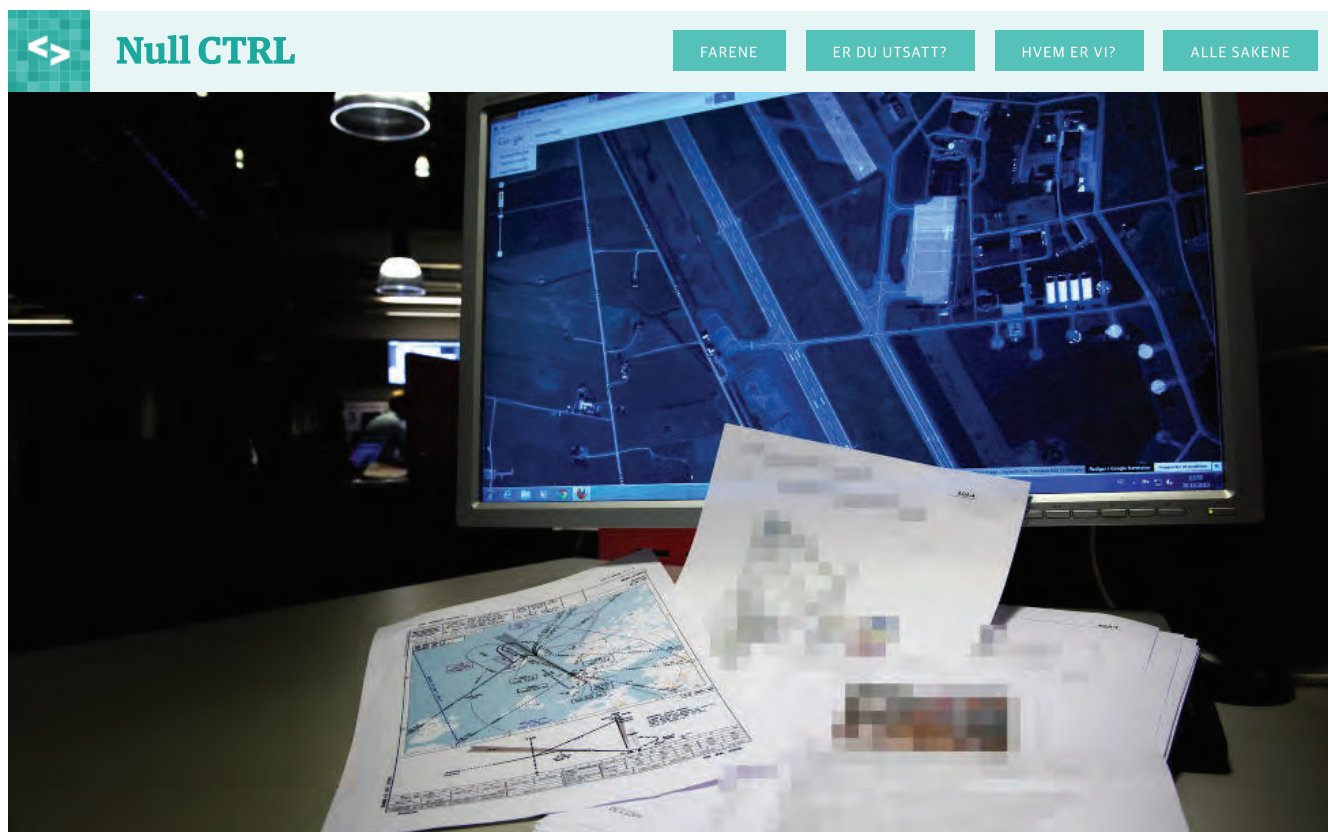
For noen som vil den enheten vondt, kan dette misbrukes.

Svein Pedersen, Seksjonssjef for flysikringsseksjonen i Luftfartstilsynet

i seinere tid. Dette er sivile dokumenter, men sett fra mitt ståsted må mye av dette være unødig informasjon å legge tilgjengelig på Internett, sier vedkommende.

Jeg anser derfor at store deler av denne dokumentmengden kunne vært «unntatt offentligheten» av hensyn til rikets sikkerhet.

Lars William Wroldsen i Luftforsvaret ønsker ikke å kommentere disse vurderingene.



MYE INFORMASJON: Sivile dokumenter om Ørland flystasjon lå tilgjengelig på en vidåpen, privat nettværkdisk. Noe av dette kan misbrukes, mener Luftfartstilsynet. Foto: Øistein Norum Monsen / Dagbladet

La ut dokumenter om Norges nye kampflybase ved en feil

- For noen som vil den enheten vondt, kan dette misbrukes.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



ØISTEIN NORUM MONSEN
onm@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): - Det vil medføre en fare for sikkerheten om dette kommer i hendene på personell med for nasjonen uheldige ideologier og intensjoner, sier en kilde høyt oppe i Cyberforsvaret.

Dagbladet har vist vedkommende en rekke dokumenter med detaljert informasjon om Ørland flystasjon, en av Luftforsvarets to hovedflystasjoner.

Dokumentene er sivile. De ble funnet på en vidåpen nettværkdisk hjemme hos en person med tilknytning til flyplassen. Vedkommende oppgir at han ikke visste at innholdet på serveren var eksponert for alle og enhver.

Mye informasjon

Her fantes blant annet:



For noen som vil den enheten vondt, kan dette misbrukes, og det er ikke heldig.

Seksjonssjef for flysikringsseksjonen i Luftfartstilsynet, Svein Pedersen.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

- Tekniske data for radarer
- Informasjon om bremsevaier og styringssystemet som brukes til å heve og senke denne
- Informasjon om flyplassbelysning og nødstrømskilder
- Forholdsregler ved bombetrussel eller terror
- Informasjon om militære øvingsområder

Ny kampflybase

På Ørland opererer F16-jagerfly, redningshelikoptre og Natos overvåkingsfly, og flyplassen er også et alliert treningssenter. I juni i fjor vedtok Stortinget at Ørland skal være Norges framtidige kampflybase.

I dag er det både sivil og militær trafikk på flyplassen. Luftforsvaret er blitt forelagt flere av dokumentene fra den åpne serveren, og mener disse ikke inneholder skjermingsverdig informasjon.

- Store deler av disse dokumentene er informasjon som skal være offentlig tilgjengelig for nedlasting slik at enhver flyger kan operere trygt i luftrommet, sier kommunikasjonssjef Lars William Wroldsen i Luftforsvaret, som presiserer at dette er informasjon om sivile systemer knyttet til avviklingen av sivil lufttrafikk i fredstid.

- Ikke skadelig

Den mest detaljerte informasjonen er i dokumenter vedrørende lokalt regelverk. Disse finnes ikke tilgjengelig på eksterne nettsider.

- Når det gjelder Avinors lokale planverk for Ørland finner vi ingenting der som er skadelig for Luftforsvaret, sier Wroldsen, men presiserer at de ikke ser noen grunn til at dette skal ligge offentlig tilgjengelig.

- Hva tenker dere om at dette ble lagt ut ved en feil?

- Hvordan og hvorfor disse konkrete Avinor-dokumentene ligger tilgjengelig kjenner jeg ikke til.

Avinor henviser til at dette ikke er gradert informasjon.

- Det er vår oppfatning, ut fra slik du har presentert saken og de dokumentene du har sendt meg, at det ikke er problematisk at en ansatt har tatt med seg dette hjem for å sette seg inn i regelverket, skriver kommunikasjonssjef Kristian Løksa ved flysikringsdivisjonen i Avinor i en e-post.

- Kan misbrukes

Seksjonssjef for flysikringsseksjonen i Luftfartstilsynet, Svein Pedersen, forklarer at en del av informasjonen Dagbladet har funnet er basert på offentlig tilgjengelige dokumenter, men at de konkrete prosedyrene ikke er tilgjengelig eksternt.

- Det er for såvidt ikke konfidensielle dokumenter, men samtidig ikke sånt som bør ligge offentlig tilgjengelig, for eksempel prosedyrer knyttet til krisehåndtering og kritisk infrastruktur, sier han.

- For noen som vil den enheten vondt, kan dette misbrukes, og det er ikke heldig, men



SIVIL OG MILITÆR FLYPLASS: Ørland flystasjon er en av Luftforsvarets to hovedflystasjoner, men det er også sivil flytrafikk der. I juni i fjor vedtok Stortinget at Ørland skal bli Norges nye kampflybase. Arkivfoto: Håkon Eikesdal / Dagbladet

Ørland flystasjon

- En av Luftforsvarets to hovedflystasjoner, og ligger i Ørland kommune i Sør-Trøndelag.
- Opererer F16-jagerfly, redningshelikoptre og Natos overvåkingsfly, og er også et alliert treningssenter.
- Flyplassen er hovedsaklig militær, men det er også sivil flytrafikk der. Kontrolltårnene drives av Avinor.
- I juni i fjor vedtok Stortinget at Ørland skal være Norges framtidige kampflybase.



UGRADERT: Kommunikasjonssjef Kristian Løksa i flysikringsdivisjonen i Avinor påpeker at dokumentene ikke var gradert. Foto: Avinor

jeg har forstått at det var en feil, sier han.

- Burde vært gradert

Dagbladets kilde i Cyberforsvaret mener deler av disse dokumentene burde vært gradert. Vedkommende ønsker ikke å uttale seg med navn eller bilde i avisa siden dokumentene er sivile, men er soleklar på at dette er informasjon som kan misbrukes og som kan gi fortrinn i forbindelse med eventuell planlegging av aksjoner.

- Dokumentene er fra perioden 2003 til 2008, og må derfor anses for å gjengi nåværende status, selv om muligens noe av dette er endret i seinere tid. Dette er sivile dokumenter, men sett fra mitt ståsted må mye av dette være unødig informasjon å legge tilgjengelig på Internett, sier vedkommende i sin vurdering av dokumentene.

- Jeg anser derfor at store deler av denne dokumentmengden kunne vært «unntatt offentligheten» av hensyn til rikets sikkerhet.

Lars William Wroldsen i Luftforsvaret ønsker ikke å kommentere disse vurderingene.



IKKE HELDIG: Seksjonssjef for flysikringsseksjonen i Luftfartstilsynet, Svein Pedersen, mener noe av informasjonen om Ørland flystasjon kan misbrukes. Foto: Luftfartstilsynet

- Det er så alvorlig at vi har stengt tjenesten, publisert onsdag 30. oktober 2013 kl. 12:23

FARENEER DU UTSATT?HVEM ER VI?ALLE SAKENE

Dine kanalerpakker: Fotkepakke

Faktureringsavgiftkr. 40,00

Tegn eFaktura/Avtalegiro for å slippe denne avgiften i fremtiden

AbonnementsnummerKundeservice02828viasat.no/kundeservice

Mandag - fredag08.00 - 21.00

Lørdag10.00 - 16.00

Fakturadato12.10.2013

Betal smartere og spar pengerSpar 480 kr i året! *

Kontakt din bank/nettbank for å tegneAvtaleGiro og/eller eFaktura

* månedlig fakturering med 40 kr i faktureringsavgift

Kvittering

Belop269,00

Betalerens kontonummer

Blankettnummer

RIV HER

Betalingsinformasjon

GIRO

Betalingsfrist

11.11.2013

Underskrift ved girering

ÅPENT FOR ALLE: På Viasats Mine sider kan hvem som helst se andres fakturaer, ved enkelt å skifte ut tall i URL-en. Foto: Skjermdump

- Det er så alvorlig at vi har stengt tjenesten

Viasats kundefakturaer lå åpent på nett.



THERESE DOKSHEIM
tdo@dagbladet.no



LINN KONGSLØ HILLESTAD
lkh@dagbladet.no

(Dagbladet): Hos TV-nettverket Viasat lå en mengde kundefakturaer vidåpne på nett, slik at hvem som helst kunne se dem.

- Det var helt nytt for meg, jeg må sjekke dette, sier selskapets pressesjef, Siv Heimdal når Dagbladet ringer.

«Sekvensnummer»

Dagbladet ble gjort kjent med saken av en av Viasats kunder, som fattet mistanke da han logget seg inn på sin egen kundeside og så at URL-en til web-fakturaen hans så ut som et sekvensnummer.

- Jeg er opptatt av informasjonssikkerhet og pleier alltid å føre noen enkle kontroller når jeg ser løsninger som kan virke sårbare. Hensikten er først og fremst å sikre at mine egne opplysninger ikke er fritt tilgjengelig for andre, sier han.



Vi har sjekket det dere fortalte oss, og det viser seg at det stemmer. Det er veldig beklagelig. Nå har vi tatt ned hele fakturatjenesten, og vi kommer ikke til å åpne den før den er helt sikret.

Siv Heimdal, pressesjef i Viasat.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL

- Jeg forsøkte å endre de siste sifrene i URL-en. Det ga meg umiddelbart tilgang til andre kunders faktura, med informasjon knyttet til vedkommendes kundeforhold.

Stengt ned

Etter at Dagbladet ringte Viasat og fortalte om funksjonen, har selskapet valgt å midlertidig legge ned tjenesten:

- Vi har sjekket det dere fortalte oss, og det viser seg at det stemmer. Det er veldig beklagelig. Nå har vi tatt ned hele fakturatjenesten, og vi kommer ikke til å åpne denne før den er helt sikret. Forhåpentligvis fikses det fort, men fram til det må kundene våre ringe kundeservice for fakturatjenester, sier Heimdal.

Viasat vet foreløpig ikke hvorfor det var mulig å sjekke andre fakturaer enn sine egne.

- Det hadde ingen umiddelbar forklaring på hvordan dette har kunne skjedd. De har nå satt seg ned for å se på dette, og hvordan problemet kan løses. Det er veldig leit for kundene, som ikke kan bruke våre fakturatjenester nå. Vi er veldig takknemlige for at kunden sa ifra til dere, sier hun.

Kunne lastes ned

Utvikler Ola Strømman i Dagbladet opplyser at IT-kyndige personer enkelt kunne ha laget et script som raskt lastet ned alle kundedataene.

I tillegg kunne potensielle svindlere for eksempel ha sendt ut fakturaene med nytt og byttet ut Viasats kontonummer med sitt eget.

Heimdal ser alvorlig på det hele, men påpeker at mye sensitiv informasjon var utelatt.

- Det er viktig å understreke at ingen personopplysninger foruten navn, adresse, kundenummer og abonnementsstype lå ute. Likevel er det selvfølgelig leit at fakturaene lå tilgjengelig, eller at man kunne søke seg fram til forskjellige fakturaer. Det er veldig alvorlig - så alvorlig at vi velger å legge ned tjenesten til problemet er fikset.

- Hadde dere sett for dere at det var mulig med et slikt sikkerhetshull?

- Nei, det var ikke noe vi hadde sett for oss at kunne gå an. Vi satte oss ned med en gang og prøvde å søke og endre tall i URL-en. Så vidt jeg kunne se var det bare helt tilfeldige fakturaer man fikk opp, man kan ikke søke seg fram til en konkret person eller faktura, men det skal jo ikke være slik.

Datatilsynet reagerer

Direktør Bjørn Erik Thon i Datatilsynet er sjokkert over opplysningene.



ALVORLIG: Pressesjef Siv Heimdal i Viasat sier at de ser såpass alvorlig på saken at de midlertidig har sperret ned hele fakturatjenesten. Foto: Viasat



- **SKAL IKKE VÆRE SLIK:** Datatilsynet-direktør Bjørn Erik Thon er overrasket over sikkerhetshullet hos Viasat. Bjørn Erik Thon. Foto: Jo Straube / Dagbladet



Tips oss på nullctrl@dagbladet.no

” Det viser at de har laget et veldig usikkert system som det er lett å gå inn i. Hele hensikten med «Mine sider» er jo at det er mine sider, ikke dine og mine

Bjørn Erik Thon, direktør i Datatilsynet.

- Det viser at de har laget et veldig usikkert system som det er lett å gå inn i. Hele hensikten med «Min side» er jo at det er *min* side, ikke din og min.

Han reagerer på opplysningene som lå ute.

- Det er ingen andre som skal vite hvilke TV-avtaler du har, eller hvilke opplysninger de har lagret om deg. Sånt skal ikke ligge ute, sier Thon.

- Svært sikkerhetshull

- Hva bør Viasat gjøre nå?

- De må absolutt lukke sikkerhetshullet, med en gang. Det er et svært sikkerhetshull, og Viasat må nå sende avviksmelding til oss i Datatilsynet, sier han.

- Må de også informere kundene sine om dette?

- Nei, det kan ikke jeg ta stilling til, men dersom det nå viser seg at personlige opplysninger har kommet på avveie, så må de gi beskjed til de som er rammet, sier Thon.

Heimdal forteller at det er usikkert når Viasats fakturatjenester vil være oppe og gå igjen.

- Vi vet ikke hvor lang tid det kommer til å ta, men vi kommer ikke til å åpne tjenesten før det er helt sikkert, sier hun.

Er du trygg på nettet?



HJEMMET



JOB BEN



BYEN

Slik eksponeres du på Internett

Tenk deg at du med noen tastetrykk kan ta kontroll over naboens overvåkingskamera, åpne konkurrentens database eller styre vitale systemer. I serien Null CTRL viser Dagbladet

hvordan dårlig datasikkerhet kan ramme deg privat, på jobb og i samfunnet generelt. Denne interaktive grafikken illustrerer noe av det vi har funnet.



Test deg selv



Facebook



Twitter



Google+

«Det som er skremmende, er hva journalister i Dagbladet uten spesielle datakunnskaper er i stand til å finne. Hva da med statsmakter, organiserte kriminelle og andre hackere?»

— Seniorrådgiver Vidar Sandland ved Norsk Senter for Informasjonssikring



- **KJEMPEALVORLIG:** Barnevernsjef Hilde Marie Myrvold (t.v.) i bydel Sagene og stedfortreder Hanne Olstad reagerer på at sensitive personopplysninger om barn under barnevernets beskyttelse har ligget åpent på nett. Video: Øistein Norum Monsen/Dagbladet

Barn på hemmelig adresse blottlagt av dataglipp

Dagbladet fant 5958 drosjekunder i åpen og søkbar database tilhørende Oslo Taxi.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLID HILLESTAD
lkh@dagbladet.no



ØISTEIN NORUM MONSEN
onm@dagbladet.no

(Dagbladet): Dagbladet kan i dag avsløre at sensitive data om flere tusen kunder av Oslo Taxi i lang tid har ligget åpent og ubeskyttet på Internett.

- Vi tror basen var åpen i cirka et år, sier daglig leder Bjørn Rebne i Oslo Taxi.

Basen som har vært tilgjengelig via en nettside tilhørende Oslo Taxi, inneholder et kartotek på 5958 kunder innen skolekjøring, TT, fastkjøring og såkalt sosial kjøring.

- Redd for barnas sikkerhet

For mange av kundene er det svært sensitiv informasjon som er lagt inn i basen, blant annet identitet og oppholdsadresse for en rekke barn under barnevernets omsorg.

- Her er det navn jeg kjenner igjen,

” Vi har jo kidnappingssaker på barn som barneverntjenesten har tatt hånd om. Det er jo en potensiell risiko for lekkasjer i et slikt system, og som kan være kjempealvorlig for det barnet det gjelder.

Barnevernsjef Hilde Marie Myrvold, Bydel Sagene



sier Hanne Olstad i barneverntjenesten i bydel Sagene.

- Vi har barn som oppholder seg på sperret adresse, så dette er helt ugreit. Det er en adresse som da ikke skal være kjent for noen andre enn oss. Det kan være en akutt plassering i en tvangsgifte-sak eller i en veldig heavy voldssak, hvor man er redd for barnets sikkerhet dersom om adressen blir kjent, sier barnevernsjef Hilde Marie Myrvold.

Barneverntjenesten frykter databasen kunne blitt utnyttet av personer som adresser og oppholdssteder er blitt holdt hemmelig for.

Vold og kidnapping

- Vi har jo kidnappingssaker på barn som barneverntjenesten har tatt hånd om. Det er jo en potensiell risiko for lekkasjer i et slikt system, og som kan være kjempealvorlig for det barnet det gjelder, sier Myrvold.

- Snakker vi da om fare for liv og helse?

- Ja! I saker hvor vi for en hver pris skal holde barnets oppholdssted skjult, er dette kjempealvorlig. Det er jo gjerne miljøer hvor det utøves en del vold i forbindelse med kidnapping. Det gjelder ungene og det gjelder de som er satt til å ha midlertidig ansvar for de ungene, sier barnevernsjefen i bydel Sagene.

I den søkbare databasen Dagbladet har funnet, er en rekke barn fra store deler av Oslo registrert.

Hemmelig identitet

I flere saker er det ført inn et nummer i databasen. Det er ikke kundennummeret i Oslo Taxi.

- Det er nummer fra vårt fagsystem. Familie, foreldre og parter vil kunne kjenne igjen de numrene. Oslo taxi kan ikke bruke barnevernets ID-nummer som identifikasjon på kjøreoppdrag. Allerede der blir det skummelt. Det er jo ikke noe morsomt dette, sier Myrvold.

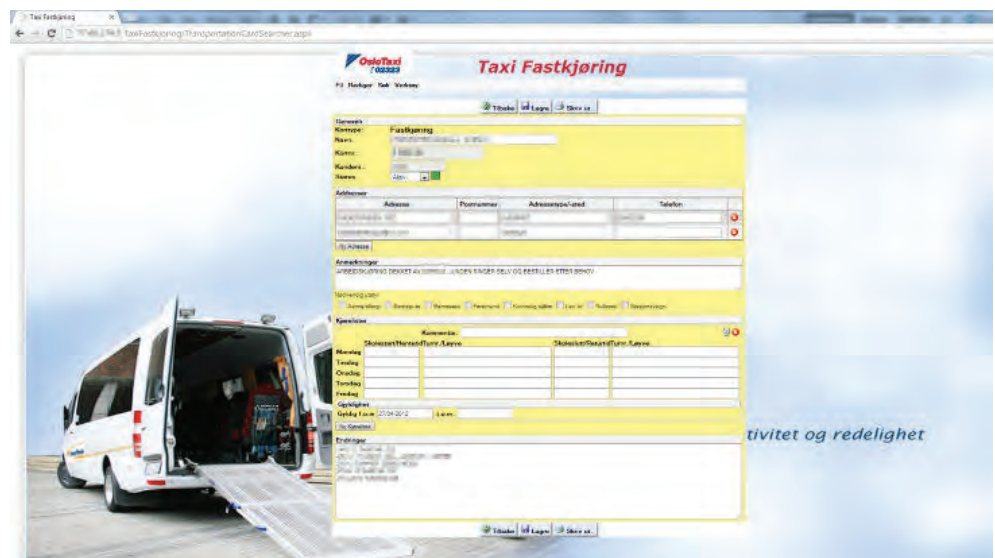
Frykter ikke lekkasje

Oslo Taxi mener det er lite trolig at noen har fått tak i informasjon fra databasen i løpet av det året den har vært tilgjengelig på nett.

ÅPEN DATABASE: Denne basen tilhørende Oslo Taxi lå åpen på Internett. Skjermbildet viser at det er 5958 kort (kunder) i basen. Rutlegardina viser at basen gjelder fastkjøring, skolekjøring, sosialkjøring og TT-kjøring. Foto: Skjermdump

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



EN AV 5958 KUNDER: Dette er eksempel på et kort tilhørende en kunde i databasen tilhørende Oslo Taxi. Informasjon er sladdet av Dagbladet. Foto: Skjermdump



- **SKAL IKKE SKJE:** Oslo Taxi beklager ifølge daglig leder Bjørn Rebne på det sterkeste at informasjonen lå tilgjengelig for uvedkommende. - Dette er et alvorlig sikkerhetsbrudd, og det skal ikke forekomme, sier han. Foto: Øistein Norum Monsen / Dagbladet

Databasene i Oslo Taxi

- Dagbladet fant to databaser, en for drosjealarmarmer og en over faste kundeoppdrag.

- Slik vi ser det i dag, har vi ingen indikasjon på at noe har tilfalt noen, sier Rebne.

- Hva baserer du det på?

- Vi har ikke fått en eneste henvendelse på dette, sier Rebne.

- Om noen har nyttegjort seg innholdet, er det vel ikke dere de ville meldt fra til?

- Nei, men sannsynligheten for det er vel ekstremt liten. Hva skal man med det, spør Rebne.

- Mulig risikosituasjon

Barneverntjenesten ser et annet alvor:

- Om du virkelig vil ha tak i en unge som er på sperret adresse, og som du da har mistanke om blir kjørt i barnehagen i drosje, så vil jeg tro at noen ville kunne tenkt så langt at de hadde søkt både på ID og på navn, og da har du med en gang en risikosituasjon, sier Myrvold.

- Vi har saker hvor identiteten til ungen ikke skal bli kjent, og ikke minst adressen hvor barnet oppholder seg. Så dette er helt klart alvorlig, sier hun.

- Vi har brukt Oslo Taxi i mange, mange år og vi har en forventning om at de vet hvem de har med å gjøre, at det er barn fra barnevernet de kjører. En skulle tro de tok slike hensyn, men dette vitner om at de ikke gjør det, sier Olstad.

Lukket databasen

Oslo Taxi lukket databasen samme dag som Dagbladet varslet om at den var åpen. De ber om å bli sitert på følgende:

- Vi setter stor pris på at Dagbladet gjorde oss oppmerksomme på sikkerhetshullet. Oslo Taxi beklager på det sterkeste at denne informasjonen lå tilgjengelig for uvedkommende. Dette er et alvorlig sikkerhetsbrudd, og det skal ikke forekomme. Tilgangen til tjenestene ble selvsagt umiddelbart stengt da vi ble gjort kjent med feilen, og opplysningene har siden ikke vært tilgjengelig for uvedkommende. Foruten å utbedre det aktuelle avviket, har vår IT-avdeling hatt en gjennomgang av bedriftens datasikkerhet, og vil fortsette dette arbeidet, sier Rebne i en e-post.

Ifølge Rebne er databasen en annen enn den sjåførene har tilgang til.

- En database inneholdt 5958 kort på kunder med sosialkjøring, TT-kjøring, skolekjøring eller fastkjøring.
- Basen inneholder blant annet navn, ID, adresser, telefonnumre og sensitive data om mange av kundene.
- Spesielt inneholder basen sensitive data om TT-kunder og klienter tilknyttet sosial kjøring.
- En annen database inneholder 26062 innrapporterte alarmlogger fra drosjebilene.
- Alarmloggene inneholder rapporter om hendelser (f.eks. ran og overfall) i drosjebilene, og hvordan situasjonene er håndtert.
- Alt dette har vært tilgjengelig fra en nettside hvor ansatte også kan laste ned programvare for teknisk utstyr tilknyttet Oslo Taxi.
- Tilgjengeligheten til databasene ble stengt da Dagbladet orienterte Oslo Taxi om sikkerhetssvikten.

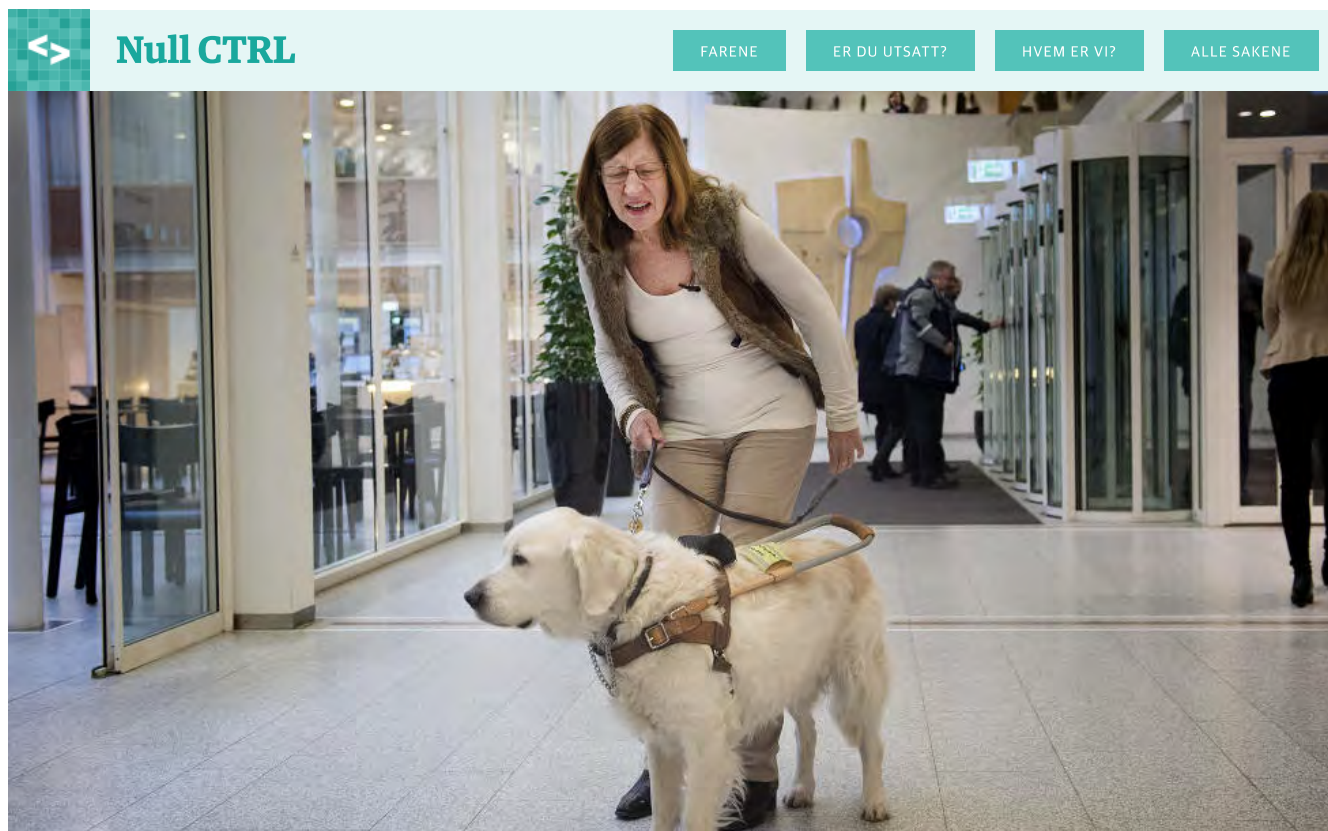
[illegible]

LANG LISTE I basen er det øyensynlig mulig å søke etter bestemte personer eller bla gjennom listene over brukere. Klikker man på ikonet «Vis kort» kommer det opp detaljert informasjon om den enkelte. Foto: Skjermdump



Tips oss på nullctrl@dagbladet.no

- Jeg reagerer med skrekk, publisert mandag 25. november 2013 kl. 13:27



- **BØR BESKYTTES:** I Oslo Taxis database lå det sensitive opplysninger om Synnøve Margrethe Nordeng og personer med spesialbehov. Hun mener basen inneholder informasjon om mange som bør beskyttes bedre, og håper Datatilsynet vil se på saken. Her er hun med førerhunden Apollo. Foto: Øistein Norum Monsen/Dagbladet

- Jeg reagerer med skrekk

Synnøve er en av flere hundre TT-brukere som er rammet av dataglipp i Oslo taxi.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLI HILLESTAD
lkh@dagbladet.no

(Dagbladet): Dagbladet har avslørt hvordan [sensitive data om flere tusen drosjekunder](#) i lang tid har ligget åpent og ubeskyttet på Internett.

Ifølge daglig leder Bjørn Rebne i Oslo Taxi kan basen ha ligget [åpent på nett i et år](#).

Basen som har vært tilgjengelig via en nettadresse tilhørende Oslo Taxi inneholder et kartotek på 5958 kunder inneforfor skolekjøring, TT-kjøring, fastkjøring og såkalt sosial kjøring.

Synnøve Margrethe Nordeng er bruker av tilrettelagt transport (TT), og blant flere hundre personer med



fast TT-avtale som er registrert med sensitive data i basen.

- Plikt å beskytte

Dagbladet møter Synnøve og førerhunden «Apollo» i kantina ved barne- og likestillingsdepartementet, hvor hun jobber. Vi leser for henne hva det står i Oslo Taxis database om henne som TT-bruker.

- Jeg reagerer med skrekk på det. Det synes jeg er prinsipielt ille at er opplysninger skal komme andre for øre og øye, sier hun.

Mer reagerer hun på de mange vanskeligstilte som i databasen er registrert med sensitive data.

- Det er enda verre, for de kan ikke forsvare seg. Mennesker som ikke har ressurser til det. Jeg synes vi har en plikt på oss til å beskytte ressursvake mennesker i en situasjon. Det er ille. Det er sensitive opplysninger som ikke skal ut, sier hun.

Prisgitt andre

- Bør det få noen konsekvenser for Oslo taxi?

- Jeg synes Datatilsynet bør påtale det, sier Nordeng.

- Får det noen konsekvenser for deg?

- Jeg vil kanskje være mer forsiktig med å utgi personlige opplysninger. Men når det gjelder transporttjenestene for funksjonshemmede er det jo bydelene her i Oslo som legger inn informasjonen, så da har du ikke så mye du skulle sagt om hva som blir lagt inn. Du er prisgitt den informasjonen som legges inn om deg i tjenesteapparatet, sier Nordeng.

- Legger oss flate

Dagbladet har vist Synnøves databaseregistrering til daglig leder Bjørn Rebne i Oslo Taxi.

- Hva har du å si til Synnøve?

- Det var veldig beklagelig at dette lå for åpent, sier Rebne - og legger til:

- Vi har et voldsomt turantall og en voldsom omsetting. Vi har moderne anlegg, så det er sagt. Vi har nå sendt ut en beklagelse til brukerne. Vi legger oss flate. Det som har skjedd har skjedd, og vi er fornøyd med at vi har gjort grep. Dette var interne hjelpeprogrammer som ikke

- **ALVORLIG:** Barnevernsjef Hilde Marie Myrvold (t.v.) i bydel Sagene og stedfortreder Hanne Olstad reagerer på at sensitive personopplysninger om barn under barnevernets beskyttelse har ligget åpent på nett. Video: Øistein Norum Monsen/Dagbladet

Oslo Taxi database record for Synnøve Margrethe Nordeng. The record shows personal information, address, and a list of vehicles (køretøyer) with their respective status and dates. The interface is in Norwegian and shows a search result for 'TT-Kjøring'.

EN AV 5958 KUNDER: Dette kortet tilhører Synnøve Margrethe Nordeng og er en av 5958 registreringer i databasen tilhørende Oslo Taxi. Flere slike skjemaer inneholder meget sensitiv informasjon. Kortet gjengis med samtykke, men Dagbladet har sladdet privat informasjon. Foto: Skjermdump

Oslo Taxi database search interface. The search results show a list of vehicles (køretøyer) with their respective status and dates. The interface is in Norwegian and shows a search result for 'TT-Kjøring'.

