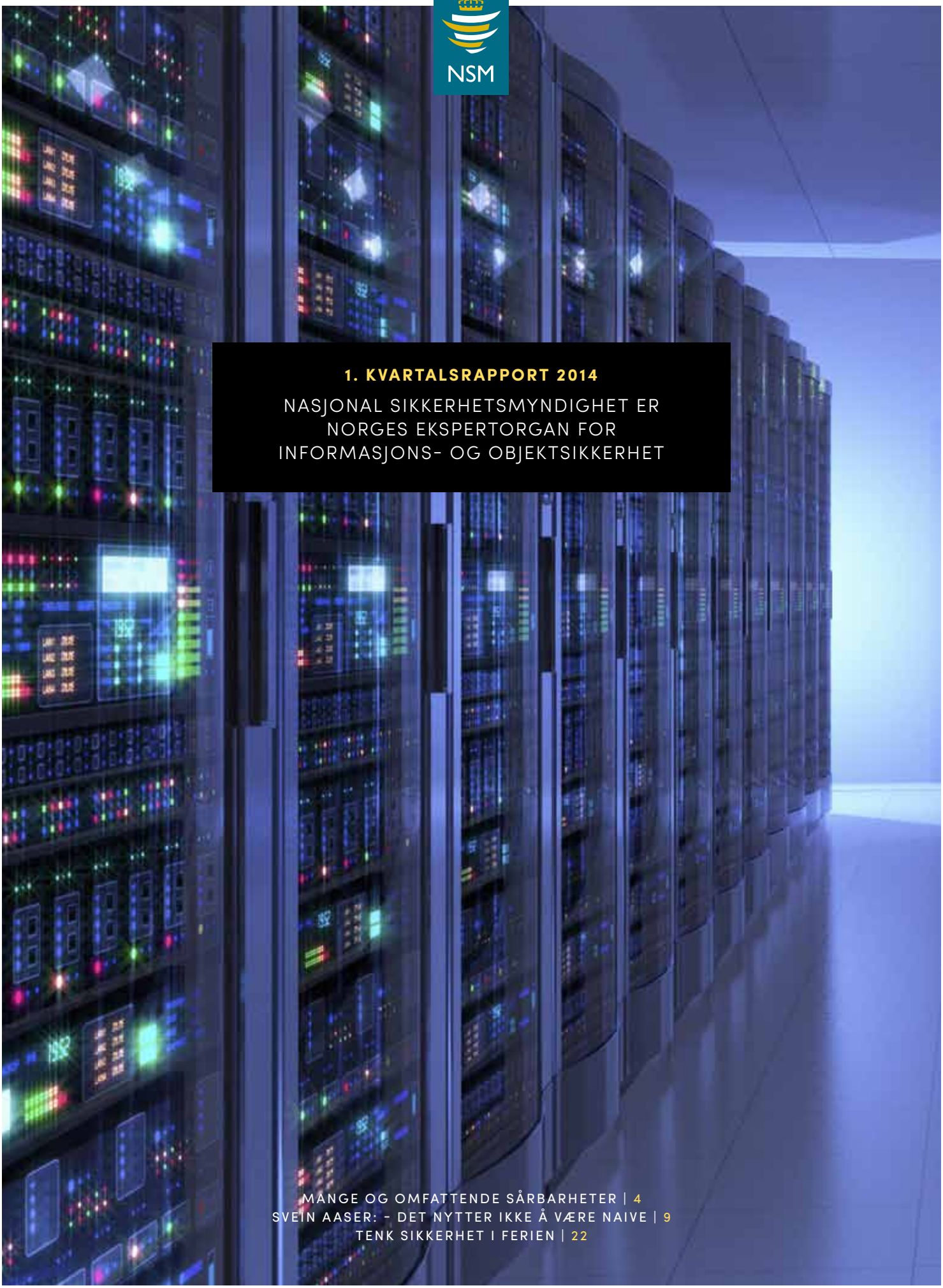


NSM

1. KVARTALSRAPPORT 2014

NASJONAL SIKKERHETSMYNDIGHET ER NORGES EKSPERTORGAN FOR INFORMASJONS- OG OBJEKTSIKKERHET

EN SPENNENDE START PÅ 2014

FØRSTE KVARTAL har vært en hektisk start på året for oss i Nasjonal sikkerhetsmyndighet. Vi lever i et samfunn og jobber i en bransje som er i stadig endring, og dette gir oss både utfordringer og muligheter. Disse mulighetene er selvfølgelig noe de som har uærlige hensikter oppdager, og dette kappløpet prøver vi hele tiden å vinne. Denne oppgaven er svært spennende og krever stor innsats fra våre ansatte.

I løpet av første kvartal ser vi at antallet saker vi håndterer i Operativ avdeling fortsatt øker. Denne våren fikk spesielt sårbarheten «Heartbleed» mye oppmerksomhet. Om oppmerksomheten var fortjent eller ikke skal være usagt, men mediedekningen viser at det fortsatt er et behov for å opplyse det norske folk om farene på Internett. Samtidig viser den at angriperne stadig finner eller får tilgang til nye metoder for å bryte seg inn eller lure brukerne.

Her i NSM gjør vi alt vi kan for å møte nye utfordringer, og å drive folkeopplysning er viktig for å styrke sikkerheten. I mars arrangerte vi vår tradisjonelle sikkerhetskonferanse, med rekordmange påmeldte og et svært spennende program. I tillegg inviterte vi i år 100 utvalgte toppledere innenfor privat og offentlig sektor, for å minne dem på at sikkerhet er et lederansvar, og at samarbeid på tvers er nødvendig. Tilbakemeldingene fra topplederseminaret har vært overveldende, og dette er noe vi satser på å fortsette med de neste årene.

At verden utvikler seg er noe vi også tar konsekvensen av. De siste årene har flere tusen nordmenn skaffet seg fjernstyrte helikoptre med innebygget kamera. Strengt tatt har de brutt loven hvis de har tatt av uten lisens fra NSM for å fotografere, men fra 2. april endret vi praktiseringen av regelverket, noe som gjør det betydelig enklere for privatpersoner å benytte denne typen teknologi. NSM er satt til å forvalte sikkerheten i Norge, og dette er et viktig signal. Sikkerhet skal ikke være til unødig hinder for befolkningen, og det er viktig at vi tar teknologien inn over oss og ser hva lovens formål er i enhver situasjon. ‹

Med vennlig hilsen

Kjetil Nilsen
Direktør
Nasjonal sikkerhetsmyndighet

1. KVARTAL 2014

SEKSJONER

Design:
REDINK

Trykk og distribusjon:
RK GRAFISK

RISIKOBILDET:
MANGE OG OMFATTENDE SÅRBARHETER

Risikonivået i Norge preges fortsatt av mange og omfattende sårbarheter. Endringer i verdenssituasjonen kan samtidig medføre at interessen for norske verdier forandrer seg. Dette betyr både at verdensbildet kan få betydning for samfunnets interesser, og at det fremdeles er behov for risikoreduserende tiltak.

SITUASJONSBILDE

Første kvartal i 2014 ble preget av konflikter i vår verdensdel. Denne konflikten pågår fortsatt. Norge har en rekke roller og interesser som kan påvirkes av endringer i verdenssituasjonen.
Andre stater har interesse for norske verdier. Politiets sikkerhetstjeneste uttalte i media i mai at Ukraina-krisen har medført at russiske etterretningsoffiserer i Norge har «spisset aktiviteten» mot norske virksomheter og beslutningstakere.

