NSM

ÅRSRAPPORT 2013

NASJONAL SIKKERHETSMYNDIGHET ER NORGES
EKSPERTORGAN FOR INFORMASJONS- OG OBJEKTSIKKERHET

DETTE ER NSM

Nasjonal sikkerhetsmyndighet er Norges ekspertorgan for informasjons- og objektsikkerhet, og er det nasjonale fagmiljøet for IKT-sikkerhet.

Direktoratet er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser.

NSM vokser for å møte dagens og fremtidens utfordringer. I 2013 ansatte direktoratet 60 nye medarbeidere.

2013: NOEN NØKKELTALL

58 539
... kryptonøkler, som gjør det mulig å kommunisere sikkert, ble produsert og distribuert nasjonalt og internasjonalt.

34 655
... klareringssaker ble avgjort med innhenting av personopplysninger fra NSM.

95
... foredrag om sikkerhetskultur ble gitt over hele landet.

334
... lisenser ble gitt til foto fra luften.

3901
3901 sikkerhetshendelser på nett ble håndtert ved varsling, dialog, analyse og bistand.

50
... alvorlige dataspionasjesaker ble håndtert i operasjonssenteret.

124
... sikkerhetsgodkjenninger ble gitt til virksomheter som har sikkerhetsgraderte datasystemer.

30/70
Vi har 200 ansatte. 30 prosent av de ansatte er kvinner, 70 prosent er menn

ORGANISERING

Slik er arbeidet med informasjons- og objektsikkerhet organisert i Norge

FORSVARS-DEPARTEMENTET
Forsvarsdepartementet har det overordnete ansvaret for informasjons- og objektsikkerhet i militær sektor. NSM er administrativt underlagt departementet.

JUSTIS-OG BEREDSKAPS-DEPARTEMENTET
Justis- og beredskapsdepartementet har det overordnete ansvaret for informasjons- og objektsikkerhet i sivil sektor. Departementet overtok 1. april 2013 ansvaret for IKT-sikkerhet i det sivile samfunn.

NASJONAL SIKKERHETS-MYNDIGHET
NSM er utøvende organ for Forsvarsdepartementet og Justis- og beredskaps-departementet

MILITÆR SEKTOR / SIVIL SEKTOR

Foto omslag: SCANPIX

Design: REDINK

Foto: NSM,ØIVIND HAUG JOHNÉR, THINKSTOCK, SCANPIX.

Illustrasjon: MARIUS HOLE

Trykk og distribusjon: RK GRAFISK

ET ÅR FOR STYRKING AV SIKKERHETEN

I 2013 ble flere tiltak satt i gang for å bedre sikkerheten i Norge. Mange sikkerhetsutfordringer gjør likevel at en fortsatt styrking av sikkerheten er nødvendig i norske virksomheter.

2013 VAR et år med fortsatt økning i de digitale truslene mot Norge. NSMs operasjonssenter håndterte tusenvis av hendelser, og jobbet også i 2013 med å bistå i håndteringen av flere titalls alvorlige dataangrep. Snowden-saken førte til store debatter rundt rettssikkerhet, personvern og sikkerhet.

I følge vår egen rapport om sikkerhetstilstanden finnes fremdeles mange og omfattende sårbarheter. og nasjonale verdier er fortsatt utsatt for en betydelig risiko i forhold til spionasje, sabotasje og terror. Derfor må samfunnet redusere sårbarhetene.

Flere tiltak ble satt i verk i 2013 for nettopp dette. La meg ta noen eksempler. IKT-sikkerhet var, og er fortsatt, et satsningsområde for Regjeringen, både gjennom langtidsplanen for forsvarssektoren, Justis- og beredskapsdepartementets samfunnssikkerhetsmelding og Nasjonal strategi for informasjonssikkerhet. Justis- og beredskapsdepartementet overtok i tillegg ansvaret for IKT-sikkerhet i det sivile samfunn 1. april 2013.

Det ble organisert holdningskampanjer om informasjonssikkerhet, blant annet gjennom Nasjonal sikkerhetsmåned. Høgskolen i Gjøvik etablerte et senter for cyber- og informasjonssikkerhet. En revisjon av sikkerhetsloven, tilpasset dagens og fremtidens utfordringer, ble satt i gang. Og det ble etablert responsmiljøer for IKT-hendelser i flere sektorer. Flere er under planlegging. Graderte kommunikasjonssystemer ble rullet ut for offentlige virksomheter.

Et robust samfunn. Også i Nasjonal sikkerhetsmyndighet satte vi i verk flere tiltak. Vi har styrket kapasiteten til å håndtere alvorlige dataangrep, og bygger nå opp en 24-timers bemanning som skal følge med på og bistå norske virksomheter døgnet rundt under dataangrep.

Vi fortsetter styrkingen av tilsyn med virksomheter underlagt sikkerhetsloven. Vi har utvidet organisasjonen kraftig, ansatt 60 nye personer, og har nå rundet 200 ansatte totalt, som blant annet skal hjelpe norske virksomheter til å styrke sin egen sikkerhet. Denne styrkingen fortsetter i 2014.

Fremdeles er det slik at vi ikke er godt nok sikret, verken når det gjelder Internett og datasystemer, eller når det gjelder bygg og installasjoner i Norge. Mange vil hevde at vi i NSM aldri vil være fornøyd med sikkerheten. Vi vil alltid være bekymret. Det er kanskje vår rolle. Men det finnes mange tiltak som kan styrke sikkerheten, og mye blir gjort, av mange ulike nasjonale aktører. Det tyder på at verden går fremover, at vi i årene fremover kan klare å skape et mer robust og motstandsdyktig samfunn, forebygge mot kritiske hendelser, og håndtere krisesituasjoner på en god måte når de skjer. ‹

FAKTA

KJETIL NILSEN

Stilling: Direktør
Alder: 53 år
Om: Utdannet politi, jurist og har en mastergrad i ledelse

HANS ROBERT BJØRNAAS
oberst, avdelingssjef Teknologi

– I 2013 har teknologiavdelingen satset betydelig på forskning og utvikling. Vi har sett på områder utover gradert informasjon, og vil i 2014 fortsette å komme med enkle tiltak som kan forbedre sikkerheten betydelig. God kunnskap muliggjør innovativ og brukervennlig sikkerhet, og tidsriktige og funksjonelle løsninger. Vi vil øke samarbeidet med offentlige virksomheter, industri, akademia og internasjonale partnere.

BENTE HOFF
avdelingsdirektør Informasjonsforvaltning

– I 2013 har vi fokusert på å fornye og styrke løsninger som vil gjøre arbeidshverdagen enklere for klareringsmyndighetene. Denne jobben fortsetter i 2014. Et annet fokusområde er å modernisere og digitalisere prosesser som støtter opp under NSMs aktivitet, levert gjennom nye løsninger og plattformer. Avdelingen er også tungt involvert i utrullingen av en kryptert mobiltelefoniløsning, som blant annet Regjeringen har tatt i bruk.

ÅSA ERIKSSON
fung. avdelingsdirektør HR

– I 2013 økte NSM bemanningen med mer enn 30 prosent, noe som har vært den viktigste oppgaven for en styrket HR-avdeling. I 2014 skal NSM vokse ytterligere, samtidig som vi skal ivareta de som allerede er ansatt. I en verden der mange konkurrerer om de beste hodene, spesielt innenfor IT-relaterte fag, er det viktig at NSM er en velfungerende arbeidsplass, med godt arbeidsmiljø, og at vi synliggjør dette. Dette vil være blant våre viktigste oppgaver i året som kommer.

HANS CHRISTIAN PRETORIUS
avdelingsdirektør Operativ

– Vårt operasjonssenter registrerte en betydelig økning i håndterte saker i 2013, også det vi definerer som alvorlige saker. Det er liten grunn til å tro at denne trenden vil endre seg, og derfor er også avdelingen styrket. Med et risikobilde som stadig er i endring er det viktig for oss å konstant ligge foran utviklingen, enten det gjelder datakriminalitet eller tekniske sikkerhetsundersøkelser og inntrengningstesting. 2014 blir et år der vi skal ytterligere forbedre oss.

VIGDIS GRØNHAUG
avdelingsdirektør Kontroll

– Tilsyn er et viktig virkemiddel for å bidra til virksomhetenes forbedring av arbeidet med sikkerhet. I 2013 gjennomførte vi 23 tilsyn og med styrket bemanning vil antallet tilsyn øke ytterligere i 2014. Flere av våre tilsyn viste forbedringer i sikkerheten, samtidig har vi avdekket sårbarheter i sikkerheten hos flere av nasjonens mest kritiske virksomheter. Dette understreker viktigheten av at vi fortsetter kontrollvirksomheten og oppfølgingen av nødvendige tiltak. Flere og flere virksomheter er avhengige av gradert kommunikasjon og da må NSM godkjenne at sikringen er god nok. Vi ser at det er et økt fokus på dette, og vi får inn stadig flere søknader om godkjenning av IKT-systemer.

MONA STRØM ARNØY
avdelingsdirektør Kommunikasjon

– Kommunikasjonsavdelingen i NSM ble betydelig styrket i 2013, og avdelingen har nå økt kapasitet og fått bredere kompetanse. I tillegg til tradisjonelle kommunikasjonsoppgaver som mediekontakt og ansvaret for NSMs merkevare i tradisjonelle og nye kanaler, er nettopp kompetanseutvikling et fokusområde for avdelingen i 2014, blant annet gjennom etableringen av et eget undervisningssenter der vi ytterligere kan dele den kunnskapen og erfaringen som sitter i NSM. Å bidra til bedre sikkerhetstilstand i samfunnet er et klart mål for arbeidet i avdelingen.

KNUT BJØRN MEDHUS
oberst, avdelingssjef Plan og strategi

– Avdeling for plan og strategi ble betydelig styrket. Vi etablerte en seksjon for strategisk analyse, som vil gjøre oss i stand til å levere bedre vurderinger av sikkerhetstilstanden og andre analyser. Samtidig har vi styrket virksomhetsstyring, drift og logistikk, for å legge til rette for en mer effektiv og smidig organisasjon. Avdelingen har også vært tungt involvert i arbeidet med revisjon av sikkerhetsloven med forskrifter. Dette arbeidet er viktig med tanke på NSMs rolle og videreutvikling fremover.

CARSTEN RAPP
avdelingsdirektør Sikkerhetsstyring

– 2013 var et svært aktivt år for Avdeling for sikkerhetsstyring. Vi har sikkerhetsklarert et rekordhøyt antall personer. Råd og veiledning om utvelgelses- og klassifiseringsprosessen etter de nye objektsikkerhetsbestemmelsene i sikkerhetsloven med forskrift, som trådde i kraft 1.1.2011, har involvert mange av våre ansatte. Dette arbeidet fortsetter i 2014, og da er det særlig sikringstiltakene vi vil fokusere innsatsen mot. Samtidig ser vi at bruken av fjernstyrte helikoptre med kamerautstyr har blitt svært populært. Det aller meste av denne bruken utgjør ikke en risiko for nasjonal sikkerhet, noe som gjør at vi i løpet av 2014 endrer regelverket for luftbårne sensorsystemer i en mer liberal retning.

SIKKERHETSTILSTANDEN FORTSATT IKKE GOD NOK

I 2013 ble flere tiltak satt i gang for å bedre sikkerheten i Norge. Likevel finnes det fremdeles mange og omfattende sårbarheter, og nasjonale verdier er fortsatt utsatt for en betydelig risiko for spionasje, sabotasje og terror.

TRUSLENE mot norske datasystemer øker. I 2013 håndterte NSM 50 alvorlige digitale infiltrasjonsforsøk. Ved flere tilfeller kan angriperne ha vært inne i datasystemene over flere år.

NSM har i 2013 avdekket at sentrale norske virksomheter som myndighetsorganer, forsvarsindustri og teknologibedrifter har vært utsatt for gjentatte, målrettede nettverksoperasjoner. For eksempel avdekket NSM at det ved en alvorlig hendelse trolig gikk 15 - 18 måneder fra systemet ble kompromittert til hendelsen ble oppdaget. Totalt ble det registrert 15 815 sikkerhetshendelser på nett. Av disse ble 3901 håndtert manuelt ved varsling, dialog og analyse.