ÅPEN DATABASE: Denne basen tilhørende Oslo Taxi lå åpen på Internett. Skjermbildet viser at det er 5958 kort (kunder) i basen. Rullegardina viser at basen gjelder fastkjøring, skolekjøring, sosialkjøring og TT-kjøring. Foto: Skjermdump

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

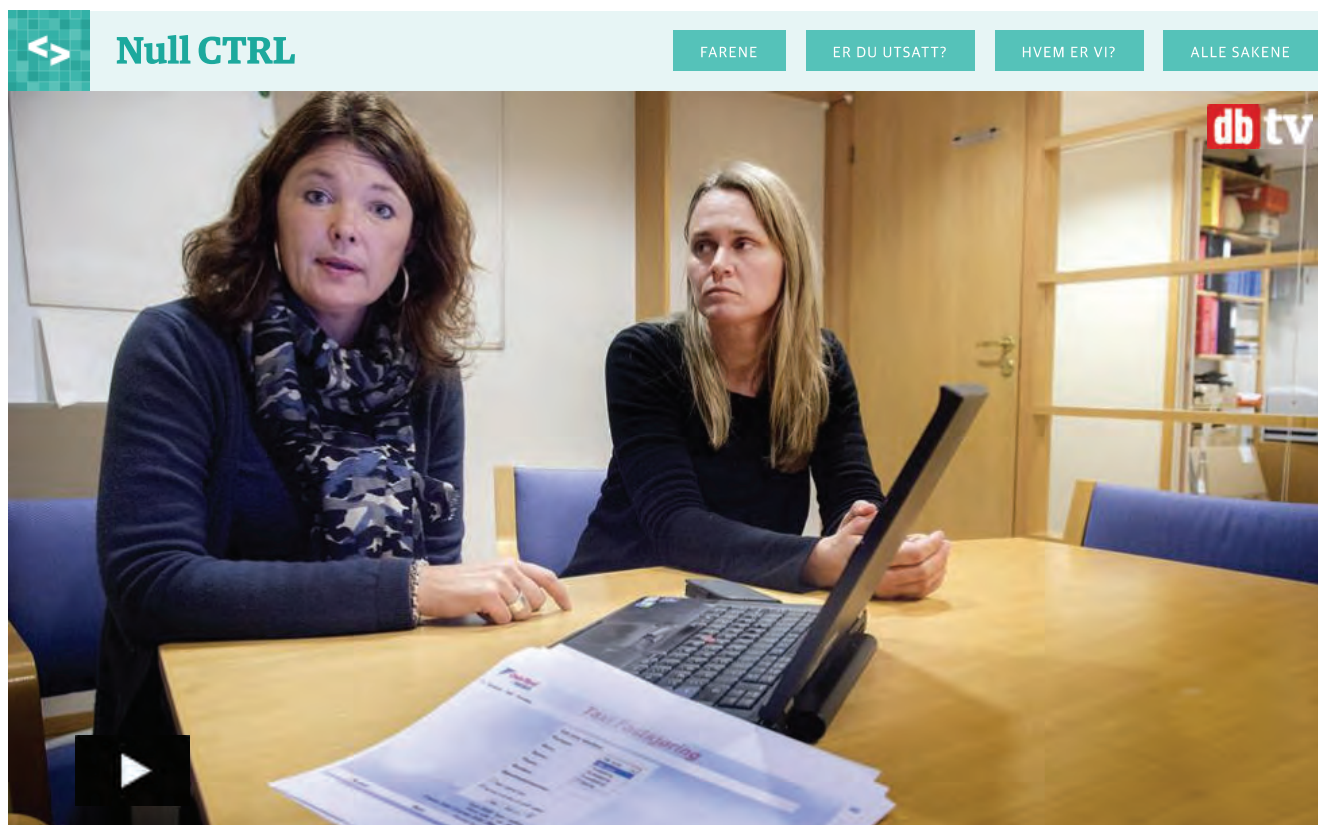
- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL

Kilde: Wikipedia

- Det kan sette barn i fare om dette kommer ut, publisert mandag 25. november 2013 kl. 17:00



- **ALVORLIG:** Barnevernsjef Hilde Marie Myrvold (t.v.) i bydel Sagene og stedfortreder Hanne Olstad reagerer på at sensitive personopplysninger om barn under barnevernets beskyttelse har ligget åpent på nett. Video: Øistein Norum Monsen/Dagbladet

- Det kan sette barn i fare om dette kommer ut

Datatilsynet reagerer på dataglipp ved Oslo Taxi.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ØISTEIN NORUM MONSEN
onm@dagbladet.no

(Dagbladet): Dagbladet har avslørt hvordan [sensitive data om flere tusen kunder av Oslo taxi](#) i lang tid har ligget åpent og ubeskyttet på Internett.

- Opplysningene dere har vist meg har absolutt ikke noe på nett å gjøre. Dette er ting som skal holdes helt internt og som ikke noen andre uvedkommende skal få se, sier direktør Bjørn Erik Thon i Datatilsynet.

Ifølge daglig leder Bjørn Rebne i Oslo Taxi kan den søkbare databasen med 5958 kunder ha ligget åpen på en nettadresse tilhørende selskapet i cirka et år.



- Barn i fare

I basen finnes detaljert informasjon om skolekjøring, TT-kjøring, fastkjøring og såkalt sosial kjøring.

- **BRØT TROLIG LOVEN:** Ifølge direktør Bjørn Erik Thon i Datatilsynet brøt Oslo Taxi trolig personopplysningsloven. Foto: Øistein Norum Monsen/Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

Det reagerer Datatilsynet sterkt på. I hånda holder direktør Bjørn Erik Thon i Datatilsynet et kort fra taxibasen Dagbladet fant på nett.

- Det jeg ser her er en utskrift fra en såkalt sosialkjøring, en kjøring for barneverntjensten på Stovner, med detaljerte opplysninger om denne jenta. Det er svært alvorlig. Dette skal egentlig være skjermet for alt innsyn. Nettopp fordi det kan være barn som er plassert av en helt spesiell grunn og som foreldrene kanskje ikke skal se. Dette kan i verste fall sette disse barna i fare om det kommer ut, sier Thon.

Konfidensielt

Dagbladet har vist ham et [intervju med synshemmede Synnøve Margrethe Nordeng](#). Hun er opprørt på egne vegne, men også [på vegne av de mange i databasen](#) som ikke har ressurser til å ta til motmæle.

- Det her skal jo ikke ligge ute på nett. Synnøve her har jo en grunn til å ha TT-kjøring, og det har ingen noe med. Her står det jo taxikortnummeret hennes, fullt navn, adresse og hvor hun hentes. Dette skal ikke ligge ute, sier Thon.

Oslo Taxi opplyser til Dagbladet at de nå har sendt inn en avviksmelding om dataglippen til Datatilsynet. Dagbladet har bedt om å få se den.

- Dette er mellom oss og Datatilsynet, sier daglig leder Bjørn Rebne i Oslo Taxi i en e-post til Dagbladet.

Trolig lovbrudd

Ifølge Thon har Oslo Taxi trolig brutt personopplysningsloven:

- Det er helt klare regler i personopplysningsloven. De reglene tror jeg vi mer eller mindre klart kan si at er blitt brutt her, fordi dette er opplysninger som ikke skal ut, sier Thon.

Han henviser igjen til Synnøve og [opplysningene i databasen om hennes TT-kjøring](#):

- Synnøve er navngitt, det står hvor hun bor, at hun har TT-kjøring. Det står også at hun har en førerhund og dermed kan vi slutte at hun er synshemmet eller kanskje blind. Og det er opplysninger som i tillegg handler om helseforhold, som er sensitive opplysninger. Det er klart de her har brutt konfidensialiteten som Synnøve og alle andre har krav på, sier Thon.

Avventer reaksjon

- Opplysningene dere har vist meg har absolutt ikke noe på nett å gjøre. Dette er ting som skal holdes helt internt og som ikke noen andre uvedkommende skal få se, konkluderer Thon.

Han ønsker ikke å forskutere eventuelle reaksjoner mot Oslo Taxi, men vil nå se nærmere på avviksmeldingen han regner med kommer fra Oslo Taxi.

- Vi beklager

Oslo Taxi ønsker å bli sitert på følgende:

- Vi setter stor pris på at Dagbladet gjorde oss oppmerksomme på sikkerhetshullet. Oslo Taxi beklager på det sterkeste at denne informasjonen lå tilgjengelig for uvedkommende. Dette er et alvorlig sikkerhetsbrudd, og det skal ikke forekomme. Tilgangen til tjenestene ble selvsagt umiddelbart stengt da vi ble gjort kjent med feilen, og opplysningene har siden ikke vært tilgjengelig for uvedkommende, skriver daglig leder Bjørn Rebne i en e-post.

Av tiltak nevner han:

- Foruten å utbedre det aktuelle avviket, har vår IT-avdeling hatt en gjennomgang av bedriftens datasikkerhet, og vil fortsette dette arbeidet. Det kan nevnes at vi allerede i midten av oktober

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



Tips oss på nullctrl@dagbladet.no

inngikk avtale med en ekstern leverandør av datasikkerhet om en gjennomgang av våre systemer på årlig basis. Denne gjennomgangen er ennå ikke gjennomført for 2013, men ville nok ha avdekket avviket, hvis ikke Dagbladet hadde gjort oss kjent med det, hevder Rebne.



STOR KONTRAKT: Oslo kommune har flere større kontrakter med Oslo Taxi. - I veldig alvorlige tilfeller kan vi si opp kontrakten, sier seksjonssjef Hedda Aas ved TT-seksjonen i Oslo kommune om TT-kontrakten. Foto: Øistein Norum Monsen/Dagbladet

Oslo kommune vurderer avtalen med Oslo Taxi

Reagerer på alvorlig dataglipp etter Dagbladet-avsløring.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLI HILLESTAD
lkh@dagbladet.no

(Dagbladet): Dagbladet har avslørt hvordan [sensitive data om flere tusen kunder av Oslo Taxi](#) i lang tid har ligget åpent og ubeskyttet på Internett.

Datatilsynet mener selskapet trolig [har brutt personopplysningsloven](#).

- Opplysningene dere har vist meg har absolutt ikke noe på nett å gjøre. Dette er ting som skal holdes helt internt og som ikke noen andre uvedkommende skal få se, sier direktør Bjørn Erik Thon i Datatilsynet.

- Skal være trygt

Ifølge daglig leder Bjørn Rebne i Oslo Taxi kan den søkbare databasen med 5958 kunder ha ligget åpen på en nettadresse tilhørende selskapet i cirka et år.



- **ALVORLIG:** Barnevernsjef Hilde Marie Myrvold (t.v.) i bydel Sagene og stedfortreder Hanne Olstad reagerer på at sensitive personopplysninger om barn under barnevernets beskyttelse har ligget åpent på nett. Video: Øistein Norum Monsen/Dagbladet



- Det står helt tydelig og klart i kontrakten at informasjon om våre brukere ikke skal falle i hendene på uvedkommende, så det er i strid

Blant brukerne er det registrert skolekjøring, sosial kjøring og TT-kjøring. En av dem som har reagert er synshemmede Synnøve Margrethe Nordeng, som er blant [TT-brukerne registrert i databasen](#).

- Det beklager jeg at har skjedd. TT-tjenesten skal være en trygg tjeneste også i forhold til informasjon. Det skal vi jobbe for at ikke skjer igjen, sier seksjonssjef Hedda Aas ved TT-seksjonen i Oslo kommune.

Ifølge Aas kjøper kommunen taxitjenester for rundt 220 millioner kroner i året knyttet til TT. De fleste av kommunens avtaler er med nettopp Oslo taxi, men ikke alle.

Vil vurdere kontrakten

Oslo kommune går nå gjennom sikkerhetsglippen og avtalen med Oslo taxi.

- Det lå informasjon om våre brukere på Internett, åpent tilgjengelig for uvedkommende. Det skal det ikke gjøre. Det ser vi meget alvorlig på, sier Aas til Dagbladet.

Den konkrete avtalen knyttet til TT-kjøringen - og som er registrert i den aktuelle databasen - har ifølge Aas en ramme på nærmere 20 millioner kroner i året.

- Vi er i ferd med å se på basen dere har funnet tilgang til. Vi vil vurdere opp mot kontrakten vår hvordan vil følge det opp, sier Aas.

Kommunen har mottatt en foreløpig rapport om dataglippen fra Oslo Taxi. Men det er etter hva Dagbladet erfarer ikke svar godt nok for kommunen på vegne av brukerne.

- Det står helt tydelig og klart i kontrakten at informasjon om våre brukere ikke skal falle i hendene på uvedkommende, så det er i strid med kontrakten at det har skjedd, sier Aas.

Aas presiserer at hun i denne sammenheng uttaler seg om den aktuelle TT-avtalen, ikke om Oslo kommunes taxi-avtaler generelt.

Særskillt data-avtale

Velferdsetaten har i tillegg til anbudsavtaler, en helt spesifikk «databehandlingsavtale» med Oslo Taxi.

Den er signert i mars 2012 og resignert i mars 2013. Avtalen gir detaljerte instruksjoner om hva Oslo kommune forventer av drosjeselskapet i dets håndtering av sensitive data.

Det handler om hvem som skal gjøre det, hvordan det gjøres og hvilke sikkerhetstiltak data skal være underlagt. Blant annet er alle som skal ha tilgang til data fra Velferdsetaten pålagt å ha individuelt passord for å få adgang til informasjon.

Kan stille krav

Avtalen presiserer også hva som kvalifiserer til mislighold.

med kontrakten at det har skjedd.

Seksjonssjef Hedda Aas ved TT-seksjonen i Oslo kommune

SAKENS KJERNE: Dagbladet fant denne databasen liggende åpen og ubeskyttet på en nettside tilhørende Oslo taxi. I basen er det mulig å søke opp eller bla seg gjennom data registrert på 5958 kundekort. Mange er registrert med sensitive data i forbindelse med skolekjøring, sosial kjøring eller TT-kjøring. Foto: Skjermdump

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



Tips oss på nullctrl@dagbladet.no

Tilrettelagt transport:

- Forkortes ofte «TT».
- Tilrettelagt transport (TT) er et norsk fylkeskommunalt transporttilbud for handikappede eller eldre som ikke kan benytte ordinær kollektivtransport.
- I de fleste fylkeskommunene gjennomføres tilrettelagt transport med drosje.
- Standarden i tilbudet samt egenandeler

- Hvilke verktøy har etaten overfor Oslo taxi ved eventuelt mislighold?

- **Ifølge kontrakten kan vi stille krav om retting, gjennomgang av rutiner, bøter - og i veldig alvorlige tilfeller kan vi også si opp kontrakten, sier Aas.**

Frykter ikke kontrakter

- Tror du dataglippen kan få kontraktsmessige konsekvenser?

- Nei, det tror jeg ikke. Vi er opptatt av å se på hva som virkelig har skjedd og være åpne med Velferdsetaten. Jeg kan ikke se at det skal få noen konsekvens per i dag, sier daglig leder Bjørn Rebne i Oslo Taxi til Dagbladet.

Ifølge Rebne har TT-brukere med såkalt hvitt kort fått en skriftlig beklagelse fra Oslo Taxi.

- Skal ikke forekomme

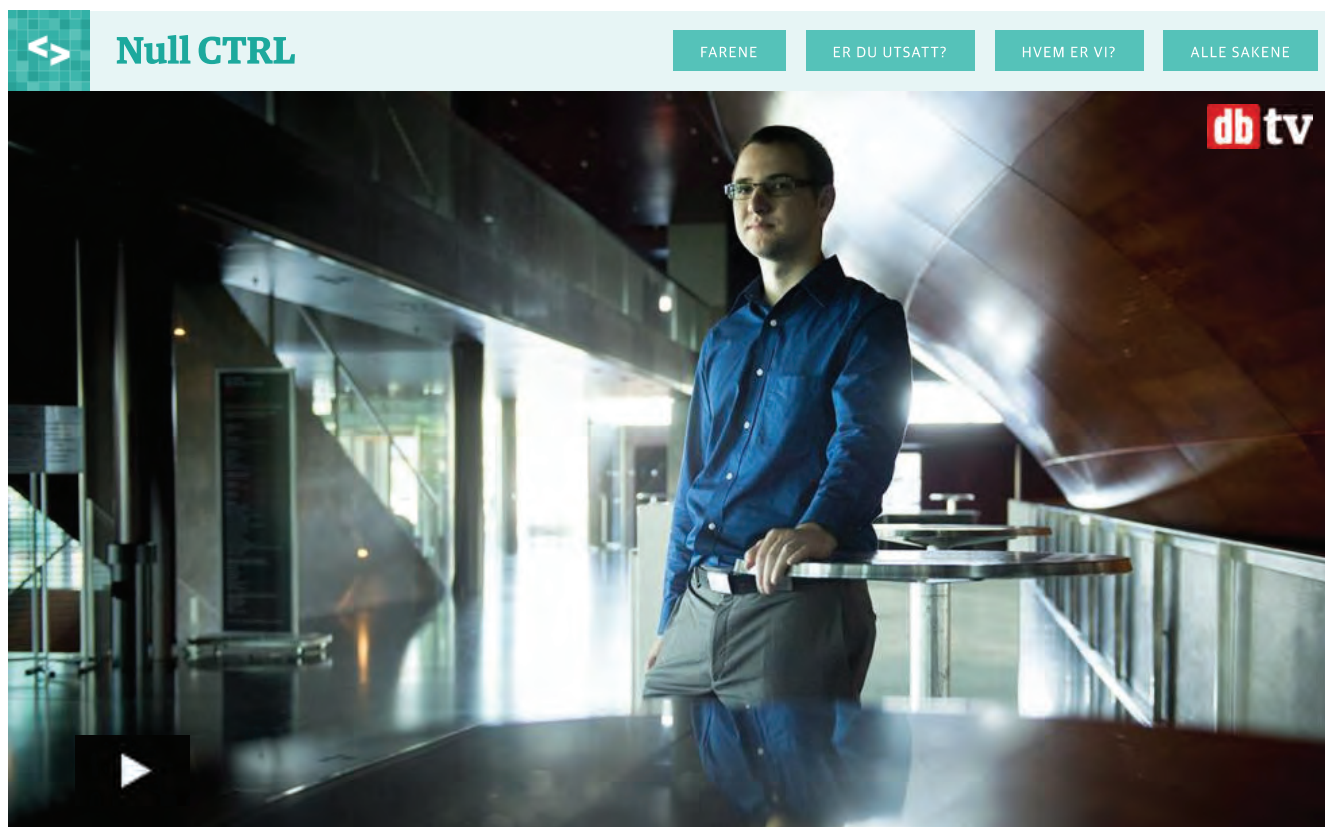
Oslo Taxi ønsker å bli sitert på følgende:

- Vi setter stor pris på at Dagbladet gjorde oss oppmerksomme på sikkerhetshullet. Oslo Taxi beklager på det sterkeste at denne informasjonen lå tilgjengelig for uvedkommende. Dette er et alvorlig sikkerhetsbrudd, og det skal ikke forekomme. Tilgangen til tjenestene ble selvsagt umiddelbart stengt da vi ble gjort kjent med feilen, og opplysningene har siden ikke vært tilgjengelig for uvedkommende, skriver daglig leder Bjørn Rebne i en e-post.

- Foruten å utbedre det aktuelle avviket, har vår IT-avdeling hatt en gjennomgang av bedriftens datasikkerhet, og vil fortsette dette arbeidet, skriver Rebne.

fastsettes av hver enkelt fylkeskommune, som medfører at tilbudet varierer fra fylke til fylke.

Kilde: Wikipedia



MEDIESKY: John Matherly er skaperen av søkemotoren Shodan. I dette eksklusive intervjuet med Dagbladet forklarer han hvorfor et slikt verktøy er «på de godes side». Video: Øistein Norum Monsen/Dagbladet

Dagbladet har overlevert 2500 IP-adresser til NSM, eiere og leverandører

Advarer om «Null CTRL».



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): I artikkelserien «[Null CTRL](#)» viser Dagbladet [gjennom fysisk testing](#) hvordan sviktende datasikkerhet rammer deg og meg hjemme, på jobb og i det offentlige rom.

Så langt har vi avdekket:

- [2048 overvåkningskameraer](#) i Norge ligger tilgjengelig på nett

- De finnes i [private hjem](#), [nattklubber](#), [butikker](#) og [restauranter](#)

- Over [2500 styringssystemer](#) i Norge er koblet til nett, med minimal eller ingen sikkerhet

- [500 av disse kontrollerer industriell eller samfunnskritisk infrastruktur](#)

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: [#null_CTRL](https://twitter.com/null_CTRL)

• [1781 printere ligger tilgjengelig](#) på nettet i Norge. Flere tilhører UiO og NTNU

• Flere tusen databaser og servere gir deg alt innhold - uten å taste et eneste passord

Varslet eiere

Totalt har vi undersøkt 535 320 unike norske IP-adresser og 707 358 åpne porter i forbindelse med «Null CTRL».

Berørte parter er blitt varslet i god tid før Dagbladet har publisert artikler, slik at de har hatt mulighet til å stenge ned systemene.

Hittil har Dagbladet overlevert lister med 2500 mulig kritiske IP-adresser til henholdsvis Nasjonal Sikkerhetsmyndighet (NSM), eiere og nettleverandører.

Alarm!

Formålet med serien er å avdekke hva sviktende datasikkerhet kan føre til - ikke teoretisk, men helt konkret.

For eksempel:

• Åpne [servere tilhørende brannberedskapen](#) i 39 av 44 kommuner i Nordland

• Sensitive dokumenter om [Norges nye kampflyplass](#)

• 15 innganger til [Jernbaneverkets brannvarsling](#)

• Sensitive kundedata tilhørende [barn med hemmelig ID](#)

• Dagbladet kunne [styre varmen i hele kvartalet](#).

• [Klining og fyll](#) for åpent kamera.

Lanserte testfunksjon

Som hjelpemiddel for leserne har Dagbladet laget [en interaktiv guide til mulige sikkerhetshull](#).

Funnene er basert på vår egen research i [søkemotoren Shodan](#), og bearbeidet i Dagbladets modifiserte versjon.

22. oktober [lanserte Dagbladet en egen testmotor](#) knyttet opp mot et Shodan-arkiv. Til nå har 250 000 unike IP-adresser blitt testet. Testen viser så langt at [en av fire har potensiell svikt i sikkerheten](#).



- **ALVORLIG:** Barnevernsjef Hilde Marie Myrvold (t.v.) i bydel Sagene og stedfortreder Hanne Olstad reagerer på at sensitive personopplysninger om barn under barnevernets beskyttelse har ligget åpent på nett. Video: Øistein Norum Monsen/Dagbladet



DIGITALE TRUSLER: Generalmajor Roar Sundseth i Cyberforsvaret ser en stadig økning i digitale trusler mot Norge. Video: Øistein Norum Monsen / Dagbladet



- **ENKELT TERRORMÅL:** Ledelsen ved fiskebollenfabrikken Vesteraalens frykter sabotasje om fabrikkinformasjon kommer på avveie. Video: Øistein Norum Monsen/Dagbladet

[Klikk her og ta testen](#)

Følg serien her:

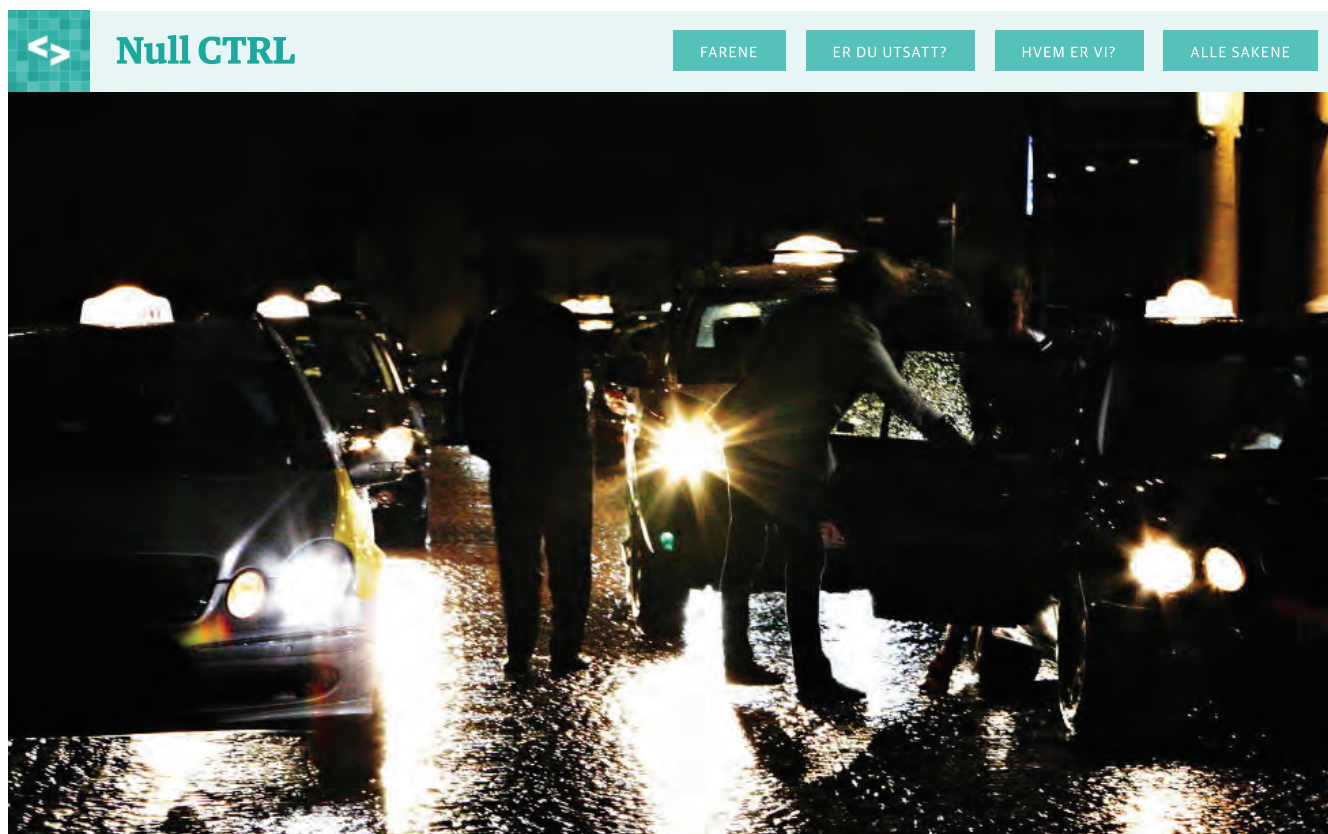
[Null CTRL](#)



Tips oss på nullctrl@dagbladet.no



SKUMMELT: Trond Kristiansen ante ikke at overvåkingskameraet hans kringkastet bilder og lyd rett ut på Internett. Uvedkommende kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet



DYSTERT: Dagbladet har avdekket en rekke drosjeselskaper med sensitive data om kunder liggende åpent på nett. Arkivfoto: Nina Hansen/Dagbladet

Dagbladet fant åtte åpne drosje-servere på nett

- Ingen forstår hvorfor.



ESPEN SANDLI
esan@dagbladet.no



TORGEIR P. KROKFJORD
tpk@dagbladet.no



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): Dagbladet har avslørt hvordan [sensitive data om flere tusen drosjekunder](#) i lang tid har ligget åpent og ubeskyttet på Internett.

Ifølge daglig leder Bjørn Rebne i Oslo Taxi kan databasen ha ligget [åpent på nett i et år](#).

Ikke alene

Men Oslo Taxi er ikke det eneste selskapet med større dataglipp. I research av serien «Null CTRL» har Dagbladet funnet tilsammen 14 dataservere tilhørende ulike taxiselskaper.

Åtte av disse lå helt åpent, uten noen form for passordbeskyttelse.

Hvem de ulike serverne tilhører, kan du lese i en egen faktaboksen.

Seks av systemene er levert av ett

Indeks for /

Navn	Størrelse	Dato endret
Dagfiler/		23.01.12 11:53:00
Data/		12.10.11 14:17:00
Firmware/		12.10.11 14:17:00
Gml/		20.03.13 16:41:00
Kommandoer/		28.01.13 15:05:00
Logoer/		13.03.13 14:13:00
Program/		23.05.13 09:53:00
Sonelister/		13.03.13 14:10:00
Takster/		20.03.13 16:38:00
UpdateTmpLogs/		25.10.13 00:22:00

RETT PÅ NETT: Seks drosjeselskaper hadde informasjon fra taksamateret liggende på en åpen FTP-server. Foto: Skjermdump

og samme selskap, Transport Data Systems AS (TDS).

«TDS har nå hovedfokus mot taxi-markedet i Skandinavia. Teknologien er banebrytende på det Skandinaviske taximarkedet,» heter det på selskapets [egne nettsider](#).

«Skjerp dere»

De aktuelle serverne inneholder informasjon for hver av bilene eller løyvene tilhørende den respektive drosjesentralen. Sortert i mapper ligger det informasjon om bilenes oppdrag, hvem kjøreoppdraget er for, betalingsinformasjon, hvor man hentes og hvor man leveres.

Store mengder data er kunde-sensitivt.

Ved enkelte sentraler framkommer også kommunikasjon og beskjeder sentralen gir til sjåførene. Som for eksempel:

- Nå må dere skjerpe dere. Vi får mange klager.

I tillegg inneholder serverne en rekke tekniske data.

- Vi forstår ikke hvorfor

- Jeg kan bekrefte at basen har ligget åpen, noe som er tilfelle for flere selskaper som bruker den samme taksameter-leverandøren, sier daglig leder Bjørn Christiansen i Taxi Sør til Dagbladet.

- Ingen forstår hvorfor det har stått åpent. Nå er den stengt. Jeg vil gjerne takke Dagbladet for at vi fikk beskjed om dette, sier Christiansen.

- Nå er det stengt

Etter Dagbladets henvendelser til drosje-selskapene, har disse henvendt seg til leverandøren TDS. Leverandøren tar imidlertid ikke på seg alt ansvar:

- Flesteparten av våre kunder drifter sine taxisystemer og brannmurer selv. Men på grunnlag av flere spørsmål fra kunder har vi vært gjennom alle kundene sine brannmurer og stengt den åpne tilgangen til ftp-serverne, skriver Ole Petter Bogen i Transport Data Systems i en e-post til Dagbladet.

- Jeg har ikke noen kommentar til dette, unntatt å fikse det, sier daglig leder Harald Danielsen i Taxi 3 Østfold.

Dagbladet er kjent med at minst to drosjeselskaper oppdaget feilen selv, og har ryddet opp på egen hånd. En av dem er Harstad taxisentral.

- Takk for at dere sier fra. Feilen ble oppdaget for en tid tilbake - og rettet, sier daglig leder Tom Jakobsen ved Harstad Taxisentral.

Seks lukkede

Dagbladet fant ytterligere seks drosjedatabaser koblet til nett, tilhørende en annen leverandør. Disse hadde imidlertid en viss datasikkerhet i form av passordbeskyttelse.

Dagbladet har tidligere omtalt dataglippen ved Oslo Taxi, hvor et [kartotek med 5958 kunder](#) lå åpent på nett. Men på samme IP-adresse fant Dagbladet også en annen database tilhørende Oslo Taxi.

Null CTRL

• Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

• I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

• Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).

• Følg serien her: <http://www.dagbladet.no/nullctrl/>

• Tips oss på nullctrl@dagbladet.no

• Si din mening på Twitter: #null_CTRL

14 drosjesentraler på nett:

Dagbladet fant seks åpne dataservere tilhørende:

- Taxi 3 (Østfold)
- Taxi 2 (Oslo)
- Taxi Sør (Agder)
- A-Taxi (Hordaland)
- Taxi Harstad (Troms)
- Ål Taxi (Buskerud)

• Serverne inneholder blant annet kjøre- og kundedata fra drosjenes betalingssystem - tur for tur, dag for dag. Basene lå på åpen FTP-server.

To fra Oslo Taxi

• Dagbladet fant [to databaser tilhørende Oslo Taxi](#) liggende på en åpen nettadresse.

• En database inneholdt 5958 kort på [kunder med sosialkjøring](#), [TT-kjøring](#), skolekjøring eller [fastkjøring](#).

• En annen database inneholdt informasjon om 26 062 innrapporterte alarmer fra drosjebilene til drosjesentralen.

• *Alle eierne ble varslet av Dagbladet i god tid før denne artikkelen ble publisert.*

Seks sikrede

Dagbladet fant også databaser tilhørende ytterligere seks drosjesentraler. Disse lå på en åpen nettside, men var sikret med passordbeskyttelse.

Navn	Størrelse	Sist endret
010709448605_GenInfo.xml	1 KB	30.06.2013 18:15:00
010709448781_ServiceSetup.xml	2 KB	30.06.2013 18:15:00
010809476161_GenInfo.xml	1 KB	31.07.2013 17:02:00
010809476163_ServiceSetup.xml	2 KB	31.07.2013 17:02:00
0108097226206_GenInfo.xml	1 KB	31.08.2013 15:07:00
0108097226206_ServiceSetup.xml	2 KB	31.08.2013 15:07:00
011006062019_GenInfo.xml	1 KB	30.09.2013 20:18:00
011006062019_ServiceSetup.xml	2 KB	30.09.2013 20:18:00
020709042674_GenInfo.xml	1 KB	01.07.2013 06:42:00
020709042674_ServiceSetup.xml	2 KB	01.07.2013 06:42:00
020808424333_GenInfo.xml	1 KB	01.08.2013 08:42:00
020808424333_ServiceSetup.xml	2 KB	01.08.2013 08:42:00
020808423525_GenInfo.xml	1 KB	01.09.2013 16:26:00
020808423525_ServiceSetup.xml	2 KB	01.09.2013 16:26:00
021008039358_GenInfo.xml	1 KB	01.10.2013 04:56:00
021008039358_ServiceSetup.xml	2 KB	01.10.2013 04:56:00
02105572413_GenInfo.xml	1 KB	31.10.2013 19:46:00
02105572413_ServiceSetup.xml	2 KB	31.10.2013 19:45:00
020708208775_GenInfo.xml	1 KB	02.07.2013 08:02:00

TUSENVIS AV FILER: For hver bil tilhørende sentralen, ligger det filer med detaljert informasjon, dag for dag. Dagbladet gjengir ikke bilder av den detaljerte informasjonen i filene du her ser. Foto: Skjermdump

Alarmer på nett

Den andre basen inneholder oversikter over alarmer utløst i drosjene, hendelsesforløp og drosjesentralens håndtering av situasjonen. I basen kunne man for eksempel sjekke hvilken drosje som oftest var utsatt for ran eller overfall - eller hente ut informasjon om konkrete episoder.

- Det skal jo ikke være åpent. Det er et system som fanger opp vår arbeidssituasjon og som jeg er fornøyd med. Men at noen andre har tilgang til det er jeg ikke fornøyd med. En arbeidstaker som har vært i en situasjon, vil varsle sin arbeidsgiver, men ikke hele Norge, sier fylkesleder Glenn Tuxen i Norges taxiforbund.

- Beklager

Oslo Taxi har i ettertid lukket begge de aktuelle databasene.