På grunn av konflikten har norske verdier og sårbarheter fått mye oppmerksomhet i løpet av årets første måneder. Den utenrikspolitiske situasjonen har gjort det naturlig for både privat og offentlig sektor å være mer bevisst sikkerhetsaspektene ved sin virksomhet. En ustabil politisk situasjon har blant annet ledet enkelte norske bedrifter til å hente hjem medarbeidere fra Ukraina.

Spesielt vekket det internasjonal oppmerksomhet da flere av NATOs hjemmesider ble utsatt for et koordinert tjenestenektangrep, hvorpå en ukrainsk gruppering påtok seg ansvaret. Vi er ikke kjent med at norske nettsteder ble skadelidende som følge av angrepet.

Det er naturlig at en vesentlig endring i den storpolitiske situasjonen påvirker sikkerhetsbevisstheten i befolkningen. Imidlertid er det menneskene og teknologien, og ikke storpolitikken, som først og fremst påvirker våre sårbarheter. Også verdiene våre vil for det meste være konstante, uavhengig av om trusselen mot dem skulle øke.

I 2013 opplevde vi en økning i trusselen mot norske datasystemer. Så langt i 2014 har vi ikke sett tegn på at utviklingen skal snu. Informasjon i og om norske IT-systemer er attraktiv både for statlige etterretningsaktører, private hackere og andre kriminelle.

> «
> Små bestanddeler av et for oss ukjent helhetsbilde kan hjelpe en trusselaktør.

SÅRBARHETER OG VERDIER

Det er fortsatt mye ugjort på sikkerhetssiden hos norske virksomheter. Mange mangler dedikerte miljøer med kompetanse til å forebygge, oppdage og håndtere forsøk på sabotasje og informasjonstyveri. Dette gjør mange virksomheter sårbare.

Erfaringene fra forrige gang Ukraina og Russland var uenige om gassleveranser skaper usikkerhet rundt gassforsyningen til europeiske land. Norge er en annen stor leverandør av gass til Europa, og gass- og øvrig energisektor har både omfattende anlegg og styrings- og prosesskontrollsystemer som er viktige å beskytte. En uønsket hendelse i forbindelse med noen av disse systemene kan ha store konsekvenser, også langt utover vår evne til å levere energi.

Konflikten mellom Russland og Ukraina har vekket ny interesse for innsidetrusselen i norske virksomheter, både i inn- og utland. Ansatte ved norske virksomheter ute kan bli utsatt for ulike typer press og fristelser som motiverer dem til å handle i strid med norske interesser. Det samme gjelder utlendinger som jobber i Norge. Dersom de har tilgang på informasjon som har fått ny verdi for en trusselaktør, kan mennesker som tidligere ikke har vært gjenstand for innhenting bli kontaktet nå.

Innsidetrusselen gjelder så vel for nordmenn som for utlendinger, og den det gjelder kan handle i tråd med en annen lojalitet enn lojaliteten til Norge, la seg motivere av gjenytelser eller bli utsatt for press mot seg eller sine nære.

Det er svært mange opplysninger som kan være av interesse for en trusselaktør, og verdien av informasjonen er ikke nødvendigvis åpenbar for den som besitter den. Små bestanddeler av et for oss ukjent helhetsbilde kan hjelpe en trusselaktør til for eksempel å skaffe seg fysisk adgang til fasiliteter, logisk adgang til IT-systemer eller en forståelse av hva norske beslutningstakere tenker.

> «
> I 2013 opplevde vi en økning i trusselen mot norske datasystemer.

TILTAK

Det er sjelden at en gjennomgang av sikkerhetssystemer, -rutiner og planverk ikke fører til at en finner svakheter. Det forteller NSM at slike gjennomganger er helt nødvendige.

I vår kontakt med virksomheter den siste tiden er det noen råd som ofte har gått igjen. Når det gjelder IT-systemer, er eksponering av kritisk infrastruktur et tilbakevendende poeng. Egne sikkerhetssoner i systemene og strenge regelsett i brannmurer kan redusere eksponeringen. Det kan også være nyttig å spørre seg om det i det hele tatt er nødvendig at de mest sensitive delene til enhver tid skal være koblet opp mot resten av infrastrukturen.

I perioder hvor man ser behov for ekstra årvåkenhet, er det viktig å følge opp med systematisk logging, og rask varsling til NSM når man avdekker mistenkelig aktivitet.

Både på www.nsm.stat.no og difi.no finnes veiledere som gjør det lettere å sørge for en god sikkerhetsstandard i virksomhetene.

NØKKELTALL FRA NSM NorCERT: STABILT HØYT NIVÅ

Ved utgangen av første kvartal 2014 ser vi at antall saker som har vært håndtert av operasjonssenteret med varsling, dialog, analyse og bistand holder seg på et stabilt høyt nivå. I første kvartal 2014 har tilsammen 1021 hendelser krevd manuell operativ håndtering. I hele 2013 var dette tallet 3901.

DET TOTALE ANTALLET saker i første kvartal 2014, som også inkluderer rutinemessig og delvis automatisert saksbehandling var 2577. Dette er en liten økning siden forrige kvartal, hvor totalt antall saker var 2429. Som illustrert i figuren har det vært en stadig økning i saksmengden siden NSM NorCERT begynte å føre statistikk på dette i 2007. Dette kan være på grunn av økende sikkerhetsfokus i samfunnet, som igjen fører til økt rapportering om hendelser fra norske virksomheter og fra våre samarbeidspartnere i sikkerhetsmiljøet nasjonalt og internasjonalt, men også at det er en reell økning i antall hendelser.

Antallet alvorlige hendelser knyttet til spionasjeoperasjoner fortsetter å øke. I første kvartal har NSM NorCERT håndtert til sammen 15 alvorlige saker. I hele fjor håndterte vi 51 alvorlige saker, hvorav hele 20 av disse ble registrert i fjerde kvartal. Det har altså vært en liten nedgang i antall alvorlige saker siden forrige kvartal, men trenden er økende.

– Der Norge angripes, brukes det avanserte angrepsmåter som ikke havner på topplisten over de mest vanlige infeksjonene. Det rene, målrettede angrepet hvor man ønsker å stjele informasjon gjøres av tunge aktører med mye kompetanse, sier Hans Christian Pretorius, som leder operativ avdeling i NSM.

Bak disse tallene skjuler det seg blant annet hendelser med gjentatte kampanjer med målrettede angrep der utvalgte personer har mottatt eposter som inneholder ondsinnede vedlegg eller linker til nettsteder som sprer avansert skadevare.

NSM har også brukt store ressurser på å koordinere og bistå i håndteringen av en spesifikk hendelse der en privat virksomhet som leverer tjenester til en virksomhet innen kritisk nasjonal infrastruktur har blitt kompromittert, mest sannsynlig i en spionasjeoperasjon hvor trusselaktør har forsøkt å komme inn i den større virksomhetens systemer via underleverandøren.