Omfattende sårbarheter. NSM erfarer at mange virksomheter mangler oversikt over sine egne verdier og egen sikkerhetstilstand. Sikkerhetsmessige utfordringer er ikke dokumentert og virksomheten har ikke formulert konkrete mål for sikkerhetsarbeidet. Ofte mangler det bevissthet omkring sikkerhetsmessig risiko og erkjennelse av at virksomheten kan være utsatt. Mange virksomheter har verken innhentet eller etterspurt trusselinformasjon som grunnlag for å utarbeide risiko- og sårbarhetsvurderinger.

Mange virksomheter synes å være villig til å akseptere en sikkerhetsmessig risiko som NSM vurderer som uakseptabel for samfunnet som helhet.

Liten bevissthet. NSM ser at topplederе i de ulike virksomhetene i svært liten grad blir målt på sikkerhet, og at bevissthetеn rundt sikkerhet er tilsvarende liten. Handlekraft og gjennomføringsevne er essensielt for at sikkerhetsarbeidet skal bli gjennomført, og dette er et lederansvar. Vi ser at det ofte tar for lang tid før sikkerhetsarbeid får prioritet og tiltakene blir implementert.

NSM har registrert at sårbarheter som har blitt observert under tilsyn ikke lukkes. I mange tilfeller har de vedvart over flere år. Dette gjelder også i sektorer og virksomheter som er spesielt utsatt for etterretning.

Mange klareringsmyndigheter har ikke tilstrekkelig klareringskompetanse. Dette øker risikoen for at personer som ikke burde vært klarert får tilgang til skjermingsverdig informasjon.

Kontrollsystemer på nett. De siste årene har stadig flere kontrollsystemer for blant annet infrastruktur og industri blitt koblet til Internett. Kontrollsystemene kan styre alt fra lys og varme til oljeutvinning og vannkraftverk. Kontrollsystemer har tradisjonelt vært utviklet for å fungere i lukkede datamiljøer, og er ikke designet for å styres og kontrolleres over Internett. Det innebærer at de blir mer utsatt for digitale trusler. Virksomhetene som bruker teknologien mangler ofte kunnskaper om hva som ligger bak systemene, og har liten mulighet til å kontrollere hva de faktisk inneholder. En mulig sikkerhetsutfordring er at virus verken blir oppdaget eller stoppet.

Objektsikkerhet. Objektsikkerhet har i rapporteringsperioden vært et særskilt satsningsområde for NSM. Arbeidet med å identifisere skjermingsverdige objekter som må sikres spesielt mot sabotasje og terror har trolig bidratt til å styrke sikkerheten i flere virksomheter.

Det at enkelte virksomheter og departementer ikke har fulgt sikkerhetslovens skadevurderingssystematikk for utpeking og klassifisering av skjermingsverdige objekter medfører en risiko for at objekter er klassifisert feil. Etter NSMs vurdering kan dette medføre at det ikke er iverksatt nødvendige sikringstiltak, og det kan medføre at det er iverksatt unødvendig ressurskrevende sikringstiltak.

Betydelig risiko. Nasjonal sikkerhetsmyndighet ser at sikkerhet er blitt satt tydeligere på dagsordenen i enkelte virksomheter og erfarer at interessen for sikkerhet er økende i samfunnet. Tiltakene har trolig økt mange virksomheters evne til å forebygge og forhindre sikkerhetstruende virksomhet. Likevel finner vi mange og omfattende sårbarheter. Dette gjør det nødvendig å opprettholde trykket på arbeidet med å styrke sikkerheten i norske virksomheter. Særlig er det viktig at ledere engasjerer seg og bidrar til at sikkerhetsarbeidet gis nødvendig prioritet. Nasjonale verdier er fortsatt utsatt for en betydelig risiko for spionasje, sabotasje og terror. <

Ugradert rapport om sikkerhetstilstanden kan lastes ned på nsm.stat.no eller bestilles på post@nsm.stat.no

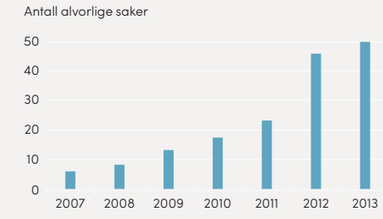
FAKTA

TILTAK I 2013

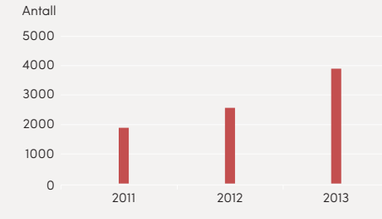
Her er noen tiltak som er planlagt eller gjennomført i 2013:

- Holdningskampanje om informasjonssikkerhet
- Etablering av et senter for cyber og informasjonssikkerhet på Høgskolen i Gjøvik
- Revisjon av sikkerhetsloven
- NSM utarbeidet en pakke med tiltak for implementering av grunnleggende IKT-sikkerhetstiltak
- Det er etablert responsmiljøer for IKT-hendelser i flere sektorer. Flere er under planlegging.
- Det utvikles graderte kommunikasjonssystemer for offentlige virksomheter.

Alvorlige hendelser siden 2007



Antall håndterte saker



FAKTA

FIRE TIPS TIL ALLE

Virksomhetene må gjøre det de kan for å ha så god grunnsikring som mulig, men et av de viktigste tiltakene er å skaffe seg evnen til å reagere og håndtere situasjonen som oppstår når trusselaktørene lykkes.

- Aksepter at du har verdier og informasjon som andre er ute etter.
- Virksomheter vil aldri kunne sikre all informasjon. Det viktige er å identifisere informasjonen med høyest verdi og sikre den deretter.
- Alle ansatte med brukernavn og passord til virksomhetens informasjonssystemer er et mål for trusselaktørene.
- Både ledere og ansatte har et ansvar og er med på å bidra til at de reelle sikkerhetstiltakene blir så robuste som mulig.

FORTSATT STYRKING I 2014

Sikkerhetsarbeidet styrkes ytterligere i 2014. Det sier assisterende direktør Annette Tjaberg i Nasjonal sikkerhetsmyndighet.

I TRÅD MED den nye langtidsplanen for forsvarssektoren har regjeringen styrket det forebyggende sikkerhetsarbeidet i 2014. Dette innebærer en styrking av NorCERT-funksjonen og objektsikkerhetsarbeidet hos Nasjonal sikkerhetsmyndighet. I tillegg skal tilsynskapasiteten og kapasiteten for inntrengingstesting og tekniske sikkerhetsundersøkelser økes. Kompetansemiljøene innenfor forebyggende sikkerhet skal styrkes både internt i NSM og i samfunnet for øvrig. Regjeringen legger i følge Prop. 1 S (2013–2014) stor vekt på samfunnets samlede evne til sikkerhet i det digitale rom, og vil videreutvikle NSM som det sentrale direktorat for beskyttelse av informasjon og infrastruktur av betydning for samfunnskritiske og andre viktige samfunnsfunksjoner.

– Dette betyr at vi kan holde et fortsatt stort trykk på sikkerhetsarbeidet, sier Tjaberg.

Mer råd og veiledning. Regjeringen ønsker også å styrke samordningen på IKT-sikkerhetsområdet, blant annet gjennom å videreutvikle NSM som det nasjonale fagmiljøet for IKT-sikkerhet i Norge. Regjeringen bevilget for 2014 16 millioner kroner til dette formålet. Fagmiljøet i NSM vil være viktig for å understøtte Justis- og beredskapsdepartementet i ansvaret for forebyggende IKT-sikkerhet på sivil side, i følge Prop. 1 S (2013–2014) fra Justis- og beredskapsdepartementet. Styrkingen av NSM skal bidra til bedret IKT-sikkerhet i samfunnet og til å møte utviklingen i det stadige mer komplekse IKT-risikobildet.

– Regjeringen legger vekt på å styrke arbeidet med forebyggende sikkerhet og IKT-sikkerhet på tvers av samfunnssektorene. Vi er glade for at NSM skal ha en sentral rolle i dette ved at vi skal videreutvikles som det nasjonale IKT-sikkerhetsmiljøet, sier Annette Tjaberg. <

FIRE GREP KAN STOPPE 80 PROSENT AV DATAANGREP

NSMs operasjonssenter håndterte rekordmange dataangrep i 2013. Studier viser at disse fire enkle grepene kan stoppe mellom 80 og 90 prosent av internettrelaterte angrep.

– Dette er hjelp til selvhjelp som vi oppfordrer norske virksomheter til å ta i bruk. Får virksomhetene orden på dette, frigjør de ressurser til å fokusere på de mer krevende hendelsene når de inntreffer, sier assisterende direktør Annette Tjaberg i NSM.

1. **Oppgrader program- og maskinvare.** Nyere produktversjoner har tettet flere sikkerhetshull enn eldre versjoner, og de har ofte flere og bedre sikkerhetsfunksjoner.
2. **Installer sikkerhetsoppdateringer så fort som mulig.** Selv de beste produktene har feil og sårbarheter som kan bli utnyttet av angripere. Systemeiere bør etablere et sentralt styrt regime for oppdatering av applikasjoner, operativsystemer og firmware (f. eks. BIOS-kode).
3. **Ikke tildel sluttbrukere administratorrettigheter.** De fleste sluttbrukere har ikke behov for administratorrettigheter. I et sentralt administrert system kan sluttbrukere få den programvaren de trenger fra et felles distribusjonspunkt.
4. **Blokker kjøring av ikke-autoriserte programmer («hvitelisting»).** Bare la brukerne kjøre godkjente applikasjoner ved å bruke verktøy som Windows AppLocker. Blokker spesielt programmer utenfor godkjente mapper og på flyttbare media, som for eksempel på CD-er og minnepinner.

Søk etter «U-01» på NSMs nettsider for mer informasjon om disse og andre tiltak.

Annette Tjaberg er assisterende direktør i Nasjonal sikkerhetsmyndighet.

NY TEKNOLOGI UTFORDRER SIKKERHETEN

For noen hundrelapper kan hvem som helst gå inn i en leketøys- eller elektronikkforretning og kjøpe et fjernstyrt helikopter eller fly med mulighet til å gjøre sylskarpe videoopptak. Denne trenden utfordrer sikkerheten på mange nivåer, og regelverket er nå under revidering, fra flere offentlige virksomheter.

DE FÆRRESTE som kjøper et fjernstyrt helikopter, drone eller «luftbårent sensorsystem» som det kalles i NSM, er klar over regelverket og ansvaret som følger med et slikt kjøp. Å «ta av» er ikke ufarlig, og er underlagt visse restriksjoner.

I tillegg til NSM håndhever også Luftfartstilsynet og Datatilsynet regelverk som påvirker bruken av denne typen modellfly. Flere av reglene er under revidering, både for hobbyflygere og for kommersielle aktører.

Rikets sikkerhet. I henhold til forsvarshemmelighetsloven med forskrift kreves det tillatelse fra NSM for å gjøre opptak fra luften over norsk territorium. Unntatt fra dette kravet, er passasjerer i luftfartøy i rute- charter- eller taxitrafikk som følger de fastsatte luftleder, samt opptak som gjøres i henhold til rustningskontrolloppgaver som Norge har ratifisert. Det er dermed ikke lov å filme, fotografere eller oppta data med andre sensorer fra luften uten tillatelse fra NSM. Formålet med regelverket er å beskytte opplysninger av betydning for rikets sikkerhet.

Dette betyr at filming eller fotografering fra for eksempel et modellfly er forbudt, uansett hva du skal bruke det til; selv om du bare skal beholde bildene selv, må du ha søkt og fått godkjenning på forhånd.

NSM har i 2013 gjort en ny vurdering av sikkerhetsbehovet, samfunnsutviklingen og den teknologiske utviklingen som påvirker ordningen. NSM vil i første halvdel av 2014 endre praksis innenfor regelverkets rammer, samt foreslå regelendringer for Forsvarsdepartementet der det vurderes som hensiktsmessig.

Sikre luftrom. Det finnes per i dag ikke noen egen forskrift som regulerer bruk av ubemannede luftfartøyer i Norge. I påvente av en ny forskrift, kom Luftfartstilsynet i juni i fjor med oppdaterte regler for bruk av ubemannede luftfartøy i Norge. Her presiseres at alle som vil operere såkalte RPAS (Remotely Piloted Aircraft Systems), må søke om særskilt tillatelse fra Luftfartstilsynet.