- Det er veldig beklagelig at de to programmene som hadde en type informasjon vi ikke ønsker skal være tilgjengelig for noen, lå åpent, sier daglig leder Bjørn Rebne i Oslo Taxi til Dagbladet.

Oslo kommune har i etterkant varslet en [gjennomgang av kontrakten](#) med Oslo Taxi. Både [Datatilsynet](#) og [taxi-brukere](#) har [reagert på lovbruddet](#).

Et tilfeldig løyve - en tilfeldig dag:

Taxiløyve nummer XX bor på adresse XX, og hører til en av de seks drosjesentralene med løsning levert av TDS.

Det er ikke Norges travleste løyve. Her er hva slags informasjon man kan finne på serveren, tre tilfeldig valgte dager.

Dag 1:

Gerd (etternavn) med bosted XX (adresse) tok taxi til XX (gatenavn) i XX (by) klokka 10. Turen kosta til sammen 821 kroner, hvorav passasjereren betalte en egenandel på 133. Resten ble satt på kreditt.

Neste tur var NN (fullt navn) som klokka 1315 tok drosjen fra XX (gateadresse og sted) til XX legesenter. Turen kosta totalt 606,-, hvorav NN betalte egenandelen på 133,-.

Neste tur var med ukjent kunde, og fant sted fra klokka 14.19 til 14.47 og kosta kr 621. Den ble også betalt med egenandel på 133,-.

Dag 2:

Klokka ni om morgenen tok NN (fullt navn), født X. mars 19XX taxi fra fysikalsk institutt til XX (adresse, sted). Mobilnummer til passasjereren er oppgitt. Turen kosta 862,-.

Dag 3:

NN (fullt navn) med XX (mobilnummer) meldte seg hos løyvet og tok taxi fra XX (adresse) til XX legesenter. Turen varte fra klokka 0904 til 0953, og kostet 904,-. Dette var også en kredittur, der NN betalte 133,- i egenandel.

Etter legebesøket, ble NN kjørt videre til sykehuset. Klokka 1041 tok NN en ny taxi til XX sykehus, der han var framme 11.29. Turen kosta 1088 kroner, men NN betalte bare egenandelen på 133,-.



Tips oss på [nullctrl@dagbladet.no](mailto:ullctrl@dagbladet.no)

Indeks for /Vogner/

Navn	Størrelse	Dato endret
[overordnet katalog]		
1096/		26.08.13 21:34:00
1116/		26.08.13 21:34:00
1120/		26.08.13 21:34:00
1122/		26.08.13 21:34:00
1124/		26.08.13 21:34:00
121/		09.10.13 14:10:00
122/		09.10.13 14:10:00
123/		09.10.13 14:10:00
1250/		26.08.13 21:34:00
126/		09.10.13 14:10:00
129/		26.08.13 21:33:00
130/		26.08.13 21:33:00
131/		26.08.13 21:33:00
132/		26.08.13 21:33:00
133/		26.08.13 21:33:00
134/		26.08.13 21:33:00
136/		26.08.13 21:33:00
1361/		26.08.13 21:33:00
137/		26.08.13 21:33:00
143/		26.08.13 21:33:00
144/		26.08.13 21:33:00
147/		26.08.13 21:32:00
2096/		26.08.13 21:32:00
2116/		26.08.13 21:32:00
2120/		26.08.13 21:32:00
2122/		26.08.13 21:32:00
222/		26.08.13 21:32:00
2250/		26.08.13 21:32:00
246/		26.08.13 21:32:00
252/		15.10.13 08:54:00
253/		26.08.13 21:32:00
254/		26.08.13 21:32:00
256/		26.08.13 21:32:00
263/		26.08.13 21:32:00
351/		26.08.13 21:32:00
352/		26.08.13 21:31:00
353/		26.08.13 21:31:00

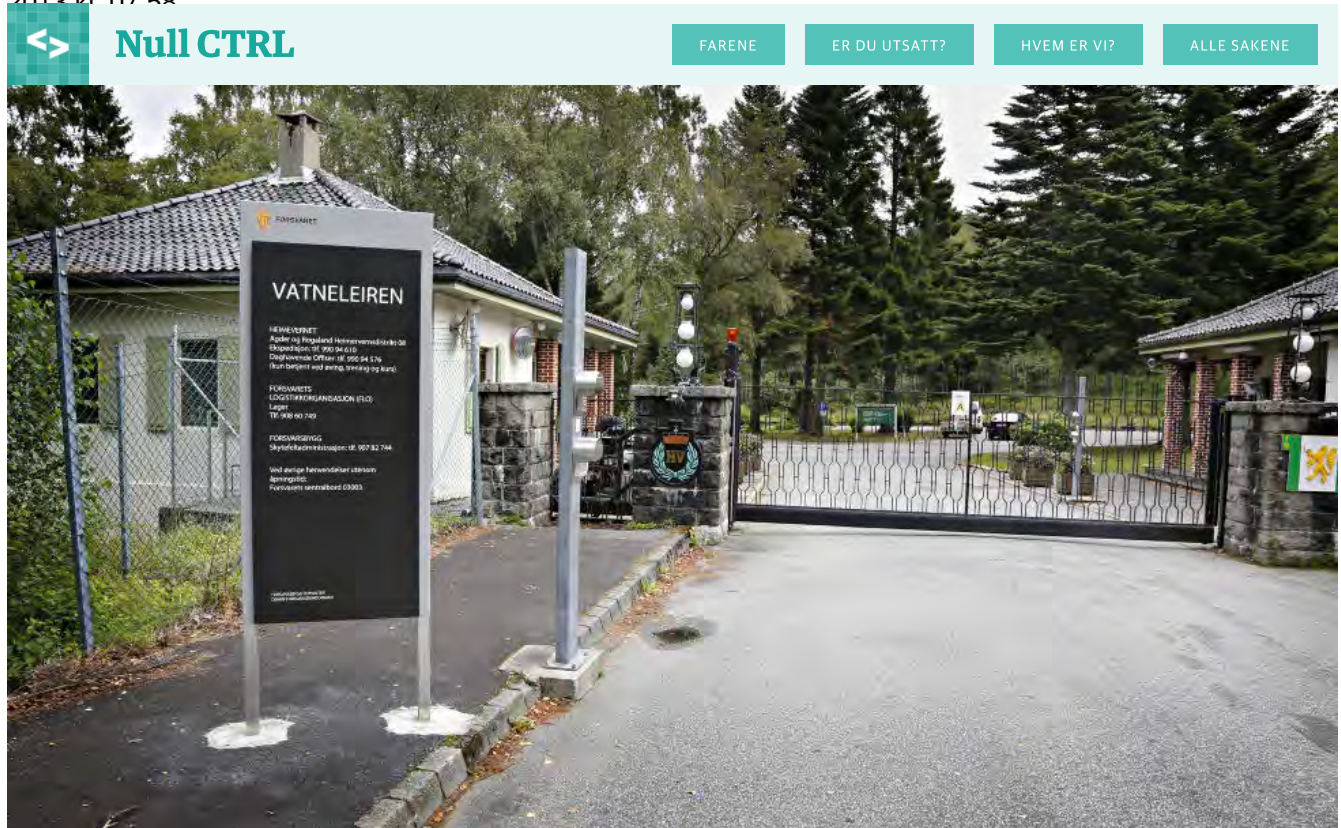
MAPPE FOR HVER BIL: For hver bil tilhørende sentralen, ligger det filer med detaljert informasjon, dag for dag. Dagbladet gjengir ikke bilder av den mest detaljerte informasjonen fra mappene du her ser. Foto: Skjermdump

Lillesand_201304020834/	26.08.13 21:25:00
Lillesand_201304020921/	26.08.13 21:25:00
Lillesand_201304021211/	26.08.13 21:25:00
Lillesand_201307311416/	26.08.13 21:25:00
TaxiSor_201303231015/	26.08.13 21:25:00
TaxiSor_201304021048/	26.08.13 21:25:00
TaxiSor_201304021953/	26.08.13 21:25:00
TaxiSor_201307311413/	26.08.13 21:25:00
TaxiSor_201310010841/	01.10.13 08:55:00
TaxiSor_201310020849/	02.10.13 09:26:00
TaxiSorBuss_201303231018/	26.08.13 21:25:00
TaxiSorBuss_201304021048/	26.08.13 21:25:00
TaxiSorBuss_201304021954/	26.08.13 21:25:00
TaxiSorBuss_201307311418/	26.08.13 21:25:00
TaxiSorBuss_201310020847/	02.10.13 09:26:00
TaxiSorBuss_201310020848/	02.10.13 09:26:00

PRISINFO: Basene inneholder også informasjon som trolig ikke er sensitiv, for eksempel gamle og nye priser. Foto:Skjermdump

Slik kan hackere ta kontroll i norske banker, skoler, sykehjem - og en militærleir, publisert onsdag 27. november

2013 kl. 07:58



SÅRBARHET: Vatneleiren utenfor Sandnes i Rogaland er ett av 290 steder hvor Dagbladet har funnet et konkret styringssystem for bygninger med kjente sårbarheter. Foto: Jacques Hvistendahl / Dagbladet

Slik kan hackere ta kontroll i norske banker, skoler, sykehjem - og en militærleir

Dagbladet fant sårbare kontrollsystemer i 290 norske bygninger.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): Med enkle grep kan uvedkommende trenge inn i systemer som er utviklet for å kontrollere alt fra lys, varme og ventilasjon til låsemekanismer og brannalarmer.

Dagbladet har funnet 290 slike kontrollsystemer i Norge, som både er av en sårbar versjon og ligger åpent mot Internett.

Stor ryddejobb

Det gjør det enkelt for hackere og inntrengere med onde hensikter å ta seg inn.

- Disse systemene har et sikkerhetshull, og med en gang du har funnet dette er det veldig lett å trenge inn. Å finne



STATOIL-KONTOR: Ett av systemene Dagbladet har funnet heter «Statoil Fornebu». Informasjonsdirektør Jannik

sikkerhetshullet er heller ikke spesielt vanskelig, sier den amerikanske sikkerhetseksperter Terry McCorkle til Dagbladet.

I Norge finnes systemene i alt fra banker og skolebygninger til sykehjem og store kontorbygg.

- Det at såpass mange ligger ute med disse sikkerhetshullene, betyr at det er en stor jobb å gjøre, sier forsker Niklas Vilhelm ved Nasjonal sikkerhetsmyndighet (NSM).

FBI advarer

For noen år siden oppdaget McCorkle og kollega Billy Rios i sikkerhetsselskapet Cylance den første sikkerhetsfeilen i de aktuelle systemene. Det førte til at FBI gikk ut med [en offisiell advarsel](#) i fjor høst.

For å bøte på problemet, har produsenten Tridium laget programvareoppdateringer.

- Tridium har tatt tak i alle innrapporterte sårbarheter i Niagara AX-rammeverket, med nedlastbare sikkerhetsoppdateringer som har vært tilgjengelige siden midten av 2012, skriver visepresident Jenny Graves i Tridiums kommunikasjonsavdeling i en e-post til Dagbladet.

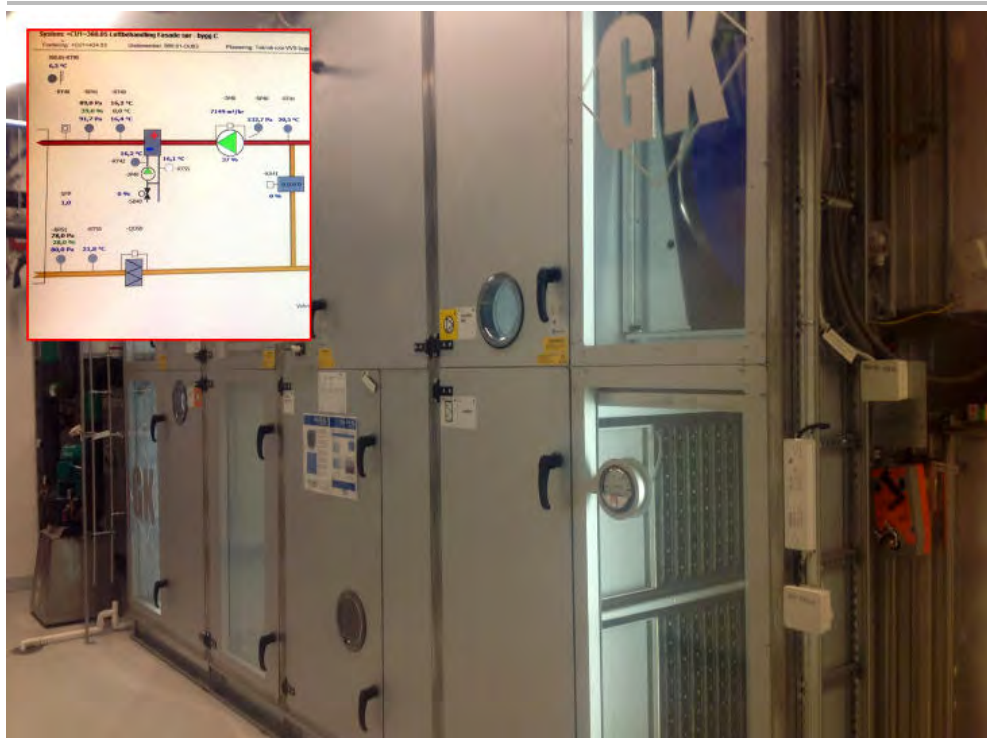
Ifølge McCorkle, som samarbeider med Tridium om å kartlegge og forstå systemenes sårbarheter, er det imidlertid «veldig, veldig uvanlig» at disse oppdateringene blir installert.

- Den typiske situasjonen er at et eksternt selskap installerer og kontrollerer disse systemene for en kunde, som eier bygningen. Kunden har for eksempel tilgang til å endre temperaturen, mens den eksterne leverandøren installerer en ADSL-linje eller lignende for å ha tilgang til kontrollpanelet fra sitt kontor. Derfor vet ofte ikke bygningseieren at systemet i det hele tatt er tilkoblet Internett, sier McCorkle.

I serien «Null CTRL» har Dagbladet kartlagt norske systemer av sårbare versjoner. Vi fant 290 stykker, og McCorkle anslår at 95 prosent av disse er sårbare.

Militærleir i Sandnes

Lindbæk jr henviser til IT Fornebu, som er ansvarlig for systemet. De ønsker ikke å kommentere saken, fordi de «ikke ønsker å fortelle utenforstående hvilke systemer vi bruker på våre bygg», opplyser kommunikasjonsdirektør Mona Jacobsen. Foto: Gorm Kallestad / NTB Scanpix



STYRINGSSYSTEM: Slik kan ett av disse styringssystemene se ut. Panelet (innfelt) tilhører et system for luftbehandling i GKs hovedkontor, og lå ikke åpent på Internett. Bildene er tatt med selskapets tillatelse. Foto: Linn K. Hillestad / Dagbladet

Disse bygningene er blant de utsatte:

- Luster sparebank, Marifjora
- Sparebank 1 SR-Bank, Haugesund
- DnBNor, Oslo
- DnBNOR, Lørenfare 1b, Oslo
- DnB Bank ASA, avdeling Sandsli
- Nordea, Allehelgens gate 2, Bergen
- Norges Bank, Allehelgens gate 2, Bergen
- Vatneleiren, Sandnes
- «Avinor_V1»
- «Avinor_OE32»
- Kongsberg Automotive AS
- Kongsberg Defence & Aerospace AS, Olav Brunborgs vei 6, Asker
- Norsk Hydro, Bergen
- Statoil, Fornebu
- «Ullevaal Stadion» - kjøpesenteret
- TV 2, Oslo
- «Ikea»
- Schweigaardsgt 15, Oslo, huser blant andre restauranten Maaemo
- Orkla, Essendrops gate 3, Oslo
- Prior/Nortura Haa AS
- Oljeserviceselskapet Aibel AS, Bergen
- KPMG, Sørkedalsveien 6, Oslo
- Nav Hordaland, C. Sundtsgate 29, Bergen
- Gulating lagmannsrett
- Skattedirektoratet, Schweigaardsgate 17, Oslo
- Toll- og avgiftsdirektoratet, Tollbodalmeningen 2A, Bergen
- Hamar politihus
- Politihuset, Nesttun
- Kasakhstans ambassade, Nedre Vollgate 3, Oslo
- Blå Kors, Oslo
- Ensjøtunet bo- og servicesenter, Oslo
- Gaustad sykehus
- Rørvik sykestue, Vikna kommune
- Rørvik skole, Vikna kommune
- Rørvik barneskole, Vikna kommune
- Austrafjord skole, Vikna kommune
- Biblioteket, Vikna kommune

Blant de vi fant, er den militære Vatneleiren ved Sandnes, hvor Forsvarsbygg er ansvarlig for driften.

- IP-adressen dere viser til går til en undersentral som styrer ett varme- og ventilasjonsanlegg i én bygning i Vatneleiren. Forsvarsbygg tar sikkerhet svært alvorlig, og har etter å ha blitt kjent med at en undersentral er koblet til nett med passordbeskyttelse, fysisk fjernet forbindelsen fra undersentralen. Man kan nå ikke kalle opp dette anlegget via IP-adressen, sier leder Atle Holten i eiendomsforvaltning ved Forsvarsbygg.

Han opplyser videre at de nå vil foreta en gjennomgang av sine systemer.

- Ikke kritisk

Et annet system Dagbladet har funnet, tilhører en filial av Sparebank1 SR-bank i Haugesund. Informasjonssjef Frode Sandal opplyser at det er huseieren som forvalter systemet, men at de uansett ikke mener det er kritisk for bankens sikkerhet.

- Det verste som kan skje hvis noen hacker seg inn her, er at de kan skru av ventilasjonen. Den fysiske sikringen av bygget ligger hos en annen leverandør, sier Sandal til Dagbladet.

Luster Sparebank opplyser til Dagbladet at også deres system styrer ventilasjonen i banken.

- Kunne vært bedre

GK Norge er den største leverandøren av disse systemene her i landet. De medgir at bransjens fokus på datasikkerhet kunne vært bedre.

- Fokuset har vært web, web, web, åpenhet og tilgjengelighet, og dette har kanskje gått utover sikkerheten, sier direktør for byggautomasjon Roar Johannesen til Dagbladet.

- Vi ønsker å fokusere mer på datasikkerhet sammen med våre kunder. Dette dreier seg like mye om å få kundene til å ha fokus på å sikre brukernavn og passord som å forsikre oss om at de sikkerhetsoppdaterer systemene, sier han.

Johannesen forteller at sikkerhet

- Høgskolen i Oslo, Werglandsveien 27
- Indre Hafslo skole, Marifjora
- Hafslo skole og samfunnshus, Marifjora
- Kongsvik skole, Nordland
- Bolstad skole, Marifjora
- Manger skole, Rådøy
- Foss skole, Oslo
- Holmlia skole
- Gamlebyen skole
- Smestad skole, Oslo
- Prinsdal skole, Oslo
- Universitetet i Bergen, Kalfarveien 31
- Universitetet i Bergen, Aarstadveien
- Norsk jernbaneskole, Oslo
- Prestmarka barnehage, Lindås
- Tårnet barnehage, Trondheim
- Bjørgene barnehage, Haugesund
- Sandslimarka barnehage, Bergen
- Fron badeland, Sør-Fron kommune
- Konsertpaleet / Bergen Kino
- Bergen Kino
- Elixia på Kokstad, Bergen
- Frelsesarmeen
- Rådøy rådhus
- Røbekk kirke, Molde
- Fredriksvern verft
- Namsskogan Hotell
- Lofotsenteret
- Byporten kjøpesenter, Mo i Rana
- Kolbotn torg kjøpesenter, Oppegård
- Kjøpesenteret Amfi Stord
- Arkaden kjøpesenter, Skien
- Mjøssenteret, Moelv
- Kontorbygget Sjølyst Arken, Oslo
- Gardermoen Businesspark
- Kontorbygget Nonnen, Bergen
- Kjøpesenteret Amfi Egersund
- Austevoll Havbruk
- Haslehallen turnsenter, Oslo
- Viss Vind AS

Eierne er varslet av Dagbladet i god tid før publisering av denne saken.



RISIKABELT: Forsker Niklas Vilhelm ved Nasjonal Sikkerhetsmyndighet (NSM) mener sikkerhetshullene i systemene Dagbladet har oppdaget, bør tettes. Foto: Øistein Norum Monsen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

er en del av dialogen med kundene de har løpende kontakt med.

- Vi mener vi stort sett har klart å nå ut til de fleste kundene, men det vi kjenner at vi kan bli bedre på, er å sende tydeligere beskjeder om eventuelle sikkerhetshull til de kundene vi ikke har kontakt med, sier han.

- Vi er sikre på at vi og hele bransjen kan bli bedre på datasikkerhet, og vi mener dere hjelper både oss og kundene våre å bli bedre på dette, supplerer systemingeniør Jan Ingar Wollebek.

Nye svakheter

Terry McCorkle opplyser til Dagbladet at det også finnes nyere versjoner som er usikre.

- Vi har ikke oppdatert alle svakheter ennå, og har derfor ikke offentliggjort disse, men flere av de nyere versjonene har lignende svakheter som den versjonen FBI advarte mot, sier han.

At hackere tar seg inn i kontrollsystemet, er bare én risiko. En annen er ifølge McCorkle at den åpne tilgangen kan være en inngang til andre områder av selskapets nettverk, fordi systemene ofte er koblet til det lokale nettverket.

- Vi har oppfordret våre leverandører og kunder verden over om å forsikre seg om at alle de Internett-tilkoblede systemene deres har installert alle sikkerhetsoppdateringer og anbefalt at de bør legge systemene bak en brannmur eller på et virtuelt privat nettverk (VPN), i tillegg til å bruke sterk passordbeskyttelse. Vi er trygge på at produktene våre er sikre hvis disse retningslinjene blir fulgt, skriver Jenny Graves i Tridium.

Uvitenhet

Niklas Vilhelm ved NSM mener det er svært viktig at disse oppfordringene etterfølges.

- Det kan være risikabelt å la situasjonen vedvare, sier han.

- Å la disse systemene ligge ute med sikkerhetshull betyr at hvem som helst kan styre dem. Derfor er det viktig at de sikres.

Vilhelm tror det store antallet sårbare systemer skyldes uvitenhet.

- Folk er ikke klar over hvor risikabelt dette er. Det er ikke før man får tilstrekkelig antall hendelser hvor det går galt og folk får se at dette faktisk også gjelder meg, at man vil ta det alvorlig.

- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL



UTSATT: Michelin-restauranten Maaemo ligger i Schweigaardsgt 15, hvor det aktuelle styringssystemet brukes. Foto: Melisa Fajkovic / Dagbladet

Sikrer systemene

- Takk for informasjon. Vi har de siste ukene blitt oppmerksomme på dette, og hadde startet arbeidet med å sikre systemene bedre. Dette er nå framskyndet, og vi mener å ha dekket dette nå, skriver daglig leder Tore Odfjell i Oddfjell eiendom i en e-post til Dagbladet.

De er ansvarlige for styringssystemet i C. Sundtsgate 29 i Bergen, hvor blant andre NAV Hordaland holder til.

Kommunikasjonsrådgiver Gry Halseth ved Hordaland politidistrikt opplyser til Dagbladet at systemet som heter «Politihuset Nesttun» tilhører eieren av bygget, og at dette er et system som styrer varme, og muligens også lys.

- Dette er et eldre system som huseier planlegger å skifte ut, men det har uansett ikke noe med politiets systemer å gjøre, sier hun.



Tips oss på nullctrl@dagbladet.no

Hacket Google

Tidligere i år tok McCorkle og Rios seg inn i styringssystemet til en av Googles kontorbygninger i Australia. McCorkle understreker imidlertid at de ikke ønsker at uvedkommende skal angripe disse systemene.

- Grunnen til at vi tok oss inn i Googles kontrollsystem, er at selskapet selv har oppfordret til å teste sikkerheten deres. Vi ønsker å vekke oppmerksomhet rundt dette og sikre at folk beskytter seg, sier McCorkle.

Han mener det kan være et stort samfunnsproblem at disse systemene er koblet til nettet.

- Systemene kontrollerer mye forskjellig. Ofte er det bare temperatur i bygninger, men de kan også kontrollere for eksempel fyrrom i fabrikker. I tillegg er det sikkert mange som vil mene at det ikke er noe problem om uvedkommende tar kontroll over airconditionen i en bygning, men hvis dette er inne i et datasenter som er avhengig av en viss temperatur, kan det få store konsekvenser. Det samme gjelder sykehus.

- Dette vil være spesielt uheldig for vårt sykehjem, publisert onsdag 27. november 2013 kl. 18:52



Null CTRL

FARENE

ER DU UTSATT?

HVEM ER VI?

ALLE SAKENE



VARMESTYRING: Ett av de sårbare kontrollsystemene Dagbladet har funnet på Internett, tilhører Rørvik sykestue. Dette brukes til å styre varme, lys og ventilasjon, opplyser kommunen. Foto: Tom Lysø / Namdalsavisa

- Dette vil være spesielt uheldig for vårt sykehjem

Sårbart kontrollsystem brukes til å styre lys og varme.



LINN KONGSLØ HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): I forbindelse med [artikkelserien «Null CTRL»](#) har Dagbladet funnet [flere hundre norske, sårbare kontrollsystemer](#) for bygninger, utviklet for å kontrollere alt fra lys, varme og ventilasjon til låsemekanismer og brannalarmer.

Alle disse systemene er koblet mot Internett uten brannmurbeskyttelse, og er av en versjon med et kjent sikkerhetshull som gjør dem [ekstra utsatt for hackere](#).

Advarer

Sju av systemene Dagbladet har funnet, brukes i bygg tilhørende Vikna kommune i Nord-Trøndelag, deriblant flere skoler og en sykestue. Disse systemene styrer varme, ventilasjon og lys, opplyser

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

kommunen.

De kjente ikke til sikkerhetshullet Dagbladet omtaler i dag, og som både amerikanske sikkerhetsmyndigheter og FBI [advarte mot](#) i fjor.

- Med en gang du har funnet dette sikkerhetshullet er det veldig lett å trenge inn. Å finne det er heller ikke spesielt vanskelig, sier den amerikanske sikkerhetseksperten Terry McCorkle.

- Uheldig

- Hvis det er mulig, er det uheldig for oss, skriver avdelingsleder for Bygg & Eiendom Erik Jakobsen ved Vikna kommune i en e-post til Dagbladet.

Han ønsker kun å besvare spørsmål skriftlig, men utdyper videre:

- Som jeg ser det, er det uheldig blant annet for forutsetningene for innneklima, økt strømforbruk, lys av/på i bygg utenom åpningstid/brukstid.

- Nedstengning av varmelegger utenom arbeidstid/helg vil være uheldig spesielt for vårt sykehjem. En risikovurdering vil eventuelt avdekke flere forhold.

I etterkant av Dagbladets henvendelse, har Vikna kommune kontaktet sin eksterne leverandør av systemene. Leverandøren opplyser til Dagbladet at de mener de har fulgt alle anbefalinger fra produsenten for å sikre disse, men vil undersøke saken nærmere.

- Risikabelt

Forsker Niklas Vilhelm i Nasjonal sikkerhetsmyndighet (NSM) ser med bekymring på [de 290 sårbare systemene Dagbladet har funnet](#).

- Det kan være risikabelt å la situasjonen vedvare, sier han.

- Å la disse systemene ligge ute med sikkerhetshull betyr at hvem som helst kan styre dem. Derfor er det viktig at de sikres.

Den amerikanske sikkerhetseksperten Terry McCorkle mener det kan være et stort samfunnsproblem at disse systemene er koblet til nettet.

- Systemene kontrollerer mye forskjellig. Ofte er det bare temperatur i bygninger, men de kan også kontrollere for eksempel fyrrom i fabrikker. I tillegg er det sikkert mange som vil mene at det ikke er noe problem om uvedkommende tar kontroll over airconditionen i en bygning, men hvis dette er inne i et datasenter som er avhengig av en viss temperatur, kan det få store konsekvenser. Det samme gjelder sykehus, sier han til Dagbladet.

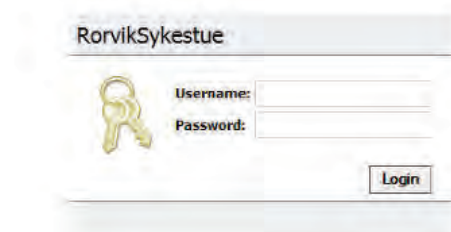
Sikkerhetsoppdateringer

For å bøte på problemet, har produsenten Tridium laget programvareoppdateringer.

- Vi har oppfordret våre leverandører og kunder verden over om å forsikre seg om at alle de Internett-tilkoblede systemene deres har installert alle sikkerhetsoppdateringer og anbefalt at de bør legge systemene bak en brannmur eller på et virtuelt privat nettverk (VPN), i tillegg til å bruke sterk passordbeskyttelse. Vi er trygge på at produktene våre er sikre hvis disse retningslinjene blir fulgt, skriver visepresident Jenny Graves i Tridiums kommunikasjonsavdeling i en e-post til Dagbladet.



RISIKABELT: Forsker Niklas Vilhelm ved Nasjonal sikkerhetsmyndighet mener det kan være risikabelt med alle de sårbare systemene som ligger tilgjengelig på Internett, uten beskyttelse av brannmur. Foto: Øistein Norum Monsen / Dagbladet

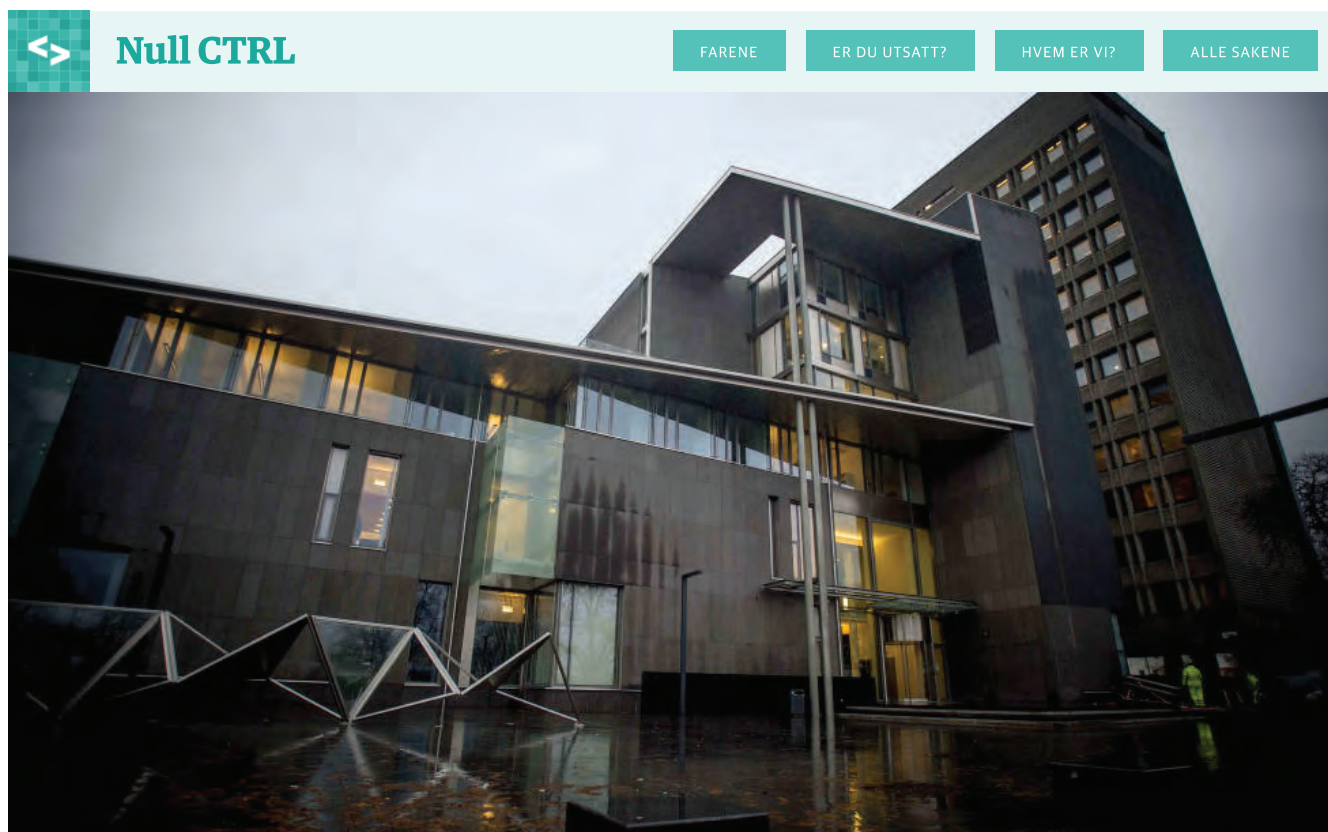


BAKDØR: Den versjonen som brukes av Rørvik sykestue, har en kjent bakdør som gjør det mulig for uvedkommende å trenge inn i systemet. Foto: Skjermdump



Tips oss på nullctrl@dagbladet.no

Alle de sårbare systemene Dagbladet har funnet, ligger imidlertid tilgjengelig på åpent nett, uten beskyttelse av en brannmur.



TILGJENGELIG FRA NETT: Avdelingsdirektør Jann Ola Berget i Domstoladministrasjonen bekrefter overfor Dagbladet at det i en periode var mulig å komme seg inn på et styringssystem i Gulating lagmannsrett via Internett. Foto: Thomas Rasmus Skaug / Dagbladet

Domstolene sjekker datasikkerheten etter «Null CTRL»-avsløring

- Vi har nok ikke hatt tilstrekkelig fokus på den typen eksterne løsninger.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): I forbindelse med [artikkelserien «Null CTRL»](#) har Dagbladet funnet [flere hundre norske, sårbare kontrollsystemer](#) for bygninger, utviklet for å kontrollere alt fra lys, varme og ventilasjon til låsemekanismer og brannalarmer.

Alle disse systemene er koblet mot Internett uten brannmurbeskyttelse, og er av en versjon med et kjent sikkerhetshull som gjør dem [ekstra utsatt for hackere](#).

Ett av systemene Dagbladet har funnet, brukes av Gulating lagmannsrett i Bergen.

Dette brukes for å styre lys og varme i lagmannsretten, opplyser avdelingsdirektør Jann Ola Berget i Domstoladministrasjonen, som har et ansvar for samtlige tinghus i



SÅRBARHET: Vatneleiren utenfor Sandnes i Rogaland er ett av 290 steder hvor Dagbladet har funnet et konkret styringssystem for bygninger med kjente sårbarheter. Foto: Jacques Hvistendahl / Dagbladet

Norge.

- Mulig å trenge inn

- Det er byggeieren Statsbyggs løsning, og det er riktig at det i bygge- og oppstartfasen for den nye rettsbygningen har vært mulig å komme seg inn fra Internett, skriver Berget i en e-post til Dagbladet.