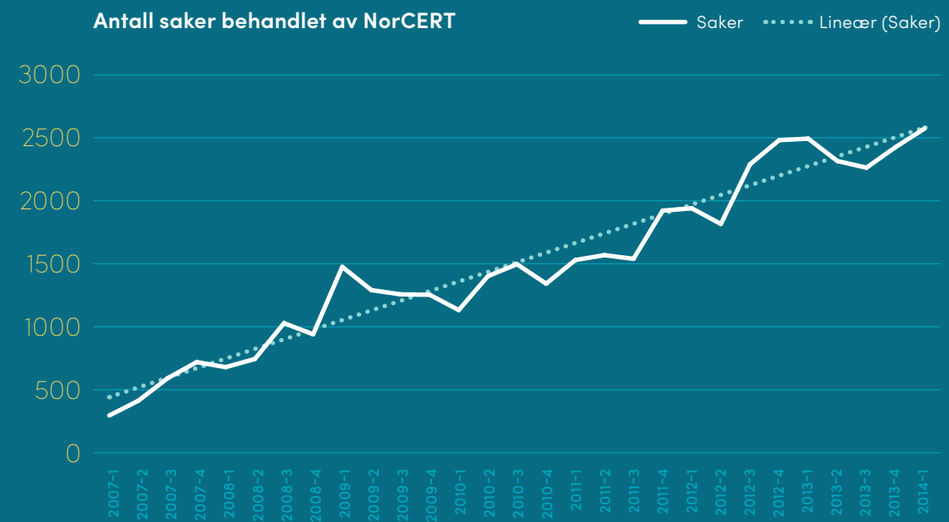
Pretorius sier at det i mange tilfeller er enkle virkemidler som kan hindre eller stoppe de målrettede angrepene.

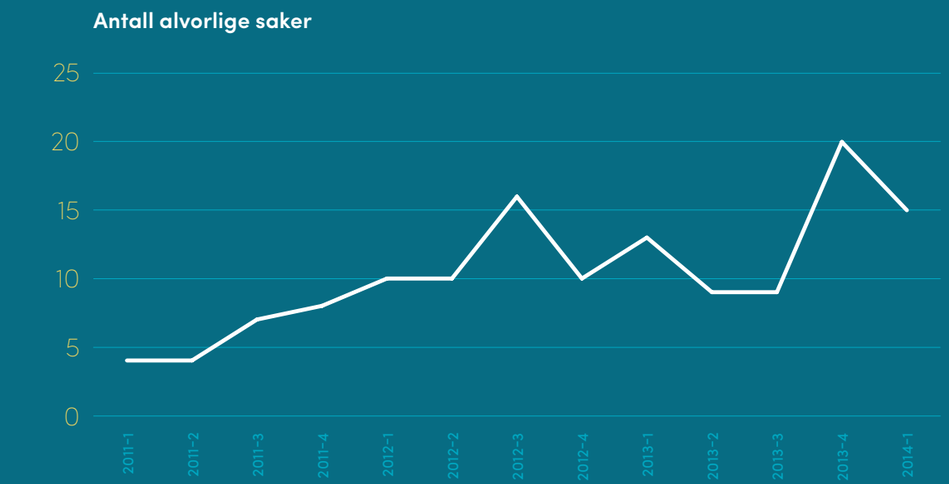
– Vi ser at man stort sett bruker kjente sårbarheter for å bryte seg inn i datasystemer. Hadde norske bedrifter gjort hjemmeleksa, og oppdatert dataprogrammer når oppdateringene kommer, hadde vi tatt ned tallene betraktelig, sier Pretorius. <

> «
> Det rene, målrettede angrepet hvor man ønsker å stjele informasjon gjøres av tunge aktører med mye kompetanse.
>
> HANS CHRISTIAN PRETORIUS

2014 Q1 (1. januar – 31. mars 2014)

- Antall saker: **2577** (2429 i Q4 2013)
- Antall saker håndtert manuelt: **1021**
- Antall alvorlige saker: **15**





TOPPLEDERE SITTER PÅ NØKKELEN TIL GOD SIKKERHET

17. mars samlet Nasjonal sikkerhetsmyndighet 100 toppledere i Norges viktigste virksomheter til topplederseminar om sikkerhet på Litteraturhuset i Oslo. Over flere år har Nasjonal sikkerhetsmyndighet observert at sikkerheten er best i de virksomhetene hvor toppledelsen engasjerer seg, er opptatt av sikkerhet, og stiller de riktige spørsmålene.

Toppledere sitter på nøkkelen til god sikkerhet. Det bekrefter også undersøkelsen Lloyds Risk Index 2013, som blir gjort blant mer enn 500 av verdens toneangivende bedriftsledere om hva slags risiko de er opptatt av. IKT-risiko har beveget seg fra å være på 12. plass i 2011 til å innta 3. plass i 2013. Dette bør oppta alle toppledere i samfunnet. På disse sidene kan du lese hva Svein Aaser fra Telenor, Jannicke Hilland fra Statoil og Kristin Skogen Lund i NHO bidro med på seminaret.

Svein Aaser: – Det nytter ikke å være naive

– Det nytter ikke å være naive. Av og til tror jeg vi skal være litt paranoide. Det har fungert så langt i Telenor, sa styreleder Svein Aaser på NSMs Topplederseminar 17. mars. Han mener toppledere må sette seg inn i og forstå cyberdomenet.

«Vi må forstå hva slags informasjon som kan være interessant for andre, og hvordan vi skal beskytte oss.»
SVEIN AASER

AASER HAR bred erfaring fra toppen i norsk næringsliv, både som president i NHO, og som konsernsjef i selskaper som Nycomed, Storebrand, og DNB. Fra 2012 har han vært styreleder i Telenor, et selskap som har håndtert en rekke sikkerhets- og beredskapshendelser.

Industrispionasje. Sikkerhetstiltakene er basert på en best mulig risikoforståelse. Allikevel skjer det uforutsette. Ekstremværet Dagmar i 2011 førte til at strøm og telefoni falt ut i flere kommuner på Vestlandet, og viste hvor sårbart samfunnet er. I fjor ble Telenor utsatt for omfattende industrispionasje. Datamaskinene til flere sjefer ble tømt for data. Industrispionasjen ble oppdaget da Telenors sikkerhetssenter registrerte uvanlig internett-trafikk fra datamaskinene til flere Telenor-sjefer.

– Hendelsen viste hvor sårbare vi er, selv om vi i utgangspunktet er godt sikret, sa Aaser.

Større sårbarheter. Det å bli utsatt for trusler er svært ubehagelig. Man blir på vakt, og mer kynisk. Det er det all grunn til å være fremover, tror Svein Aaser, spesielt når det gjelder cyberdomenet, altså alt som har med IKT og Internett å gjøre. Cyberdomenet gjør sårbarhetsflatene mye større.

– Dette er et domene toppledere må forstå. Vi må forstå hva slags informasjon som kan være interessant for andre, og hvordan vi skal beskytte oss.

Nye trusler. Han mener truslene mot norsk næringsliv er i ferd med å forandre seg. Tidligere ønsket trusselaktørene penger. Nå handler det om spionasjeangrep, hvor motivet enten er kortsiktig gevinst ved å få tak i informasjon, eller et mer langsiktig perspektiv ved å svekke eller ødelegge bedrifter på sikt.

– Vi i det norske samfunnet er litt naive. Vi ønsker å stole på folk. Men de som ønsker å skade oss, er ikke naive, sa han. Og hans råd til norske toppledere er klart.

– Gå hjem og undersøk hvor godt dere er sikret. Det kan hende dere blir overrasket.

Jannicke Hilland: – Dette kan hende oss alle

- Mitt hovedbudskap er: Vi må forstå at dette kan hende oss alle, sa direktør for konsernsikkerhet i Statoil, Jannicke Hilland, på Topplederseminaret i mars.

«Ingen kunne vært forberedt på denne hendelsen, uansett hvor god sikkerheten var.

JANNICKE HILLAND

HILLAND HAR blant annet vært plattformsjef, produksjonsdirektør og direktør for Fellesoperasjoner på norsk sokkel. I fjor gikk hun inn i ny jobb som direktør for konsernsikkerhet etter terrorangrepet på anlegget i In Amenas i Algerie.