Inntil videre er det luftfartsloven som gjelder, med visse justeringer. Blant annet er det krav om at:

- Piloten/operatøren skal ha visuell kontakt med fartøyet, hele tiden (unntak må godkjennes i hvert enkelt tilfelle)
- Maksimal flyhøyde er 400 fot over bakken, det vil si 100 fot under minimum flyhøyde for bemannede fartøy
- Det skal tegnes ansvarsforsikring for alle ubemannede luftfartøy, uansett startvekt

Privatlivets fred. Fotografering fra luften kan også innebære utfordringer for personvernet. Disse problemstillingene håndteres av Datatilsynet. <

FAKTA

DRONER OG KRAV

334 lisenser til foto fra luft ble gitt av Nasjonal sikkerhetsmyndighet i fjor. Tilsvarende tall fra 2012 var 98, og 114 i 2011.

Piloten/operatøren skal ha visuell kontakt med fartøyet, hele tiden (unntak må godkjennes i hvert enkelt tilfelle).

Maksimal flyhøyde er 400 fot over bakken, det vil si 100 fot under minimum flyhøyde for bemannede fartøy.

Det skal tegnes ansvarsforsikring for alle ubemannede luftfartøy, uansett startvekt.

SIKRER SIGNALENE FRA ROMMET

Vi navigerer etter satellitter på mobiltelefonen vår. Treningsapper viser hvor langt vi har løpt. Redningstjenesten, skipsfart, oljeindustrien og katastrofeberedskapen er avhengig av satellittnavigasjon. Hva skjer hvis signalene forsvinner?

Foto: ESA/Fermin Alvarez Lopez

I JAMES BOND-FILMEN «Tomorrow Never Dies» manipulerer den onde mediemogulen Elliot Carver satellittsignalene til et britisk marinefartøy slik at det blir lurt inn i kinesisk farvann. Umulig? Ikke i følge seniorrådgiver i Nasjonal sikkerhetsmyndighet, Kjetil Birkeland Daatland.

– I Nasjonal sikkerhetsmyndighet fokuserer vi på å redusere sårbarheter som kan utnyttes til sabotasje, terrorisme eller spionasje mot Norges eller våre alliertes romvirksomhet. Sårbarhetene finner vi både i menneske, organisasjon og teknologi. En trusselaktør kan for eksempel prøve å hacke datasystemer, manipulere ansatte i en virksomhet, eller fysisk bryte seg inn. Sammen med en rekke andre virksomheter skal vi hindre at det skjer.

En sentral aktør. Du visste det kanskje ikke, men Norge er en sentral aktør i Europas største fellesindustrielle prosjekt, Galileo. Galileo er intet mindre enn et helt nytt rombasert satellittnavigasjonssystem, og skal fra 2018 være fullt operativt med 30 satellitter i bane rundt jorden. Sammen med blant annet amerikanske GPS skal systemet sikre oss alle med rombaserte tjenester, som satellittnavigasjon.

Norge verner om navigasjonssignaler til et verdensomspennende nettverk av satellitter fra bakkestasjoner plassert på Svalbard, Jan Mayen og Antarktis. På Svalbard har Norge verdens største nedlastingsstasjon for satellitter i polar bane. Norge er rett og slett nasjonen med nest flest bakkestasjoner i prosjektet, etter Frankrike.

Multinasjonale forpliktelser. Med bakkestasjoner som understøtter et multinasjonalt prosjekt følger forpliktelser. Nasjonal sikkerhetsmyndighet følger opp sikkerhetsarbeidet i Norge i samarbeid med Norsk Romsenter, det Europeiske Romfartssenteret og EU. Det er et omfattende arbeid som krever nasjonal og internasjonal koordinering.

– Særlig tett samarbeider vi med Norsk Romsenter, som er nasjonal koordinator i prosjektet, sier seniorrådgiver Kjetil Birkeland Daatland. I fjor besøkte han blant annet bakkestasjonen Troll i Antarktis.

– Feltturen til Troll var sentral for sikkerhetsgodkjenningen av stasjonen, sier Daatland. Her jobbet han med å koordinere en tverrfaglig sikkerhetsinnsats i samarbeid med Norsk Romsenter, EU og den Europeiske Romfartsorganisasjonen.

Et samvirkeprosjekt. Nasjonal sikkerhetsmyndighet deltar i interdepartementale forum. Internasjonalt gir vi råd til EU og den europeiske romfartsorganisasjonen ESA. Vi bidrar med sikkerhetsekspertise innenfor blant annet internasjonale relasjoner, krypto, juridiske standarder, tilsyn, kommunikasjon og IKT.

– NSMs sikkerhetsarbeid i Galileo er et samvirkeprosjekt. I Nasjonal sikkerhetsmyndighet har dette vært et samlet løft på tvers av avdelinger og seksjoner, og nasjonalt samarbeider vi tett med Norsk Romsenter som har en helt sentral rolle innenfor all romvirksomhetsarbeid. Det gir resultater når det kommer til sikkerhet, sier seniorrådgiver Kjetil Birkeland Daatland. ‹

FAKTA

EUROPEISK STORINDUSTRI

Satellittnavigasjons-systemet Galileo er Europas største fellesindustrielle prosjekt. Norsk romindustri drar inn cirka 6 milliarder kroner årlig, og er i ferd med å passere norsk skog som næring. Sikkerhet er en forutsetning, og gir tillit til at Norge kan være med på prosessene.

30

30 Galileo-satellitter i bane rundt jorden skal fra 2018 gi navigasjonssignaler til jorden, i tillegg til amerikanske GPS. Trafikken til og fra satellittene må sikres.

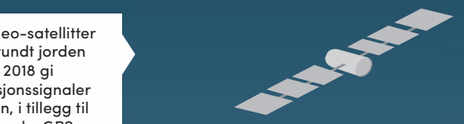
GOD SIKKERHET GIR GEVINSTER

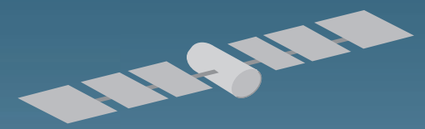
Som et land utenfor EU, men fullt innenfor satellittnavigasjonsprogrammet (Galileo), er det viktig å være blant de beste til å bidra faglig og for å sikre at de sikkerhetsmessige forpliktelsene som programdeltagelsen innebærer ivaretas på en god måte, sier Steinar Thomsen ved Norsk Romsenter.

– Det er viktig for å få innflytelse i programmet og for å bidra til at Norge og norsk industri får like vilkår som EUs medlemsland. NSMs bidrag inn i arbeidsgruppene på et tidlig tidspunkt hvor regelverkene skapes er viktige siden Norge ikke deltar i noen av EUs mer politiske organer.

Akkreditering av de norske Galileobakkestasjonene er nødvendig for at de skal få en fullverdig operativ status. Det er først da vi får utløst verdien av de investeringene som er gjort, og bakkestasjonene kan gi vesentlige bidrag til at systemet får den ytelsen som er spesifisert.

30 Galileo-satellitter i bane rundt jorden skal fra 2018 gi navigasjonssignaler til jorden, i tillegg til amerikanske GPS. Trafikken til og fra satellittene må sikres.





SIKKERHET I VERDENSROMMET

Hva? Nasjonal sikkerhetsmyndighet jobber med å styrke sikkerheten for romvirksomheten.

Hvorfor? Vi er alle avhengige av at satellittsignalene fra rommet fungerer, og ikke blir satt ut av spill.

Hva har vi gjort? Nasjonal sikkerhetsmyndighet (NSM) er tillagt en særlig oppgave knyttet til oppfølgingen av sikkerhetsarbeidet i de europeiske satellittprogrammene, herunder deltakelse i Galileos sikkerhetsorganer, oppfølging av avtaler om utveksling av sikkerhetsgradert informasjon, gjennomføring av leverandørklarering av norske selskaper som deltar i programmet og sikkerhetsmessig godkjenning av infrastruktur på norsk territorium.

Signalene fra satellittene kan blant annet du og jeg bruke til navigasjon og stedsplassering på mobiltelefonen. I tilllegg vil myndigheter, eks: politi og brannvesen, gis signaler med ekstra beskyttelse. Trafikken må sikres.

Tre norske bakkestasjoner tar ned signaler fra satellittene og videresender dem til EU. En av dem sørger i tillegg for å laste opp data fra EU til satellitten. Sikkerheten ved bakkestasjonene og trafikken til og fra må sikres.

ØKT SATSING GIR RESULTATER

NSM skal forebygge alvorlige angrep mot samfunnskritisk infrastruktur og informasjon, varsle om alvorlige angrep, trusler og sårbarheter og koordinere responsen i forbindelse med alvorlige dataangrep. Oppdraget fortsetter å øke i omfang.

2012 VAR ET REKORDÅR for håndtering av alvorlige saker ved operasjonssenteret til NSM på Bryn i Oslo, og 2013 lå på omtrent samme nivå. Det reflekteres også i at NorCERT-funksjonen var et erklært satsingsområde i statsbudsjettet for 2013. Ved slutten av året har NSM håndtert 50 alvorlige saker, noe som inkluderer både nye saker for året, og saker som har krevd oppfølging over lengre tid.

Det totale antallet saker var betydelig høyere i 2013 enn året før, på nærmere 16 000 saker. Det er særlig innrapportering av infiserte nettsider som driver denne utviklingen.

Å forebygge og håndtere digital spionasje mot Norge er en prioritert oppgave i NSM. I 2013 har NSM vært involvert i håndteringen av en rekke forsøk på målrettede spionasjeoperasjoner. NSM har flere ganger fortalt om hvordan dette rammer mange ulike sektorer i samfunnet, for eksempel myndigheter, forsvarsindustri, olje- og gass, og telekom. Med den nasjonale CERT-funksjonen er NSM i en unik posisjon til både å danne seg et helhetlig bilde og varsle mulige utsatte virksomheter.

Tett samarbeid. I 2013 har NSM i økende grad samarbeidet tettere med andre sektorvise responsmiljøer. I fjor ble det etablert IKT-responsmiljøer blant annet i finanssektoren. FinansCERT er sammen med IKT-responsmiljøene i helsesektoren, universitetsmiljøene og i forsvarssektoren en viktig samarbeidspartner. Disse spesialiserte miljøene gir NorCERT uvurderlig informasjon og hjelper til med å danne et overordnet bilde. Også sektor-CERTene gir uttrykk for å være fornøyde med samarbeidet med NorCERT.

– NSMs folk er positive og imøtekommende, og vi føler at vi får støtte i etableringen av FinansCERT. Jeg hadde også gleden av å hospitere hos NorCERT en uke før jul, noe jeg er sikker på vil bidra til at vi kan jobbe enda bedre sammen i 2014. For oss er det viktig å få informasjon fra NorCERT som vi kan dele med finansnæringen, vårt mantra er åpenhet og deling, sier Morten Tandle i FinansCERT.