Den amerikanske sikkerhetseksperten Terry McCorkle i sikkerhetsselskapet Cylance har vært sentral i å avdekke sikkerhetshullene i disse systemene, og samarbeider også med produsenten Tridium.

- Med en gang du har funnet dette sikkerhetshullet er det veldig lett å trenge inn. Å finne sikkerhetshullet er heller ikke spesielt vanskelig, sier han til Dagbladet.

Sjekker datasikkerheten

At hackere tar seg inn i kontrollsystemet og får mulighet til å styre dette, er bare én risiko. En annen er ifølge McCorkle at den åpne tilgangen kan være en inngang til andre områder av selskapets nettverk, fordi systemene ofte er koblet til det lokale nettverket.

Berget medgir at

Domstoladministrasjonen trolig ikke har hatt tilstrekkelig fokus på denne typen eksterne løsninger, men poengterer samtidig at det ikke finnes noen forbindelse mellom det aktuelle systemet og domstolenes egne datanettverk.

- Vi vil også undersøke om det kan finnes lignende løsninger i andre tinghus. Statsbygg har bekreftet at den konkrete løsningen for Gulating lagmannsrett de nærmeste dagene vil bli overført til deres lukkede nett.

Anbefaler brannmur

Dette er ett av tiltakene produsenten Tridium anbefaler for å sikre disse systemene.

- Vi har oppfordret våre leverandører og kunder verden over om å forsikre seg om at alle de Internett-tilkoblede systemene deres har installert alle sikkerhetsoppdateringer og anbefalt at de bør legge systemene bak en brannmur eller på et virtuelt privat nettverk (VPN), i tillegg til å bruke sterk passordbeskyttelse. Vi er trygge på at produktene våre er sikre hvis disse retningslinjene blir fulgt, skriver visepresident Jenny Graves i Tridiums kommunikasjonsavdeling i en e-post til Dagbladet.

- Risikabelt

Forsker Niklas Vilhelm i Nasjonal sikkerhetsmyndighet (NSM) ser med bekymring på [de 290 sårbare systemene Dagbladet har funnet](#).

- Det kan være risikabelt å la situasjonen vedvare, sier han.

- Å la disse systemene ligge ute med sikkerhetshull betyr at hvem som helst kan styre dem. Derfor er det viktig at de sikres.



RISIKABELT: Forsker Niklas Vilhelm ved Nasjonal sikkerhetsmyndighet (NSM) mener sikkerhetshullene i systemene Dagbladet har oppdaget, bør tettes. Foto: Øistein Norum Monsen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en ny serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



Tips oss på nullctrl@dagbladet.no

Den amerikanske sikkerhetseksperten Terry McCorkle mener det kan være et stort samfunnsproblem at disse systemene er koblet til nettet.

- Systemene kontrollerer mye forskjellig. Ofte er det bare temperatur i bygninger, men de kan også kontrollere for eksempel fyrrom i fabrikker. I tillegg er det sikkert mange som vil mene at det ikke er noe problem om uvedkommende tar kontroll over airconditionen i en bygning, men hvis dette er inne i et datasenter som er avhengig av en viss temperatur, kan det få store konsekvenser. Det samme gjelder sykehus, sier han til Dagbladet.

Fant sensitive dokumenter om



LÅ ÅPENT P

TILGJENGELIG INFORMASJON: Dagbladet fant fem åpne og søkbare servere med detaljerte, tekniske dokumenter vedrørende oljeaktivitet på norsk sokkel.



HADDE ÅPEN DISK: En ingeniør med oppdrag for oljeindustrien gjorde disken sin tilgjengelig for alle ved en feil. Her lå blant annet detaljert informasjon om hva slags styringssystemer som brukes på ulike prosjekter i Nordsjøen. Foto: Øistein Norum Monsent

Dagbladet har funnet flere åpne servere på internett med detaljerte dokumenter om norsk oljebransje. Det er svært bekymringsfullt, mener Statoil.

Tekst: **Linn Kongsli Hillestad**
lkh@dagbladet.no
Espen Sandli
esan@dagbladet.no

Totalt har Dagbladet funnet fem åpne og søkbare servere med detaljerte, tekniske dokumenter vedrørende aktivitet på norsk sokkel.

Det betyr at dokumentene

har ligget åpne på internett, i prinsippet tilgjengelige for hvem som helst.

Eierne av serverne er underleverandører eller konsulenter for store oljeselskaper som opererer i Norge.

–Vi synes dette er svært bekymringsfullt. Vi har samme forventninger til sikkerheten hos våre underleverandører som oss selv, sier informasjonssjef Jannik Lindbæk jr. i Statoil når Dagbladet gir en overordnet beskrivelse av problematikken.

De er ett av flere oljeselskaper som er berørt av den sviktende datasikkerheten. Når Dagbladet gir en mer konkret beskrivelse av innholdet på de ulike serverne, ønsker ikke Statoil å kommentere saken spesifikt, fordi de ikke ønsker å uttale seg om andre selskaper. De understreker imidlertid at de har



FOKUS:
Jannik
Lindbæk jr.



DATATAP:
Bunny
Nooryani.

«skarpt fokus på informasjonssikkerhet».

– Absolutt ikke offentlig

På de åpne serverne Dagbladet fant i forbindelse med artikkelserien «Null CTRL», finnes blant annet detaljert informasjon om hva slags styringssystemer som brukes på ulike installasjoner i Nordsjøen, programvare, passord, tekniske tegninger og inngående informasjon om oljerør, ventiler og instru-

norsk oljebransje

PÅ NETT

menteringsløsninger – for å nevne noe.

– Det ligger blant annet informasjon om boreutstyr her. Jeg har lenge trodd at jeg har tatt en del grep for å holde dette låst, men jeg ser jo her at dette ikke har virket så godt, sier en ingeniør, som hadde store deler av sin backup-disk åpent tilgjengelig på nettet.

– Er dette sensitiv informasjon?
– Det kommer an på hvem som ser på det. Men dette skal absolutt ikke være offentlig, sier mannen, som blant annet har hatt flere oppdrag for Aker Solutions.

En annen av de åpne serverne

” Dette skal absolutt ikke være offentlig.

Ingeniør med oppdrag for oljeindustrien

Dagbladet har funnet, tilhører en ingeniør i Aker Solutions. Her lå blant annet rapporter, presentasjoner og programfiler. Også denne lå åpen ved en feil.

Datatap

– Vi, som de fleste andre, har gjort oss noen erfaringer med det som kan se ut som datatap. Vi jobber fortløpende med dette, både med tanke på å søke i eksterne kilder og å øke kunnskapen til våre ansatte, skriver kommunikasjonsjef Bunny Nooryani i en e-post.

Hun ønsker ikke å gå nærmere inn på hvordan de jobber med datasikkerhet.

– Jo mer vi forteller, desto mer sårbar blir vi, skriver hun.

Store oljeplattformer

En server inneholdt inspeksjonsrapporter og mapper med oljesel-

skapenes egne standarder, noen av dem med interne dokumenter, kommentarer fra selskapene og diskusjoner om krav til utstyr.

Selskapet Krohne, som leverer målesystemer til oljebransjen, hadde også interne dokumenter i en åpen server. Her fantes informasjon om prosjekter på over 30 plattformer på norsk sokkel, som opereres av noen av verdens største oljeselskaper.

Krohne oppdaget selv feilen.
– Det var bare snakk om eldre, uaktuelle dokumenter, og sett i lys av at vi raskt oppdaget feilen og fikk sperret tilgang, anser vi at skadeomfanget er meget begrenset, skriver administrerende direktør Eivind Omarhaug i en e-post til Dagbladet.

– Kan medføre store tap

Petroleumstilsynet ber bransjen sikre at sensitiv informasjon ikke kommer på avveie, av hensyn til

Foto: Eirik Helland Urke



sikkerhet og beredskap.

Avtroppende generalmajor Roar Sundseth i Cyberforsvaret frykter at dårlig datasikkerhet i små og mellomstore bedrifter kan medføre tap av sensitiv informasjon – særlig innenfor oljeindustrien.

– Vi ligger jo på verdenstoppen i forhold til ny teknologi på mange områder innenfor olje- og energisektoren, og det er klart at i verste fall kan dette føre til tap av verdier i 100-millionersklassen, sier Sundseth på generelt grunnlag.



Dagbladet 29. oktober



Dagbladet 28. oktober



Dagbladet 17. oktober



Dagbladet 8. oktober

FØLG SAKEN

Null CTRL

• Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens webkamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

• I en serie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

• Følg serien her: www.dagbladet.no/nullctrl

• Tips oss på: nullctrl@dagbladet.no

• Si din mening på Twitter: [#null_CTRL](https://twitter.com/null_CTRL)



OLJEDOKUMENTER: I forbindelse med artikkelserien «Null CTRL» har Dagbladet funnet fem åpne og søkbare servere med detaljerte, tekniske dokumenter om norsk oljebransje. Arkivfoto: Eirik Helland Urke / Dagbladet

Sensitive oljedokumenter lå åpent på nett

Statoil: - Svært bekymringsfullt.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): Totalt har Dagbladet funnet fem åpne og søkbare servere med detaljerte, tekniske dokumenter vedrørende aktivitet på norsk sokkel. Eierne er underleverandører eller konsulenter for store oljeselskaper som opererer i Norge.

- Vi synes dette er svært bekymringsfullt. Vi har samme forventninger til sikkerheten hos våre underleverandører som oss selv, sier informasjonsdirektør Jannik Lindbæk jr. i Statoil når Dagbladet gir en overordnet beskrivelse av problematikken.

De er ett av flere oljeselskaper som er berørt av den sviktende datasikkerheten. Når Dagbladet gir en mer konkret beskrivelse av innholdet på de ulike serverne, ønsker ikke Statoil å kommentere saken spesifikt, fordi de ikke ønsker å uttale seg om andre selskaper.

” Det ligger blant annet informasjon om boreutstyret her. Jeg har lenge trodd at jeg har tatt en del grep for å holde dette låst, men jeg ser jo her at dette ikke har virket så godt.

Oljeingeniør



FOKUS: Informasjonsdirektør i Statoil, Jannik Lindbæk Jr., understreker overfor Dagbladet at de har skarpt fokus på

De understreker imidlertid at de har «skarpt fokus på informasjonssikkerhet».

- Absolutt ikke offentlig

På de åpne serverne Dagbladet fant i forbindelse med [artikkelserien «Null CTRL»](#), finnes blant annet detaljert informasjon om hva slags styringssystemer som brukes på ulike installasjoner i Nordsjøen, programvare, passord, tekniske tegninger og svært detaljert informasjon om oljerør, ventiler og instrumenteringsløsninger - for å nevne noe.

- Det ligger blant annet informasjon om boreutstyr her. Jeg har lenge trodd at jeg har tatt en del grep for å holde dette låst, men jeg ser jo her at dette ikke har virket så godt. Eventuelt er det et eller annet jeg har bomma på, sier en ingeniør, som hadde store deler av sin backup-disk åpent tilgjengelig på nettet.

- Er dette kritisk informasjon?

- Det kommer an på hvem som ser på det. Men dette skal absolutt ikke være offentlig, sier mannen, som blant annet har hatt flere oppdrag for Aker Solutions.

Vinsjer og boremaskiner

På disken hans lå blant annet programvare til å styre store vinsjer og boremaskiner. Dette er en oppskrift på hvordan utstyret brukes hvis det blir lastet inn på en kontrollør og en operatør bruker et betjeningspanel for å operere det.

Dersom man er koblet direkte til kontrolløren, er det også mulig å simulere operatørsignaler.

En annen av de åpne serverne Dagbladet har funnet, tilhører en ingeniør i Aker Solutions. Her lå blant annet rapporter, presentasjoner og programfiler. Også denne lå åpen ved en feil.

Datatap

Dagbladet har beskrevet innholdet på serverne overfor Aker Solutions.

- Vi, som de fleste andre, har gjort oss noen erfaringer med det som kan se ut som datatap. Vi jobber fortløpende med dette, både med tanke på å søke i eksterne kilder og å øke kunnskapen til våre ansatte, skriver kommunikasjonssjef Bunny Nooryani i en e-post etter at de har gjennomgått opplysningene.

informasjonssikkerhet og forventer det samme fra leverandører og samarbeidspartnere. Foto: Kent Skibstad / NTB Scanpix



DATATAP: Kommunikasjonssjef Bunny Nooryani i Aker Solutions opplyser til Dagbladet at de har erfaringer med «det som kan se ut som datatap», og at dette er noe de jobber fortløpende med. Foto: Aker Solutions



HADDE ÅPEN DISK: En ingeniør med oppdrag for oljeindustrien gjorde disken sin tilgjengelig for alle ved en feil. Her lå blant annet detaljert informasjon om hva slags styringssystemer som brukes på ulike prosjekter i Nordsjøen. Foto: Øistein Norum Monsen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

De ønsker ikke å gå nærmere inn på hvordan de jobber med datasikkerhet.

- Når jeg har diskutert temaet med våre sikkerhetsekspert, kommer alle til samme konklusjon: At vi ikke bør dele hvordan vi innretter oss for å beskytte oss mot denne situasjoner. Jo mer vi forteller, desto mer sårbare blir vi. Derfor ønsker vi ikke å beskrive våre erfaringer eller løsninger rundt problemstillingen.

Store oljeplattformer

En annen server inneholdt inspeksjonsrapporter og mapper med oljeselskapenes egne standarder, noen av dem med kommentarer fra selskapene og diskusjoner om krav til utstyr.

Selskapet Krohne, som leverer målesystemer til oljebransjen, hadde også interne dokumenter i en åpen server. Her fantes blant annet informasjon om prosjekter på over 30 norske oljeplattformer, som opereres av noen av verdens største oljeselskaper.

Krohne oppdaget selv feilen før Dagbladet tok kontakt.

Administrerende direktør Eivind Omarhaug forklarer at det var en server-oppgradering som førte til at enkelte mapper utilsiktet ble gjort tilgjengelig.

- Det var kun snakk om eldre, uaktuelle dokumenter, og sett i lys av at vi raskt oppdaget feilen og fikk sperret tilgang, anser vi at skadeomfanget er meget begrenset, skriver han i en e-post til Dagbladet, men presiserer at selskapet tar hendelsen veldig alvorlig.

Endrer rutiner

- Vi har endret våre interne IT-rutiner slik at vi er sikre på at tilsvarende ikke vil skje igjen.

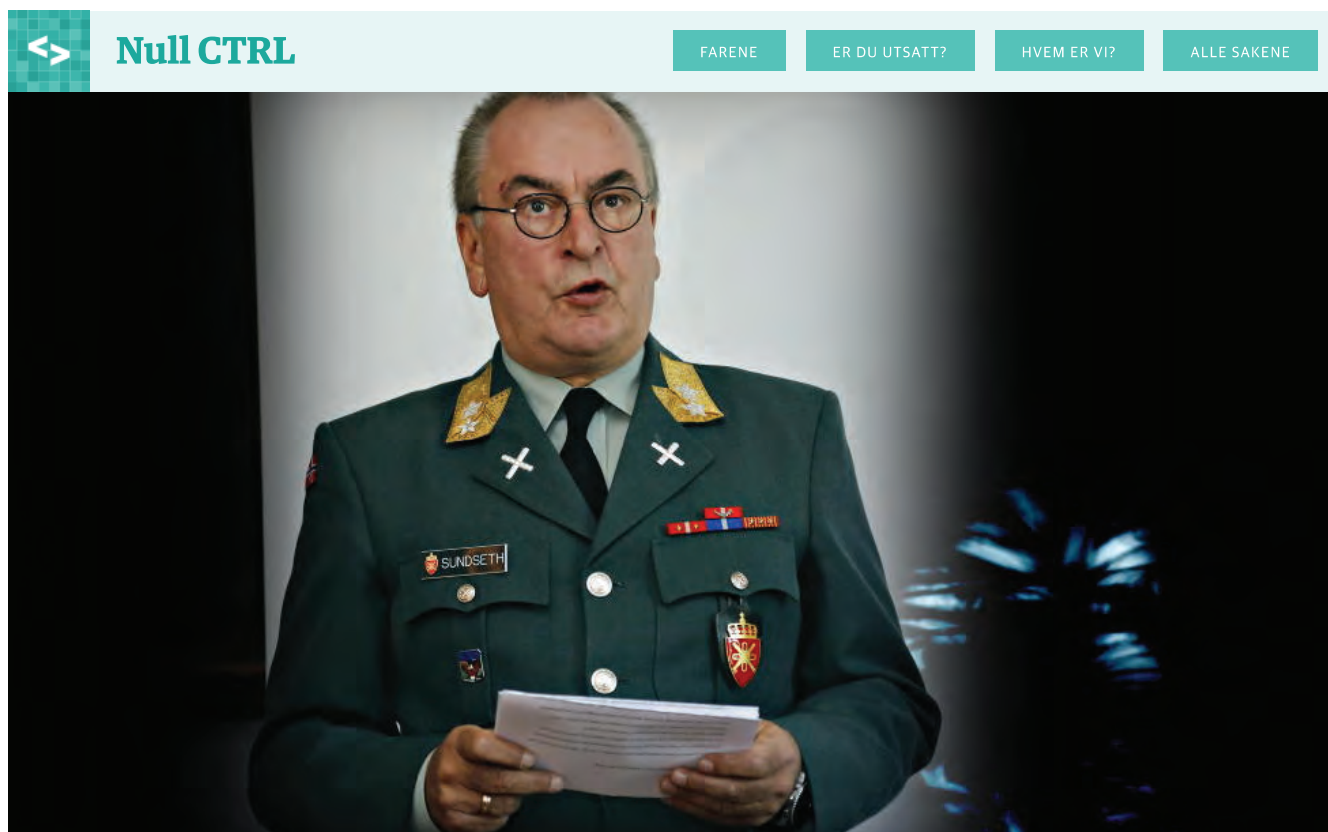
Dagbladet har beskrevet innholdet på serverne til Petroleumsstilsynet, som på dette stadiet kun kan gi følgende, generelle kommentar:

- Det er viktig at selskapene har systemer som sikrer at sensitiv informasjon ikke kommer på avveie. Dette er særlig viktig med tanke på sikkerhetskritisk informasjon knyttet til sikring og beredskap. Per nå vet vi ikke om informasjonen som dere viser til er av en slik art, og om dette faller inn under vårt myndighetsområde, som er sikkerhet, skriver pressekontakt Eileen Brundtland i en e-post til Dagbladet.



Tips oss på nullctrl@dagbladet.no

- I verste fall kan dette føre til tap av verdier i 100-millionersklassen, publisert mandag 9. desember 2013 kl.



BEKYMRET: Avtroppende sjef for Cyberforsvaret, generalmajor Roar Sundseth, mener det bør bli mer fokus på datasikkerheten hos små og mellomstore bedrifter. Foto: Jacques Hvistendahl / Dagbladet

- I verste fall kan dette føre til tap av verdier i 100-millionersklassen

Underleverandører kan medføre en stor fare for norsk datasikkerhet, mener sjefen for Cyberforsvaret.



LINN KONGSLID HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): Underleverandører og små og mellomstore bedrifter med få ressurser kan representere en stor fare for norsk datasikkerhet, mener avtroppende sjef for Cyberforsvaret, generalmajor Roar Sundseth.

- De store selskapene vi har, bare for å nevne Statoil, er profesjonelle på informasjonssikkerhet. Men små og mellomstore bedrifter har ikke ressurser til å ha sine egne sikkerhetsorganisasjoner på samme måte, der må det tas et krafttak, sier Sundseth til Dagbladet.

Fant oljedokumenter

Dagbladet omtaler i dag hvordan flere ulike servere med dokumenter



UAKSJEPTABELT: Dagbladet har tidligere avslørt at sensitiv informasjon, som beredskapsdokumenter, lå åpent tilgjengelig på en database tilhørende Midtre Hålogaland 110-sentral. Video: Øistein Norum Monsen / Dagbladet

vedrørende aktivitet på norsk sokkel [lå åpne og søkbare på Internett](#). Eierne er underleverandører eller konsulenter for store oljeselskaper som opererer i Norge.

På serverne finnes blant annet detaljert informasjon om hva slags styringssystemer som brukes på ulike prosjekter i Nordsjøen, software, passord, tekniske tegninger og svært detaljert informasjon om oljerør, ventiler og instrumenteringsløsninger - for å nevne noe.

Dagbladets funn bekymrer Nasjonal sikkerhetsmyndighet (NSM).

- **Oljeindustrien og annen høyteknologisk industri i Norge er utsatt for industrispionasje, så vi er jo bekymret når vi nå får informasjon om at dere har funnet databasene til underleverandører av oljebransjen åpent på nett, sier leder for NSMs operasjonssenter, Marie Moe.**

- Vi er bekymret for at man ikke har tilstrekkelig kontroll over denne informasjonen.

Store tap

Generalmajor Sundseth frykter at dårlig datasikkerhet hos små og mellomstore bedrifter kan medføre tap av sensitiv informasjon.

- **Vi ligger jo på verdenstoppen i forhold til ny teknologi på mange områder innenfor olje- og energisektoren, og det er klart at i verste fall kan dette føre til tap av verdier i 100-millionersklassen, sier Sundseth, som uttaler seg på generelt grunnlag.**

- Det er klart at det kan skje hvis sikkerheten blir brutt, og man mister bedriftshemmeligheter, for å kalle det det, fortsetter han.

Internasjonal trend

Marie Moe mener også at dårlig datasikkerhet hos mindre selskaper kan skape utfordringer.

- Det er jo et problem at man ikke kan bruke like mye ressurser på informasjonssikkerhet hvis man er en liten underleverandør. I så fall bør man se om man kan kjøpe tjenester av andre som kan gjøre den sikringen av informasjon og

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyrte vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



ØKENDE TRUSLER: Generalmajor Roar Sundseth er sjef for Cyberforsvaret. De ser en stadig økning i digitale trusler mot Norge. Video: Øistein Norum Monsen / Dagbladet



FOKUS: Informasjonsdirektør i Statoil, Jannik Lindbæk Jr., understreker overfor Dagbladet at de har skarpt fokus på informasjonssikkerhet og forventer det samme fra leverandører og samarbeidspartnere. Foto: Kent Skibstad / NTB Scanpix

tilby tjenester for overvåking av nettverk og sikring av informasjon, sier hun.

Sundseth påpeker at industrispionasje er en omfattende virksomhet.

- Kanskje ikke spesielt rettet mot oss, men det er en trend i verden. Mange satser store ressurser på å hente inn teknologi fra andre nasjoner, som de nyttegjør seg selv, sier Sundseth, som mener dette er et område som krever langt større fokus.

Ønsker statlig støtte

Problemet med åpne servere skyldes som regel feilkonfigurasjoner, mener seniorrådgiver Vidar Sandland i Norsk Senter for Informasjonssikring (Norsis).

- Ett av problemene er at de fleste bedrifter ikke vet at disse serverne er tilgjengelige for alt og alle, og det kan jo selvfølgelig få katastrofale konsekvenser for en bedrift, da for eksempel patenter og annen type sensitiv informasjon kan komme på avveie uten at disse er klar over det, sier han.

Generalmajor Sundseth ønsker at myndighetene skal trå til med direkte støtte til små og mellomstore selskaper for å gi dem muligheten til å fokusere mer på datasikkerhet.

- Jeg synes det er grunn til å se nærmere på hvordan man fra staten sin side kan gå inn og støtte de som ikke har ressurser til å avsette til dette - i hvert fall ikke nok ressurser, sier han.



OPERASJONSENTRAL: Seksjonssjef Marie Moe ved Nasjonal Sikkerhetsmyndighet og hennes kollegaer i operasjonsrommet behandler rundt 40 saker hver dag. Foto: Øistein Norum Monsen/Dagbladet.



Tips oss på nullctrl@dagbladet.no



VIDÅPENT: Dette kartet viser hvor mange som har åpnet innholdet på sin egen datamaskinen for hele verden. Grafikk: Ola Strømman



”TABBEN jeg aldri skal gjøre igjen

FORTROLIG OG PRIVAT: Avdelingsleder Knut Nyhagen ved Veksthuset på Otta hadde ingen anelse om at serveren deres lå tilgjengelig for alle på Internett. Der lå både fortrolig kan

Noen få tastetrykk kan åpne innholdet på datamaskinen din for alle. Den tabben gjorde et rekrutteringsselskap da de la ut fortrolig informasjon om jobbsøkere – uten å være klar over det.

NULL CTRL



OTTA (Dagbladet): På nett fant Dagbladet en server tilhørende bemanningsbyrået Veksthuset. På den lå det store mengder

data om bl. a. jobbsøkere.

– Jeg var helt sikker på at dette var godt sikret, det er det som er så skummelt. Men jeg vet i hvert fall at jeg ikke skal gjøre den feilen igjen, sier Knut Nyhagen til Dagbladet.

Han er avdelingsleder for Otta-kontoret til Veksthuset, et rekrutteringsselskap med kontorer sju ulike steder i landet og en omsetning på 59 millioner kroner i fjor.

For noen år siden fikk Otta-avdelingen installert en server, hvor ansatte fikk tilgang til delte jobbdokumenter hjemmefra. Serveren ble satt opp slik at det var mulig å logge seg på med IP-adresse, brukernavn og passord. Tilsynelatende fungerte det helt etter planen.

Fortrolig informasjon

Men samtidig sto en annen inngangsport til serveren på vidt gap, noe som gjorde innholdet tilgjengelig også for alle andre.

På serveren lå blant annet kun-

deavtaler og en kandidatbase med cv-er.

Og ikke minst interne vurderinger av kandidater til ulike stillinger.

– Når du arbeider med jobbsøkere og kandidater, er det klart du sitter på en del fortrolig informasjon. Det er beklagelig, selv om dette rett nok er eldre ting. Samtidig lå også en kopi av alt mitt private inne på denne serveren, både bilder og sikkert bankinformasjon og annen personinformasjon. Her kan det blant annet ha ligget noen private passord, sier Nyhagen.

Slik blott-legges dokumenter

Dagbladet har funnet flere tusen åpne servere og databaser på Internett. Nasjonal sikkerhetsmyndighet er bekymret.

Ett feil høyreklikk, og plutselig kan sensitive dokumenter være tilgjengelige for alle.

Veksthusets avdeling på Otta er ikke de eneste som uforvarende har delt dokumenter med langt flere enn det som var meningen.



BEKYMRET: Seksjonssjef Marie Moe.

Den enkleste og vanligste protokollen for å dele filer i et Windows-nettverk, kalles SMB. Men hvis du huker av for alternativet «del med alle», kan filene også bli tilgjengelige utenfor nettverket.

Det er det nok mange som ikke er klar over.

Dagbladet har funnet 3573 slike porter i Norge, mange av dem på vidt gap. Innenfor noen av disse fantes dokumenter om norsk oljebransje, som Dagbladet omtalte i går.

Beredskapsdokumenter

En annen tabbe folk ofte gjør, er via en annen form for deling, såkalt FTP. FTP brukes ofte for å dele filer med andre, men her er det flere fallgruver. En feil Dagbladet ofte har sett eksempler på, er at denne porten til en server er blitt åpnet uten at det var meningen. I andre tilfeller er innholdet ment delt med en ringere krets, men eierne har glemt å begrense innsyn for andre.

Dagbladet har lokalisert 18 000 FTP-servere i Norge. Minst 1000 av disse er usikrede og mange av dem tilhører større eller mindre norske bedrifter.

Det var via en slik usikret FTP-server at Dagbladet fant brannberedskapen for 39 av 44 kommuner i Nordland.

Nasjonale konsekvenser

Nasjonal sikkerhetsmyndighet (NSM) ser med bekymring på alle de åpne serverne.

– Det er ikke bra for bedriften, som gir ut informasjon de kanskje ikke ønsker skal være tilgjengelig. Men det er heller ikke bra fra et nasjonalt perspektiv – hvis dette gjelder mange bedrifter i Norge – at mulig sensitiv informasjon er tilgjengelig for andre nasjoner eller for noen som ønsker å drive industrispionasje for norsk industri, sier seksjonssjef Marie Moe ved NSMs operasjonssenter til Dagbladet.

Hun oppfordrer hver enkelt bedrift til å gjøre en sikkerhetsvurdering.

– Ved å få en oversikt over alt man har av verdifull informasjon, vil man forhåpentligvis også oppdage om deler av den informasjonen ikke har den beskyttelsen den burde hatt, sier Moe.



didatinformasjon og kopi av hans private bilder og dokumenter, blant annet bankinformasjon.

– Når det gjelder kundeinformasjon, er dette greit nok, vi har full åpenhet om våre kunder. Men det skulle selvsagt heller ikke ligget ute sånn. Jeg er glad for å bli gjort oppmerksom på dette, sier han.

Ble sjokkert

Det er skremmende enkelt å dele innholdet på datamaskinen sin med omverdenen.

Tenk deg for eksempel at samboeren din skal lage julekort og derfor trenger tilgang til feriebildene som er lagret på din pc. Du

høyreklikker på bildemappa og velger «del». Ettersom det bare er dere som er koblet til hjemmenettverket, huker du av for alternativet «del med alle».

Problemet er at modemet ditt med dette også kan åpne for trafikk utenfra. Det betyr at hvem som helst kan få tilgang til filene dine, uten at du er klar over det selv.

– Jeg tenkte: «Dette går jo ikke an». Jeg ble mildt sagt sjokkert. Jeg var ikke klar over at det fantes noen slik mulighet, sier Nyhagen.

Han betrakter seg selv som re-

lativt IT-kyndig, og tok raskt kontakt med vedkommende som installerte serveren for dem. Sammen fant de ut hvordan det var mulig for uvedkommende å få tilgang til alle dokumentene.

– I tillegg prøvde jeg datasikkerhetstesten til Dagbladet, og da skjønnte jeg at jeg var avslørt, sier Nyhagen.

Han sperret raskt ned alle tilkoblingsmuligheter til serveren.

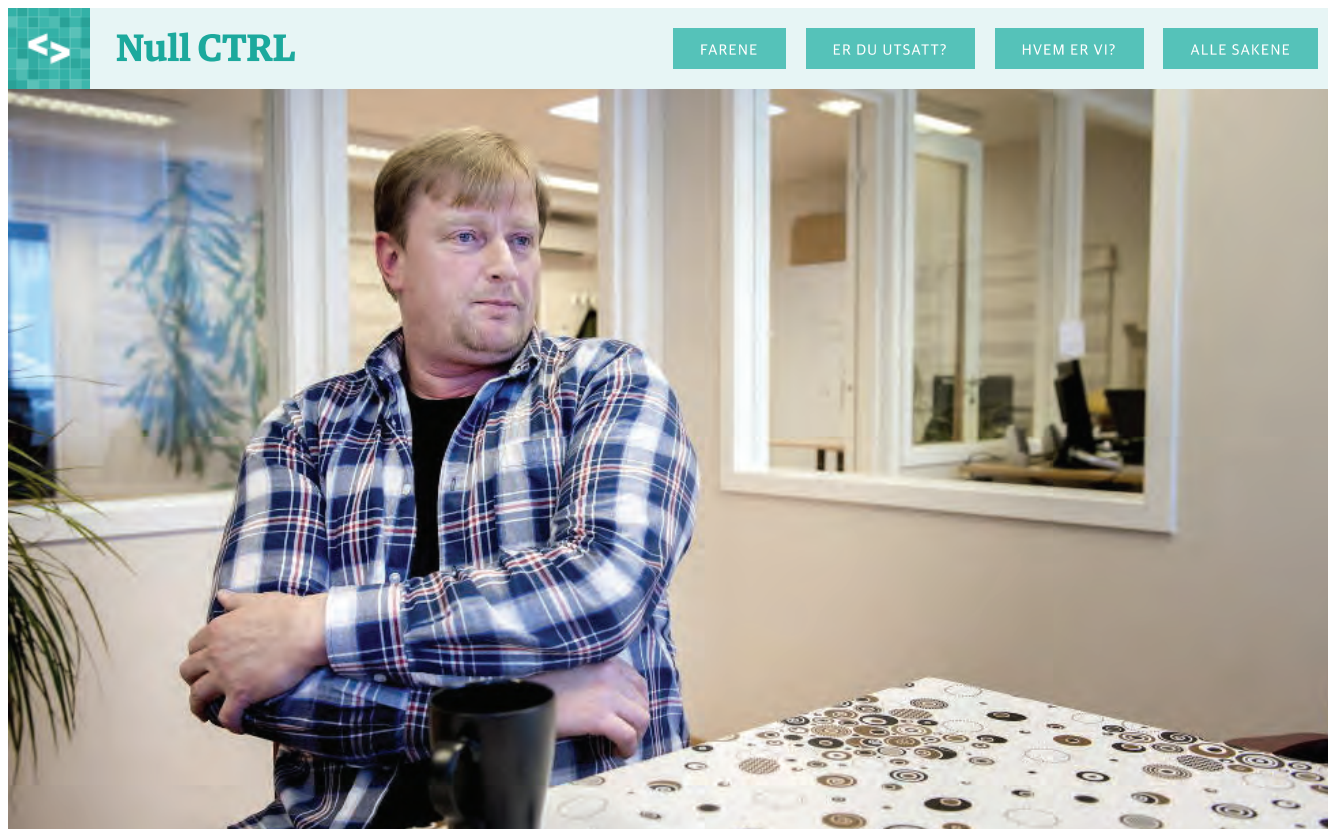
– I etterpåklokskapens lys burde jeg jo ha testet denne løsningen, sier han.

Foto: Øistein Norum Monsen

– Hva ville du ha gjort annerledes i dag?

– Alliere meg med eksperter: Leie inn folk som kan dette og som kan garantere for et godt resultat. Uavhengig av dette så har Veksthuset Rekruttering siden mars i år også investert i weblesning der profesjonelle håndterer både drift og sikkerhet. Og jeg ser jo at det trengs, sier smiler han.

Hovedkontoret til Veksthuset er kjent med innholdet i denne artikkelen og har ingen ytterligere kommentarer.



SJOKKERT: Avdelingsleder Knut Nyhagen ved Veksthuset på Otta hadde ingen anelse om at serveren deres lå tilgjengelig for alle på Internett. Foto: Øistein Norum Monsen / Dagbladet

- Den feilen gjør jeg ikke igjen

Rekrutteringsselskap la ut fortrolig informasjon om jobbsøkere - uten å være klar over det.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

OTTA (Dagbladet): På nett fant Dagbladet en server tilhørende bemanningsbyrået Veksthuset. På den lå det store mengder data om blant annet jobbsøkere.

- Jeg var helt sikker på at dette var godt sikret, det er det som er så skummelt. Men jeg vet i hvert fall at jeg ikke skal gjøre den feilen igjen, sier Knut Nyhagen til Dagbladet.

Han er avdelingsleder for Otta-kontoret til Veksthuset, et rekrutteringsselskap med kontorer sju ulike steder i landet og en omsetning på 59 millioner kroner i fjor.

For noen år siden fikk Otta-avdelingen installert en server, hvor ansatte fikk tilgang til delte jobbdokumenter hjemmefra.