En tøff oppgave. – Ingen kunne vært fullt ut forberedt på denne hendelsen, selv ikke vi som har sikkerhet høyt på agendaen, sa hun på Topplederseminaret.

Under og etter terrorangrepet var hun en av ledelsens representanter på pårørendesentret i Bergen. Det var en tøff oppgave. Statoil hadde noen enkle prinsipper for hvordan de håndterte informasjon under krisen. Kommunikasjonen skulle være åpen og faktabasert. De skulle ikke spekulere. Pårørende skulle få ny informasjon først. Og det ble holdt informasjonsmøter hver time, også når det ikke var ny informasjon.

Bevissthet viktig. Håndteringen var bra. Men Statoil var ikke godt nok forberedt som organisasjon, var blant hovedkonklusjonene etter angrepet. Forståelsen av risiko måtte blant annet forbedres. Informasjonstilfanget måtte blant annet utvides.

Generelt når det gjelder sikkerhet er bevissthet utrolig viktig, sa Hilland på seminaret. I dag jobber vi med å bygge kompetanse på sikring og dermed bli bedre på risikostyring. Det som skiller dette fra vårt vanlige sikkerhetsarbeid er at det dreier seg om trusler. Dette risikobildet må vi forstå og kunne håndtere. ‹

BLANT RÅDENE TIL TOPPLEDERNE PÅ SEMINARET VAR:

- Sørg for at du har oppdatert informasjon om trusselbildet
- Ta utgangspunkt i det verste som kan skje
- Bygg kompetanse internt i organisasjonen
- Utvikle robuste eksterne nettverk

Kristin Skogen Lund: Viktig å øve på sikkerhet

Toppledelse og styremedlemmer i næringslivet må ta risikobildet innover seg, og trene og øve på sikkerhetshendelser, sa administrerende direktør i NHO, Kristin Skogen Lund, på Topplederseminaret i mars.

EN MÅTE å møte trusselbildet på Internett på er å øke kompetansen på sikkerhet, og øke samarbeidet med dem som har kompetanse på området, sa Skogen Lund. Alle næringslivsledere må samarbeide med det offentlige om å møte truslene på en best mulig måte. Mer operativt samarbeid, og mer konkret rådgivning fra det offentlige, er to viktige måter å bli bedre på, sa hun. Og øving på sikkerhetshendelser er viktig.

– Man vil være bedre forberedt ved å øve, sa Kristin Skogen Lund, som også la til at det skjer mye bra på sikkerhetsområdet i Norge. Det er blant annet opprettet en egen rådgiver rettet mot norsk næringsliv i Kripos, og en egen Cybersecurity Task Force i regi av Næringslivets sikkerhetsråd. ‹

REKORDOPPSLUTNING PÅ NSMs SIKKERHETSKONFERANSE

18. og 19. mars gikk Sikkerhetskonferansen av stabelen på Oslo Kongressenter. Nærmere 650 deltakere var samlet til en faglig oppdatering som dekket de aller fleste av Nasjonal sikkerhetsmyndighets arbeidsområder, fra foto fra luften til sikre møterom, IKT-sikkerhet og eksterne foredragsholdere.

SAMTIDIG MED KONFERANSEN la NSM frem både sin årsrapport for 2013 og Rapport om sikkerhetstilstanden, noe direktør Kjetil Nilsen også presenterte etter at konferansen hadde blitt åpnet av forsvarsminister Ine Marie Søreide Eriksen fra Forsvarsdepartementet og statssekretær Hans Røsjorde fra Justisdepartementet.

Et av mange høydepunkter under årets konferanse var innlegget fra Espen Sandli i Dagbladet, som har jobbet med avisens artikkelserie «Null CTRL». Sandli har sammen med journalistkollega Linn Kongsli Hillestad og programmerer og utvikler Espen Sandli samt programmerer og utvikler Ola Strømman testet alt fra overvåkingskameraer til databaser og kontrollsystemer som ligger åpent på internett, og har blant annet avdekket at over 2000 overvåkningskameraer i norske hjem, butikker, nattklubber og restauranter ligger tilgjengelig på nett. Dette har de vunnet både SKUP-prisen for i Norge og European Press Prize for, og innlegget til Sandli åpnet øynene til mange i salen.

Vi i NSM gleder oss allerede til neste års konferanse, og ser frem til å se enda flere deltakere i mars 2015. ‹

1. Mange styringssystemer for kritiske funksjoner i samfunnet er ikke utviklet med tanke på sikkerhet, sa forsker Niklas Vilhelm i Nasjonal sikkerhetsmyndighet.

2. – Er man død, så hjelper ikke godt personvern, sa forsker Karsten Friis fra NUPI, og høstet motbør blant annet fra Datatilsynets Bjørn Erik Thon.

3. Direktør Kjetil Nilsen i Nasjonal sikkerhetsmyndighet åpnet konferansen.

4. Norge gjør seg sårbart for dataangrep utenfra av personer eller organisasjoner med uærlige hensikter, sa direktør Kjetil Nilsen blant annet til NRK.

5. – Ikke bare sitt der som noen torsker, da! sa driftsleder Roy Narvestad i Tertitten borettslag, som foreslo nytt slagord for NSM.

NY PRØVEORDNING FOR FOTO FRA LUFTEN

Skal du opp og filme med modellfly, fjernstyrt helikopter eller drone? Nå slipper du å søke om tillatelse fra NSM – så lenge dronen er innen synsrekkevidde, og den ikke er i nærheten av et område med fotoforbud.

SALGET AV FJERNSTYRTE helikoptre og droner med kamera har eksplodert de siste årene. Inntil 2. april måtte alle ha tillatelse fra NSM for å gjøre opptak fra luften, med unntak av passasjerer på rutefly. NSM lemper nå på kravene for når man må søke om å gjøre opptak fra slike ubemannede plattformer.

Ny prøveordning. NSM har besluttet at det som en prøveordning fra 2. april og ut året ikke lenger er nødvendig å søke om tillatelse for fotografering og filming fra luften så lenge dronen er innen synsrekkevidde og man flyr utenfor restriksjonsområder. Et restriksjonsområde er militære områder med fotoforbud. Også sivile områder kan være merket med forbud mot foto.

– De aller fleste droner blir fløyet av vanlige folk, og denne aktiviteten utgjør ingen risiko for det NSM skal bidra til å beskytte. Denne nye løsningen skal bidra til at regelverket ikke er til unødig hinder for folk flest, samtidig som vi ivaretar behovet for nasjonal sikkerhet, sier avdelingsdirektør Carsten Rapp i NSM.

Fortsatt forbud. Det vil fortsatt være forbudt å fotografere og filme restriksjonsområder fra luften. Brudd kan medføre straffeansvar. Ved tvil skal opptak unngås, og publikum kan eventuelt kontakte NSM for veiledning.

Det må også fortsatt søkes om tillatelse for andre typer opptak med luftbårne sensorsystemer, f. eks. kartlegging med fly og bruk av andre sensorer enn foto.

Andre hensyn. Vi gjør oppmerksom på at det i mange tilfeller er et krav om operative flytillatelser fra Luftfartstilsynet, og oppfordrer til å ta kontakt med dem for veiledning.

Når det gjelder privat bruk, finnes det også bestemmelser utenfor NSMs ansvarsområde. Blant annet i åndsverkloven, som regulerer midlertidig publisering, men ikke selve opptaket, og i straffeloven, som går på krenkelse av privatlivets fred. <

HVA SKJULER SEG BAK TALLENE?