Arbeidet fortsetter. Å forebygge spionasje er en heldagsjobb og mer til. Stadig flere nettsider blir kompromittert. Som det har blitt påpekt flere ganger tidligere, er det ikke lenger utelukkende mindre nettsider som utsettes for dette. Motivet er gjerne å tilrettelegge for økonomisk kriminalitet, for eksempel spredning av banktrojanere. Det er derfor attraktivt å kompromittere store og kjente nettsider med mange besøkende. Det innebærer et potensielt veldig stort skadeomfang. ‹

FAKTA

HÅNDTERING AV DATAANGREP

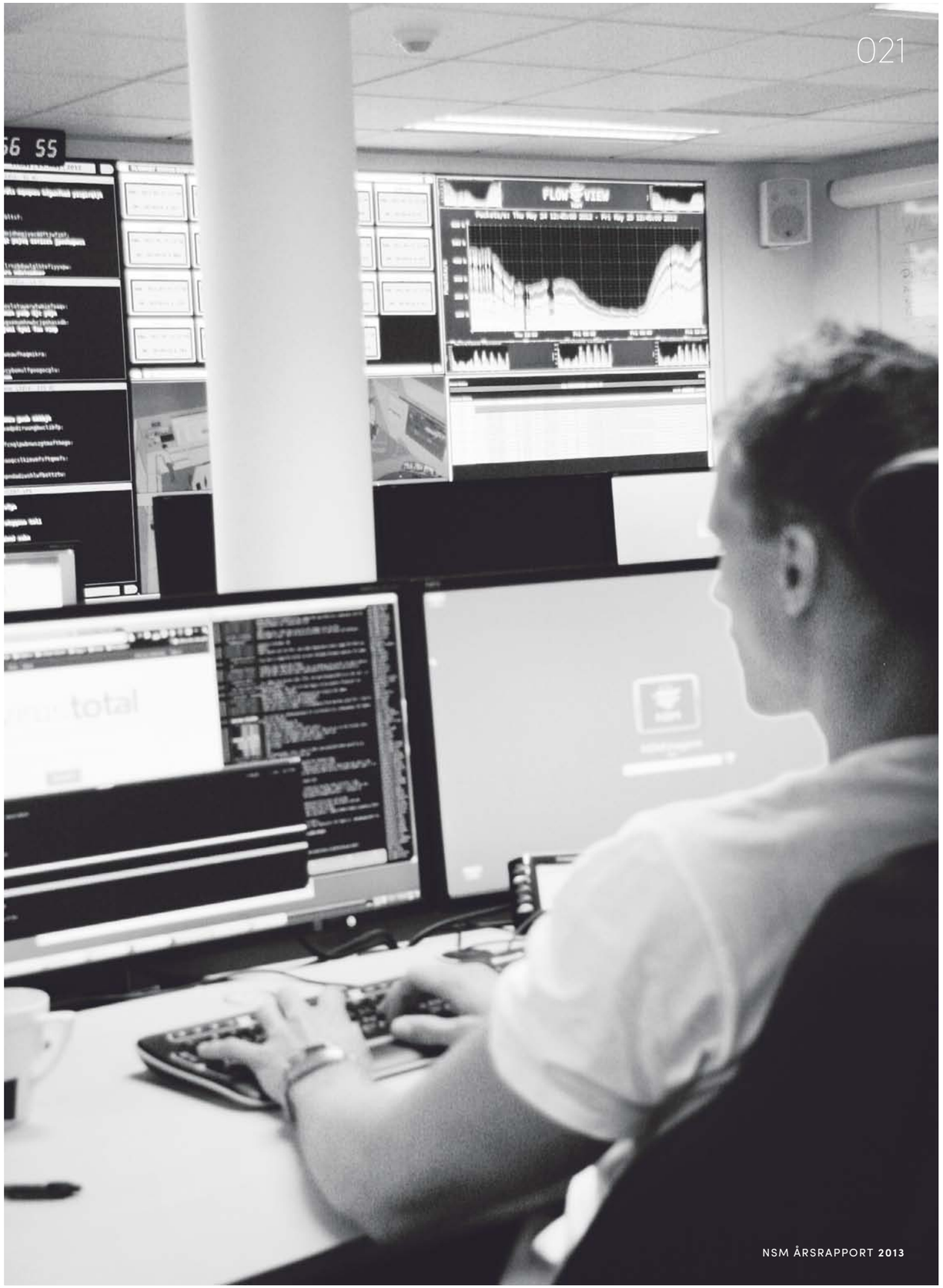
3901

3901 saker ble håndtert i 2013 i operasjonssenteret i Nasjonal sikkerhetsmyndighet. Håndteringen gjøres ved varsling, dialog, analyse og bistand.

Hva? Nasjonal sikkerhetsmyndighet håndterer koordineringen av alvorlige digitale angrep mot Norge.

Hvorfor? Antallet dataangrep stiger stadig, og kan true både økonomi, velstand og kritiske samfunnsfunksjoner.

Hva har vi gjort? Håndtert en økende mengde dataangrep, og bygd opp kapasiteten på nasjonalt nivå.

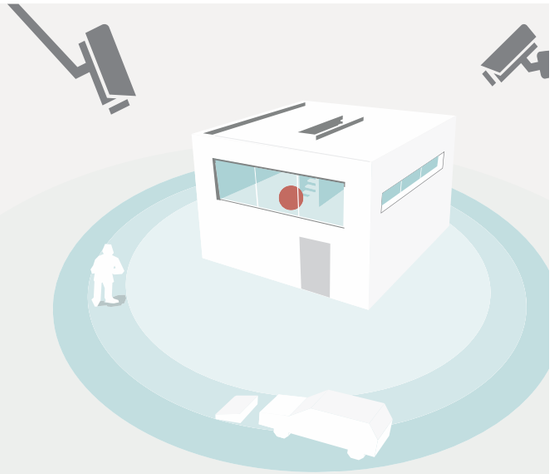


NÅR HVER METER TELLER

Først – et smell. Så fyker splintene gjennom lufta og borer seg gjennom alt som er i veien. – Hver meter teller når det gjelder å sikre bygg og installasjoner mot terror og sabotasje, sier ekspertene på objektsikkerhet i Nasjonal sikkerhetsmyndighet. I fjor gav de råd til nærmere 100 virksomheter.

HVORDAN SIKRE BYGG OG INSTALLASJONER?

- Kjenn dine verdier, og hva som må sikres spesielt.
- Bygg lag på lag med sikkerhet, begynn innenfra og jobb deg utover.
- Vurdér sikkerhetstiltak tilpasset det du skal sikre. Noen stikkord: Sikre rom. Adgangskontroll. Overvåkingskamera. Strøm inn og ut til kritiske installasjoner. Betongbarrierer mot bombebiler. For å nevne noe. Alle sikringstiltak må være effektive, funksjonelle, og ikke mer inngripende enn nødvendig.



TERRORAKSJONEN 22. juli 2011 viste med all tydelighet at sikkerhet handler om hvordan vi sikrer våre mest kritiske bygg og installasjoner mot terror og sabotasje. Angrepet mot In Amenas i fjor viste at internasjonal olje- og gassindustri er blitt et attraktivt mål for terrorister, og at også norske interesser er truet.

Objektsikkerhet har vært et satsingsområde for Nasjonal sikkerhetsmyndighet også i 2013. I fjor ga fire rådgivere til sammen 1692 timer med råd og veiledning, til sentrale norske virksomheter i alle sektorer.

Falsk trygghet. – Vi har blant annet funnet kjøretøysbarrierer som ikke har holdt det de har lovet. Mangel på forståelse og bestillerkompetanse har gjort at organisasjoner har endt opp med å kjøpe inn feil produkter, som igjen har ført til bortkastede sikkerhetstiltak. De har rett og slett kjøpt seg falsk trygghet, sier Håvard Walla.

Arbeidet med objektsikkerhet har blitt intensivert de siste årene, etter at en ny forskrift kom i 2011. I løpet av 2013 har de fleste sektorene pekt ut til sammen flere hundre skjermingsverdige objekter, altså objekter som trenger spesiell beskyttelse mot sabotasje og terror.

Hacking av kontrollsystemer. De fleste tenker tiltak mot bilbomber og terror når det gjelder objektsikkerhet. Men et objekt slik det defineres i sikkerhetsloven kan være så mangt. Det kan være en server, et bygg, en pumpe, eller en node for datatrafikk. Felles er at det vil kunne medføre stor skade for nasjonal krisehåndtering, forsvar av landet, samfunnsviktige funksjoner, miljøet eller befolkningen dersom objektene blir satt ut av spill eller brukes ulovlig av andre. Og sammenhengen mellom fysiske objekter og logiske objekter er glidende, forteller Håvard Walla og Bjørn Egeland.

– Det hjelper for eksempel ikke å ha en stor fin lås hvis du kan hacke deg inn på adgangskontrollsystemet og gi deg selv tilgang, sier Bjørn Egeland.

For å sikre bygg og installasjoner, må du først finne ut hva som faktisk trenger sikring.

– Verdivurdering, og det å få folk til å tenke helhetlig og i sammenhenger, er helt vesentlig. Hvis du ikke vet hva du skal sikre, kan du ende opp med å bruke masse penger på sikringstiltak, men det hjelper ikke, legger Håvard Walla til.

En sektor som har gjort en betydelig innsats i 2013, er helsesektoren.

– Helsesektoren er vant til å håndtere vanskelige situasjoner. De har tatt grep, og ligger ganske langt fremme i sikringsarbeidet. De har jobbet systematisk, og resultatene viser seg nå, sier Håvard Walla. ‹

FAKTA

SKJERMINGSVERDIGE OBJEKTER

Skjermingsverdige objekter er i følge sikkerhetsloven objekter som har betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket, betydning for kritiske funksjoner for det sivile samfunn, symbolverdi, og mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse.

OBJEKTSIKKERHET

Hva? Nasjonal sikkerhetsmyndighet gir råd og fører tilsyn med at sikkerheten knyttet til skjermingsverdige objekter, objekter som må sikres spesielt mot sabotasje og terror, er god nok.

Hvorfor? Bygg og installasjoner må beskyttes bedre mot spionasje, sabotasje og terror. Beskyttelsestiltak er vesentlig for å motvirke eller redusere effekten av eventuelle anslag eller angrep.

Hva har vi gjort? Gitt 1692 timer med råd og veiledning til norske virksomheter i 2013.

Foto: Øivind Haug

ET KONSTRUKTIVT SAMARBEID

For oss er det å verne om liv og helse sentralt på alle områder, fra å sikre rent drikkevann, trygg mat, godt strålevern, godt smittevern og en god primær- og spesialisthelsetjeneste, ikke minst akuttmedisinsk beredskap, sier departementsråd Bjørn-Inge Larsen i Helse- og omsorgsdepartementet.

LARSENS DEPARTEMENT har det overordnede ansvaret for helse- og omsorgsberedskapen i Norge.

–Sektoren har stor bevissthet knyttet til sin rolle ved ulykker og akutte hendelser. Sektoren arbeider systematisk med beredskapsplaner for å være forberedt på uforutsette hendelser. Krav om å ha en god helseberedskap har vært lovpålagt siden helseberedskapsloven ble vedtatt i 2000.

– Sikkerhetsloven og objektsikkerhetsforskriften har et litt annet perspektiv enn det vi vanligvis arbeider med, og vi kom nok noe sent i gang med å peke ut skjermingsverdige objekter. I 2013 tok departementet tak i dette på en mer kraftfull måte og involverte i større grad aktuelle virksomheter i egen sektor i et samarbeid med Nasjonal sikkerhetsmyndighet.

Økt trygghet. – Jeg tror at vi gjennom denne prosessen har fått en større gjensidig forståelse for hva som er forventingen til oss og hva vi må levere. Fra vår side har vi opplevd en konstruktiv dialog med NSM og aktørene i sektoren, som har gjort at vi har kunnet arbeide effektivt med objektsikring i vår sektor, sier Larsen.

– Hvordan har dere samarbeidet med Nasjonal sikkerhetsmyndighet?

– Tidlig i 2013 inviterte vi ekspertene fra Nasjonal sikkerhetsmyndighet til oppstartmøte med det vi oppfattet som aktuelle aktører, objekteiere, i vår sektor. Formålet med dette var å skape en felles forståelse av hva objektsikkerhetsforskriften krever av oss som departement og objekteiere.

Nasjonal sikkerhetsmyndighet har veiledet vår sektor i vårt arbeid med skadevurderinger og vurderinger knyttet til utpeking av skjermingsverdige objekter. Dette samarbeidet ga oss økt trygghet om våre konklusjoner før innmelding til Nasjonal sikkerhetsmyndighet i desember 2013.

Innsikt og forståelse. – *Hvordan har samarbeidet med Nasjonal sikkerhetsmyndighet fungert, og hva er det viktigste dere har fått av leveranser fra direktoratet?*

– Utgangspunktet har hele tiden vært klart. Helse- og omsorgsdepartementet har ansvaret for å følge opp objektsikkerhetsforskriften i vår sektor. Medarbeiderne fra NSM har gjennom hele 2013 deltatt med veiledning og avklaringer. Vi opplever at NSM i dette løpet er blitt mer konkret i sin veiledning. Vi opplever også at NSM er blitt mer offensiv og i større grad deler av sin spisskompetanse. Dette har gitt oss økt innsikt og forståelse, og ikke minst gitt oss en mulighet til å arbeide mer effektivt med disse problemstillingene sier Bjørn-Inge Larsen.

– Avslutningsvis vil jeg benytte anledningen til å berømme samarbeidet med tilsynsmyndighetene og aktørene i egen sektor. Alle har bidratt til at vi som sektor har økt vår kompetanse på dette området, sier Bjørn-Inge Larsen. ‹

Bjørn-Inge Larsen er departementsråd i Helse- og omsorgsdepartmentet.