Jeg ble mildt sagt sjokkert. Jeg var ikke klar over at det fantes noen slik mulighet.

Knut Nyhagen, Veksthuset Otta



Serveren ble satt opp slik at det var mulig å logge seg på med IP-adresse, brukernavn og passord. Tilsynelatende fungerte det helt etter planen.

Fortrolig informasjon

Men samtidig sto en annen inngangsport til serveren på vidt gap, noe som gjorde innholdet tilgjengelig også for alle andre. På serveren lå blant annet kundeavtaler og en kandidatbase med CV-er, samt interne vurderinger av kandidater til ulike stillinger.

- Når du arbeider med jobbsøkere og kandidater, er det klart du sitter på en del fortrolig informasjon. Det er beklagelig, selv om dette rett nok er eldre ting. Samtidig lå også en kopi av alt mitt private inne på denne serveren, både bilder og sikkert bankinformasjon og annen personinformasjon. Her kan det blant annet ha ligget noen private passord, sier Nyhagen.

- Når det gjelder kundeinformasjon, er dette greit nok, vi har full åpenhet om våre kunder. Men det skulle selvsagt heller ikke ligget ute sånn. Jeg er glad for å bli gjort oppmerksom på dette, sier han.

Ble sjokkert

Det er skremmende enkelt å dele innholdet på datamaskinen sin med omverdenen. Tenk deg for eksempel at samboeren din skal lage julekort og derfor trenger tilgang til feriebildene som er lagret på din PC. Du høyreklikker på bildemappa og velger «del». Ettersom det bare er dere som er koblet til hjemmenettverket, huker du av for alternativet «del med alle».

Problemet er at modemmet ditt med dette også kan åpne for trafikk utenfra. Det betyr at hvem som helst kan få tilgang til filene dine, uten at du er klar over det selv.

- Jeg tenkte: «Dette går jo ikke an». Jeg ble mildt sagt sjokkert. Jeg var ikke klar over at det fantes noen slik mulighet, sier Nyhagen.

Ny løsning

Han betrakter seg selv som relativt IT-kyndig, og tok raskt kontakt med vedkommende som installerte serveren for dem. Sammen fant de ut hvordan det var mulig for uvedkommende å få tilgang til alle dokumentene.

- I tillegg prøvde jeg [datasikkerhetstesten til Dagbladet](#), og da skjønnte jeg at jeg var avslørt, sier Nyhagen.

Han sperret raskt ned alle tilkoblingsmuligheter til serveren.

- I etterpåklokskapens lys burde jeg jo ha testet denne løsningen, sier han.

- Hva ville du ha gjort annerledes i dag?

- Heretter skal jeg nok alliere meg med eksperter, da skal jeg leie inn folk som kan dette og som kan garantere for et godt resultat. Uavhengig av dette så har Veksthuset Rekruttering siden mars i år også investert i webløsning der profesjonelle håndterer både drift og sikkerhet. Og jeg ser jo at det trengs, sier Nyhagen med et skeivt smil.

Hovedkontoret til Veksthuset er kjent med innholdet i denne artikkelen og har ingen ytterligere kommentarer.

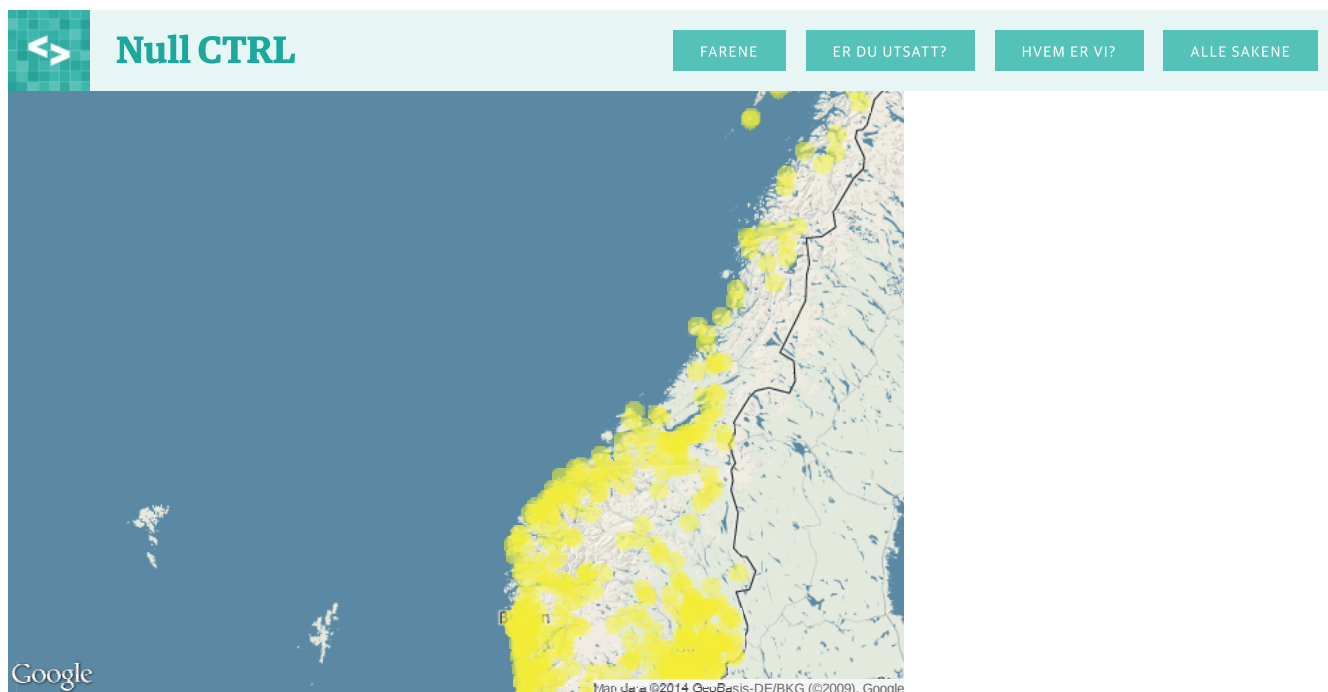
FORTROLIG OG PRIVAT: På serveren lå det ifølge Knut Nyhagen både fortrolig kandidatinformasjon og kopi av hans private bilder og dokumenter, blant annet bankinformasjon. Foto: Øistein Norum Monsen/Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



Tips oss på nullctrl@dagbladet.no



RASKERE DELING: FTP er en delingsmåte som er spesielt godt egnet for filer, men i noen tilfeller åpnes serveren også for alle andre. Dagbladet har lokalisert 18 000 FTP-servere i Norge, av disse er minst 1000

Slik blottlegges dokumenter på Internett

Dagbladet har funnet flere tusen åpne servere og databaser på Internett. Nasjonal sikkerhetsmyndighet er bekymret.



LINN KONGSLØ HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): Ett feil høyreklikk, og plutselig kan sensitive dokumenter være tilgjengelige for alle. [Veksthusets avdeling på Otta](#) er ikke de eneste som uforvarende har delt dokumenter med langt flere enn det som var meningen.

Den enkleste og vanligste protokollen for å dele filer i et Windows-nettverk, kalles SMB. Men hvis du huker av for alternativet «del med alle», kan filene også bli tilgjengelige utenfor nettverket.

Det er det nok mange som ikke er klar over.

Dagbladet har funnet 3.573 slike porter i Norge, mange av dem på vidt gap. Innenfor noen av disse fantes [dokumenter om norsk oljebransje](#), som Dagbladet omtalte i går.



FIKK SJOKK: Avdelingsleder Knut Nyhagen ved Veksthuset på Otta hadde ingen anelse om at serveren deres lå tilgjengelig for alle på Internett. Foto: Øistein Norum Monsen / Dagbladet

Beredskapsdokumenter

En annen tabbe folk ofte gjør, er via en annen form for deling, såkalt

FTP. FTP brukes ofte for å dele filer med andre, men her er det flere fallgruver. En feil Dagbladet ofte har sett eksempler på, er at denne porten til en server er blitt åpnet uten at det var meningen. I andre tilfeller er innholdet ment delt med en ringere krets, men eierne har glemt å begrense innsyn for andre.

Dagbladet har lokalisert 18 000 FTP-servere i Norge. Minst 1000 av disse er usikrede og mange av dem tilhører større eller mindre norske bedrifter.

Det var via en slik usikret FTP-server at Dagbladet fant brannberedskapen [for 39 av 44 kommuner i Nordland](#).

Uvitethet

Seniorrådgiver Vidar Sandland ved Norsk Senter for Informasjonssikring (Norsis) påpeker at de aller fleste bedrifter med åpne servere trolig er helt uvitende om at hvem som helst kan få tilgang til dokumentene deres.

- En av hovedårsakene til at dette blir tilgjengelig på Internett er jo rett og slett at dette er en feilkonfigurasjon. Så her er det nok ofte dårlig risikovurdering, dårlig planlegging, og det er rett og slett dårlig sikkerhetsarbeid, sier Sandland til Dagbladet.

- Det kan jo selvfølgelig få katastrofale konsekvenser for en bedrift, da for eksempel patenter og annen type sensitiv informasjon kan komme på avveie uten at de er klar over det, legger han til.

Nasjonale konsekvenser

Nasjonal sikkerhetsmyndighet (NSM) ser med bekymring på alle de åpne serverne.

- Det er ikke bra for bedriften, som gir ut informasjon de kanskje ikke ønsker skal være tilgjengelig. Men det er heller ikke bra fra et nasjonalt perspektiv - hvis dette gjelder mange bedrifter i Norge - at mulig sensitiv informasjon er tilgjengelig for andre nasjoner eller for noen som ønsker å drive industrispionasje for norsk industri, sier seksjonssjef Marie Moe ved NSMs operasjonssenter til Dagbladet.

Hun oppfordrer hver enkelt bedrift til å gjøre en sikkerhetsvurdering

- Ved å få en oversikt over alt man har av verdifull informasjon, vil man forhåpentligvis også oppdage om deler av den informasjonen ikke har den beskyttelsen den burde hatt, sier Moe.



BEKYMRET: Seksjonssjef Marie Moe ved Nasjonal Sikkerhetsmyndighet oppfordrer alle bedrifter til å gjøre en sikkerhetsvurdering. Foto: Øistein Norum Monsen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



Tips oss på nullctrl@dagbladet.no

FTP og SMB

- SMB (Server Message Block) er en protokoll for deling av filer, skrivere, serie-porter etc. Dette er den enkleste og vanligste fildelingen i et Windows-nettverk, ettersom den bare er et lite høyreklikk unna og finnes på alle Windows-maskiner. Huker du

av for «del med alle», vil imidlertid resten av verden også kunne få tilgang til filene dine.

- FTP (File Transfer Protocol, filoverføringsprotokoll) er en standard protokoll for overføring av filer i et TCP/IP-basert nettverk.
- Både SMB og FTP gir tilgang til filsystemet og gir brukerne potensiell mulighet til opp- og nedlasting av filer, sletting, redigering av innhold mm.
- I tillegg finnes det flere tusen servere på nett i Norge som er blitt gjort tilgjengelige via andre delingsmetoder.

Trodde de måtte taste brukernavn og passord for å komme inn på bedriftsserveren, publisert tirsdag 10.

desember 2013 kl. 22:11



Null CTRL

FARENE

ER DU UTSATT?

HVEM ER VI?

ALLE SAKENE



USIKRET: Serveren til Bergen Kuldeteknikk lå åpent ut mot nettet, uten at de visste det selv. Her fantes blant annet ansattes personopplysninger og detaljerte produkttegninger. Foto: Benjamin A. Ward / Dagbladet

Trodde de måtte taste brukernavn og passord for å komme inn på bedriftsserveren

I virkeligheten var den åpen for absolutt alle.



LINN KONGSLIE HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

BERGEN/OSLO (Dagbladet):
Ansattes skattekort med personnummer og andre personlige opplysninger. Detaljerte produkttegninger, kundeinformasjon og prisoversikter.

Alle disse dokumentene lå inne på webserveren til selskapet Bergen Kuldeteknikk, godt beskyttet med brukernavn og passord - trodde de i hvert fall.

I virkeligheten lå hele serveren vidåpen på nett, noe den kan ha gjort helt siden den ble opprettet for snart tre år siden.

- Dette ligger jo helt åpent. Det er jo krise, sier daglig leder Christer Stålheim etter at Dagbladet har vist ham lenken med alt innholdet.



ØKENDE BEVISSTHET: John Matherly skapte søkemotoren Shodan, og håper den kan øke folks bevissthet om hva de kobler til Internett. Video: Øistein Norum Monsen / Dagbladet

Brukte eksternt firma

Bergen Kuldeteknikk leverer kuldeprodukter og kuldetjenester til bedrifter i og rundt Bergen og i Nordsjøen.

Vi fant serveren i forbindelse med [artikkelserien «Null CTRL»](#), som viser hvordan det er mulig å [se og styre naboens web-kamera](#) og [ta kontroll over industrielle styringssystemer](#) med noen tastetrykk - blant annet.

Stålheim forteller at de brukte det eksterne selskapet Webhuset AS til å sette opp serveren.

I denne forbindelse fikk de tilsendt brukernavn og passord, som de måtte bruke for å koble seg til serveren når de var utenfor kontoret.

- Det har vært en liten vekker dette her. En ting er jo en sånn liten skute som oss, som er helt ubetydelig i den store sammenheng. Noe annet er hvis dette skulle skje med andre, mye større selskaper. Det er skremmende, sier Stålheim.

- Ikke bra

Noen av dokumentene deres, deriblant de ferskeste skattekortene, ligger på en egen server.

- Når det gjelder tegninger og prisinformasjon, er det jo ikke bra at det ligger åpent, men det er ikke helt krise i seg selv. Vi ønsker det selvsagt ikke, men jeg tror ikke folk i vår bransje er så datakyndige at noen ville kommet seg inn og utnyttet disse opplysningene, sier han.

Etter at Dagbladet hadde vist Stålheim lenken med innholdet på serveren, kontaktet han Webhuset AS for å høre hva som hadde gått galt.

- De sa at det var vi som måtte opprettholde sikkerheten, men vi har jo bestilt dette produktet fra dem. Vi er jo ikke spesielt flinke på data, vi driver med kjølesystemer, sier Stålheim.

- Ikke vårt ansvar

Daglig leder ved Webhuset AS, Erik Olsen, holder fast ved at Bergen Kuldeteknikk har ansvar for sikkerheten.



SKUMMELT: Trond Kristiansen ante ikke at overvåningskameraet hans kringkastet bilder og lyd rett ut på Internett. Fremmede kunne blant annet se bilder fra kjøkkenet og datterens soverom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet



UAKSEPTABELT: - Denne type informasjon skal på ingen måte være offentlig, sa brannsjef Rolf Sørtorp, etter at Dagbladet gjorde ham oppmerksom på at en database tilhørende Midtre Hålogaland 110-sentral lå usikret på nett. Video: Øistein Norum Monsen.



ENKELT TERRORMÅL: Ledelsen ved fiskebollefabrikken på Sortland tror det ville vært enkelt å sabotere med brannvesenets beredskapsplaner, som lå åpent tilgjengelig på Internett. Video: Øistein Norum Monsen/Dagbladet.

- Maskinen har ikke blitt konfigurert slik som dette av oss. Kunden har seinere slått på web-serveren på maskinen sin og dermed gjort alle filene på filserveren sin tilgjengelige over Internett, sier han til Dagbladet.

- Hadde vi hatt et driftsansvar for maskinen ville vi oppdaget og forhindret at dette skjedde. Vi har imidlertid ikke fått et slikt driftsansvar og kunden har derfor gjort alle tilpasninger selv siden den gangen maskinen først ble levert av oss.

På spørsmål om hvordan de kan være sikre på at ikke serveren ble opprettet med denne feilen, svarer Olsen at denne sikkerhetsmekanismen ble testet og funnet i orden da serveren ble konfigurert i 2010.

- Veldig synd

- Hva tenker dere om at kunden ikke har forstått at det er de selv som er ansvarlige for dette?

- Det er veldig synd, men samtidig overraskende. Det står helt klart i vår avtale med kunden at «produktet inkluderer ingen drift eller sikkerhetsoppdateringer med mindre det er inngått en egen avtale om dette. Kunden er selv ansvarlig for å holde operativsystem og annen programvare forsvarlig oppdatert til enhver tid», sier Olsen.

- Lett å gå i fella

Ifølge Seniorrådgiver Vidar Sandland i Norsk Senter for Informasjonssikkerhet (Norsis), er det lett å tro at IT-leverandører er ansvarlige for sikkerheten, uavhengig av hva som er avtalen mellom partene.

- Det vi ofte ser, er at selskaper ofte ikke har den bestillerkompetanse de bør ha. De vet ikke alltid hva de trenger av sikkerhet og hvordan dette skal fungere, sier han, og legger til at det i slike situasjoner er viktig å konsultere leverandøren.

- Du må være veldig klar på at du er avhengig av en sikker løsning og at leverandøren dokumenterer hva de har gjort for å sikre produktet ditt.

Christer Stålheim takker for at de ble gjort oppmerksomme på sikkerhetshullet, så de fikk gjort noe med det. Han opplyser at Bergen Kuldeteknikk nå har sagt opp avtalen med Webhuset AS.

- Det er alltid synd å ikke komme til enighet med en kunde - uansett hvem som mener han har rett, sier Webhusets daglige leder Erik Olsen.



REFSER: Tidligere Datatilsynet-direktør Georg Apenes refser den påtroppende regjeringen for å ikke snakke om datasikkerhet. Video: John Terje Pedersen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



Tips oss på nullctrl@dagbladet.no

UKENS BESTE JULEGAVER

Pusle-
spill
**30%
rabatt**

Ukens
tilbud
149,-
Spar 250,-



Send
KUPP
til 2407
og få den-
ne boken
til kun
kr. 99,-
(spar
400,-)

**Du blir automatisk
med i trekningen av
10 gavekort à kr 2000,-**

1 kr. pr. sms.

Tilbudene gjelder kun i uke 50.

norli ;libris



USIKRET: Serveren til Bergen Kuldeteknikk lå åpent ut mot nettet, uten at de visste det selv. Her fantes blant

Nav-dokumenter, sykemeldinger og andre intime opplysninger om arbeidstakere flyter på Internett – helt ubeskyttet for uvedkommende.

Intime og personlige opplysninger er ikke nødvendigvis så trygge hos sjefen som du kanskje trodde.

I forbindelse med artikkelserien «Null CTRL» har Dagbladet funnet flere tusen åpne databaser og servere på nettet i Norge, mange tilhørende større og mindre norske selskaper.

Brannberedskapen for 39 av 44 kommuner i Nordland, dokumenter om norsk oljebransje, informasjon om barn på hemmelig adresse og dokumenter om Ørland flystasjon er bare noe av det som har ligget ubeskyttet.

Nav-dokumenter

Men også sensitive data om ansatte blir lagt i åpne servere og databaser på Internett.



DIREKTØR

Bjørn Erik Thon i Datatilsynet.

NULL CTRL



Dagbladet har kommet over alt fra sykemeldinger og Nav-dokumenter til medarbeidersamtaler og lønnsdata, lagret ubeskyttet av sjefen – tilsynelatende helt uforvarende.

– Veldig mye av det du nevner dere har funnet, er enten personlig eller sensitiv informasjon. Det er klare regler for at arbeidsgiver har et ansvar for å sikre at dette ikke kommer på avveie, sier direktør Bjørn Erik Thon i Datatilsynet.

– Veldig alvorlig

– Dette er ikke noe som har noe i offentligheten å gjøre. Dette er strengt interne ting, som ikke engang alle på arbeidsplassen skal se. Det er veldig alvorlig det dere har avdekket, sier han videre.

– Hva kan gjøres for å bedre situasjonen?

– Dette fører seg jo inn i rekken av saker Dagbladet har avslørt, men det handler jo om å ha ordren i eget hus. Dette betyr at alle må

gå gjennom sårbarheten sin, og rett og slett bruke litt tid og penger på dette.

– Helt krise

Selskapet Bergen Kuldeteknikk, som leverer kuldeprodukter og kuldetjenester til bedrifter i og rundt Bergen og i Nordsjøen, trodde de måtte taste brukernavn og passord for å få tilgang til sin bedriftsserver. I virkeligheten lå den ute på en egen side på Internett, åpen og søkbar for absolutt alle.

På serveren fantes blant annet ansattes skattekort med personnummer og andre personlige opplysninger.

– Dette ligger jo helt åpent. Det er jo krise, sa daglig leder Christer Stålheim etter at Dagbladet hadde vist ham lenken med alt innholdet.

Noen av dokumentene deres, deriblant de ferskeste skattekortene, lå imidlertid på en egen server.

– Lett å gå i falla

Bergen Kuldeteknikk brukte Webhuset AS til å sette opp serveren. De mener kunden seinere har slått på webserveren på maskinen sin og dermed gjort alle filene tilgjengelige over Internett.

Ifølge Seniorrådgiver Vidar Sandland i Norsk Senter for Informasjonssikkerhet (NorSIS), er det lett å tro at eksterne IT-leverandører er ansvarlige for sikkerheten, uavhengig av hva som er avtalen mellom partene.

– Det vi ofte ser, er at selskaper ofte ikke har den bestillerkompetanse de bør ha. De vet ikke alltid hva de trenger av sikkerhet og hvordan dette skal fungere, sier han.

Alle må gå gjennom sårbarheten sin, og rett og slett bruke litt tid og penger på dette.

Bjørn Erik Thon, direktør i Datatilsynet



annet ansattes personopplysninger.

Foto: Benjamin A. Ward

Draps-siktede er løslatt

Politiet står uten avgjørende bevis mot de tre som er siktet for drapet på Per Vålnes (50). Derfor slipper de nå ut fra varetekt etter 13 måneder.

Tekst: **Ralf Lofstad**
rlo@dagbladet.no

De tre – Vålnes' samboer (41), hennes nye kjæreste (40) og en mannlig felles bekjent av dem (42) – er fremdeles siktet i saken. De har sittet 13 måneder i varetekt.

– Tung periode

– Det har vært en veldig lang og tung periode. Hun er utrolig glad for å slippe ut nå, sier samboerens advokat, Randolph Schumann Hansen, til Dagbladet.

Den 41-årige kvinnen, som har sittet i Troms fengsel, befinner seg nå på ukjent sted.

Etterforskningsleder Morten Hermansen opplyser at politiet opprinnelig hadde planlagt å få Vålnes-saken for retten til våren – men at han løslater de siktede fordi framdriftsplanen for den videre etterforskningen nå er såpass usikker at videre varetektsfengs-



TROLIG DREPT: Per Vålnes.

ling «vil kunne medføre et uforholdsmessig inngrep» for dem.

VG skrev i forrige uke at Riksadvokaten overveide å reise tiltale mot de siktede. Saken ble til slutt sendt tilbake til politiet, som fikk beskjed om å etterforske mer.

Forsvant etter fest

50-årige Per Vålnes forsvant etter sin egen fødselsdagsfeiring for to år siden, og antas drept. Samboeren, hennes nye kjæreste samt den 42-årige felles bekjente ble et år etterpå pågrepet og siktet i saken. De nekter alle straffskyld.

På tross av iherdig og langvarig leting på land og til sjøs har politiet ikke funnet liket av Vålnes.



KNIVSKADD:

En mann (22) er skadd og tre personer er pågrepet etter knivstikking i Borggata på Tøyen i Oslo i går formiddag. De tre pågrepne er 22, 23 og 26 år gamle. (NTB)



LETTBRUS:

En omfattende undersøkelse av søtningsstoffet aspartam som EU-organet EFSA har gjennomført, viser at søtningsmiddelet ikke er skadelig. Maksimalt anbefalt daglig inntak av søtningsmiddelet oppgis til sju liter for en voksen mann, fem liter for en voksen kvinne og fire liter for et barn. (NTB)

zero Emission



100% ELEKTRISKE NYE NISSAN LEAF.
SPENNINGEN ØKER.

KUN KR 2 122* PER MÅNED – GARANTERT!

For å gi deg et forutsigbart bilhold tilbyr vi en lånefinansiering med restverdigaranti. Priseksempelen er beregnet på toppmodellen Nissan LEAF TEKNA inkludert vinterhjul.

BILLIG Å EIE

- Ingen moms eller engangsavgift
- Gratis parkering på offentlige plasser
- Under 2 kroner per mil.
- Ingen bom- og fergeavgifter

NORGESPAKKEN INKLUDERT

VERDI KR 35 000

- 3 års gratis service
- Kromdetaljer
- 20 leiebildegner gjennom Hertz

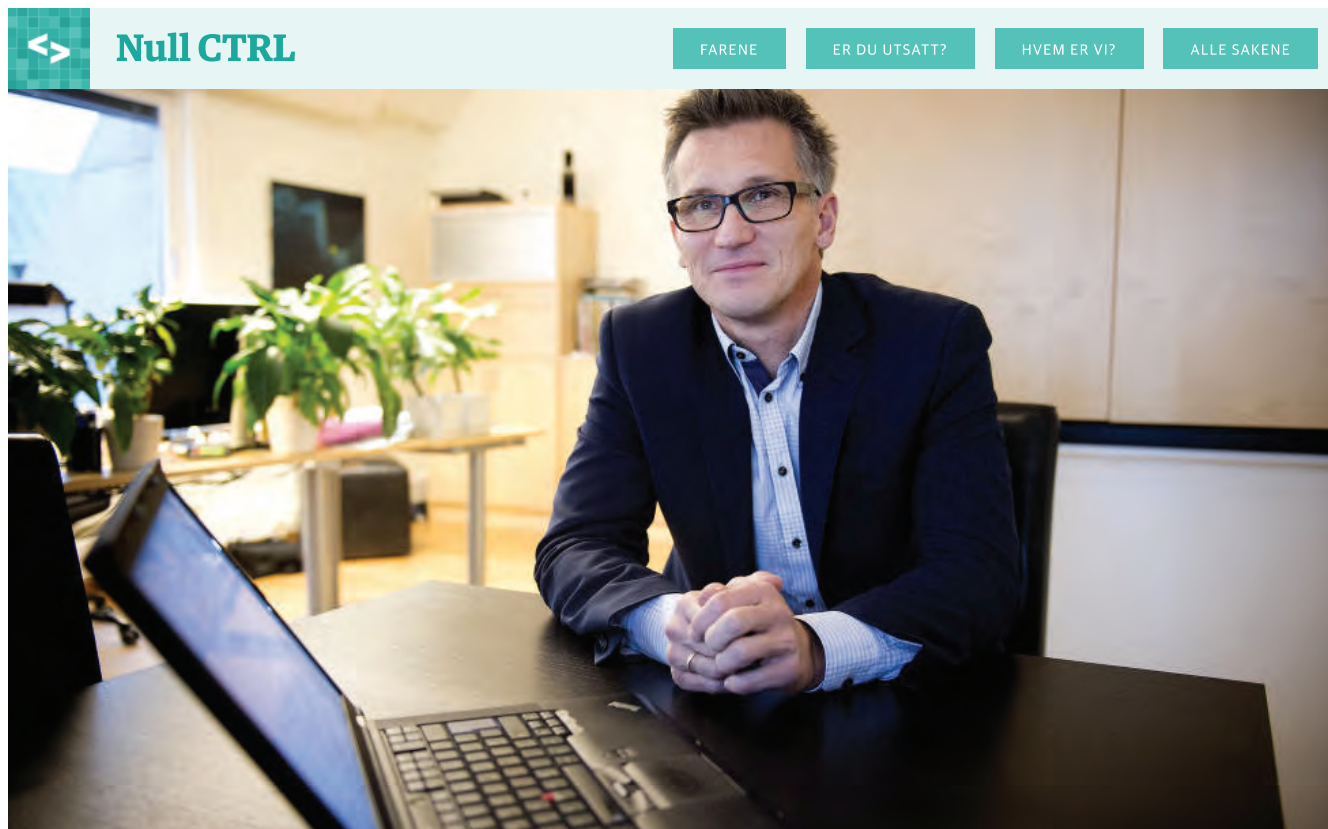
Det har aldri vært mer gunstig å kjøpe og eie en Nissan LEAF!

Nye NISSAN LEAF fra kr 228 600*

Nissan.no | * Tilbudet forutsetter 35% kontantandel (kr 99 480). Nominell rente 5,95%. Effektiv rente 7,70%. Løpetid 36 mnd/45 000 km. Kredittkøpris: 320 012. Kredittkostnad: 35 786. Etablering og tinglysning på 5 300 tilkommer. Leiebiltilbudet inkluderer 20 leiebil-døgn med bil i samme størrelse. Beregnet kostnad per mil er et estimat basert på gjennomsnittlige strømpriser og forbruk. Kjøreteknikk, vei- og føreforhold m.m. kan påvirke resultatene. Veil. pris levert Drammen inkl. lev.omk. med kr 8900.



- Dette har ikke noe i offentligheten å gjøre, publisert onsdag 11. desember 2013 kl. 11:24



REAGERER: Direktør Bjørn Erik Thon i Datatilsynet påpeker at det er klare regler for at arbeidsgivere skal sikre at data om ansatte ikke kommer på avveie. Han mener Dagbladets avsløringer er svært alvorlige. Foto: Øistein Norum Monsen/Dagbladet.

- Dette har ikke noe i offentligheten å gjøre

NAV-dokumenter, sykemeldinger og andre intime opplysninger om arbeidstakere flyter på internett.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): Intime og personlige opplysninger er ikke nødvendigvis så trygge hos sjefen som du kanskje trodde.

I forbindelse med [artikkelserien «Null CTRL»](#) har Dagbladet funnet flere tusen [åpne databaser og servere på nettet i Norge](#), mange tilhørende større og mindre norske selskaper.

[Brannberedskaper for 39 av 44 kommuner i Nordland](#), detaljerte dokumenter om [norsk oljebransje](#), informasjon om [barn på hemmelig adresse](#), [sensitive kundedata](#) og [dokumenter om Ørland flystasjon](#) er bare noe av det som har ligget ubeskyttet på Internett.

NAV-dokumenter

Men også sensitiv informasjon om



OLJEDOKUMENTER: Dagbladet har bant annet funnet fem åpne og søkbare servere med detaljerte, tekniske dokumenter om norsk oljebransje i forbindelse med artikkelserien «Null CTRL». Arkivfoto: Eirik Helland Urke / Dagbladet

ansatte blir lagt i åpne servere og databaser på nettet.

Dagbladet har kommet over alt fra sykemeldinger og NAV-dokumenter til medarbeidersamtaler og lønnsdata, lagret ubeskyttet av sjefen - tilsynelatende helt uforvarende.

- Veldig mye av det du nevner dere har funnet, er enten personlig eller sensitiv informasjon. Det er klare regler for at arbeidsgiver har et ansvar for å sikre at dette ikke kommer på avveie, sier direktør Bjørn Erik Thon i Datatilsynet.

- Veldig alvorlig

- Dette har ikke noe i offentligheten å gjøre. Dette er strengt internt, som ikke engang alle på arbeidsplassen skal se. Det er veldig alvorlig det dere har avdekket, sier han videre.

- Hva kan gjøres for å bedre situasjonen?

- Dette føyer seg jo inn i rekken av saker Dagbladet har avslørt, men det handler jo om å ha orden i eget hus. Dette betyr at alle må gå gjennom sårbarheten sin og rett og slett bruke litt tid og penger på dette. Det er helt klart et ansvar arbeidsgiver har, og det må inngå som en helt naturlig del av jobben.

- Helt krise

Dagbladet omtalte i går selskapet Bergen Kuldeteknikk, som leverer kuldeprodukter og kuldetjenester til bedrifter i og rundt Bergen og i Nordsjøen. De trodde de måtte taste brukernavn og passord for å få tilgang til sin bedriftsserver. I virkeligheten lå den ute på en egen side på Internett, åpen og søkbar for absolutt alle.

På serveren fantes blant annet ansattes skattekort med personnummer og andre personlige opplysninger.

- Dette ligger jo helt åpent. Det er jo krise, sa daglig leder Christer Stålheim etter at Dagbladet hadde vist ham lenken med alt innholdet.

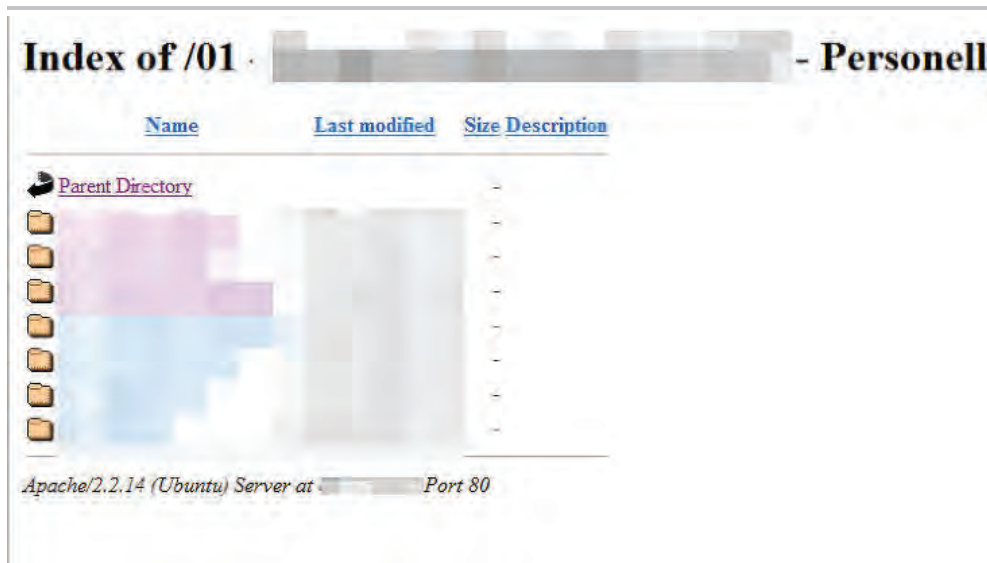
Noen av dokumentene deres, deriblant de ferskeste skattekortene, lå imidlertid på en egen server.

- Lett å gå i fella

Bergen Kuldeteknikk brukte det eksterne selskapet Webhuset AS til å sette opp serveren. De



USIKRET: Serveren til Bergen Kuldeteknikk lå åpent ut mot nettet, uten at de visste det selv. Her fantes blant annet ansattes personopplysninger. Foto: Benjamin A. Ward / Dagbladet



ANSATTOPPLYSNINGER: Dette skjermbildet viser mapper med opplysninger for hver enkelt ansatt i en norsk bedrift.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).

- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL

mener kunden seinere har slått på web-serveren på maskinen sin og dermed gjort alle filene tilgjengelige over Internett.

Ifølge Seniorrådgiver Vidar Sandland i Norsk Senter for Informasjonssikkerhet (Norsis), er det lett å tro at eksterne IT-leverandører er ansvarlige for sikkerheten, uavhengig av hva som er avtalen mellom partene.