Det kan fort bli slik at hendelsene som ligger bak 2013 statistikken fra operativ avdeling i NSM forblir nettopp det – statistikk og tall. Men bak tallene ligger det mye hardt arbeid. Arbeid for å hindre hendelser, oppdage dem og begrense skadevirkningene av hendelsene når de oppstår.

DETTE ARBEIDET skjer selvsagt sammen med virksomhetene som blir angrepet og ikke minst med viktige bidrag fra andre offentlige og private virksomheter som NSM samarbeider med. Det ligger mye kunnskap og kompetanse bak arbeidet som gjøres og vi lærer stadig mer om sårbarheter, hvordan de utnyttes, hvordan enkelte aktører arbeider m.m.

Det er allikevel en risiko for at kunnskapen forblir internt eller er svært begrenset til en liten gruppe med mennesker og virksomheter. Når jeg beskriver det som en risiko er det fordi jeg mener vi fortsatt trenger økt bevissthet i alle lag i samfunnet på hvor store og alvorlige utfordringene er i det digitale rom. Dette får vi stadige påminnelser om i møte med politikere, toppledere, mellomledere, ansatte og befolkningen generelt. En indirekte påminnelse fikk vi også på en pressekonferanse under nasjonal sikkerhetsmåned i fjor når de foreløpige tallene for 2013 ble fremlagt. Journalistene var ikke så interessert i tallene fordi de har hørt dem før, selv om de varierer noe. De vil ha detaljer om hendelsene, kjøtt på beinet eller sensasjonene om jeg skal kalle dem det.

Dette må vi ta inn over oss på flere nivåer, ikke fordi vi skal gjøre media fornøyd, men fordi vi trenger at flere blir enda mer bevisst problemstillingene. Flere må ta på alvor behovet for kunnskap, samarbeid og ressurser. For å få til dette kan vi ikke bare snakke om tall. Tall blir abstrakt i denne sammenhengen. Som den danske forfatter Storm P skal ha sagt «Statistikk er som en gatelykt. Ikke særlig opplysende, men god å støtte seg til.»

Vi må derfor våge å si mer om hendelsene bak statistikken. Vi må få flere til å ta trusselen som vi alle møter i vårt nettverksbaserte og teknologiske samfunn på alvor. Vi trenger en kollektiv økning i kunnskap og bevissthet om de eksisterende trusler og risiko vi daglig møter i det digitale rom. Vi trenger samtidig økt kunnskap og forståelse om hvordan samfunnet, virksomhetene og enkeltindivider bør håndtere truslene og redusere risiko. For å få et høyere felles kunnskaps- og bevissthetsnivå må vi da dele mer om det som skjer. Samtidig er det naivt å forvente full åpenhet. Slik fungerer ikke verden. Vi har alle behov for å ha noen hemmeligheter.

NSM håndterer daglig hendelser eller informasjon om hendelser som vi holder kjeft om i den forstand at det er den hendelsesutsatte virksomhet som «eier» sin egen hendelse. Det er virksomheten som avgjør om saken skal politianmeldelse, om de ønsker å informere sine kunder, eller offentliggjøre hendelsen. Dette er en grunnleggende forutsetning for det gode samarbeidet NSM har med en rekke virksomheter og noe vi i NSM selvsagt respekterer og beskytter med vår taushetsplikt og i mange saker med henvisning til rikets sikkerhet og sikkerhetslovens bestemmelser.

Allikevel ønsker vi i NSM en større åpenhet om hendelsene fordi vi gjennom større åpenhet kan sikre oss bedre i fremtiden. Dersom vi er i stand til å etablere en større åpenhet nå, vil vi sannsynligvis kunne skape en kunnskaps- og informasjonsdeling som kan bli et fortrinn for norske virksomheter i den fremtidige kampen for å beskytte seg mot digitale trusler for fremtiden. Det er å håpe at virksomhetene forstår at det å stå frem hjelper andre og andre som står frem hjelper tilbake, fordi erfaring, kunnskap og forståelse spres fortere. Er det noe vi trenger for å beskytte oss bedre mot digitale trusler, så er det nettopp det!

Roar Thon

« Vi må få flere til å ta trusselen som vi alle møter i vårt nettverksbaserte og teknologiske samfunn på alvor.

ROAR THON

Større åpenhet betyr ikke nødvendigvis at virksomhetene skal fortelle om alt. Men at vi har en vei å gå mener jeg ble klart etter fremlegging av statistikken for 2013. Statistikken fikk en del oppmerksomhet i media og i forbindelse med dette ble også noen sektorer intervjuet med konkrete spørsmål om dataangrep var et økende problem. Noen nektet å uttale seg om spørsmålet da det var for sensitivt å snakke om! Virkelig? Dersom vi ikke en gang kan uttale oss om det, har vi en lang vei å gå for å erkjenne utfordringene i det digitale rom. Jeg mistenker at svaret om at det er for sensitivt å uttale seg om, har en bakgrunn i at man rett og slett ikke har en grunnleggende oversikt over situasjonen. At det er sensitivt forstår jeg, fordi det er flaut!

Under Nasjonal sikkerhetsmyndighets sikkerhetskonferanse i mars presenterte NSM to reelle, men grundig «vaskede» og anonymiserte digitale spionasjesaker fra virkeligheten. Hensikten med å anonymisere sakene var for å hindre at identiteten til virksomhetene som var målet i de to sakene ble offentlig kjent. Når vi «vasker» en sak før vi uttaler oss, er det for å redusere risikoen for at vi gjennom detaljer avslører konkrete tekniske beskyttelsestiltak eller rutiner, på en slik måte at vi i forsøket på å drive folkeopplysning og kunnskapsformidling også skaper sårbarheter som trusselaktørene kan utnytte til nye forsøk mot norske interesser. For mye informasjon om tekniske detaljer kan også indirekte avsløre identiteten til den virksomheten som har vært utsatt for hacking, dataangrep eller digital spionasje (ukjært barn har også mange navn).

Hensikten med presentasjonen var i noe mer detalj å informere om hva som skjer når norske bedrifter og offentlige virksomheter blir utsatt for avanserte digitale spionasjeforsøk. Vi ønsker at flere virksomheter gjør som Telenor. Telenor fortjener virkelig ros for at de i 2013 stod frem kort tid etter at de ble utsatt for det som ble definert som et alvorlig tilfelle av industrispionasje mot konsernet. Det er ingen som ønsker seg slike hendelser, men Telenor har stått med rak rygg i offentlighetens lys, senest med styreleder i Telenor – Svein Aasers innlegg om hendelsen under NSMs toppledersemiar i mars. Åpenheten har etter vår mening bidratt til å skape en ytterligere forståelse for utfordringene i det digitale rom, men hva med alle de andre som kunne ha bidratt til det samme? For det var ikke bare Telenor som ble utsatt for industrispionasje i 2013! For alt du som leser vet – så er det ikke en gang sikkert at Telenor var de som ble hardest rammet i 2013?

Vi forstår at det kan virke svært vanskelig å stå frem offentlig med dette. Men det handler ikke om en åpenhet som er så detaljert at den ytterligere blottlegger eksisterende sårbarheter som igjen kan utnyttes av trusselaktørene, men en åpenhet som bidrar til å skape forståelsen om at vi alle, på et eller annet tidspunkt blir utsatt for dette. Jeg tror vi kommer lenger med at virksomheter åpent sier at de utsettes for dette daglig og at de er i en konstant kamp for å beskytte seg – enn å si at det er for sensitivt å snakke om.