Foto: Helse- og omsorgsdepartementet/Bjørn Stuedal

FORENKLING AV SIKKERHETSKLARERING I ALTINN

Prosessen med å få sikkerhetsklarering skal bli enklere. Snart blir det mulig å fylle ut opplysningene som trengs i en elektronisk personopplysningsblankett.

HVERT ÅR sikkerhetsklareres over 30 000 personer av klareringsmyndigheter. Så langt har dette vært en manuell prosedyre hvor hver person sender inn opplysninger om seg selv på en personopplysningsblankett. I 2013 inngikk NSM en avtale med Altinn som vil gjøre det mulig å fylle ut og levere blanketten digitalt via altinn.no.

– Dette er en viktig milepæl for oss. I tråd med regjeringens digitaliseringsprogram ønsker vi å ha en større grad av elektronisk behandling, der det er mulig. Noen av de 30 000 som årlig sikkerhetsklareres må fortsatt fylle ut deler av blanketten på papir, men de fleste opplysningene kan rapporteres elektronisk når den nye tjenesten er realisert i Altinn, sier Carsten Rapp, avdelingsdirektør for Sikkerhetsstyring i NSM.

Løsning med høyere sikkerhet.
Et samarbeid med Altinn kan gi flere positive effekter i årene fremover.

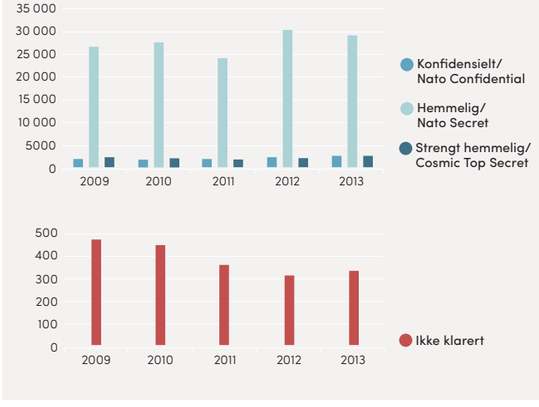
– Gjennom et samarbeid kan vi få avklart muligheter for å utvikle Altinn, slik at løsningen på sikt kan håndtere gradert informasjon i henhold til sikkerhetsloven. Det kan også være nyttig for andre å ha tilgang til en løsning med høyere sikkerhet, sier Rapp.

I henhold til fremdriftsplanen vil det nye systemet testes utover høsten for å være klar til bruk i januar 2015. ‹

Carsten Rapp fra NSM og Kjersti Lauritzen fra Altinn er fornøyd med å ha innledet et samarbeid som vil gi gevinster for alle som skal ha sikkerhetsklarering.

Foto: Brønnøysundregisteret/Hege Sæthre Lind

Antall sikkerhetsklareringer utført av klareringsmyndigheter



FAKTA

SIKKERHETS-KLARERINGER

35 000

Over 35 000 klareringssaker blir behandlet i løpet av et år i Norge

Hva? Nasjonal sikkerhetsmyndighet innhenter alle personopplysninger som brukes til sikkerhetsklareringer gjennom personopplysningsblanketten.

Hvorfor? Personer som skal behandle sikkerhetsgradert informasjon må klareres, for å sikre at statshemmeligheter ikke kommer på avveie.

Hva har vi gjort? Nasjonal sikkerhetsmyndighet har inngått en avtale med Altinn for å effektivisere klareringsprosessen.

KRYPTERT MOBILTELEFONI-LØSNING PÅ PLASS

I oktober 2013 skrev flere medier at et nytt krypteringssystem for mobiltelefoni er etablert i Norge, slik at kommunikasjonen mellom blant annet politikere skal være avlyttingssikkert.

NSM HAR i lang tid jobbet med etableringen av det avlyttingssikre systemet. Løsningen er basert på blåtannfunksjonalitet som utfører talekryptering.

Systemet skal gjøre det vanskeligere for utenlandske stater å få kjennskap til hva blant annet norske politikere snakker om.

– Det gjelder ikke minst statsrådene, for å sikre oss at den informasjonen vi gir oss imellom, blir tryggere håndtert, sa justis- og beredskapsminister Anders Anundsen til NTB etter lanseringen.

NSM har også publisert generelle råd om sikrere bruk av mobiltelefoni.

- Tenk over hva du bruker mobiltelefonen til, og hvor du bruker den.
- Ikke bruk mobiltelefonen til å utveksle sikkerhetsgradert informasjon.
- Unngå å bruke mobiltelefonen til å utveksle annen informasjon uvedkommende ikke skal ha tilgang til.
- Ikke ta mobiltelefonen med inn i rom der det diskuteres sikkerhetsgradert informasjon eller informasjon uvedkommende ikke skal ha tilgang til. Be andre møtedeltakere om å legge fra seg mobiltelefonen før møtet starter.
- Pass godt på mobiltelefonen! Ikke la uvedkommende få tilgang til den. Benytt skap for sikker oppbevaring av mobiltelefon dersom dette finnes.
- Slå av blåtannfunksjonen i mobiltelefonen når denne funksjonen ikke er i bruk.
- Ta kontakt med din lokale sikkerhetsleder for å få råd samt veiledning i mobiltelefonoppsett.
- Sørg for at virksomheten har regler for sikker mobilbruk og bidra til at disse følges.

Vær spesielt varsom på reise i utlandet. ‹

FAKTA

SIKRERE MOBIL-TELEFONER

Hva? Nasjonal sikkerhetsmyndighet jobber med å finne sikrere løsninger for mobiltelefoni.

Hvorfor? Vi er alle avhengig av mobiltelefonen, men hva hvis vi skal si noe andre ikke skal høre? Mobiler kan avlyttes på flere forskjellige måter.

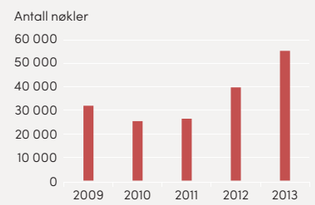
Hva har vi gjort? NSM har etablert en sikrere mobilløsning for blant annet statsråder og toppledere.

Anders Anundsen (FrP) er justis- og beredskapsminister.

Foto: Thomas Haugersveen/ Statsministerens kontor

Kraftig økning i produksjon av kryptonøkler

Antallet produserte kryptonøkler, som gjør det mulig å kommunisere sikkert, har økt kraftig de siste årene. I 2013 produserte og distribuerte NSM totalt 58 539 elektroniske nøkler.



TILSYN STYRKET SIKKERHETEN

Tilsyn er et hovedsatsningsområde for Nasjonal sikkerhetsmyndighet. I fjor gjennomførte direktoratet blant annet tilsyn i Kulturdepartementet.

TILSYNET har bidratt til å styrke sikkerheten, sier assisterende departementsråd, Henning Henriksen.

– Et tilsyn oppfattes alltid som krevende. Det føles som å komme opp til eksamen, sier han.

Det var god kontakt mellom Kulturdepartementet og Nasjonal sikkerhetsmyndighet i forkant, slik at departementet fikk oversendt relevant informasjon, sier Henriksen, som mener tilsynet ble gjennomført på en effektiv og profesjonell måte.

– Personene som representerte Nasjonal sikkerhetsmyndighet fremstod som godt forberedt, og gjennomførte både intervjuer og kontroller på en god og tillitvekkende måte. Måten tilsynet ble gjennomført på har bidratt til å styrke, utvikle og forbedre den forebyggende sikkerhetstjenesten i Kulturdepartementet. God dialog under tilsynet har også gjort det lettere for oss å ta kontakt med Nasjonal sikkerhetsmyndighet for råd og veiledning i andre saker, sier Henning Henriksen i Kulturdepartementet. ‹

Henning Henriksen er assisterende departementsråd i Kulturdepartementet.

Foto: Kulturdepartementet

FAKTA

TILSYN

23

23 stedlige tilsyn ble gjennomført i 2013. Målet er å øke tilsynsvirksomheten i årene fremover for å styrke sikkerheten hos flere virksomheter.

Hva? Nasjonal sikkerhetsmyndighet fører tilsyn med virksomheter som er underlagt sikkerhetsloven.

Hvorfor? Tilsyn er et viktig virkemiddel for å hjelpe norske virksomheter til å styrke informasjons- og objektsikkerheten.

Hva har vi gjort? Nasjonal sikkerhetsmyndighet gjennomførte i fjor 23 stedlige tilsyn i Norge og i utlandet.

TWITTER-KVITTER OM SIKKERHET I 2013

11. januar

Alle bør avinstallere programmet Java fra datamaskinene sine. Det anbefaler Nasjonal sikkerhetsmyndighet. Hør Alltid Nyheter 1630

...

Ida Creed/@idacreed

18. februar

For første gang: En samlet trusel- og sårbarhetsvurdering fra E-tjenesten, NSM og PST. Gratulerer!

...

Morten Irgens/@mirgens

19. februar

Av og til arbeider jeg mer med usikkerhet enn sikkerhet!

...

Roar Thon/@Secdefence

20. mars

Må si det jobber mange dyktige og hyggelige folk ved Nasjonal sikkerhetsmyndighet. #NSMKonf viser at tjenesten er i utvikling og på rett vei

...

Anders Romarheim/ @Andersrom

1. juli

«Informasjon som er på nett er allerede på avveie. Oppfør deg deretter!» blogg.nsm.stat.no/archives/3927 Klokt fra Nasjonal sikkerhetsmyndighet

...

Fredrik Matheson/@movito

12. august

Sikkerhet bør ikke sees på som en utgift. I beste fall er det en investering. I det minste er det en forsikring!

...

Roar Thon/@Secdefence

LEVERANSER FRA A TIL Å

Nasjonal sikkerhetsmyndighet leverer en rekke produkter til samfunnet i løpet av et år. Her er et utvalg.

Analyse: Vi leverer ukentlig sikkerhetsanalyser til Justis- og beredskapsdepartementet, Forsvarsdepartementet, og flere av våre nære samarbeidspartnere.

Foto fra lufta: Skal du opp og ta bilder fra fly? Nasjonal sikkerhetsmyndighet gir lisens til foto fra lufta. Grunnen er behovet for å skjerme detaljer rundt skjermingsverdige objekter.

Inntrengingstesting: Er det mulig å hacke seg inn i datasystemene dine? Vi tester sikkerheten i datasystemer. Testingen er nøye avtaleregulert mellom oss og virksomhetene det gjelder.

Hendelseshåndtering: Operasjonssenteret i Nasjonal sikkerhetsmyndighet, NorCERT-funksjonen, håndterer over 3000 saker i løpet av et år. Senteret varsler og håndterer alvorlige dataangrep.

Konferanser: Vi arrangerer både alene og sammen med andre flere større konferanser om sikkerhet. Den årlige sikkerhetskonferansen samlet i fjor over 500 deltakere.

Kryptering: Kryptering er bokstavelig talt nøkkelen du sikrer informasjonen din med. Vi produserer og distribuerer kryptonøklene som brukes til sikkerhetsgradert informasjon i Norge, og utvikler nye kryptoløsninger.

Leverandørklarering: Private selskaper trenger ofte tilgang til sikkerhetsgradert informasjon for å levere varer og tjenester blant annet til Forsvaret. Vi gir selskapene leverandørklarering.

Råd og veiledning: Nasjonal sikkerhetsmyndighet bruker tusenvis av timer i året på råd og veiledning både på datasikkerhet, personellsikkerhet, objektsikkerhet og en rekke andre fagområder.

Sertifisering: Gjennom ordningen SERTIT sertifiserer vi flere IT-sikkerhetsprodukter i løpet av et år.

Sikkerhetsklareringer: Vi innhenter personopplysninger til om lag 35 000 saker om sikkerhetsklarering årlig. NSM er også klageinstans for klareringsvedtak fattet av andre klareringsmyndigheter.

Sikkerhetsgodkjenninger: Datasystemer som skal behandle sikkerhetsgradert informasjon må ha sikkerhetsgodkjenning av Nasjonal sikkerhetsmyndighet.