- Det vi ofte ser, er at selskaper ofte ikke har den bestillerkompetanse de bør ha. De vet ikke alltid hva de trenger av sikkerhet og hvordan dette skal fungere, sier han.

VARMLUFT: På knappe 42 timer steg temperaturen i Kautokeino med rundt 45 grader – fra minus 40 til pluss 5. Den store temperaturendringen fant sted fra mandag kveld til i går formiddag, melder YR på Twitter. Årsaken er varmluft fra Kanariøyene. (NTB)

Skoleportal: - Driver du med intimbarbering?

En spørreundersøkelse på en videregående skole i Bergen har vakt bekymring blant foreldre.

– Hvor ofte intimbarberer du deg? Får du røde nupper av barberingen? Er det viktig at partneren barberer seg nedentil?

Dette er blant spørsmålene blir stilt i undersøkelsen. Elevene ved Nordahl Griegs videregående skole skal lage et livsstilsmagasin hvor denne undersøkelsen er et av prosjektene deres, melder Bergens Tidende.

Rådgiver i Datatilsynet, Andreas J. Hofstad, er skeptisk til at

slike spørsmål stilles gjennom skolens læringsportal på nett.

Joachim Laberg, lektor på skolens medielinje, vil ikke bagatellisere kritikken.

– Men dette handler i utgangspunktet om moralsk kritikk, ikke om datasikkerhet, sier han til BT.

HACKING: Svenske Forsvarets radioanstalt (FRA) samarbeider aktivt med USA om å hacke seg inn på datamaskiner, ifølge SVT. Samarbeidet fremgår i dokumenter som er lekket av amerikaneren Edward Snowden, rapporterer det svenske TV-programmet Uppdrag granskning. (NTB)



NYE TRUSLER: Selv om vassdrags- og energidirektør Per Sanderud (t.h.) og seniorrådgiver Frank Skapalen i NVE ønsker nye IT-løsninger i energibransjen velkommen, påpeker de at dette også medfører nye farer for strømforsyningen. Foto: Thomas Rasmus Skaug

Frykter hacking av strømmnettet

Energibransjen blir stadig mer avhengig av IT-systemer. Det øker sårbarheten for ondsinnede dataangrep, advarer statens eget kontrollorgan.

– Vårt utgangspunkt er at et samfunn som vårt ikke tåler at strømmen blir borte over lengre tid. Men samtidig gir vi ingen garantier. Dette er et krevende område, sier vassdrags- og energidirektør Per Sanderud til Dagbladet.

I en kronikk i dagens avis setter han fokus på hvordan økende bruk av IT-systemer kan gjøre strømforsyningen

NULL CTRL



mer utsatt for dataangrep.

«Omfanget av informasjonsteknologi knyttet til strømleveransene blir større og antallet punkter som kan rammes av et ondsinnert angrep blir flere. Selv om vi ikke kjenner til noen forsøk på å angripe kontrollsystem som har truet energiforsyningen her i landet skal vi ikke være naive å tro at vi ikke vil oppleve slike forsøk i

framtida,» skriver Sanderud.

I 2019 skal en ny type strømmålere være på plass i alle norske hjem, såkalte AMS-målere. Disse er ment å gi mange fordeler, blant annet skal forbrukerne hele tida få oppdatert informasjon om strømprisene, som varierer mye både i forhold til årstid og tid på døgnet.

– Mer sårbare

– Men denne type tiltak gjør også at vi blir mer sårbare for ondsinnede angrep. Vi ønsker jo ikke at det norske strømmettet skal være et lavterskeltilbud for den type aktivitet, sier Sanderud, som samtidig understreker at IT-utviklingen er ønsket, blant annet på grunn av effektivitet.

Nettopp det at hackere skal få tilgang denne type instrumenter i tusenvis av hjem, er

noe av det som bekymrer John Matherly, skaperen av søkemotoren Shodan.

Kritikk

– Hvis du skader en, er det ingen som vil bry seg. Men hvis du kan skade 100 000 av disse, blir det et nasjonalt problem, sier Matherly til Dagbladet.

– For enkelte kan det øke motivasjonen at det kan være mulig å ramme et stort antall samtidig, supplerer den britiske sikkerhetseksperten Eireann Leverett.

– Dette var utgangspunktet med AMS-målerne: Hvis du hacket nok målere, kunne du få en kritisk situasjon i strømmettet, for plutselig var X-antall megawatt borte fra husene. Dette er også grunnen til at vi ønsker god sikkerhet i disse målerne, sier seni-

orrådgiver Frank Skapalen i seksjon for beredskap ved NVE.

Per Sanderud påpeker imidlertid at de smarte strømmålerne bare er ett eksempel.

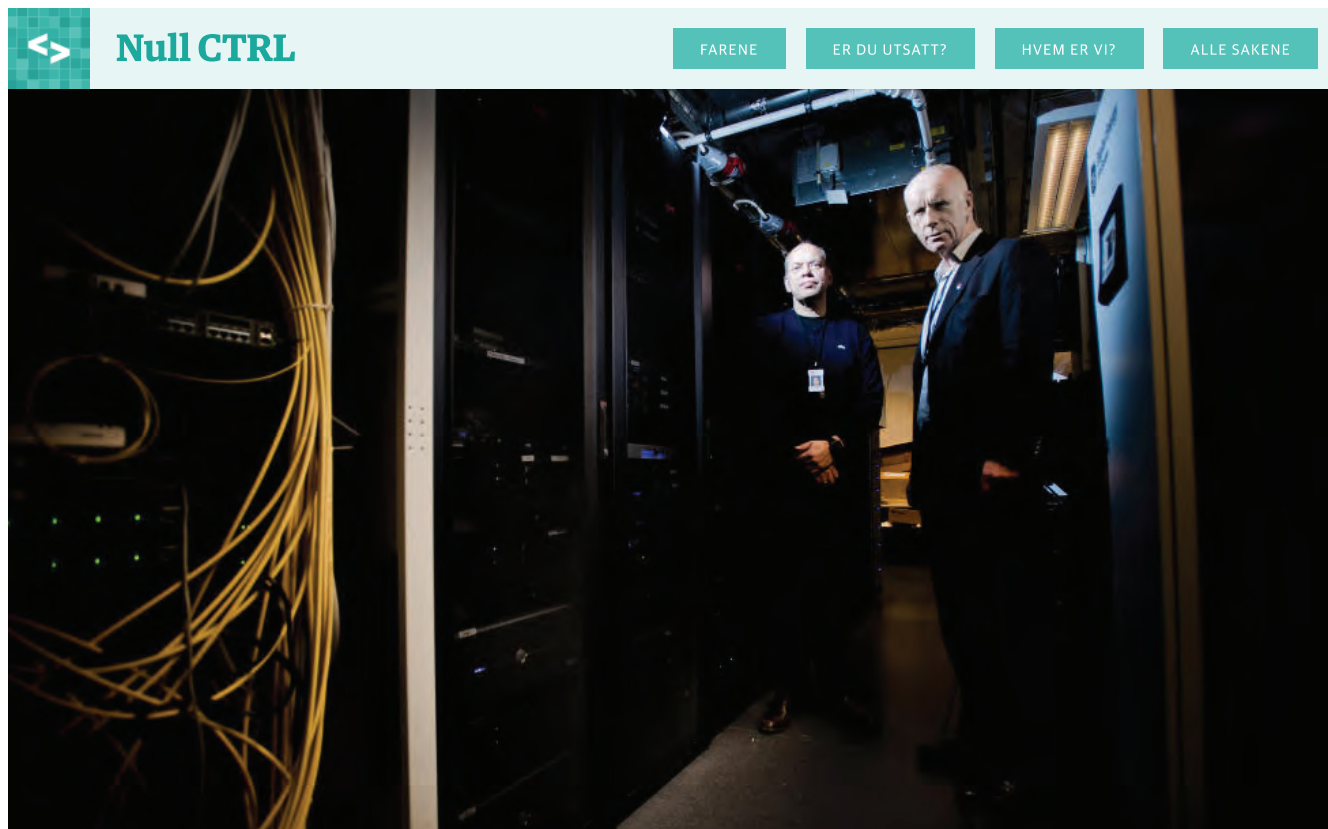
I forbindelse med artikkelserien «Null CTRL» har Dagbladet funnet over 2500 styringssystemer i Norge koblet til Internett med lite eller ingen beskyttelse.

Kan ødelegge

Flere eksperter mener infrastruktur så vital som det strømforsyning er, bør være fullstendig avsondret fra Internett. NVE er ikke enig:

– Vi snur det heller litt på hodet og sier at det skal være mulig å drive disse kraftstasjonene selv om IT-systemene er nede. Det er et sentralt krav, sier Sanderud.

- Denne typen tiltak gjør oss mer sårbare for ondsinnede angrep, publisert torsdag 12. desember 2013 kl. 21:11



NYE TRUSLER: Selv om vassdrags- og energidirektør Per Sanderud (t.h.) og seniorrådgiver Frank Skapalen i NVE ønsker nye IT-løsninger i energibransjen velkommen, påpeker de at dette også medfører nye farer for strømforsyningen. Foto: Thomas Rasmus Skaug / Dagbladet

- Denne typen tiltak gjør oss mer sårbare for ondsinnede angrep

NVE advarer om nye trusler mot strømmettet.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no

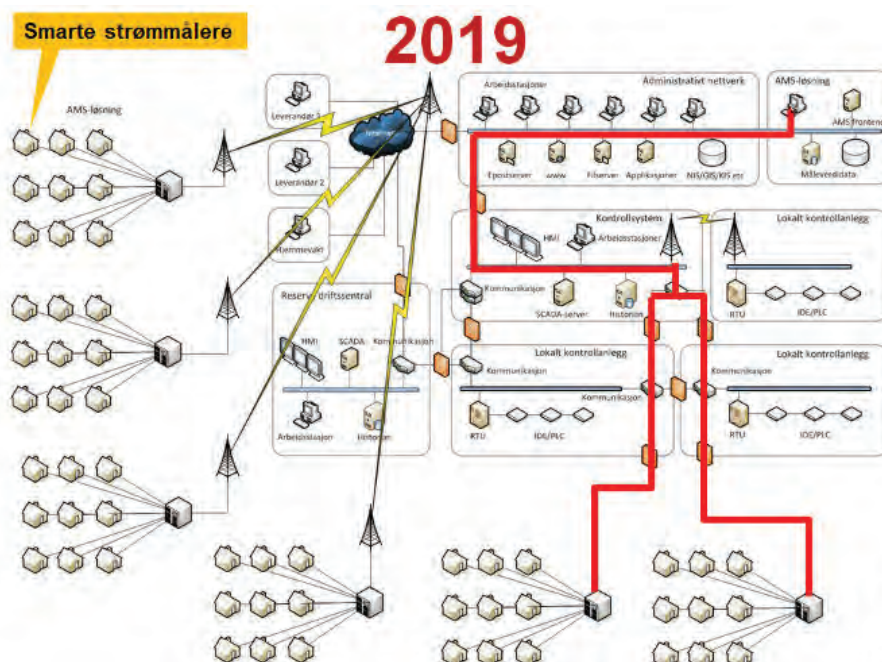


ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): - Vårt utgangspunkt er at et samfunn som vårt ikke tåler at strømmen blir borte over lenger tid. Men samtidig gir vi ingen garantier. Dette er et krevende område, sier vassdrags- og energidirektør Per Sanderud til Dagbladet.

I en [kronikk i dagens avis](#) setter han fokus på hvordan økende bruk av IT-systemer kan gjøre strømforsyningen mer utsatt for dataangrep.

«Omfanget av informasjonsteknologi knyttet til strømløseleveransene blir større og antallet punkter som kan rammes av et ondsinnet angrep blir flere. Selv om vi ikke kjenner til noen forsøk på å angripe kontrollsystem som har truet energiforsyningen her i landet skal vi ikke være naive å tro



at vi ikke vil oppleve slike forsøk i framtida,» skriver Sanderud.

«Smarte målere»

I 2019 skal en ny type strømmålere være på plass i alle norske hjem, såkalte AMS-målere. Disse er ment å gi mange fordeler, blant annet skal forbrukerne hele tida få oppdatert informasjon om strømprisene, som varierer mye både i forhold til årstid og tid på døgnet.

Dette kan også føre til en mer fornuftig strømbruk, håper Sanderud.

- Men denne typen tiltak gjør også at vi blir mer sårbare for ondssinnede angrep. Vi ønsker jo ikke at det norske strømmettet skal være et lavterskeltilbud for den type aktivitet, sier Sanderud, som samtidig understreker at IT-utviklingen er ønsket, blant annet på grunn av hensyn til effektivitet.

Nettopp det at hackere skal få tilgang denne type instrumenter i tusenvis av hjem, er noe av det som bekymrer John Matherly, [skaperen av søkemotoren Shodan](#).

Kritisk

- Hvis du skader en, er det ingen som vil bry seg. Men hvis du kan skade 100 000 av disse, blir det et nasjonalt problem, sier Matherly til Dagbladet.

- For enkelte kan det øke motivasjonen at det kan være mulig å ramme et stort antall samtidig, supplerer den britiske sikkerhetseksperten Eireann Leverett.

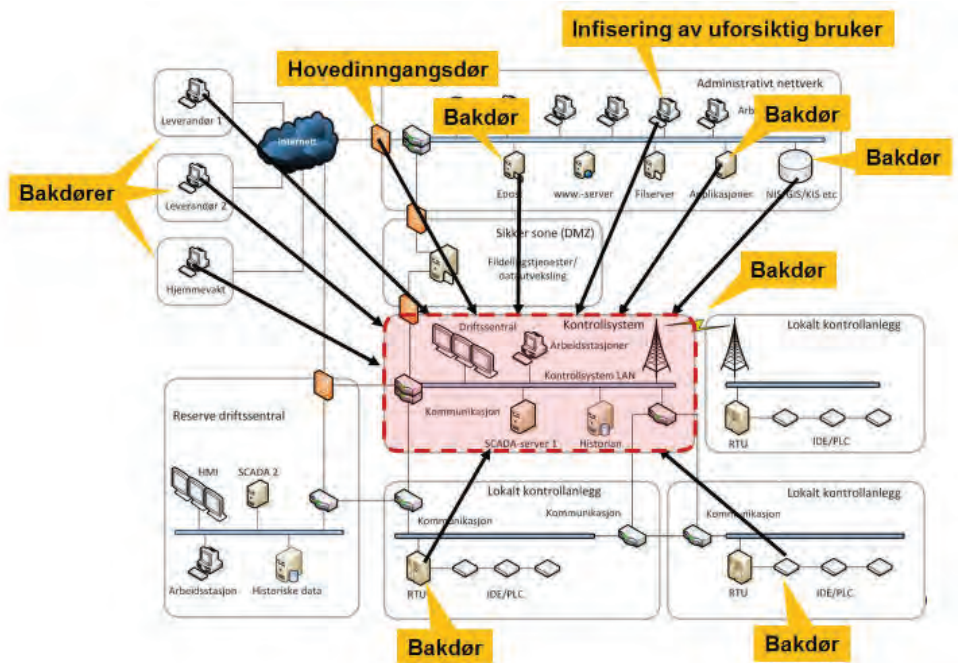
Matherly kaller problematikken «criticality of numbers».

- Dette var utgangspunktet med AMS-målerne: Hvis du hacket nok målere, kunne du få en kritisk situasjon i strømmettet, for plutselig var X-antall megawatt borte fra husene. Dette er også grunnen til at vi ønsker god sikkerhet i disse målerne, sier seniorrådgiver Frank Skapalen i seksjon for beredskap ved NVE.

Styres via nett

Per Sanderud påpeker imidlertid at de smarte strømmålerne bare er ett eksempel.

NY TEKNOLOGI: I 2019 skal såkalte smarte strømmålere være på plass i alle norske hjem. Disse skal gi forbrukerne flere fordeler, men denne type tiltak øker også sårbarheten for hackerangrep. Illustrasjon: NVE



SÅRBARE: Energisektoren blir stadig mer basert på IT-løsninger. Her har NVE skissert ulike sårbarheter i energiforsyningen. Illustrasjon: NVE



BEKYMRET: Mannen bak «verdens farligste søkemotor», John Matherly, frykter at noen skal angripe såkalte hverdagsinstrumenter i tusenvis av hjem samtidig. Video: Øistein Norum Monsen / Dagbladet



I forbindelse med [artikkelserien «Null CTRL»](#) har Dagbladet funnet [over 2500 styringssystemer i Norge koblet til Internett](#) med lite eller ingen beskyttelse.

Denne type systemer har NVE vært svært opptatt av når de utformet nye sikkerhetsregler for energibransjen.

- Vi var med å åpne Engebrets Foss nå, et nytt elvekraftverk og et fantastisk fint miljøprosjekt, men der er det ingen. Alt fjernstyres fra et helt annet sted gjennom styringssystemer, påpeker Sanderud.

MOTIVASJON: Den britiske sikkerhetseksperter Eireann Leverett påpeker at såkalte smarte strømmålere øker faren for hacker-angrep. Foto: Espen Sandli / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

Kan ødelegge

Flere eksperter mener infrastruktur så vital som det strømforsyning er, bør være fullstendig avsondret fra Internett. NVE er ikke enig:

- Vi snur det heller litt på hodet og sier at det skal være mulig å drive disse kraftstasjonene selv om IT-systemene er nede. Det er et sentralt krav, sier Sanderud.

Selskapene har krav om å analysere det verste som kan skje med sine systemer.

- Det absolutt verste er jo hvis noen trenger seg inn i et styringssystem og klarer å ødelegge anlegg, men et slikt målrettet angrep er veldig vanskelig. Det er mange barrierer som må forseres for å få tilgang. Du må faktisk ha inngående kjennskap til hvert enkelt system for å komme deg inn i dem, sier seniorrådgiver Frank Skapalen.

- Er det tilgang til kontroll- panelene eller at det går alarmer dere reagerer på?, publisert torsdag 19. desember

2013 kl 11:44

**Null CTRL**

FARENEER DU UTSATT?HVEM ER VI?ALLE SAKENE

CMC-TC
Name: Rack B4
Location: Datahall 3
Contact: @songnetworks.no

Status

1	IO Unit: Rack B4		2	IO Unit: Rack B4	
1 Skap A	Alarm		1 Humidity Sensor	↓ 36%rH	
2 Skap B	OK		2 Temperature Sensor	↑ 26°C	
3 Skap C	Alarm		3 not available		
4 Skap D	OK		4 not available		
Alarm			Alarm		
3 not available			4 not available		

BLINKER RØDT: Styringspanelet reagerer på avvikende temperatur og fuktighet i denne datahallen tilhørende TDC. Foto: Skjermdump

- Er det tilgang til kontroll- panelene eller at det går alarmer dere reagerer på?

Slik gikk det da Dagbladet sjekket datasikkerheten hos telegiganten TDC.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLI HILLESTAD
llu@dagbladet.no

(Dagbladet) «Datahall 3» står det på ei nettside - hvor det blinker i røde alarmer på skjermen.

Nettadressen tilhører den danske telegiganten TDCs norske hovedkontor. Den aktuelle adressen inngår i en serie IP-adresser med samme eier og type innhold.

- Det dere ser er et overvåkningssystem for varme- og kjølesystemet i en datahall, sier avdelingsdirektør Brede Bergskaug.

Overvåker

På hver av sidene Dagbladet åpnet, dukket det opp et web-basert kontrollpanel.

- Er det tilgang til kontrollpanelene eller at det går alarmer dere



FJERNET ALARMENE: Administrerende direktør Ketil Kivedahl (t.v.) og avdelingsdirektør Brede Bergskaug i TDC hevder nettpanelene ikke lar seg manipulere av uvedkommende, men vil fjerne dem fra nett «for å unngå misforståelser». Foto: Øistein Norum Monsen / Dagbladet

reagerer på, spør administrerende direktør Ketil Kivedahl da Dagbladet viser ham nettsidene.

- Det er all grunn til at jeg får spørsmål om dette. Men det dere ser er ikke knyttet til vårt sentrale overvåkingssystem, så hackere kan ikke ta seg inn via dette oppsettet, legger han til.

Bransjegigant

TDC er den privatiserte etterfølgeren av selskapet som en gang var monopolbedriften TeleDanmark (TD). Selskapet har i dag nærmere ti millioner kunder innen telefoni, bredbånd og TV.

TDC Norge har gjennom oppkjøp av EITele Øst og Song Networks Norge et betydelig nett av optisk fiber og mange norske kunder, spesielt i de største byene. Selskapet har de siste åra vunnet flere store offentlige bredbåndskontrakter.

Dagbladet fant de mange alarmsidene i forbindelse med serien «[Null CTRL](#)» om datasikkerhet.

- Ikke i bruk

Ikke på noen av sidene Dagbladet fant, blir man bedt om å skrive inn noe passord for å få adgang. Tilsynelatende var det mulig å endre innstillingene via panelene på nett.

Etter å ha sjekket systemet nærmere, mener Kivedahl at passord heller ikke var nødvendig. Ifølge TDC kunne man bare lese, ikke gjøre endringer i oppsettet.

- Via panelene har du kun leserett. Panelene overvåket enkelte rack i datahallen, som for øvrig ikke er i bruk, skriver Kivedahl i en e-post.

Han utdyper:

- IP-adressene benyttes til å lese temperatur og luftfuktighet i rack som er plassert i en datahall hos TDC. Via IP-adressene er det kun tilgang til å lese miljøparametre, og endringer av temperatur kan ikke gjøres via systemet. Overvåkingen ble satt opp for å gi brukere av datahallen enkel tilgang til informasjon om temperatur, skriver Kivedahl.

Fjernet fra nett

TDC har i ettertid valgt å ta alarmsidene fra «Datahall 3» vekk fra nett.

- Vi fjerner dem for å unngå misforståelser, sier Kivedahl.

Hva konkret som befinner seg i «Datahall 3» ønsker ikke TDC å si noe om:

- Spør du meg hvem som leier av oss i de datahallene, så vet ikke jeg det. Det er av sikkerhetsmessige årsaker.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.

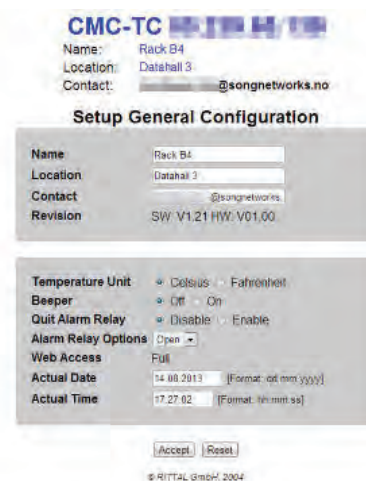
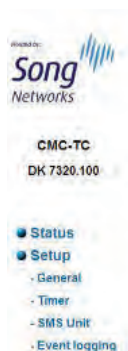
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.

- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).

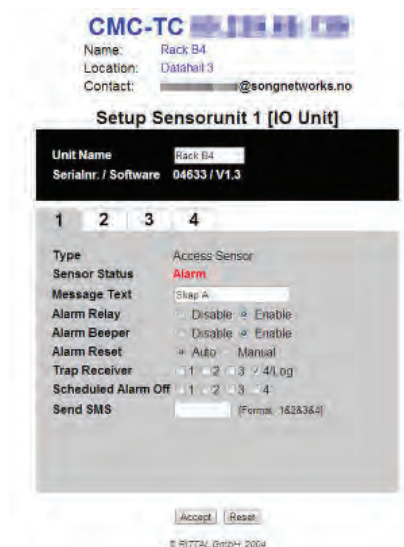
- Følg serien her: <http://www.dagbladet.no/nullctrl/>

- Tips oss på nullctrl@dagbladet.no

- Si din mening på Twitter: #null_CTRL



FLERE INNSTILLINGER: En rekke innstillinger var tilsynelatende tilgjengelig på nett. Ifølge TDC kunne man bare lese, ikke gjøre endringer i oppsettet. Foto: Skjermdump



SENSOR: En rekke innstillinger var tilsynelatende tilgjengelig på nett. Ifølge TDC kunne man bare lese, ikke gjøre endringer i oppsettet. Foto: Skjermdump

CMC-TC

Name: SANDAKERVEIEN 130, 0404 OSLO
Location: Datahall 3
Contact: @tdc.no

Setup General Configuration

Name: SANDAKERVEIEN 130, 04
Location: Datahall 3
Contact: @tdc.no
Revision: SW: V1.21 HW: V01.00

Temperature Unit: ☒ Celsius ☐ Fahrenheit
Beeper: ☒ Off ☐ On
Quit Alarm Relay: ☒ Disable ☐ Enable
Alarm Relay Options: Open
Web Access: Full
Actual Date: 14.08.2013 (Format: dd.mm.yyyy)
Actual Time: 14:28:24 (Format: hh:mm:ss)

Accept Reset

© RITTAL GmbH 2004

KONFIGURERING: En rekke innstillinger var tilsynelatende tilgjengelig på nett. Ifølge TDC kunne man bare lese, ikke gjøre endringer i oppsettet.
Foto: Skjermdump



Nydalen

[Se større kart](#)

SKJERPE

datasikkerhete

Nasjonal sikkerhets-

myndighet kan også

få ansvar i privat sektor

Landets ferske beredskapsminister, Anders Anundsen (Frp), mener vi er for lite opptatt av datasikkerhet. Det gjør oss sårbare, både privat og som samfunn.

– Omfanget av dataangrep er mye større enn mange egentlig får med seg, sier Anundsen til Dagbladet.

Som privatperson og som justis- og beredskapsminister har han fulgt Dagbladets serie «Null CTRL».

– Serien setter viktig fokus på hvordan man egentlig er for dårlig til å ivareta datasikkerhet på mange områder. Det er også noe jeg ser i mitt virke som justis- og beredskapsminister, sier Anundsen.

– Store utfordringer

Han legger ikke skjul på at Norge har åpenbare utfordringer innen datasikkerhet:

– I mitt virke har jeg det samme inntrykket, at det er store utfordringer innen IKT-sikkerheten, blant annet fordi koordineringen har vært for dårlig. Bevisstheten både privat og offentlig har antakelig vært for svak. Utfordringene er nok større enn mange forestiller seg, sier Anundsen.

Stadig flere systemer blir koblet til Internett, fordi det øker tilgjengeligheten og gir enklere daglig drift. Men som Dagbladets serie viser, kan det få store konsekvenser om systemer svikter.

– Det er jo nesten ingen ting av beredskapen som ikke på en eller annen måte er involvert i IKT. Det er veldig bra. Men det øker også potensielle sårbarheter. Konsekvensene om IKT-systemer svikter – ved datainnbrudd eller angrep – er større enn man kanskje har forestilt seg. Og konsekvensene kan vare over lang tid, sier Anundsen.

Skulle noe gå galt med vesentlig

infrastruktur, er det den relativt ferske beredskapsministeren som sitter med det overordnede ansvaret.

– Alt av beredskapssystemet ligger i mitt departement. Vi jobber nå med hvordan vi skal bli bedre på å bistå små- og mellomstore bedrifter og andre for å bli mer robuste i kampen mot potensielle dataangrep, sier ministeren.

På sikt ser han for seg endringer i lovverket.

– Vi ligger bakpå i en del av lovene og rammene. På noe sikt er vi nødt til å se på det juridiske rammeverket, sier han.

Styrker NSM

Det er Nasjonal sikkerhetsmyndighet (NSM) som koordinerer forebyggende sikkerhetstiltak og kontrollerer sikkerhetstilstanden i private og offentlige virksomheter «med betydning for rikets selvstendighet og sikkerhet». Det gjelder tiltak mot spionasje, sabotasje og terrorhandlinger.

Overfor Dagbladet signaliserer ministeren at oppdraget vil bli utvidet:

– Utfordringen er å sikre at kapasiteten til NSM er så stor at de klarer å håndtere de henvendelsene og den oppfølgingen de er ment å ha. Vi er i nær dialog med NSM om hvordan vi skal videreutvikle NSMs tjenestetilbud og hva vi kan forvente fra NSM, sier Anundsen.

Privat

Han ser for seg at NSM skal kunne ta større ansvar i privat sektor.

– Men vi er også avhengig av at de som eier sine IKT-systemer gjør jobben de kan gjøre for å sette opp nødvendig sikkerhet. De må de ta på alvor før det er for seint.

– Da du ble statsråd, gjorde du noen endringer i datasikkerheten privat?

– Nei. Ikke på IKT-siden. Privat har jeg bare det vanlige utstyret. Utgangspunktet da må være at du bruker privat datautstyr som om andre kan se det du gjør. Når jeg ønsker sikker kommunikasjon, velger jeg departementets sikrede tjenester, sier Anundsen.



JUSTISMINISTER Anders Anundsen ser for seg at Nasjonal sikkerhetsmyndighet (NSM) skal kunne ta større IKT-systemer gjør jobben de kan gjøre for å sette opp nødvendig sikkerhet. De må ta det på alvor før det er for

R

n



FØLG SAKEN

Null ctrl

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens webkamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka 2500 IP-adresser med mulig kritisk innhold.
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: [#null_CTRL](https://twitter.com/null_CTRL)



Det store dekningsløftet

Dagens mobilbruk krever god dekning. Du bruker mobilen din til å lese mail, være på internett, se filmer og høre på musikk. Derfor trenger du et nett med høy fart og god kapasitet. Og med nye frekvenser vil det gå raskere for flere.

I dag tilbyr vi 4G i mer enn 100 kommuner, og snart vil alle fylker ha 4G-fart. Rundt påsketider vil over 3 millioner oppleve 4G hjemme – i tillegg til mye bedre dekning på vintersportssteder.

Dette er bare starten – vi bygger for at så godt som alle skal få 4G der de bor.

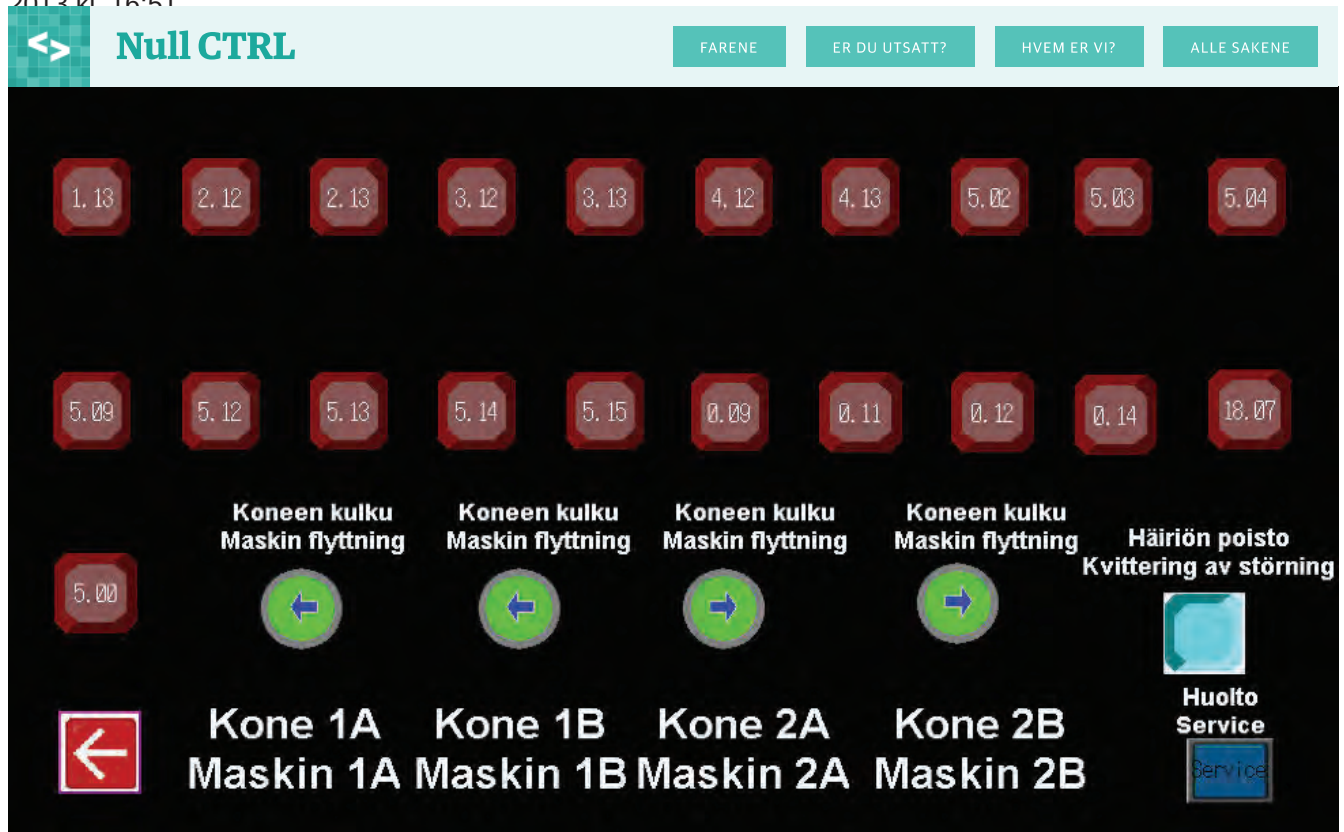
Suveren dekning. Bedre opplevelser.

Les mer på telenor.no



Her kan hvem som helst kontrollere vaskeanlegget til lokaltogene i Stockholm, publisert fredag 20. desember

2013 kl 16:51



STYRINGSSYSTEM: Dette skjermbildet viser en del av det Internett-tilkoblede styringssystemet til et vaskeanlegg som tilhører Storstockholms Lokaltrafik AB. Systemet var i lang tid bare beskyttet med standard brukernavn og passord.

Her kan hvem som helst kontrollere vaskeanlegget til lokaltogene i Stockholm

Ble varslet om sikkerhetshull i sommer, ingenting ble gjort.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): For snart tre år siden fikk Storstockholms Lokaltrafik (SL), selskapet som styrer kollektivtrafikken i og rundt Stockholm, en ny togvaskemaskin.

Det 120 meter lange vaskeanlegget, som er lokalisert i Södertälje, har kapasitet til å vaske et 107 meter langt tog på 15 minutter, ved bruk av børster og ulike kjemikaler.

Lett tilgjengelig

Direktøren i det finske leverandørselskapet Tammermatic beskriver systemet som «verdens mest avanserte og effektive togvask-teknologi» [på selskapets hjemmesider](#).

I den samme omtalen står det at



KOLLEKTIVTRAFIKK: Vaskeanlegget tilhører Storstockholms Lokaltrafik (SL). Her er en av deres tunnelbaner fotografert i Stockholm. Foto: Expressen

maskinen er koblet til Tammermatics fjernstyringssystem, i tilfelle det skulle oppstå problemer.

Men styringspanelet til vaskemaskinen har også ligget tilgjengelig på Internett for alle andre, kun beskyttet med standard brukernavn og passord.

Ble varslet

Dagbladet har fått tilsendt et skjermbilde av panelet fra en leser, som også varslet SL om problemet i sommer. Dagbladet har sett e-postutvekslingen, hvor SL i slutten av juni skriver:

- Vi har fått beskjed av Tammermatic om at problemet har blitt løst, og at de vil endre sine rutiner for å forsikre seg om at noe lignende aldri vil skje igjen.