For et par år tilbake ble en større norsk bedrift intervjuet i en lokalavis hvor de nettopp forklarte at de slåss daglig med å holde trusselaktører utenfor sine nettverk. Nabobedriften ble også intervjuet og deres svar var at – "nei, det har vi heldigvis ikke merket noe til" Hvem av de to bedriftene tror du har best fokus på sin sikkerhet?

Vi kan på ingen måte kreve at norske virksomheter skal stå offentlig frem og fortelle hva de utsettes for i det digitale rom, men vi ønsker allikevel så inderlig at de gjør det. Det vil styrke vår og virksomhetenes egen evne til å beskytte seg selv bedre i det lange løp og det vil sannsynligvis være en bekreftelse på at vi i større grad forstår utfordringene og tar de på alvor.

Måtte flere komme ut av skapet i det digitale rom! ‹

GOD HELSETILSTAND PÅ NETT, MEN MÅLRETTEDE ANGREP ØKER

Den digitale helsetilstanden i Norge er god sammenlignet med resten av verden, viser Microsofts Security Intelligence Report. Men målrettede dataangrep øker kraftig.

RAPPORT NUMMER 16 fra Microsoft ble lagt frem i begynnelsen av mai. Rapporten er svært omfattende, og er basert på én milliard sensorpunkter over hele verden, blant annet gjennom Windows Malicious Software Removal Tool, som skanner PCer for sårbarheter før de setter i gang med oppdatering.

Et rent land. Både forsøkene på infeksjoner av norske maskiner, og faktiske infeksjoner, er lav i Norge sammenlignet med resten av verden. Derfor er det en god helse på nettet i Norge, sa Ole Tom Seiersted i Microsoft på en pressesamling i mai.

– Dette viser at Norge er et rent land i verdenssammenheng. Men bildet er noe mer nyansert når det gjelder vellykkede dataangrep, sa avdelingsdirektør i Nasjonal sikkerhetsmyndighet, Hans Christian Pretorius, på samlingen.

Målrettede angrep. – For samtidig som antallet infiserte PCer i Norge er fallende, er antallet målrettede dataangrep kraftig økende.

I fjor håndterte Nasjonal sikkerhetsmyndighet totalt 51 alvorlige IKT-hendelser. Flesteparten av hendelsene handler om målrettede spionasjeforsøk. Trenden er kraftig stigende. Angrepsmåtene er avanserte.

Kjente sårbarheter. Han fikk støtte av Ole Tom Seiersted i Microsoft.

– Det som benyttes i målrettede angrep havner ikke på topp ti-lista, fordi angrepene er få, og målrettede.

Men det er mulig å gjøre noe med de målrettede angrepene, sa Pretorius, med enkle virkemidler.

Stort sett bruker angriperne kjente sårbarheter for å bryte seg inn i datasystemene. Tallene hadde blitt betydelig redusert dersom norske bedrifter rett og slett oppdaterer alle programmer når oppdateringene kommer.

Ansatte som sensorer. Tore Orderløkken fra NorSIS deltok også på pressesamlingen. NorSIS har et brukerperspektiv, og jobber mot små- og mellomstore bedrifter. De ser en økning i såkalte phishing-angrep, hvor målet er å få vanlige brukere til å gi fra seg informasjon ved å trykke på en lenke på en epost eller legge igjen informasjon i et skjema.

– Vi har fått flere henvendelser i det siste. Mange tar kontakt etter at de allerede har gitt fra seg informasjon, men skjønner de har gjort noe dumt, sa han. Sensorer for å se hva som skjer i nettverkene er bra, sa han.

– Men de ansatte er også gode sensorer. De må læres opp i hva de skal se etter og hjelpe til med å stoppe angrepene. ‹

FAKTA

HVORDAN STOPPE ANGREPENE?

Lurer du på hvordan du skal stoppe mesteparten av dataangrepene mot bedriften din? Les og innfør disse rådene (og tro oss, dette er tiltak som stopper 80–90 prosent av de vanligste angrepene, men som alt for få har innført):

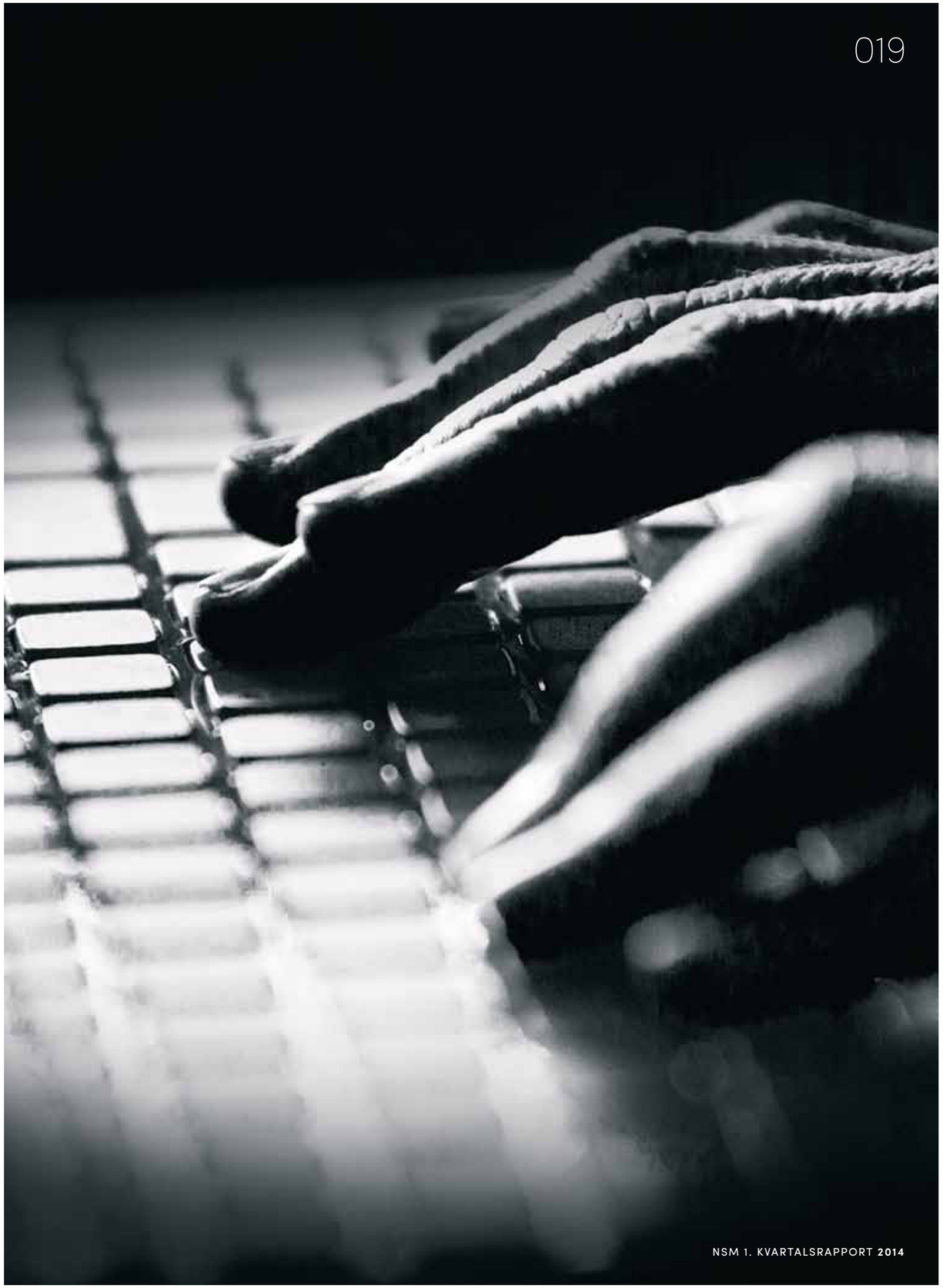
1. Oppgrader program- og maskinvare. Nyere produktversjoner har tettet flere sikkerhetshull enn gamle, og er bedre på sikkerhet.