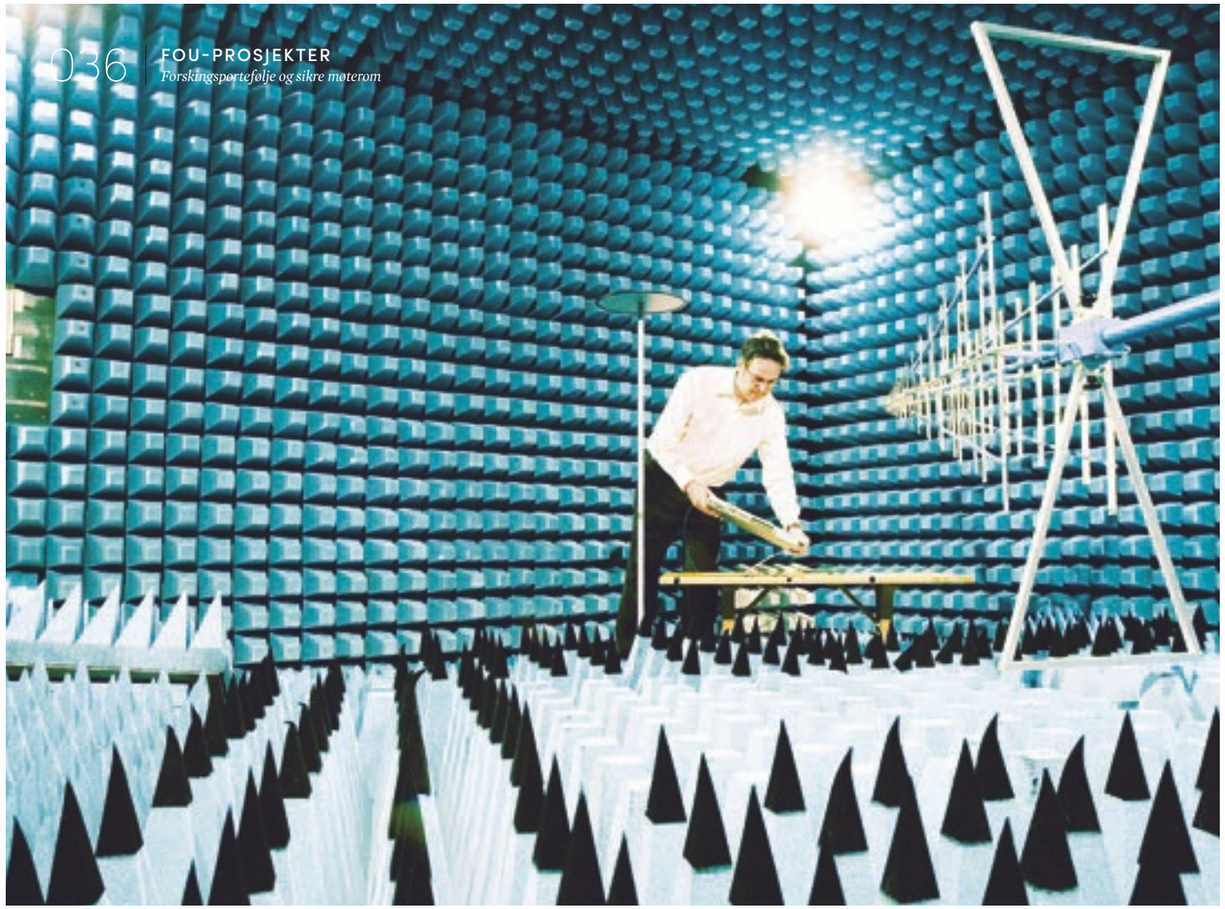
Sikkerhetskultur: Virksomheten din har allerede en sikkerhetskultur, spørsmålet er om den er god eller dårlig. I fjor leverte Nasjonal sikkerhetsmyndighet 95 foredrag over hele landet om sikkerhetskultur.

Tekniske sikkerhetsundersøkelser: Er møterommet ditt sikret godt nok mot avlytting? Vi sikrer møterom og andre sensitive rom mot spionasje og avlytting.

Tilsyn: Nasjonal sikkerhetsmyndighet fører tilsyn med over 20 norske virksomheter i løpet av et år.

Undervisning: Kompetanse er en nøkkel til styrket sikkerhet. Vi arrangerer et bredt undervisningstilbud på sikkerhet i løpet av året.

Varslingssystem for digital infrastruktur (VDI): Vi leverer et sensornettverk for å avdekke forsøk på datainnbrudd mot kritisk infrastruktur på tvers av sektorer. VDI er kort fortalt en innbruddsalarm for AS Norge.



Illustrasjon: ProfiShield, EMP-Tronic AB

STOR FORSKINGSPORTEFØLJE

Han styrer totalt 27 forskings- og utviklingsprosjekt i Nasjonalt tryggingsorgan. NSM er ein innovasjonsdriven organisasjon som alltid søkjer ny kunnskap, seier prosjektdirektør Christian Reusch.

NASJONALT TRYGGINGSORGAN (NSM) har ein portefølje på 27 kontinuerlege forskings- og utviklingsprosjekt. Ni ulike prosjekt blei avslutta i 2013, mens ni nye er sette i gang på nyåret 2014.

– Blant dei prosjekta vi har starta opp, blir det forska på fleire spennande problemstillingar. Nokre av prosjekta NSM driv er graderte og vi kan derfor ikke informere om dei offentleg, men innhaldet i disse er svært viktige for dei det gjeld. Andre forskingsprosjekt er ugraderte og mange ulike miljøer vil kunne ta lærdom av desse etter kvart, seier Christian Reusch, prosjektdirektør i NSM.

Han fortel at NSM tradisjonelt har hatt ein forskingsportefølje som er teknologisk driven og retta.

– No begynner vi å få større breidd i forskingsporteføljen vår, og det er svært positivt. Forskingsprosjekta som går i samarbeid med SIMLab i Trondheim og Bergen arkitektskole er eksempel på dette. Vi er eit relativt lite forskingsmiljø, men det blir også drive forsking i organisasjonen utanom sjølve forskingsprosjekta, understrekar Reusch.

Byggjer opp. Etter at NSM blei etablert som eige direktorat med utspring frå tryggleiksstaben i Forsvarets overkommando i 2003, mista organisasjonen ein del av Forsvarets forskingsportefølje.

– Vi har etter kvart fått etablert ein eigen forskingsportefølje med ein eigen handlingsplan for FoU. I tillegg til våre eigne prosjekt er vi involverte i ei lang rekkje forskingsprosjekt som vi ikkje leier sjølve, mellom anna Forsvaret. Vi har òg viktige samarbeidspartnarar i Forsvarets forskingsinstitutt, universitet og høgskular, fortel Reusch, som understrekar at NSM har ein innovasjonsdriven organisasjon som alltid søkjer ny kunnskap.

– Forskinga vår skal medverke til å sikre samfunnsverdiar, eit meir robust samfunn, poengterer han. ‹

Totalt 27 forskings- og utviklingsprosjekt blir styrte av prosjektdirektør Christian Reusch.

KVEN HØYRER KVA DU SEIER?

I moderne kontorlokale sit dei tilsette tett, gjerne i opne landskap med store vindaugsflater. Kva gjer du dersom du skal dele sensitiv informasjon?

NSM, som mellom anna jobbar med sikring og godkjenning av rom for gradert tale, har drive eit prosjekt for å finne fram til eit avlyttingssikkert møterom. Rommet eignar seg der ein ikkje har tilstrekkeleg kontroll med omgivnadene.

– Det var fleire krav til det avlyttingssikre møterommet, mellom anna at det skulle kunne godkjennast for hemmeleg. Det skulle vere modulbasert og fleksibelt og kunne etablerast som eit «rom i rommet». Rommet skulle i tillegg til å ha best mogleg akustisk demping også vere robust mot elektroniske angrep og lekkasjar, fortel kommandørkaptein Vidar Kristiansen, seksjonssjef for tekniske undersøkingar.

Ope landskap. Skjerma møterom er ikkje av ny dato – det første Faraday-buret blei utvikla allereie i 1836. Men mykje har skjedd sidan den tid. Den rivande teknologiske utviklinga medfører stadig nye utfordringar når det gjeld deling og vern av sensitiv informasjon.

I moderne kontorlokale sit dei tilsette tett, gjerne i opne landskap med store vindaugsflater. Mindre stillerom er relativt vanlege, men desse romma gir ikkje på langt nær den akustiske dempinga og det vernet som trengst.

Prosjektet førte fram til ei «rom i rommet»-løysing med vern mot akustisk, elektronisk og visuell avlytting. Konseptet krev ikkje spesielle bygningstekniske tiltak, utover generell fysisk sikring.

Kristiansen vurderer løysinga som spesielt veleigna for Forsvaret, utanriksstasjonane, departementa, andre etatar i statsforvaltninga og verksemder som treng skjerming av sensitiv informasjon. ‹

– Eit rom i rommet sikrar gradert og sensitiv informasjon, poengterer seksjonssjef Vidar Kristiansen.

STØTTER FORSKING OM OBJEKTSIKRING

Korleis kan byar, bygg og konstruksjonar vernast mot bomber og terrorangrep? For å undersøkje dette nærmare løyvde Nasjonalt tryggingsorgan (NSM) i 2013 10 millionar kroner over ni år til SIMLab ved NTNU i Trondheim.

SENTERET vil jobbe med eit prosjekt som granskar korleis ulike typar sikringsmateriale og konstruksjonar greier seg ved bombeeksplosjonar og andre typar belastning. Senteret blir støtta med 2 millionar i 2013 og deretter 1 million kroner i året over ein åtteårsperiode fram til 2022.

Betre sikringstiltak. – Prosjektsamarbeidet med SIMLab ved NTNU vil gi NSMs miljø for objektsikring og fysisk sikring tilgang til vitskaplege testar av høgaste internasjonale kvalitet. Eit slikt prosjekt vil danne grunnlag for utvikling av betre og meir tilpassa sikringstiltak for verdiar som må vernast, seier avdelingsdirektør Carsten Rapp i avdeling for tryggingsstyring. Han legg til at SIMlab, eller Structural Impact Laboratory, er eit leiande fagmiljø innan ingeniørteknikk.

NSM har ansvaret for å gi råd om, og føre tilsyn med, objektsikring i Noreg. Ved å delta i prosjektet vil NSM ha høve til å styre og bestille ulike typar testar og gjennom dei få stadfesta om dei tiltaka vi tilrår, verkar etter formålet. Direktoratet vil blant anna kunne bruke testane til å verifisere korleis ulike sikringstiltak og materiale taklar fysiske påkjenningar som eksplosjonar, prosjektil, kollisjonar og anna. Testane blir òg brukte til å utvikle og forbetre verktøy for datasimulering.

Bombelast. Prosjektet er delt inn i to fasar, og første fase inneber utvikling av ein testrigg. Testriggen kan brukast til å verifisere korleis heilt konkrete sikringstiltak fungerer når dei blir utsette for ei bombelast.

Testane vil NSM bruke både for å kunne gi konkrete råd og for å utvikle standardar. I fase to vil NSM dessutan få tilgang til alle testfasilitetar som finst i dag, og få informasjon om alle tidlegare testar. Dette gir mykje betre høve til å drive testing, og ein kan verifisere korleis forskjellige andre fysiske påkjenningar, som kollisjonar og prosjektil av definert storleik, påverkar sikringstiltak og materiale.

Også Forsvarsbygg, som NSM har eit fagleg samarbeid med om fysisk sikring, har i mange år hatt eit nært samarbeid med SIMLab, og dei kjem til å halde fram med det i åra framover. ‹

PASSORDKNEKKJARANE

Kor sikkert er eigentleg passordet ditt? Eit av forskings- og utviklingsprosjekta til Nasjonalt tryggingsorgan testar kor lett det er å knekkje passorda folk bruker.

– SVAKE PASSORD er ein gjengangar. Det seier seksjonssjef for inntrengingstesting i Nasjonalt tryggingsorgan, Jørgen Botnan. Gjennom året gjennomfører dei fleire inntrengingstestar, kontrollerte dataangrep, for å teste tryggleiken i datasystem i både sivil og militær sektor.

– Det gir god pedagogisk effekt å avdekkje reelle eksempel på svake passord som blir brukte i verksemda sine eigne informasjonssystem, seier han.

Rå kraft. Metodane for å knekkje passord blir stadig utvikla og har som fellesnemnar at dei utnyttar rå prosessorkraft. I nyare tid har fagfolk merka ei auka interesse for bruk av prosessoren i skjermkorta, som er laga for å gjere mange operasjonar samtidig. Lange passord kan dermed knekkjast dersom dei har ei oppbygging som er kjend, slik at tida det tek å knekkje dei, blir kraftig redusert.