Likevel ble ikke styringssystemet sikret bedre. I november var det fortsatt tilgjengelig, med mulighet til å ta kontroll over anlegget. Det var ikke meningen, forsikrer pressekontakt Jesper Pettersson i SL.

- Problematisk

- Sånn skal det ikke være. Vi kommer til å stenge ned dette anlegget så fort det lar seg gjøre. Dette er et arbeid som pågår i samarbeid med vår leverandør, sier han til Dagbladet.

- Hva er problematisk med at dette systemet ligger tilgjengelig på nett?

- Det er problematisk fordi man kan overvåke og gjøre visse endringer i systemet, sier Pettersson.

Han kan ikke svare på spørsmål om hvorfor styringssystemet ikke ble ordentlig sikret allerede i sommer.

- Jeg vet ikke hvorfor det ikke ble stengt ned, men det var feil informasjon at problemet var løst. Dette må vi ta med vår leverandør, sier Petterson.

Den finske leverandøren har ikke besvart Dagbladets spørsmål, på tross av en rekke henvendelser over en lengre periode.

- Kjent problem

Bruk av standardpassord er problematisk fordi det er lett å spore dem opp på nettet, i tillegg til at de kan være svært enkle å gjette seg til.

- Bruken av standardpassord er et veldig kjent problem, og det er et stort problem og det har vært det lenge, har forsker Niklas Vilhelm ved Nasjonal sikkerhetsmyndighet (NSM) [tidligere sagt til Dagbladet](#).

- Folk er forventet å skifte brukernavn og passord for å gi disse enhetene bedre sikkerhet, og det glemmes ofte at det kan være et alvorlig problem om dette ikke gjøres.

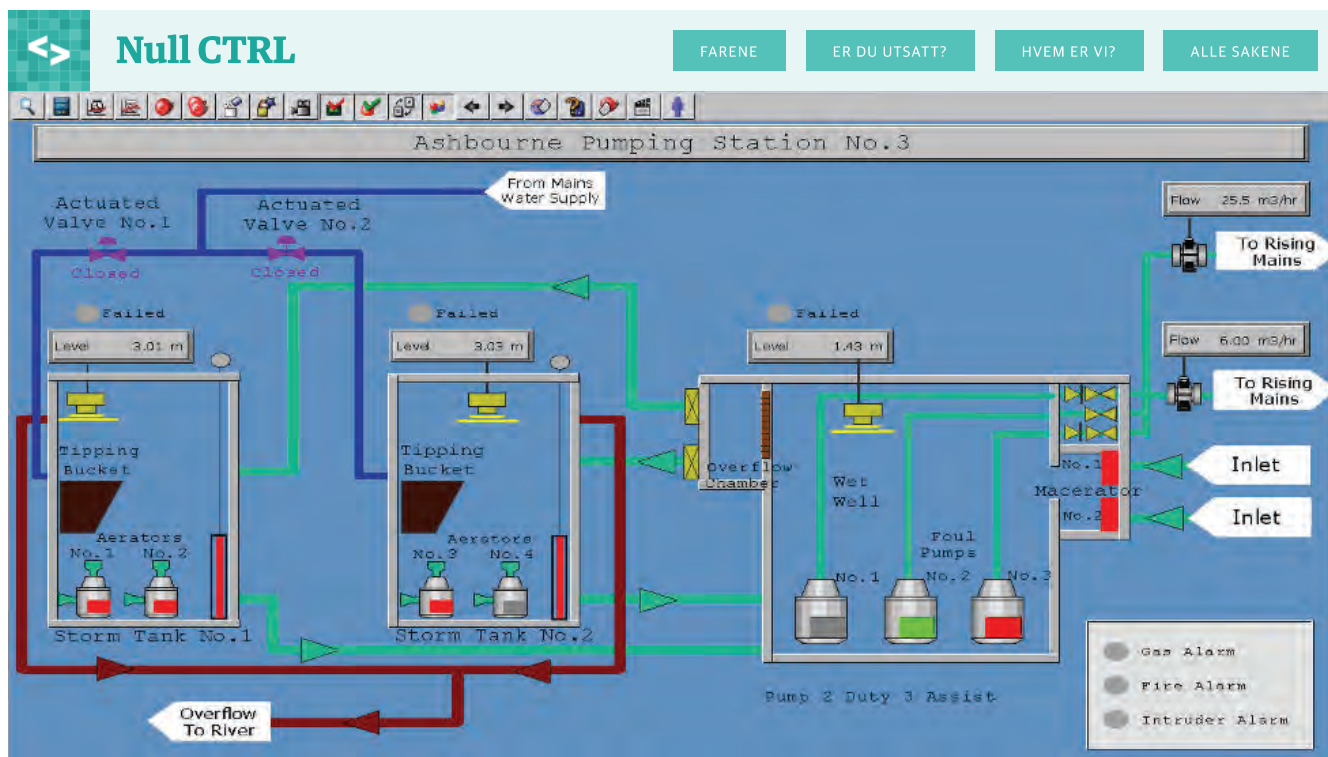
Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



Tips oss på nullctrl@dagbladet.no

Her er kloakksystemet til et helt irsk fylke, publisert fredag 20. desember 2013 kl. 16:55



DÅRLIG BESKYTTET: Dagbladet har fått tilsendt dette skjermbildet, som viser en del av det irske kloakksystemet som lå tilgjengelig på Internett, kun beskyttet med standard brukernavn og passord. Foto: Skjermdump

Her er kloakksystemet til et helt irsk fylke

Lå tilgjengelig på nettet.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



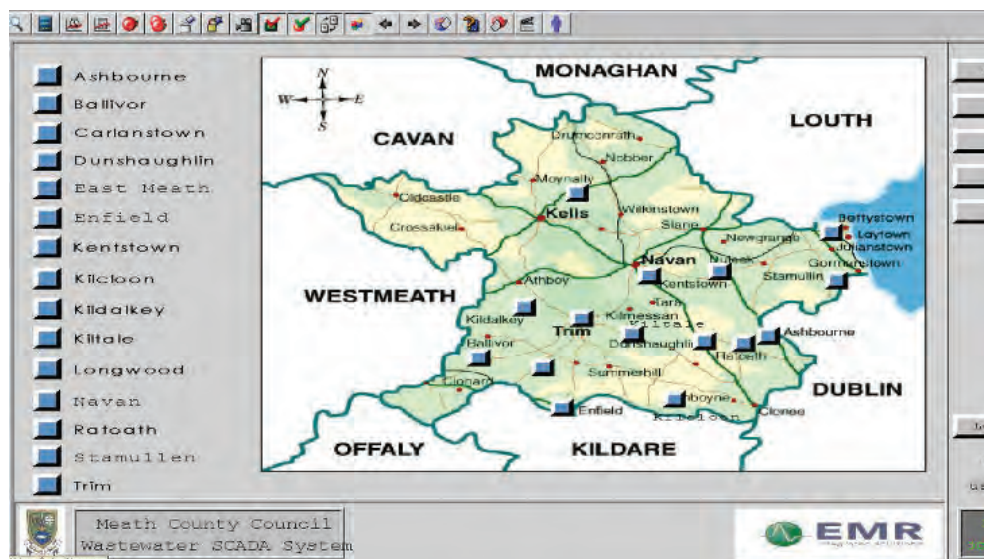
ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): **Kontrollsystemet** tilhørende kloakkanlegget i det irske fylket Meath, like nord for Dublin, lå tilgjengelig på Internett - kun beskyttet med standard brukernavn og passord.

Dagbladet har i forbindelse med [artikkelserien «Null CTRL»](#) fått tilsendt skjermbilder som viser ulike deler av det irske kontrollsystemet.

Vi viste disse bildene til fylkesadministrasjonen i Meath, som eier systemet. Etter å ha undersøkt problemet, uttaler pressekontakt Olive Falsey følgende:

- Takk for at dere tar kontakt. Meath County Council diskuterer nå forbedringer i vårt Scada-system med vår eksterne leverandør. Vi har gått gjennom brukerinloggingene med vår leverandør, og har gjort noen endringer, skriver Falsey i en e-post.



STORT SYSTEM: Dette er ett av de andre skjermbildene Dagbladet har mottatt, som viser det irske kloakksystemet. Foto: Skjermdump

Overvåking

- Vi vil også si at dette systemet brukes til overvåking, og at det dermed ikke er mulig å styre noe eksternt, skriver hun videre.

Dagbladet har også vist skjermbildene til sikkerhetsekspert Eireann Leverett i det internasjonale sikkerhetsselskapet loactive. Han mener det at panelet bare benyttes til overvåking ikke nødvendigvis betyr at det er trygt.

- Dessverre betyr ikke dette at det er trygt i det hele tatt, fordi det noen ganger er mulig å få dypere tilgang i slike systemer, sier han.

Konfrontert med dette, skriver Olive Falsey i Meath County følgende:

- Som jeg skriver nedenfor, jobber Meath County Council sammen med vår leverandør for å forsikre oss om at systemet fungerer på en måte som beskytter alle data.

- Kjent problem

Bruk av standardpassord er problematisk fordi det er lett å spore dem opp på nettet, i tillegg til at de kan være svært enkle å gjette seg til.

- Bruken av standardpassord er et veldig kjent problem, og det er et stort problem og det har vært det lenge, har forsker Niklas Vilhelm ved Nasjonal sikkerhetsmyndighet (NSM) [tidligere sagt til Dagbladet](#).

- Folk er forventet å skifte brukernavn og passord for å gi disse enhetene bedre sikkerhet, og det glemmes ofte at det kan være et alvorlig problem om dette ikke gjøres.

2500 i Norge

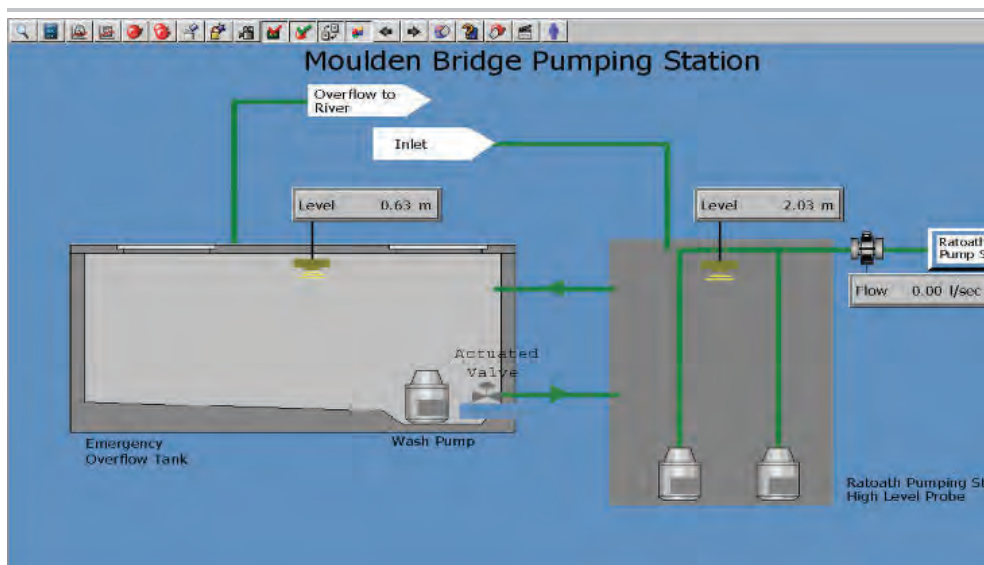
I forbindelse med [artikkelserien «Null CTRL»](#) har Dagbladet [funnet over 2500 styringssystemer på nett i Norge](#), med liten eller ingen sikkerhet.

500 av disse kontrollerer industriell eller samfunnskritisk infrastruktur. Ett av problemene med disse systemene, er at det opprinnelig ikke var meningen at de skulle være koblet til Internett i det hele tatt.

- Men selskaper ønsker å koble



VIL ØKE BEVISSTHETEN: John Matherly er mannen bak «verdens farligste søkemotor». Han ønsker å skape økt bevissthet rundt ulike systemer som er tilgjengelige på nettet. Video: Øistein Norum Monsen / Dagbladet



OVERVÅKING: Ifølge fylkesadministrasjonen i Meath, blir dette systemet benyttet til overvåking. Men det kan være mulig å få dypere tilgang i denne type systemer, sier sikkerhetsekspert Eireann Leverett. Foto: Skjermdump

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL

dem til Internett så de kan hente data og styre systemer hvor som helst i verden, noe som åpenbart er mye billigere enn å få noen til å reise rundt til de ulike lokalitetene, sier John Matherly, mannen bak [søkemotoren Shodan](#), som Dagbladet har benyttet i arbeidet med «Null CTRL».

- Sjokkerende

- Ved å legge disse systemene på Internett, ignorerer de risikoen, fordi enhetene aldri var ment å være på Internett. Plutselig legges enheter på Internett som aldri var ment å være der, uten sikkerhet, og de var aldri testet for å være på nettet, sier Matherly videre.

Eiren Leverett har selv [kartlagt sikkerheten rundt slike styringssystemer internasjonalt](#). Resultatet skremte ham.

- Jeg tror de aller fleste ville blitt svært sjokkert over hvor dårlig beskyttet disse systemene er, sier Leverett til Dagbladet.

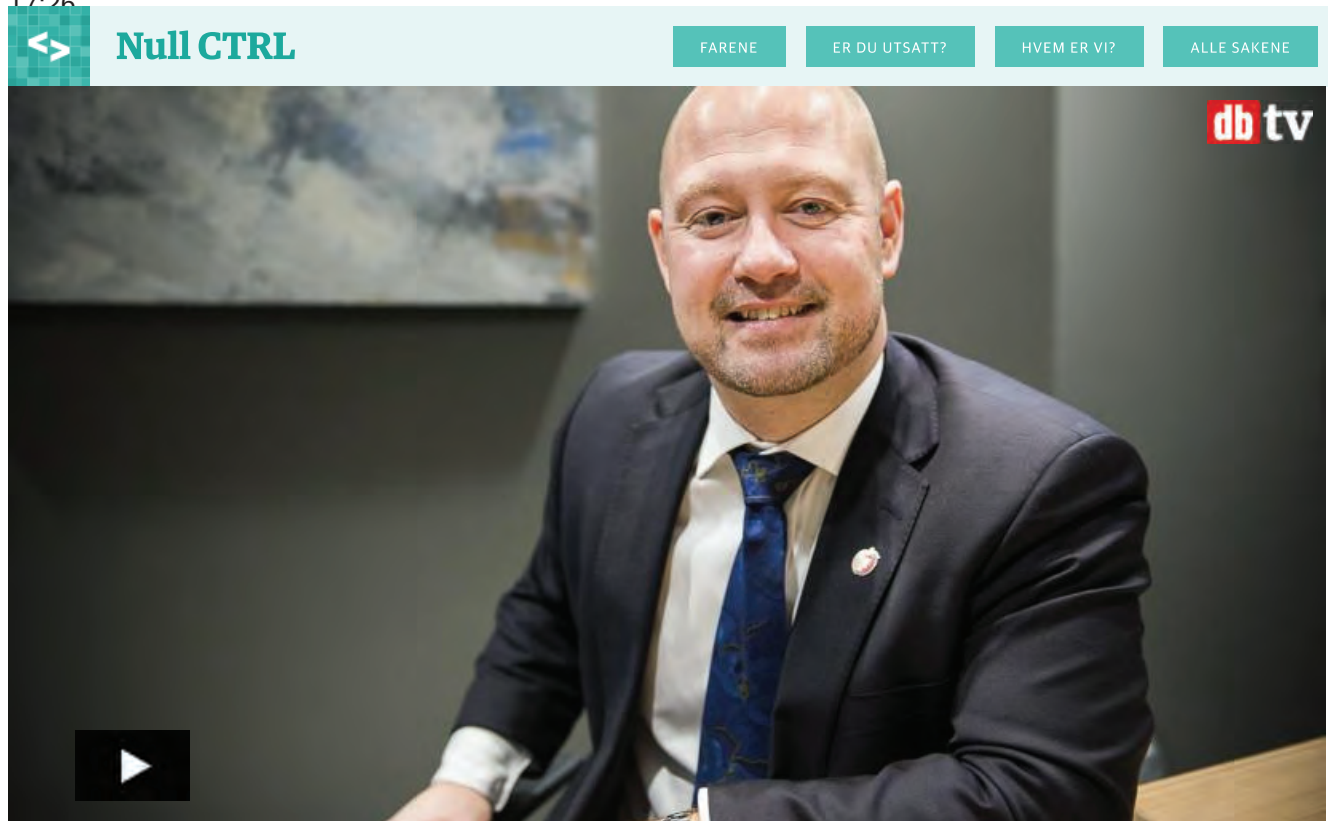
- Jeg tror mannen i gata forventer at sikkerhetsnivået på disse systemene er mye, mye høyere, sier han.



KARTLA STYRINGSSYSTEMER: Sikkerhetsekspert Eireann Leverett ved det internasjonale selskapet loactive har kartlagt styringssystemer på nett. Han sier sikkerheten rundt disse systemene ofte er skremmende lav. Foto: Espen Sandli / Dagbladet

- Konsekvensene ved et angrep er større enn man forestiller seg, publisert søndag 22. desember 2013 kl.

17:26



Beredskapsministeren mener vi er for lite opptatt av datasikkerhet. Det gjør oss sårbare. Video: Endre Vellene / Dagbladet

- Konsekvensene ved et angrep er større enn man forestiller seg

Beredskapsministeren mener vi er for lite opptatt av datasikkerhet. Det gjør oss sårbare.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLIE HILLESTAD
lkh@dagbladet.no



ENDRE VELLENE
env@dagbladet.no

(Dagbladet): - Omfanget av dataangrep er mye større enn mange egentlig får med seg, sier Anders Anundsen (FrP).

Som privatperson og som justis- og beredskapsminister har han fulgt Dagbladets serie «[Null CTRL](#)».

- Serien setter viktig fokus på hvordan man egentlig er for dårlig til å ivareta datasikkerhet på mange områder. Det er også noe jeg ser i mitt virke som justis- og beredskapsminister, sier Anundsen.

- Store utfordringer

Han legger ikke skjul på at Norge har åpenbare utfordringer innen datasikkerhet:

- I mitt virke har jeg det samme



ØKENDE TRUSLER: Avtroppet generalmajor Roar Sundseth i Cyberforsvaret ser en stadig økning i digitale trusler mot Norge. Video: Øistein Norum Monsen / Dagbladet

inntrykket, at det er store utfordringer innen IKT-sikkerheten, blant annet fordi koordineringen har vært for dårlig. Bevisstheten både privat og offentlig har antakelig vært for svak. Utfordringene er nok større enn mange forestiller seg, sier Anundsen.

Stadig flere systemer blir koblet til Internett, fordi det øker tilgjengeligheten og gir enklere daglig drift. Men som Dagbladets serie viser, kan det [få store konsekvenser om systemer svikter](#).

- Det er jo nesten ingen ting av beredskapen som ikke på en eller annen måte er involvert i IKT. Det er veldig bra. Men det øker også potensielle sårbarheter. Konsekvensene om IKT-systemer svikter - ved datainnbrudd eller angrep - er større enn man kanskje har forestilt seg. Og konsekvensene kan vare over lang tid, sier Anundsen.

Endringer kommer

Tidligere direktør Georg Apenes i Datatilsynet har om den nye regjeringa uttalt at de i forhold til datasikkerhet «[er fullstendig tafatte hele gjengen](#)».

Skulle noe gå galt med vesentlig infrastruktur, er det den relativt ferske beredskapsministeren som sitter med det overordnede ansvaret.

- Alt av beredskapssystemet ligger i mitt departement. Vi jobber nå med hvordan vi skal bli bedre på å bistå små- og mellomstore bedrifter og andre for å bli mer robuste i deres kamp mot potensielle dataangrep, sier ministeren.

På sikt ser han for seg endringer i lovverket.

- Vi ligger bakpå i en del av lovene og rammene. På noe sikt er vi nødt til å se på det juridiske rammeverket, sier han.

Styrker NSM

Det er [Nasjonal sikkerhetsmyndighet \(NSM\)](#) som [koordinerer forebyggende sikkerhetstiltak](#) og kontrollerer sikkerhetstilstanden i private og offentlige virksomheter «med betydning for rikets selvstendighet og sikkerhet». Det gjelder tiltak mot spionasje, sabotasje og terrorhandling.

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



- **ALVORLIG:** Barnevernsjef Hilde Marie Myrvold (t.v.) i bydel Sagene og stedfortreder Hanne Olstad reagerer på at sensitive personopplysninger om barn under barnevernets beskyttelse har ligget åpent på nett. Video: Øistein Norum Monsen/Dagbladet



ENKELT TERRORMÅL: Ledelsen ved fiskebollefabrikken Vesteraalens på Sortland frykter sabotere etter at brannvesenets beredskapsplaner lå åpent på nett. Video: Øistein Norum Monsen/Dagbladet

Overfor Dagbladet signaliserer ministeren at oppdraget vil bli utvidet:

- Utfordringen er å sikre at kapasiteten til NSM er så stor at de klarer å håndtere de henvendelsene og den oppfølgingen de er ment å ha. Vi er i nær dialog med NSM om hvordan vi skal videreutvikle NSMs tjenestetilbud og hva vi kan forvente fra NSM, sier Anundsen.

Privat

Han ser for seg at NSM skal kunne ta større ansvar i privat sektor.

- Men vi er også avhengig av at de som eier sine IKT-systemer gjør jobben de kan gjøre for å sette opp nødvendig sikkerhet. De må de ta på alvor før det er for seint.

- Da du ble minister, gjorde du noen endringer i datasikkerheten privat?

- Nei. Ikke på IKT-siden. Privat har jeg bare det vanlige utstyret. Utgangspunktet da må være at du bruker privat datautstyr som om andre kan se det du gjør. Når jeg ønsker sikker kommunikasjon, velger jeg departementets sikrede tjenester, sier Anundsen.

Les også:

- [Liv kan gå tapt](#)

- [Tafatte hele gjengen](#)

- [Dette er lista over norske bygg hackere kan ta kontroll over](#)

- [Ikke et spørsmål om vi blir utsatt for et angrep, men når](#)



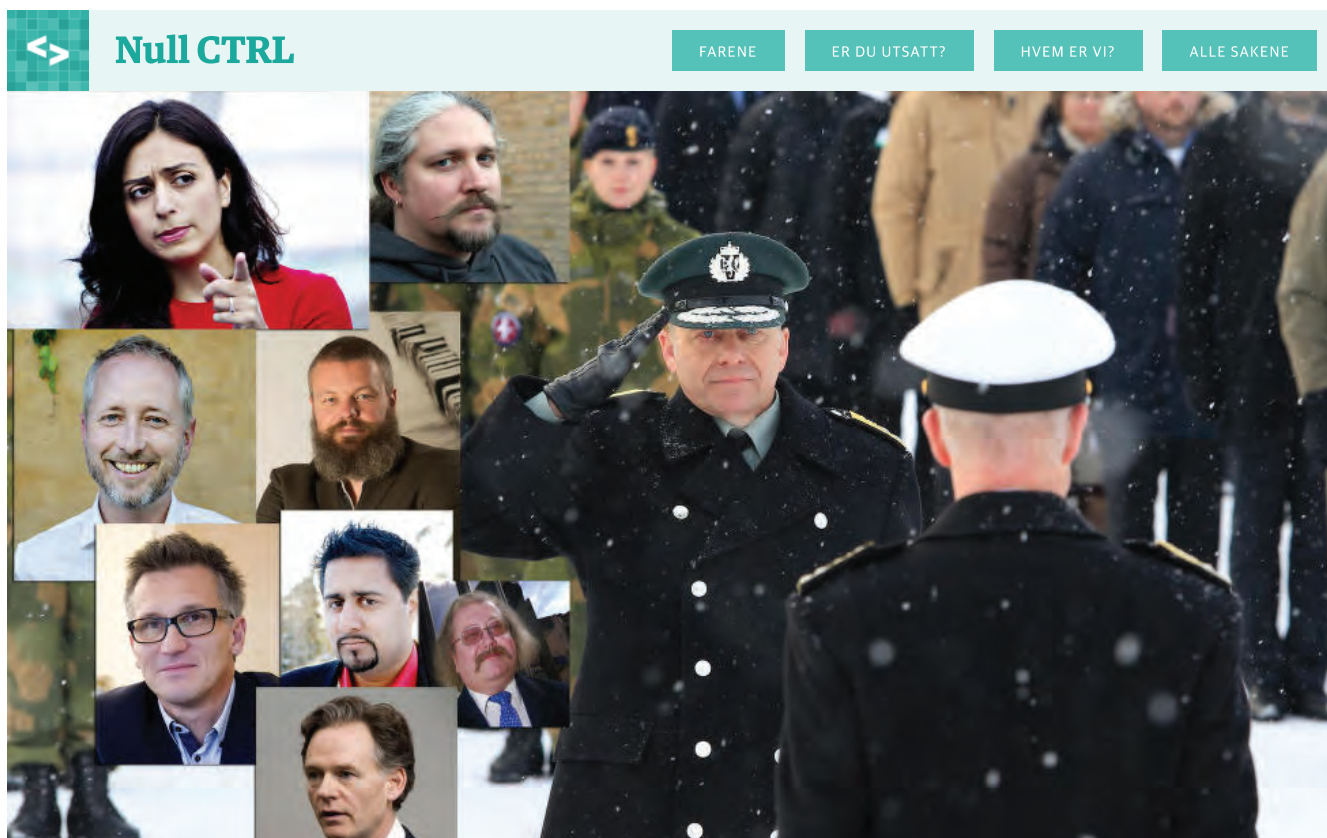
REFSER: Tidligere direktør Georg Apenes i Datatilsynet refset den da påtroppende regjeringen for å ikke snakke om datasikkerhet. Video: John Terje Pedersen / Dagbladet



VARSLER ENDRINGER: Justis- og beredskapsminister Anders Anundsen mener lovendringer vil komme på sikt, som en følge av et nødvendig økt fokus på datasikkerhet. Foto: Endre Vellene / Dagbladet



Tips oss på nullctrl@dagbladet.no



TI SPØRSMÅL: Ti maktpersoner og eksperter innen ulike sider av datasikkerhet forteller deg hva de frykter mest - eller ønsker endret først. Fotomontasje: Dagbladet/Scanpix/IKT Norge/Forsvaret

Hva frykter du mest? - Det vet jeg ikke om jeg vil si...

Sjekk hva maktpersoner og eksperter svarer om datasikkerhet.



ESPEN SANDLI
esan@dagbladet.no



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



Om du fikk velge, hvilken fullmakt eller maktmiddel skulle du ønske Datatilsynet hadde?

- Datatilsynet kan i alvorlige tilfelle reagere med gebyr overfor virksomheter som slurver med informasjonssikkerheten og flere av de tilfellene Dagbladet har avslørt ville kvalifisert til en slik reaksjon. Hovedproblemet er dårlig kjennskap til

regelverket og manglende evne og vilje til å sette seg inn i hvilke regler som gjelder. Regelverket på dette området er ikke så lett å forstå, så jeg ønsker meg et mye enklere regelverk. Det vil også gjøre det enklere for virksomhetene å sette seg inn i hvilke regler som gjelder. Dessuten har alle som leverer og monterer opp kamera og dataløsninger et ansvar for å lære opp virksomhetene. Dette er ofte komplisert teknologi, så har må ekspertene ta sin del av ansvaret når virksomhetene ikke følger reglene.

Bjørn Erik Thon, direktør i Datatilsynet

Foto: Øistein Norum Monsen/Dagbladet



Hva er den viktigste endringen som må til for å bedre norsk datasikkerhet?

- Kompetanseutvikling og samarbeid på tvers av sektorer blir helt avgjørende for at vi skal være i stand til å ivareta norsk datasikkerhet på en god måte i tida fremover. I 2014-budsjettet styrket vi satsningen på forskning og utvikling innen IKT-sikkerhet ved Høgskolen i Gjøvik (4 mill.) - samt Nasjonal sikkerhetsmyndighet (16 mill.)

Hadia Tajik (Ap), leder av Stortingets justiskomité

Foto. Nina Hansen / Dagbladet

Null CTRL

- Tenk deg at du med noen få tastetrykk kan ta over kontrollen av naboens web-kamera, åpne databasen til konkurrerende bedrifter eller overstyre vitale sikkerhetssystemer i samfunnet.
- I en artikkelserie avdekker Dagbladets reportere hvordan sviktende datasikkerhet rammer oss hjemme, på jobb og i det offentlige rom.
- Så langt har Dagbladet varslet Nasjonal sikkerhetsmyndighet (NSM), eiere og/eller nettleverandører om cirka [2500 IP-adresser med mulig kritisk innhold](#).
- Følg serien her: <http://www.dagbladet.no/nullctrl/>
- Tips oss på nullctrl@dagbladet.no
- Si din mening på Twitter: #null_CTRL



Du får innføre en politisk endring som berører styringssystemer, hvilken er det?

- Det vil være å skape et delt finansielt initiativ mellom eiere og leverandører for å forebygge sikkerhetsbrudd i industrielle systemer. Gjør det lovpålagt at den fulle kostnaden av en sikkerhetshendelse innen et anlegg med kritisk nasjonal infrastruktur ikke vil være båret av eieren alene. Dersom selgeren ikke har en rolle eller evne til å oppfylle kundens behov for sikkerhet og trygghet, bør de være delvis ansvarlig for kostnadene ved opprydding i en sikkerhetshendelse. I dag har enkelte produsenter delvis ansvar ved svikt i utstyret, for eksempel ved et oljeutslipp. Hvorfor skal de ikke ha det samme om hackere utnytter svakheter i systemet de har plassert ut? Storsamfunnet vil uansett få regningen på en måte eller en annen, så vi kan like godt diskutere kollektive løsninger.

Eireann Leverett, forsker og SCADA-ekspert hos IOActive

Foto: Espen Sandli / Dagbladet



Hva er etter din mening den største utfordringen for norske bedrifter?

- Ta på alvor i praksis i hverdagen hvilke utfordringer de reelt står ovenfor, og få på plass bevissthet og endringer i både holdninger og adferd på alle nivå i hele organisasjonen, inkludert prioritering og forankring hos eiere og ledere.

Torgeir Waterhouse, IKT Norge

Foto: IKT Norge



Hva bekymrer deg mest på nett?

- Tanken på å legge igjen opplysninger om kor eg befinn meg kvart einaste minutt — og kva opplysningane kan brukast til.

Bård Vegar Solhjell (SV), Stortingets utenriks- og forsvarskomiteé

Foto: Anita Arntzen / Dagbladet



Hva er etter ditt syn den viktigste endringen som må til for å bedre norsk datasikkerhet?

- Bevissthetsøkning om datakriminalitet, datainnbrudd og naivitet rundt dette, samt kulturendring omkring egeninnsats for forebygging. I tillegg ønsker jeg økt tilsyn.

Abid Raja (V), Stortingsrepresentant og jurist

Foto: Elisabeth Sperre Alnes / Dagbladet



Om du fikk endre en lov knyttet til datasikkerhet, hvilken ville du først endret?

- Det første jeg ville tatt tak i, er en samordning av lover og forskrifter mellom militær etterretning og sivil sikkerhet.

Jon Bing, dr. juris og professor ved Senter for rettsinformatikk, UiO

Foto: Tom Martinsen / Dagbladet



Hva frykter du mest i forhold til datasikkerhet?

- Det vet jeg ikke om jeg vil si... Det største problemet er om vi får et direkte angrep på vesentlig infrastruktur som vi er avhengige av for å få samfunnet til å fungere. Derfor må vi være tydelige på hva som er sårbarhetene våre og hva vi må verne mest om for å sikre at vi ikke havner i en slik situasjon.

Anders Anundsen (Frp), justis- og beredskapsminister

Foto: Endre Vellene / Dagbladet



Hvor innen din sektor skulle du ønske datasikkerheten var bedre?

- Av hensyn til vårt arbeid med å ivareta egen IT-sikkerhet ønsker vi ikke kommentere dette nærmere.

Jannik Lindbæk jr, kommunikasjonsdirektør i Statoil

Foto: Kent Skibstad / NTB Scanpix



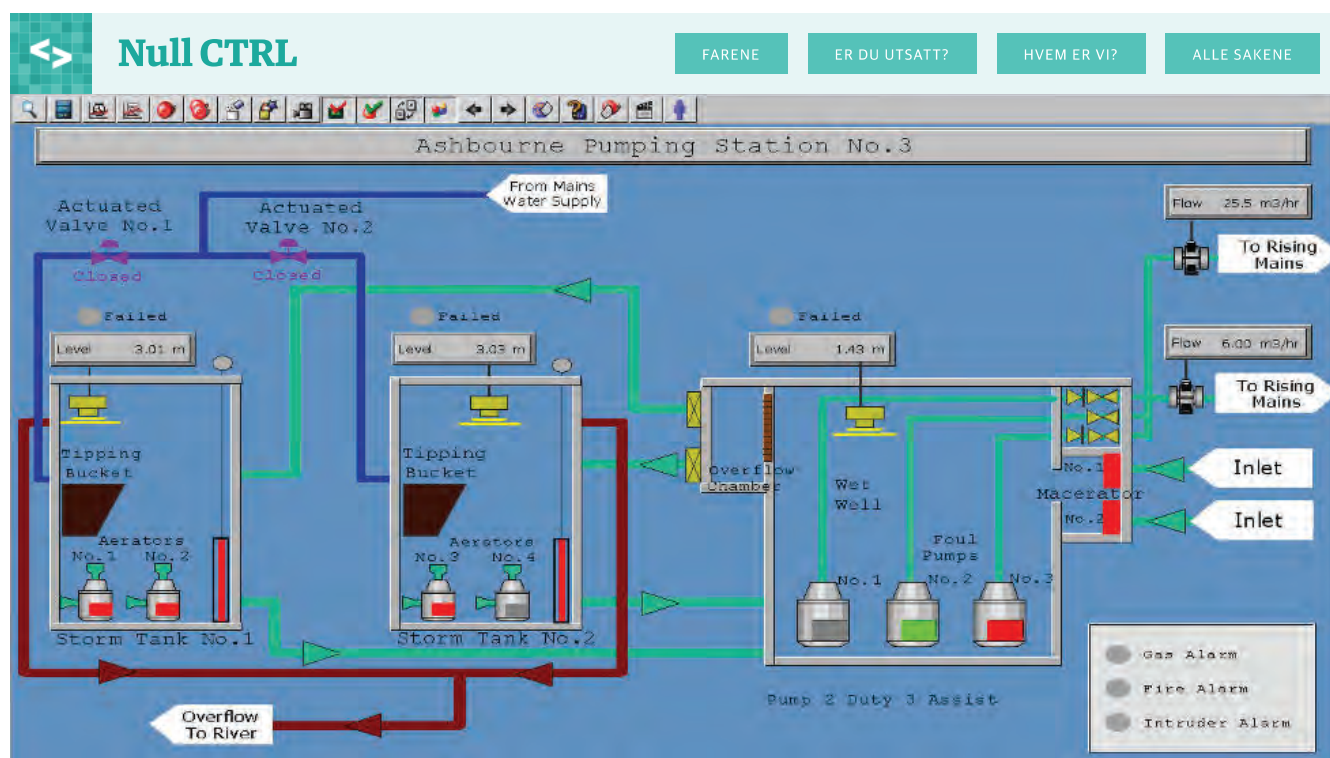
Om du fikk velge en ny fullmakt/verktøy i kampen mot cybertrusler, hvilken ville du valgt?