2. Vær rask med å installere sikkerhetsoppdateringer. Kunnskap om nye sårbarheter sprer seg raskt. Derfor bør systemeiere være tilsvarende raske med å oppdatere, før noen bruker sårbarhetene til å bryte seg inn.

3. Ikke tildel sluttbrukere administrator-rettigheter. De fleste vanlige brukere har ikke behov for å installere programvare på maskinen. Overlat administrasjon og distribusjon av programvare til de som kan det.

4. Blokker kjøring av ikke-autoriserte programmer. Bare la brukerne kjøre godkjente programmer ved å bruke verktøy som Windows AppLocker.

Les mer på nsm.stat.no.



– OPPTATT AV GODE LØSNINGER

Hans Robert Bjørnaas leder teknologiavdelingen i Nasjonal sikkerhetsmyndighet (NSM), og har med det ansvaret for et bredt fagfelt i stadig endring. Å levere gode løsninger som er både sikre og brukervennlige står i høysetet for Bjørnaas' avdeling.

TEKNOLOGIAVDELINGEN omfatter seksjoner med ansvar for kryptotjenester, kryptoutvikling, IKT-sikkerhet, emisjonssikkerhet og sertifisering og prosjekter. Tradisjonelt har avdelingen jobbet mest med graderte systemer, men med NSMs utvidede ansvar innenfor sivil sektor dekker avdelingen i økende grad løsninger for «mannen i gata» også.

– Et bredere ansvar for NSM, med Justisdepartementet som et av våre styrende departement, er en erkjennelse av samfunnets behov for sikre løsninger totalt sett, ikke bare innenfor militær sektor. Dette er et ansvar vi tar på alvor, og vi jobber i dag med å sikre IKT-løsninger på alle nivåer, fra ugraderte systemer til systemer som er gradert strengt hemmelig, sier Bjørnaas, som har vært ansatt i NSM siden 2002.

Svært rask utvikling. Teknologiutviklingen innenfor IKT har gått svært raskt de siste årene, med stadig nye enheter, formfaktorer og programvare. Dette har vært en utfordring for sikkerhetsmiljøene, siden ny teknologi ofte har blitt tatt i bruk lenge før de har blitt testet godt nok for sårbarheter og andre sikkerhetsrisikoer.

– Vår jobb er slett ikke å forhindre at ny teknologi tas i bruk, men vi oppfordrer til at man tar i bruk ny teknologi på en fornuftig måte. Denne utviklingen er ikke noe som er isolert til Norge, men en internasjonal trend, og vårt ønske er at vi kan ta i bruk sikre løsninger så raskt som mulig. Disse løsningene må selvfølgelig også være brukervennlige, og helst så enkle at brukerne ikke merker at sikkerhetsnivået er høyere enn på en standardmodell, sier Bjørnaas.

Etterlyser mer akademisk fokus. Til tross for et økende samfunnsfokus på forebyggende sikkerhet, mener Bjørnaas at dette fortsatt kan bli bedre. Han ønsker at sikkerhet skal komme høyere i folks bevissthet, både gjennom utdanning og generelt i hverdagen.

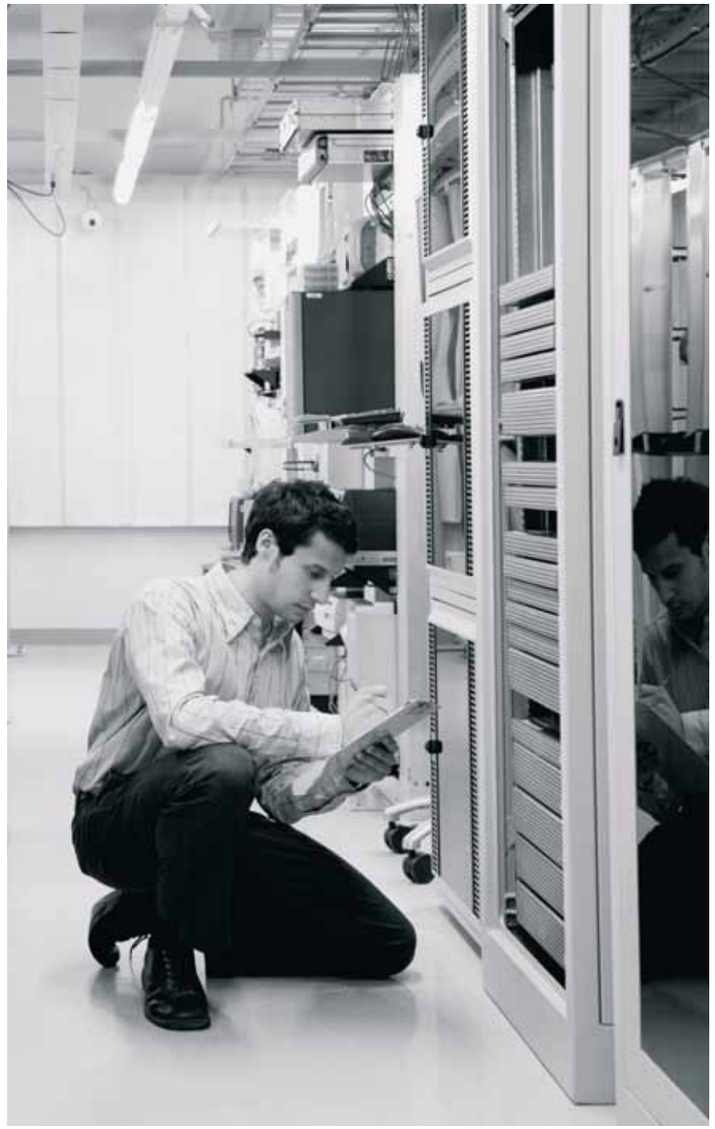
– Vi ser at hendelser av forskjellige størrelser, fra 22. juli til avsløringen av «Heartbleed»-sårbarheten i våres, øker bevisstheten rundt sikkerhet, og løftene kommer ofte etter slike hendelser. Vi savner en mer helhetlig tilnærming til sikkerhet allerede i utdanningen, nesten uavhengig av fagretning, og derfor er kontakt med akademia, både i Norge og internasjonalt, viktig for oss i NSM. Samtidig skulle vi ønske at sikkerhet fikk en større plass i produktutviklingen, og ikke noe som ble lagt til i etterkant. Her kan vi lære mye av bransjer som har mer fokus på «safety», som for eksempel oljebransjen, sier Bjørnaas.

Som et ledd i satsingen mot akademiske miljøer har teknologiavdelingen god kontakt med universiteter i inn- og utland. I tillegg til formelle samarbeid med blant annet Høgskolen i Gjøvik og Universitetet i Bergen, er en av NSMs forskere gjesteforsker ved det Danske Tekniske Universitet, samtidig som forelesninger om herding av operativsystemer har kommet på timeplanen i Norge. I tillegg er en rekke av NSMs forsknings- og utviklingsprosjekter forankret i teknologiavdelingen.

Hans Robert Bjørnaas

Bygger opp rådgiverkorps. Et av hovedsatsingsområdene til teknologiavdelingen i 2014 er å bygge opp et miljø med rådgivere som kan være bindeledd mellom operativ avdeling, som håndterer saker i et kortere tidsperspektiv, og forskningsmiljøene, som gjerne har en lengre tidshorisont.