– Passordknekking har vist seg å vere ein svært effektiv framgangsmåte for å vurdere passordstyrken til brukarane, som er ein viktig del av tryggleiken i informasjonssystem, og ikkje minst for å sørgje for riktig fokus ved opplæring av brukarane, fortel Botnan.

Auka kunnskap. Inntrengingstesting er strengt regulert i tryggingslova, og det er ingen andre enn Nasjonalt tryggingsorgan som kan gjennomføre inntrengingstesting av sikkerheitsgradert datasystem.

– Også andre som ikkje forvaltar sikkergraderte informasjonssystem, må sjølvsagt ha eit medvite forhold til verdiane dei forvaltar, og vern av dei. NSM har også mange oppdrag utanfor området til tryggingslova og treng auka kapasitet i passordknekking. Forskingsprosjektet vårt vil gi auka kapasitet og kunnskap, opplyser han.

Svak praksis. NSMs bruk av passordknekking som metode ved inntrengingstestinga har medverka til å avdekkje fleire tilfelle av svak praksis ved val av passord i samfunnskritisk og sikkergradert IKT-infrastruktur. Tilfella er funne i både militær og sivil sektor. Svake passord er med på å gjere infrastruktur sårbar for angrep.

– Hovudaktiviteten i prosjektet er å byggje opp og utvikle kapasitet for best mogleg gjennomføring av passordknekking innanfor tidsramma for inntrengingstesten. Kunnskap og erfaringar om utforming av passord som vi får i prosjektet, er viktige for å auke kvaliteten ved vidare passordtesting, og for å gi råd til verksemda.

Resultata av passordtesting gir derfor viktig tilbakemelding til systemeigaren og kan brukas til opplæring av brukarane, understrekar Botnan, som har store forventningar til dette forskingsprosjektet. ‹

FAKTA

SLIK BØR PASSORDET DITT VERE

Passordet bør innehalde minst 15 teikn og ha mellomrom eller andre spesialteikn, seier ekspertane i Nasjonalt tryggingsorgan. Ei undersøking frå NorSIS i 2012 viste at gjennomsnittsbrukaren har minimum 25 passord å halde styr på på jobb og privat. Korleis skal ein hugse alle passorda?

Eitt tips er å skrive heile setningar, men dei bør ikkje vere for enkle å gjette. Eit anna tips er å bruke passord med for eksempel forbokstavar i songar som er lette å hugse. «Jvedlsdsffvovidth» er samansett av forbokstavane i dei to første verselinjene av «Ja vi elsker». Men ikkje bruk akkurat dette passordet, då.

TRYGGLEIK I OFFENTLEG ARKITEKTUR

Terrorhandlingar retta mot offentlege bygningar har dessverre ikkje lenger berre akademisk interesse. Nasjonalt tryggingsorgan (NSM) er fagstyresmakt og skal medverke til at det blir sett i verk vernetiltak.

DERSOM TRYGGLEIK som tema kjem tidleg inn i prosessen kring nye, offentlige bygg kan ein inkludere sikringstiltak i arkitekturen på ein heilt annan måte enn om dei blir lagde på til slutt.

– Prosjektet som vi starta i fjor, er eit pilotprosjekt innan akademisk tryggleikstenking. I samarbeid med PST og Bergen arkitektskole er det sett i gang ein masterstudie med tittelen «Secure by Design», fortel Håvard Walla i seksjon for objektsikring.

Prosjektet skal munne ut i ei tospråkleg lærebok (norsk og engelsk), finansiert av NSM som vil prøve å kombinere urban arkitektur og tryggleikstenking i både norsk og internasjonal samanheng.

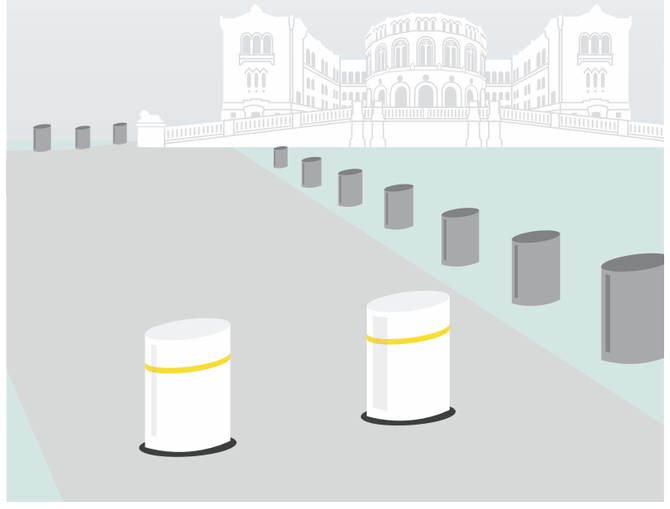
Konkrete tiltak. – Læreboka vil innehalde fotodokumentasjon som viser både gode og mindre gode løysingar i internasjonal og nasjonal samanheng. Ho vil trekkje fram prosjekt som foreslår konkrete tiltak på ulike stader, og internasjonal forsking og analyse innanfor temaet. Boka blir eit oppslagsverk i tryggleiksarkitektur og kjem ut i slutten av 2014, seier Walla.

Håvard Walla understrekar at prosjektet er viktig for å skaffe fram og gjere tilgjengeleg kunnskap om korleis tryggleik kan integrerast på ein god måte for å balansere ulike interesser ved sikring av bygg og byområde.

– Dette prosjektet vil auke kunnskapen om korleis ein kan sikre bygg og anlegg mot ulike typar tryggleikstruslar i både sivil og militær sektor. Det vil òg kunne påverke ein ny generasjon arkitektar til å tenkje på sikring av bygg og byrom, slik at både openheit og demokrati er i harmoni med sikringsbehov, seier avdelingsdirektør Carsten Rapp i Nasjonalt tryggingsorgan (NSM). ‹

SECURE BY DESIGN

- Mastergradsstudie i arkitektur gjennomført ved Bergen arkitektskole (BAS) hausten 2013
- Studiet har tittelen «Between Freedom & Security» og utforskar sikre løysingar i bygg og byrom
- Studiet er eit samarbeidsprosjekt mellom PST, NSM og BAS. Rådgivningsfirmaet COWI har også bidrege.
- Studieturer med rettleiing frå NSM og PST er gjennomført til London, Oslo og Jerusalem for å samanlikne ulike løysingsforslag for ulike situasjonar.
- NSM er ein pådrivar for gode, funksjonelle og sikre løysingar innan fysisk sikring.



AVSLØRTE SIKKERHETSSVIKT

Journalistene i Dagbladet dro i land skup etter skup med avsløringer om hvor dårlig datasikkerheten er i Norge. Etter hvert fikk de bare vondt i magen.

– UTGANGSPUNKTET var hva amatører kan finne på nett, med et minimum av kompetanse.

Åpent landskap. Knallrøde skillevegger. Nyheter som produseres til langt på natt av konsentrerte journalister. Vi er i lokalene til Dagbladet i Oslo havnelager, innerst i kroken til utvikler Ola Strømman. En hvitmalt vegg fungerer som tusjtavle.

Minimal sikkerhet. Høsten 2013 avslørte avisen hvordan sviktende datasikkerhet rammer oss alle, enten det er hjemme, på jobb eller i det offentlige rom. 2048 overvåkingskameraer lå åpent på Internett. Hvem som helst kunne kikke inn på soverommet til folk, til nattklubber og kjøpesentre, fra Internett. Brann- og beredskapsplaner for 39 kommuner lå usikret på nett. Kontrollsystemer for industrien hadde minimalt med sikkerhet. *Ble journalistene overrasket?*

– I begynnelsen, ja, men etter hvert, nei, sier Espen Sandli og Linn Kongsli Hillestad, som sammen med utvikler Ola Strømman stod bak serien.

Tabloide funn. – Til å begynne med ble vi glad for hvert skup og hvert tabloide funn vi gjorde. Etter hvert ble det mer til at vi fikk vondt i magen av hva folk gjør feil, sier Espen Sandli.

Serien startet med et tips om sensitiv informasjon som lå åpent på nett. Etter hvert fant de frem til søkeverktøyet Shodan, som leter etter usikrede porter, det vil si åpne dører og vinduer på Internett. Før de satte i gang avklarte de juridiske og etiske problemstillinger. De tastet ikke inn brukernavn og passord, og de advarte i god tid på forhånd før publisering slik at folk kunne tette sikkerhetshull. Flere saker om alvorlige sårbarheter ble ikke publisert.

Menneskelig feil. *Hvorfor gjør folk feil?*

– Det er for enkelt å bruke utstyret. Plugger du inn et webkamera, snakker det gjerne med ruteren, som så legger utstyret automatisk tilgjengelig rett på nett, sier Ola Strømman.

– Det er mye menneskelig feil, sier Linn Kongsli Hillestad.

– Private gjør ofte feilen selv. Hos mellomstore bedrifter skyldes det ofte at man stoler på en leverandør og tror man ikke har noe ansvar selv, eller at selve leverandøren gjør feil. Store selskaper er ofte seriøse på sikkerhet og har tunge kontrollsystemer, men de kjøper tjenester av underleverandører som ikke har samme grad av sikkerhet, sier Espen Sandli.

– Jeg tror det er mye slik at folk ikke gidder, sier Linn Kongsli Hillestad. Journalistene har sett flere tilfeller hvor IT-folk har varslet selskaper om sikkerhetshull, uten at noen ting blir gjort.

– Det sier noe om at da er du litt slapp, sier hun.

Positive reaksjoner. Journalistene hadde hele tiden fokus på å ikke gå for langt i hvordan de har behandlet folk og virksomheter som har vært rammet av datasvikt. Reaksjonene på serien, også hos de som har vært rammet, har vært overraskende positive, sier Espen Sandli.

– De har satt pris på at de har blitt advart, vi har fått kaffe og kaker når vi har kommet til folk. Jeg synes det er betegnende med han som drev et dataselskap, og sa at dette er kroken på døra for butikken min, men takk for at dere sa ifra. ‹

FAKTA

DETTE FANT DAGBLADET

2048 overvåkingskameraer i Norge lå tilgjengelig på nett. De fantes i private hjem, nattklubber, butikker og restauranter.

1781 printere lå tilgjengelig på nettet i Norge. Flere tusen databaser og servere gav deg alt innhold – uten å taste et eneste passord.

2500

Over 2500 styringssystemer i Norge var koblet til nett, med minimal eller ingen sikkerhet. 500 av disse kontrollerte industriell eller samfunnskritisk infrastruktur.

Funnene ble gjort i data indeksert i perioden 1. januar til 30. august 2013. Hele Dagbladets serie «Null CTRL» finner du her: www.dagbladet.no/nullctrl/

Til å begynne med ble journalistene i Dagbladet glade for hvert skup de gjorde, etter hvert fikk de bare vondt i magen. Fra venstre: Ola Strømman, Linn Kongsli Hillestad og Espen Sandli.

FIKK SIKKERHETSPRIS

Dagbladet fikk i november IT-sikkerhetsutmerkelsen Rosingprisen for sitt arbeid. Prisen deles ut av Den Norske Dataforening. – 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, heter det i følge juryuttalelsen.

7 RÅD FRA «NULL CTRL» TIL BEDRE KONTROLL:

1 Husk å endre standardpassordet

2 Benytt gode passord, og bruk forskjellige passord på forskjellige tjenester

3 Gjør en vurdering: Det er enkelt, men må utstyret være koblet til nett?

4 Vurder sikkerhet – ikke bare pris og funksjonalitet

5 Spør om råd hvis du ikke er sikker på hva du driver med – hent ekstern ekspertise om du er i tvil

6 Ikke stol blindt på eksterne leverandører, vit også hva som er ditt ansvar

7 Dobbeltsjekk alltid dine IP-adresser utenfra

DEN STORE LEKKASJESAKEN

Tapping av informasjon fra undersjøiske kabler. Knekking av kryptonøkler. Telefonavlytting av Angela Merkel og andre toppolitikere. Avsløringene i kjølvannet av Snowden-saken har ført til at datasikkerheten i Norge har blitt styrket, tror seniorrådgiver Karsten Friis ved Norsk Utenrikspolitisk Institutt (NUPI).

– KONSEKVENSENE i Norge har skjedd indirekte i form av at du har fått mer bevissthet blant folk, organisasjoner og myndigheter om hva moderne teknologi kan gjøre når det gjelder datasikkerhet og personvern.