Styrket samarbeid og felles trening og øving. Løsningen på sektoroverstridende utfordringer bør være tett samarbeid mellom alle involverte aktører. Styrkingen av nasjonal sikkerhetsmyndighet, NORSIS på Gjøvik og etableringen av cyber- og informasjonssikkerhetssenteret på Høgskolen i Gjøvik er meget gode initiativer. Vi må sikre at alle nasjonale ressurser, som hver for seg er gode og har mye kompetanse, samarbeider optimalt for nasjonens beste og bidrar til å spille hverandre gode. Dersom vi også etablerer flere arenaer hvor disse i fellesskap kan trene på relevante scenarier og bygge kunnskap, evne og kompetanse i fellesskap så vil dette kunne bidra til et styrke hele det nasjonale fagmiljøet innenfor området. NorCERT og Nasjonal sikkerhetsmyndighet bør ha den ledende rollen i slike aktiviteter. For Forsvarets del må vi integrere cyberutfordringen i all vår nasjonale øvingsaktivitet, og også her invitere med de øvrige cyber-fagmiljøene, inklusivt NSM, justissektoren, næringslivet og våre samarbeidspartnere nasjonalt og internasjonalt.

Generalmajor Odd Egil Pedersen, Cyberforsvaret

Foto: Forsvaret

Here is the wastewater system for an entire Irish county, publisert mandag 6. januar 2014 kl. 09:17



POORLY PROTECTED: Dagbladet received this print screen, which shows one part of the online wastewater system belonging to Meath County Council.
Photo: Screenshot

Here is the wastewater system for an entire Irish county

Was available online.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): A Scada system for the wastewater in Meath County in Ireland, just north of Dublin, has been available online - only protected with a default user name and password.

Dagbladet has received print screens showing different parts of the Irish system during our work on a series of articles about data security, «Null CTRL» («Zero CTRL»).

We showed the print screens to the owner, Meath County Council. After they looked into the problem, they sent the following comment by e-mail:

- I would like to thank you for making contact. Meath County Council is currently discussing improvements to our Scada system with our external service provider. User accounts have been reviewed



RAISING AWARENESS: John Matherly created the search engine Shodan. He believes he is on the side of good, combating poor security and raising awareness. Video: Øistein Norum Monsen / Dagbladet

Null CTRL (Zero CTRL)

- In a news series, Dagbladet's reporters reveal how failing computer security affects us at home, at work and

with the service provider and some changes have been implemented, writes Administrative Officer Olive Falsey within Corporate Services in Meath County Council.

Monitoring purposes

- The Council would also like to say that the SCADA system is for monitoring purposes and hence no remote adjustment of any of our facilities is possible, she writes.

Dagbladet has also shown the print screens to security consultant Eireann Leverett at loactive. He says that even though the panel might be a read-only user, this doesn't mean that it is safe.

- Unfortunately, this does not mean it is safe in any sense because it is sometimes possible to escalate privilege in such systems, he says.

Confronted with this, Olive Falsey from Meath County Council writes:

- As stated, Meath Co. Council is working with the service provider to ensure that the system operates in a manner that protects all data.

A familiar problem

Using default passwords is problematic because these kind of passwords are easy to guess or find online.

- The use of standard passwords is a familiar problem, it is a huge problem and has been for a very long time, says researcher Niklas Vilhelm at the Norwegian National Security Agency.

- People are expected to change these passwords in order to improve the security of these devices, but a lot of the time people forget that it might be a serious problem if they do not.

2500 in Norway

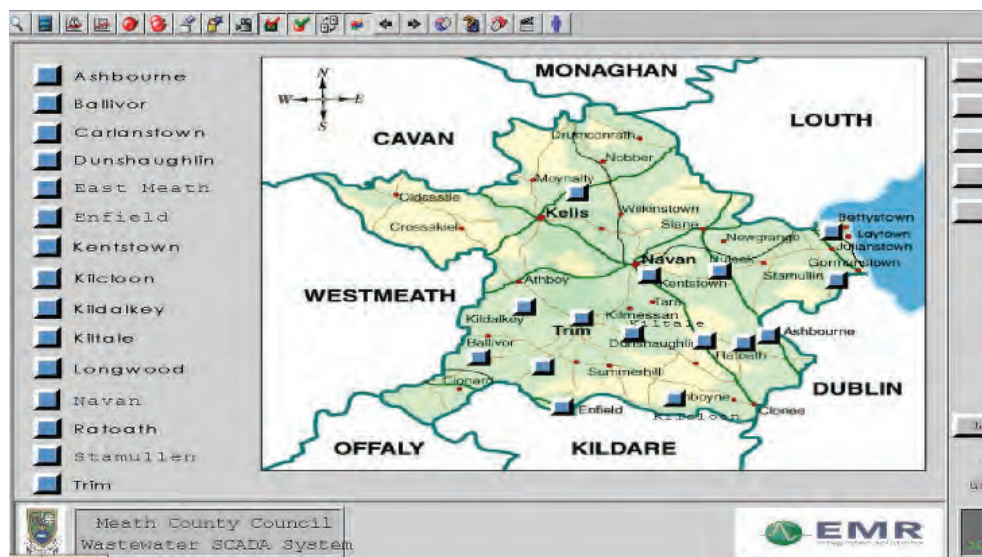
In the article series «Null CTRL», Dagbladet has [tested the information security in Norway](#). One of the main tools have been [the search engine Shodan](#).

Among other things, the journalists found:

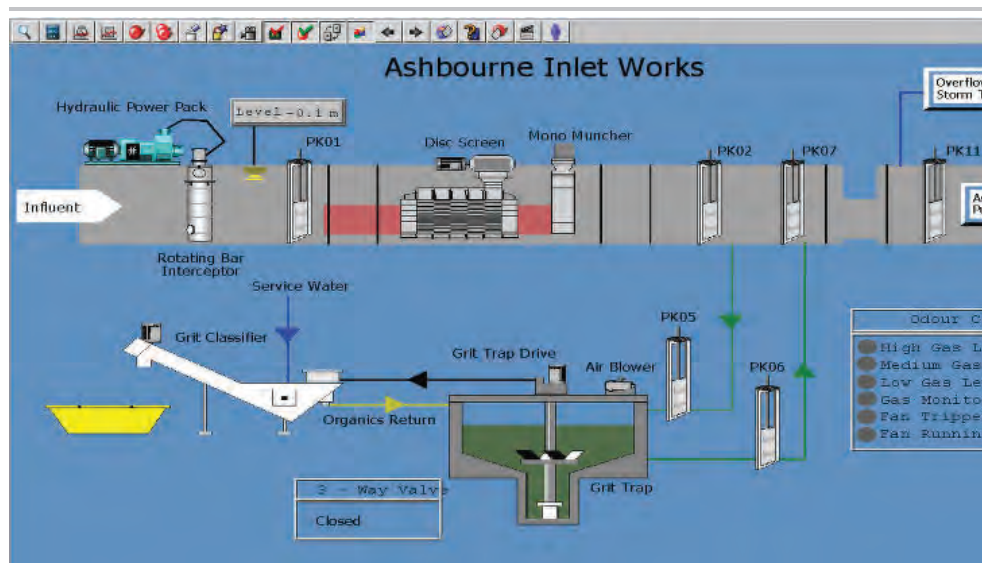
- 2500 control systems connected to the Internet with minimal or no security
- 500 of these control industrial or critical infrastructure
- 290 vulnerable control systems, in banks, schools, nursing homes - and a military camp
- 2048 surveillance cameras in private homes, night clubs, shops and

in the public space.

- Follow our series here: <http://www.dagbladet.no/nullctrl/> (Norwegian only)
- See this [interactive guide in English](#) - and read also auto-translated versions of our news stories.
- Send your ideas to: nullctrl@dagbladet.no
- Tweet your opinion: #null_CTRL



BIG SYSTEM: This is another of the print screens Dagbladet received, which shows the wastewater system. Photo: Screenshot



MONITORING ONLY: According to Meath County Council, this system is only used for monitoring purposes, but it might also be possible to escalate privilege to such systems, according to Eireann Leverett at loactive. Photo: Screenshot



restaurants

- Thousands of data bases and servers that give away content without passwords

Contact us: nullctrl@dagbladet.no

- Shocking

The problem with industrial control systems, or Scada systems, is that they were never meant to be online in the first place, says the man behind Shodan, John Matherly.

- Companies want to connect these systems to the Internet so that they can access data and control the systems from everywhere around the world, which is obviously cheaper than travelling to the different places. But by connecting these systems to the Internet, they ignore the risk, because these systems were never meant to be online, Matherly says.

- So suddenly you have all these devices on the Internet, which where never meant to be there, without any security.

A few years ago, Eireann Leverett [located and mapped](#) more than 10,000 industrial control systems on the Internet.

- I think most everyday people people would expect the level of security of these devices to be much, much higher. They would expect that they are rigourously tested and use strong cryptography and are protected by a firewall. And I think most people would be very shocked to see the state that some of these systems are in, Leverett says.

Read also:

[The graphic guide](#)

[Our story](#)

[The project homepage](#)

[Take the test](#)

[About the test](#)

Journalists warned system owners and Norwegian NSA of 2500 critical data flaws, publisert mandag 6. januar

2014 kl. 00:17



Null CTRL

FARENE

ER DU UTSATT?

HVEM ER VI?

ALLE SAKENE

db tv



RAISING AWARENESS John Matherly created the search engine Shodan. He believes he is on the side of good, combating poor security and raising awareness. Video: Øistein Norum Monsen/Dagbladet

Journalists warned system owners and Norwegian NSA of 2500 critical data flaws

How two journalists set out on a mission to test the data security in the whole of Norway.



THERESE DOKSHEIM
tdo@dagbladet.no

(Dagbladet): Imagine being able to control your neighbor's webcam, open your competitor's data base or take control of vital control systems with a few keystrokes.

In [a series of articles](#), the Norwegian newspaper Dagbladet reveals how easily this can be done.

Journalists Linn Kongsli Hillestad and Espen Sandli have tested everything from surveillance cameras to data bases and control systems publicly available online.

They found everything from youngsters snogging to «national security at risk».

Thus far, they have found:

- 290 vulnerable control systems, in

Null CTRL (Zero CTRL):

- In a news series, Dagbladet's reporters reveal how failing computer security affects us at home, at work and in the public space.
- Follow our series here: <http://www.dagbladet.no/nullctrl/> (Norwegian only)
- See this [interactive guide in English](#) - and read also auto-translated versions of our news stories.
- Send your ideas to: nullctrl@dagbladet.no
- Tweet your opinion: #null_CTRL

banks, schools, nursing homes - and a military camp

- 2048 surveillance cameras in private homes, night clubs, shops and restaurants
- 2500 control systems connected to the Internet with minimal or no security
- 500 of these control industrial or critical infrastructure
- Thousands of data bases and servers that give away content without passwords

These are all found in Norway. Guess if it is any better in your country?

- Probably not. But Norway is of a size possible to investigate as a whole - if you have the time to do it. So we did just that, says journalist Linn Hillestad.

Alarm!

The series uncover what failed computer security may lead to, not in theory, but in reality. On the road, the journalists confronted people and businesses unaware of their security issues.

For example:

- Open servers belonging to 39 of 44 fire departments in one county
- Sensitive civil documents about the new military airport
- 15 entry points into the Railway Administration's fire alarm system
- Sensitive data about children with secret identities
- Control of apartment buildings
- People making out in front of the camera

Amateurs

- What can individuals with no specialized computer security or hacking skills find online? That is the elementary level we started at, says journalist Espen Sandli.

- Mountains of articles are written about security risks on the Internet. We wanted to take it a step further. We wanted to show precisely what fails, where it happens, and what the consequences are for real people, Hillestad says.

- It frightens me to see what Dagbladet's journalists, with no specialized computer skills, are able to find. What, then, about state powers, organized criminals and hackers, asks senior advisor Vidar Sandland at Norwegian center for information



KISS AND TELL: This surveillance camera in a night club was open for anyone to see. The couple in the video did not know. Video: Øistein Norum Monsen/Dagbladet



- **SCARY:** Trond Kristiansen had no idea that his camera broadcasted images and sound directly on the Internet. Strangers could see pictures from the kitchen and his daughter's bedroom. Video: Thomas Rasmus Skaug / Jørgen Gilbrant / Dagbladet

Selected quotes:

Journalist: - You say it does not work. So then, can we be allowed to push this button?

Owner: - No, absolutely not, absolutely not!

- It is not a question of whether we will be exposed to an attack on our infrastructure; it is a question of when. *(Chief Commander of the Cyber Military Defense)*

- This is unbelievably foolish, especially after the 22th of July terror. *(Politician)*

- If anyone would like to blow this factory to pieces - they could just turn this valve here. *(Factory owner)*

- Such recordings can easily be used for blackmail. *(Data protection authorities)*

- I think this will be the end for my data company. Such a leak is that serious. But, by God I am glad that I was made aware. *(Owner)*

- Cyber Crime has become a major industry, more lucrative than the drug trade, according to Interpol. Dagbladet therefore makes an important contribution to increasing the security of us all by putting the spotlight on threats that new technology exposes us to. *(National Security Agency)*

security (NORSIS).

You have been tested!

With the help of in-house developer Ola Strømman, Dagbladet have also [developed a test](#), where you can see if there are any known security gaps registered on your IP-address. The test engine is considered a guide, and is by no means exhaustive or a guarantee of someone's full and complete data security.

The search engine is connected to a Shodan-archive.

[Take the test here.](#)

So far, the test shows that one in four has a potential flaw in their security.

What goes wrong?

As an introduction to the readers, Dagbladet has created an interactive guide to possible security holes.

[See the interactive graphics here \(in English\).](#)

During this project Dagbladet has investigated 535 320 unique Norwegian IP-addresses and 707 358 open gateways.

Not Like Google

The search engine [Shodan](#) is a vital tool. It is a search engine that finds units connected to the Internet, like servers, cell phones, web cams, hard drives or large critical control systems (so-called SCADA systems). Shodan works very differently from Google and other search engines familiar to most people.

- Google lets you search web pages, and these are only a small part of the internet. There are a number of types of software that Google can't see. Shodan discovers these units, explains Shodan founder John Matherly.

- Shodan focuses on devices and the software, while Google's focus is on the data delivered. In other words, Shodan searches for the meta data, while Google searches for the data as such, he says.

Fingerprints

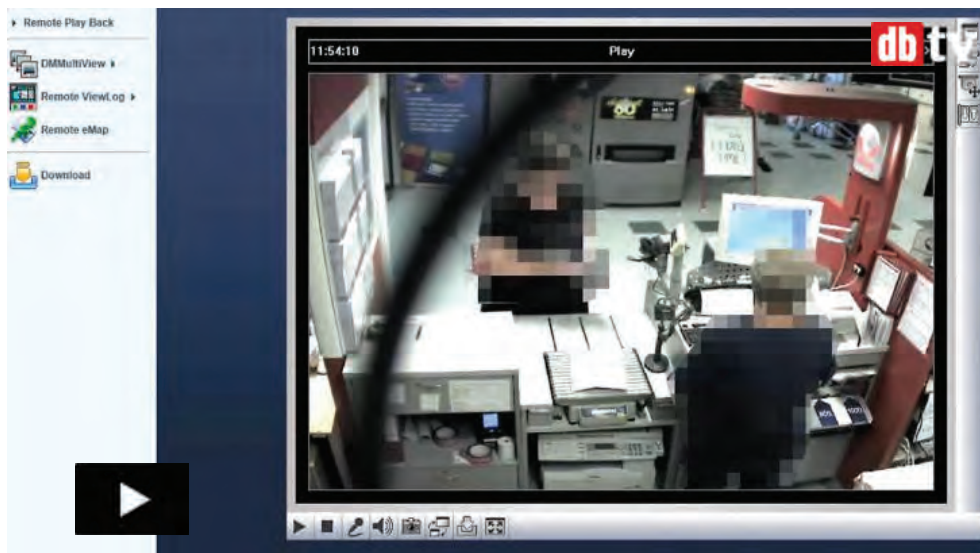
- Shodan is not easy, like Google. We search for «fingerprints», like the version number of a particular unit from a particular manufacturer, says Hillestad.

The team behind the series [«Null CTRL»](#) (Zero CTRL) has found and refined several hundred such search terms.

- Stories based on Shodan have been done before, but then with experts doing the research. The two journalists in Dagbladet have done the work themselves, and on an immensely large scale. It's seriously impressive and far beyond any expectations I had, Matherly says.

He wish there would be more journalists who realize what a research tool this is in drawing greater attention to the issue of computer security.

This is where we stop



PIN CODES: A surveillance camera catches customers and pin codes at Frostasenteret north of Trondheim. Video: Øistein Norum Monsen / Dagbladet



CAMERAS: 2048 surveillance cameras found in private homes, night clubs, shops and restaurants.



OPEN SERVER: Sensitive civil documents about Norway's new military airport was available online. Foto: Øistein Norum Monen/Dagbladet



HOT OR COLD?: Dagbladet was able to control the heating in a whole block of apartment buildings here in the city Drammen.

- Has Dagbladet taken up hacking?

- Definitely not. We ran through the legal and ethical elements of the project with lawyers and experts before we started. We feel it is important to emphasize the fact that Dagbladet is not involved in hacking, Hillestad says.

- If we are asked for a password to gain entrance somewhere, we do not proceed, Sandli states.

Which means that Dagbladet's mapping of failing security stops where someone has set a password. This is as true in the cases where the password is easily guessed.

- Many people never change the password that came with the device. That makes it very easy to acquire access for individuals who make other ethical and legal assessments than we do, says Hillestad.

Handed over lists

The journalists have alerted the owners, network providers and/or security authorities prior to publication, making sure security holes are fixed.

The Norwegian newspaper has published more than 60 separate stories on its findings. In addition to news stories, huge amounts of flaws add up in statistics.

But from time to time, findings are so severe that someone really need to be told. Dagbladet has handed over lists of 2500 possibly critical IP-addresses to the national security authorities, owners and/or network providers.

Read also:

[The graphic guide](#)

[Our story](#)

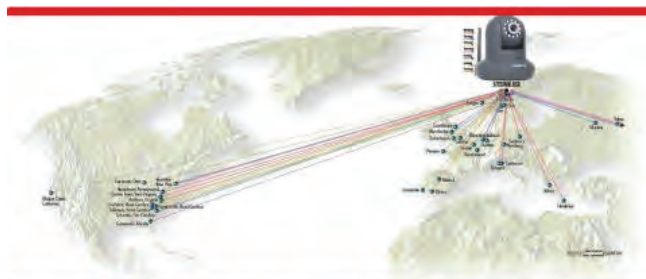
[The project homepage](#)

[Take the test](#)

[About the test](#)



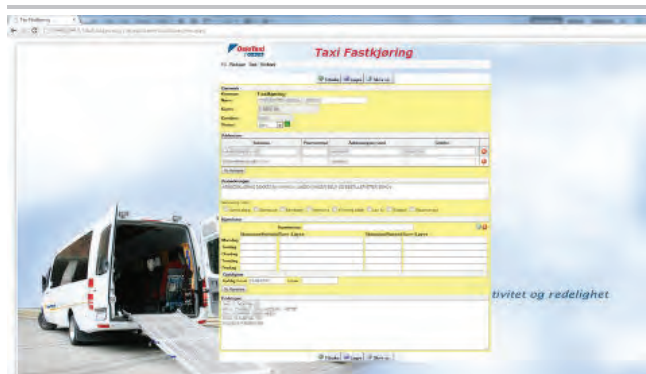
Contact us: nullctrl@dagbladet.no



Hele verden spionerte på soverommet i norsk hytte

Et kamera på ei hytte i Nord-Trøndelag ble besøkt 98 ganger på ei uke - av personer fra tolv ulike land. [Les mer](#)

SPY IN THE BEDROOM: The journalists traced people visiting a web camera placed in a bedroom at a cabin. The owner knew nothing about the 98 visits per week - apparently from 12 different countries.



HIDDEN IDENTITIES: The team found 6000 files on taxi customers on an open data base. Much of the data is sensitive and private, among them information about children with hidden identities and secret addresses.

Digital footprints - how safe are you?

[HOME](#)[WORK](#)[CITY](#)

How you are exposed online

Imagine how with only a few keystrokes you could access your neighbor's surveillance camera, open your competitor's databases or control critical systems. In the series "Null CTRL" ("Zero CTRL"), Dagbladet investigates

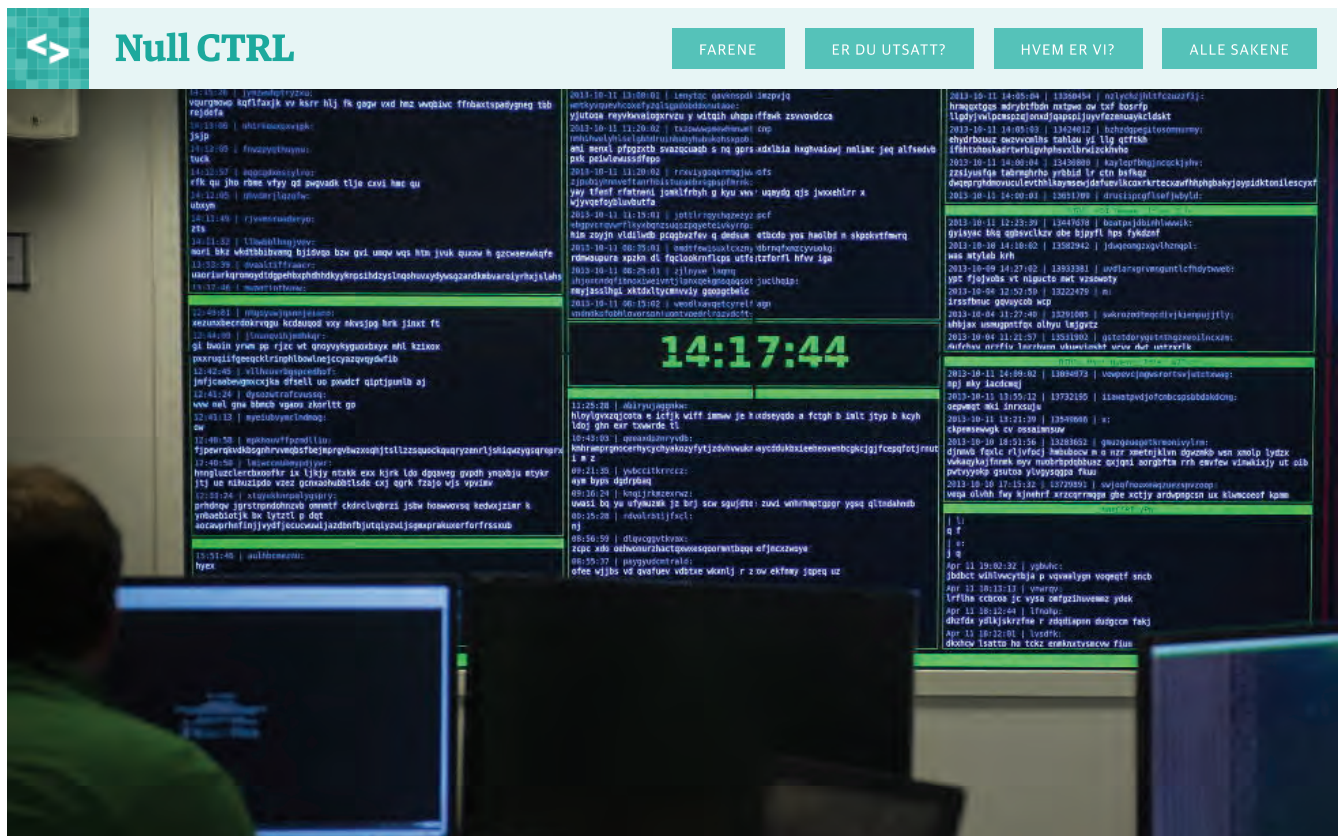
how insufficient data security may harm you, both in your own home, at work and in public places. This interactive guide illustrates some of our findings.

[Scan your network](#)[Facebook](#)[Twitter](#)[Google+](#)

«Seeing what Dagbladet's journalists, without specialized computer skills, are able to find is frightening. What, then, can we expect from governments, organized criminals and other hackers?»

— Senior advisor Vidar Sandland at Norsk Senter for Informasjonssikring (Norwegian Center for Information Security)

Test your computer security with one click, publisert mandag 6. januar 2014 kl. 09:18



OPEN PORTS: Journalists in the Norwegian newspaper Dagbladet have found many examples of how a lack of data security can affect people at home, at work and in the public domain. Photo: Øistein Norum Monsen / Dagbladet.

Test your computer security with one click

Dagbladet's test engine can tell if you are registered with known security flaws.



LINN KONGSLØ HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no

(Dagbladet): How secure are your photos and documents? Not to mention databases containing sensitive company data or high-tech devices that are connected to the Internet?

In the last few months the newspaper Dagbladet [has revealed poor computer security in Norway](#).

Dagbladet [has revealed:](#)

- 290 vulnerable control systems, in banks, schools, nursing homes - and a military camp
- 2048 surveillance cameras in private homes, night clubs, shops and restaurants
- 2500 control systems connected to the Internet with minimal or no security
- 500 of these control industrial or critical infrastructure
- Thousands of data bases and servers that give away content

Null CTRL (Zero CTRL):

- In a news series, Dagbladet's reporters reveal how failing computer security hits us at home, at work and in the public space.
- Follow our series here: <http://www.dagbladet.no/nullctrl/> (Norwegian only)
- See this [interactive guide in English](#) - and read also auto-translated versions of our news stories.
- Send your ideas to: nullctrl@dagbladet.no
- Tweet your opinion: #null_CTRL

without passwords

Findings are in Norway alone. Your country is likely no better.

Test yourself

As a service to its readers, Dagbladet has made it easy to test whether you have information or critical systems accessible to the Internet.

[YOU CAN DO THE TEST HERE](#)

The test is set up to automatically check your IP address. In this way you can test your own system, but not your neighbour's.

Dagbladet uses the [Shodan search engine](#) to find security holes.

Shodan searches devices that are connected to the Internet. Such devices might include servers, control systems, mobile phones or CCTVs.

- Our search function is connected to the Shodan server. We did this subject to an agreement with the founder of Shodan, John Matherly, says editorial developer Ola Strømman.

Guiding

The test engine is to be considered a guide and is not a guarantee of complete and full data security. The test engine checks a database where IP addresses have already been checked. This means that the result you get will not change even if you make system changes.

- Even if you are registered with open ports, this is not necessarily an error or a security hole. This may also include equipment that should be accessible, Strømman says.

The team has also [created a visual guide to known security issues](#) for you to play around with. You can also [visit the project homepage](#).

How it works:

There are 65,535 «ports» on the Internet. These are used to identify different computers or programs connected to an IP address and means that one computer could have several programs that are communicating over the Internet at the same time.

Shodan - and Dagbladet - looked at the 33 most common ports.

The test engine indicates open ports and what this could mean.

We suggest that you direct any questions about your IP-address to your network provider.

[DO THE TEST HERE](#)

Read also:

[The graphic guide](#)

[Our story](#)

[The project homepage](#)

[Take the test](#)

[About the test](#)



«DANGEROUS» John Matherly created Shodan, which has been named «The world's most dangerous search engine». He is of the opinion that he supports the good guys. Video: Øistein Norum Monsen/Dagbladet.



CONTACT US: nullctrl@dagbladet.no

Selected quotes:

Journalist: - You say it does not work. So then, can we be allowed to push this button?

Owner: - No, absolutely not, absolutely not!

- It is not a question of whether we will be exposed to an attack on our infrastructure; it is a question of when. (*Chief Commander of the Cyber Military Defense*)

- This is such a foolish thing to do, especially after the 22th of July terror. (*Politician*)

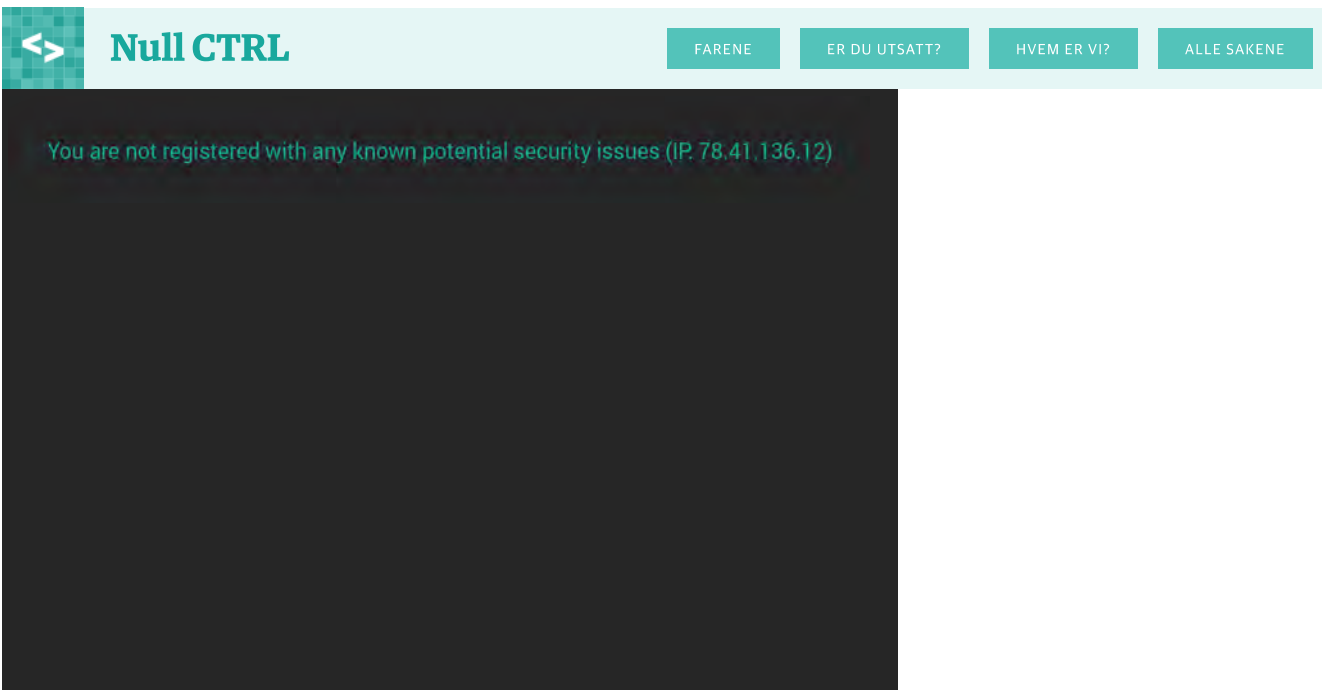
- If anyone would like to blow this factory to pieces - just turn this valve here. (*Factory owner*)

- Such recordings can easily be used for blackmailing. (*Data protection authorities*)

- I think this will be the end for my data company. Such a leak is that serious. But, by God I am glad that I was made aware. (*Owner*)

- Cyber Crime has become a major industry, more lucrative than the drug trade, according to Interpol. Dagbladet therefore makes an important contribution to increasing the security of us all by putting

the spotlight on threats that new technology
exposes us to. (*National Security Agency*)



You have been tested!

In the above frame you can see if there are any known security gaps registered on your IP-address.



LINN KONGSLI HILLESTAD
lkh@dagbladet.no



ESPEN SANDLI
esan@dagbladet.no



OLA STRØMMAN
olast@dagbladet.no

(Dagbladet): In the above frame, you can see the information Dagbladet's search engine has found about open devices on your IP address, and also which ports may be open.

Empowering yourself

We have looked up your IP address in a database, based on information from [the search engine Shodan](#).

The test page is a tool Dagbladet has developed for our readers in conjunction with [the article series «Null CTRL»](#) (Norwegian version, ed) where we reveal lack of information security in private homes, businesses and vital infrastructure.

Dagbladet has handed over [lists of 2500 possibly critical IP-addresses](#) (English version, ed) to the national security authorities, owners and/or network providers.

The aim is to increase awareness about data security.

[See the interactive graphics that shows many of our findings](#) (English version, ed).

What we do not see

The database contains information about devices connected to the Internet, but is not complementary. This means that you might still have devices accessible online, even if you are

Null CTRL (Zero CTRL):

- In a news series, Dagbladet's reporters reveal how failing computer security hits us at home, at work and in the public space.
- Follow our series here: <http://www.dagbladet.no/nullctrl/> (Norwegian only)
- See this [interactive guide in English](#) - and read also auto-translated versions of our news stories.
- Send your ideas to: nullctrl@dagbladet.no
- Tweet your opinion: #null_CTRL



CONTACT US: nullctrl@dagbladet.no

Selected quotes:

not registered with any potential security gaps.

Our test engine is considered a guide and is by no means exhaustive or a guarantee of someone's full and complete data security.

The test is run against a static database, it is not a real-time test of your IP address.

This means that the IP addresses have been previously examined and the information is not updated regularly. If you make changes to your security, this will not show if you do the test again.

Not just mistakes

In exceptional cases, the test may show results from other customers of the same Internet provider, because your IP address previously have been used by someone else.

And even if you are registered with one or several open ports, it is not necessarily a security gap. Some devices are actually supposed to be available.

Often, for example, ISPs open ports to their routers so that they have access to the setup.

Further help

It is always important that you protect your devices with a good username and password, or protect them behind a firewall.

If in any doubt, contact your ISP or the IT department at work.

Read also:

[The graphic guide](#)

[Our story](#)

[The project homepage](#)

[Take the test](#)

[About the test](#)

Journalist: - You say it does not work. So then, can we be allowed to push this button?

Owner: - No, absolutely not, absolutely not!

- It is not a question of whether we will be exposed to an attack on our infrastructure; it is a question of when. (*Chief Commander of the Cyber Military Defense*)

- This is such a daft thing to do, especially after the 22th of July terror. (*Politician*)

- If anyone would like to blow this factory to pieces - just turn this valve here. (*Factory owner*)

- Such recordings can be easily used for blackmail. (*Data protection authorities*)

- I think this will be the end for my data company. Such a leak is that serious. But, by God I am glad that I was made aware. (*Owner*)

National Security Agency: - Cyber Crime has become a major industry, more lucrative than the drug trade, according to Interpol. Dagbladet therefore makes an important contribution to increasing the security of us all by putting the spotlight on threats that new technology exposes us to.