– I løpet av sommeren håper vi å ha på plass de første rådgiverne i teknologiavdelingen. Vi får en rekke henvendelser, og ser at vi har behov for å kunne gi råd og veiledning til virksomheter i både sivil og militær sektor som dreier seg om problemstillinger på middels kort sikt. Dette er en av hovedsatsingsområdene våre i år, og noe vi gleder oss til å få på plass. Dette vil gjøre NSM til en bedre rådgiver for alle våre kontakter, avslutter Bjørnaas. ‹



TENK SIKKERHET I FERIEN

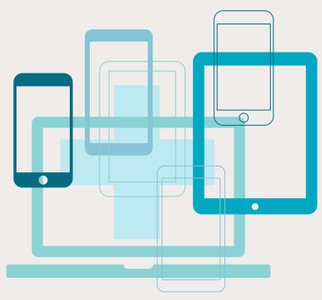
Sommerferien er ikke langt unna, og uansett om du er på ferie eller arbeidsreise minner vi om risikoen det er å være på reise.

PÅ REISE er det større sjanse for at du kan befinne deg i omgivelser som er så godt kontrollert teknologisk og menneskelig av andre at informasjon eller passord til å lese informasjon kan kompromitteres.

Gjør en verdivurdering. En av de viktigste tingene du bør gjøre før du starter reisen er å gjøre en verdivurdering. Et sentralt spørsmål bør være om man trenger å ta med seg elektroniske enheter som mobil, PC eller nettbrett, som inneholder store mengder med informasjon som samlet sett kan ha en høy verdi. Trenger du virkelig å dra med deg alt du og dine kolleger har produsert de siste 7 årene? Eller holder det med en enhet som kan sende e-post og lese nyheter? Har du virkelig bruk for å ha tilgang til den aller viktigste informasjonen hos din arbeidsgiver, når du egentlig skal kose deg på ferie?

Kun for reisebruk. Flere virksomheter har skaffet seg reisemobiler og -PCer som brukes når deres ansatte skal på reiser. Enhetene kontrolleres og renses etter bruk før de er klare for ny reise. Dette er et særdeles fornuftig tiltak som vi anbefaler at flere gjør.

Har du ikke mulighet til å dra med enheter som kun er til reisebruk, bør du tenke på hva du har lagret på enheten av alt fra virksomhetskritisk informasjon til personlige passord. ‹



IKKE FRISKMELD DEG SELV OG DINE ENHETER TO DAGER ETTER HJEMKOMST.

Konsekvensene ved å ha blitt kompromittert kan komme over tid. Vi legger igjen en rekke digitale spor på reiser og du kan f.eks. ha gitt fra deg din e-post adresse til en rekke mennesker og virksomheter. Vær spesielt oppmerksom på e-poster med vedlegg som kommer i ettertid.

FAKTA

NOEN TIPS OG RÅD:

Forstå og aksepter at du er et mål på internett

Tilbud som er for gode til å være sanne, er som regel det

Ta ikke med deg flere enheter enn det du trenger

Ta ikke med deg mer informasjon på dine enheter enn det du må

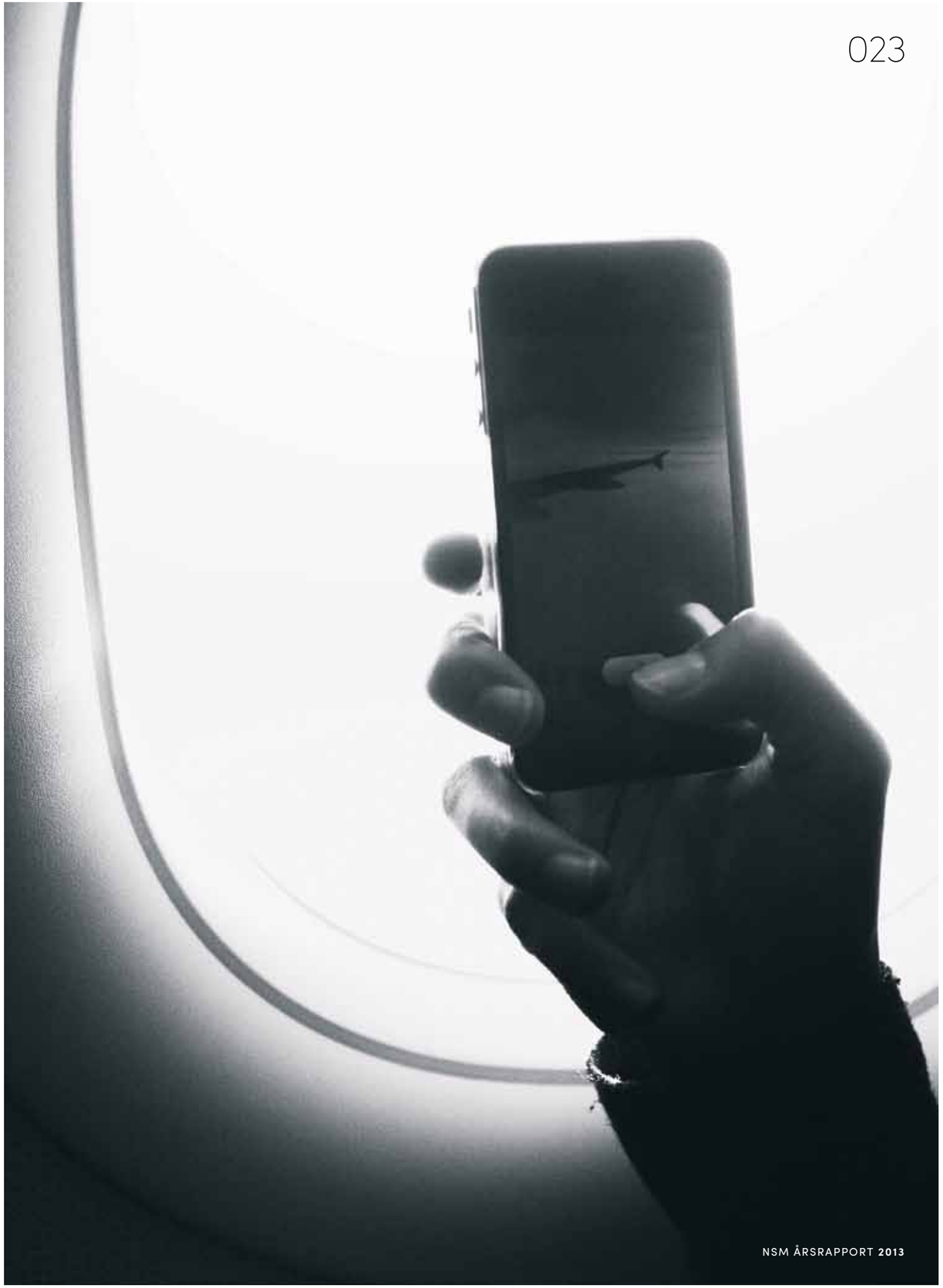
Krypter informasjonen din

Slå av blåtann og trådløs forbindelse dersom du ikke må bruke det

Bruk VPN løsninger og andre sikkerhetsmekanismer når dette er tilgjengelig for deg

Når du kommer hjem – Sjekk enhetene dine, eller la noen kyndige kontrollere dem

Når du kommer hjem - Endre dine passord!



NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

Tlf. 67 86 40 00
post@nsm.stat.no
www.nsm.stat.no