Sjelden har en sak om datasikkerhet og overvåkning fått så stor omtale, og så store konsekvenser, på verdensbasis. Etter at den amerikanske IT-teknikeren Edward Snowden lekket store mengder informasjon blant annet til The Guardian-journalist Glenn Greenwald, har sak etter sak om avlytting og overvåkning vært på dagsordenen i månedsvis. I Norge har seniorrådgiver Karsten Friis ved Norsk Utenrikspolitisk Institutt fulgt saken tett. I disse dager leverer han sitt bidrag til en større europeisk rapport om konsekvensene ved Snowden-saken.

Sikkerhet vs. frihet. Nasjonalt tror han saken har hatt en indirekte effekt, ved at folk er blitt mer bevisste på hva som kan fanges opp på nettet.

– Økt bevissthet gjør at sikkerheten blir styrket. Flere kommer til å ha mer bevissthet rundt det å bedre sin egen sikkerhet. Selv internt i NSA blir det ikke mulig å gjøre det Snowden gjorde etter denne saken.

Et svekket omdømme. Globalt har saken først og fremst svekket USAs omdømme, tror han. Friis mener den viktigste debatten i kjølvannet av Snowden-saken er sikkerhet versus frihet.

– Det er en debatt som alle demokratiske samfunn må ta, og det er en debatt som er sentral både for NSM, PST og alle etterretningstjenester.

Og det er en debatt som det stadig vil bli mer av fremover, tror han, blant annet fordi teknologien gir så mange muligheter.

Ikke overrasket. – *Har saken hatt skader når du tenker på nasjonal sikkerhet?*

– Amerikanerne sier saken kan ha hatt stor skade for deres nasjonale sikkerhet. Det er vanskelig å vurdere, og det er avhengig av hvor mange som visste hva amerikanerne hadde kapasitet til. De fleste er overrasket over omfanget, mens de fleste eksperter ikke er så overrasket. Jeg tror ikke dette er helt nye avsløringer som er sjokkerende for eksempel for kinesere eller russere, sier Friis.

Frykt det verste. – *Hvordan bør Snowden-saken påvirke sikkerheten for virksomheter og privatpersoner i Norge?*

– Dette med å bruke kryptering er et klassisk råd. Vi må også ha alternative måter å rute datatrafikk på, og ikke bare via ett land, som Sverige. Jeg tror også man må gå noen runder på dette med datalagring. Det handler mye om bevissthet. Teknologiutviklingen går så fort, løsningene vi har i dag vil ikke holde i morgen. Man må frykte det verste, og jobbe ut fra det, sier Karsten Friis ved Norsk Utenrikspolitisk Institutt. ‹

Debatten om sikkerhet versus frihet er en debatt alle demokratiske samfunn må ta, sier Karsten Friis ved Norsk Utenrikspolitisk Institutt (NUPI).

5. juni 2013
Lekkede sikkerhetsgraderte dokumenter avslører at NSA samler telefondata om millioner av amerikanske kunder hos selskapet Verizon.

6. juni 2013
The Guardian hevder NSA har direkte tilgang til systemene til Google, Facebook, Apple og andre internettselskaper gjennom PRISM-programmet.

7. juni 2013
Guardian avslører at NSA skal ha tilgang til store mengder data fra telefon- og datanettverk gjennom verktøyet Boundless Informant.

21. juni 2013
Britiske GCHQ skal ha tilgang til å tappe fiberoptiske kabler for informasjon, i følge The Guardian.

23. juni 2013
Edward Snowden lander i Moskva, og blir sittende fast på flyplassen.

31. juli 2013
Verktøyet XKeyscore blir kjent, som skal gjøre det mulig å samle nesten alt en hvilken som helst bruker gjør på Internett.

5. september 2013
NSA og GCHQ skal være i stand til å låse opp informasjon som er kryptert, skriver The Guardian.

14. oktober 2013
Angela Merkel beskylder USA for mobilavlytting.

17. desember 2013
Norske Dagbladet har fått tilgang til Snowden-dokumenter og skriver flere saker.

RAPPORTERING FOR 2013

2013 var det første året i inneværende langtidsplanperiode for forsvarssektoren. Langtidsplanen medfører økt ambisjonsnivå for NSM, spesielt innen hendelseshåndtering, objektsikkerhet, tilsyn, kompetanse og IKT-sikkerhetsløsninger. Virksomheten fikk i 2013 et historisk stort løft i driftsbudsjettet, med en økning på over 30 prosent av budsjettet på ett år.

TALL I MILLIONER KRONER	2013	2012	2011	2010	2009	2008
Lønnsutgifter	**111,4**	88,5	81,5	78,2	77,9	71,5
Utgifter til varer og tjenester	**80,9**	66,6	70,7	47,6	41,5	44,5
Sum driftsutgifter	**192,4**	155,1	152,2	125,9	119,4	116,0
Inntekter og refusjoner	**17,3**	16,0	9,1	12,3	11,4	9,9
Netto	**175,1**	139,1	143,1	113,6	108,0	106,1

(løpende kroneverdier)

NSM HAR VIDEREUTVIKLET og styrket kompetansemiljøene innen forebyggende sikkerhetsarbeid i 2013. Virksomheten har gjennom året hatt stor kurs-, foredrags- og rådgivningsaktivitet utad. Tiltakene har, slik NSM ser det, økt mange virksomheters evne til å forebygge og forhindre sikkerhetstruende virksomhet. Samtidig er trusselbildet uforutsigbart og samfunnsutviklingen fører til at nye verdier og sårbarheter oppstår.

NSM skal sikre at aktiviteten er i tråd med ressursene som er tilgjengelig. Både når det gjelder budsjett til drift og investeringer, og forskning og utvikling (FoU), gikk NSM i balanse i 2013.

Økt tilsynskapasitet. NSM har økt tilsynskapasiteten i 2013. Det er gjort et stort arbeid med å ta igjen etterslep av tilsynsrapporter, samt kursing og opplæring av nytilsatte innen tilsyn.

Til tross for utfordringer med å rekruttere personell er NSM optimistisk med tanke på å nå målsettingen om døgnkontinuerlig drift av NSMs operasjonssenter i løpet av 2014. Det er en fortsatt kraftig økning i antall hendelser i det digitale rom. Operativiteten i VDI anses for tilfredsstillende, og alvorlige saker håndteres på en tilfredsstillende måte.

Håndteringen av de fleste alvorlige hendelsene har vært god i 2013. NSM har deltatt på en rekke øvelser, både interne og eksterne.

Objektsikkerhet. NSMs rådgivnings- og veiledningskapasitet innen objektsikkerhet er styrket. NSM har i 2013 nådd alle mål innenfor dette området. Det forventes en dreining av rådgivningsaktiviteten mot praktisk sikring av objekter i 2014.

NSM har vært en pådriver for innmelding av skjermingsverdige objekter fra de ulike sektordepartementene. Det er fremdeles enkelte departementer som ikke har rapportert inn objekter, eller som trolig har underrapportert. I flere sektorer er det trolig mangelfull budsjettering av sikkerhetstiltak. NSM oppdaterer regelmessig sin oversikt over innmeldte objekter.

Økt kompetanse. Det har i 2013 vært gjort et omfattende arbeid med å styrke sikkerhetskompetansen og bevisstheten om sikkerhet i samfunnet. Råd og veiledning har vært levert innen en rekke områder. 150 foredrag er blant annet holdt over hele landet.

Galileo. Den nasjonale oppfølgingen av deltakelsen i Galileo ble utøvd i prosjektets sikkerhetsorganer, hvor NSM i perioden blant annet har deltatt i arbeidsgrupper som berører akkreditering av Galileos bakkestasjoner plassert på norsk jord.

Revisjon av sikkerhetsloven. NSM har i 2013 bidratt i arbeidet med revisjon av sikkerhetsloven. Arbeidet ledes av Forsvarsdepartementet, og gjennomføres av en arbeidsgruppe som i tillegg består av representanter fra Justis- og beredskapsdepartementet og NSM. Forsvarsdepartementet har sekretariat for arbeidsgruppen.

NSM har gjennom året gitt vesentlige bidrag til arbeidsgruppens drøftingsnotater på ulike fagområder, blant annet gjennom å innhente oversikt over relevant regelverk fra andre stater, utarbeide statistikk, og bistå i utredningen av økonomiske og administrative konsekvenser. NSM arbeider også med et forslag som tar sikte på å etablere et godt rettslig grunnlag for å videreutvikle arbeidet med å varsle og håndtere alvorlige dataangrep.

Sikkerhetsavtaler. Sikkerhetsavtaler med andre land er vesentlig for å være i stand til å utveksle sikkerhetsgradert informasjon. I 2013 ble det undertegnet sikkerhetsavtale med Luxembourg. Island ratifiserte som siste nasjon den nordiske sikkerhetsavtalen. Det er i 2013 fremforhandlet et sikkerhetsarrangement for Forsvarssektoren med New Zealand. For øvrig pågår det prosesser, i ulike stadier, med Nederland, Estland, Georgia, Brasil og Chile. ‹

FAKTA

STATUS 2013/2014

198

198 millioner kroner i driftsbudsjett.

200 ansatte.

30 prosent av de ansatte er kvinner, 70 prosent er menn

JOBB I NASJONAL SIKKERHETSMYNDIGHET?

I fjor ansatte Nasjonal sikkerhetsmyndighet 60 nye personer, og har nå totalt i overkant av 200 stillinger. Til neste år skal direktoratet vokse med enda flere ansatte. Hvorfor jobbe i NSM?

– VI ER EN VIRKSOMHET med veldige gode og sterke fagmiljøer. Det er et bredt spekter av arbeidsoppgaver. Og mange sitter tett på saker som skal videre til departementer og andre styrende organer. Det gjør hverdagen spennende, og til tider hektisk. Det sier fungerende avdelingsdirektør for HR, Åsa Eriksson i NSM.

I tillegg til at man får drive med det man er god til, er Nasjonal sikkerhetsmyndighet en arbeidsplass som ønsker balanse mellom jobb og fritid. Her skal det være tid til henting av barn på skoler og barnehager, og det er lagt til rette for trening i arbeidstiden.

Nasjonal sikkerhetsmyndighet er også en del av kompetansereformen i forsvarssektoren. Reformen skal forbedre måten sektoren tiltrekker, ivaretar og utvikler menneskelige ressurser på. Sektoren skal bli en moderne kompetanseorganisasjon som er i stand til å møte fremtidens behov for mangfold, og både bredde- og spisskompetanse.

– Hva slags stillinger er det behov for i NSM?

– Vi trenger både jurister, samfunnsvitere og teknologer. Vi er ofte ute etter folk med IKT-faglig bakgrunn, som for eksempel ingeniører, sier Eriksson.

– Hva skal folk gjøre hvis de ønsker å jobbe i NSM?

– Følg med oss på våre nettsider, sier hun. – Møt oss på messer og konferanser, hvor vi kommer til å være i tiden fremover. Vi har også en åpen søknadsløsning hvor du kan søke om å jobbe hos oss, uavhengig av hva slags stillinger som er lyst ut. ‹

– NSM er en virksomhet med veldig gode og sterke fagmiljøer, sier Åsa Eriksson, som er fungerende HR-direktør.

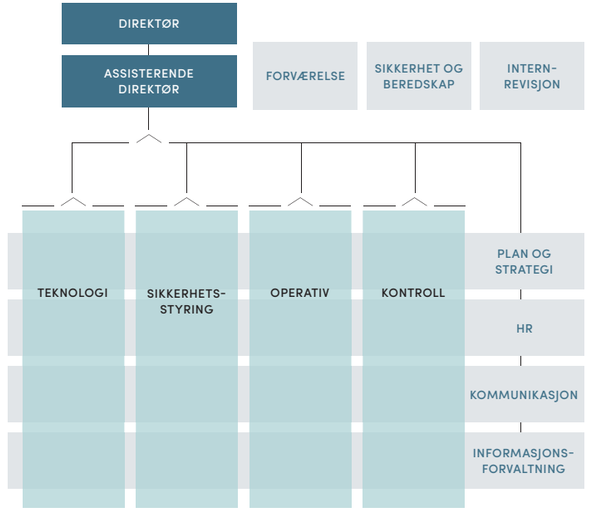
HVA GJØR NASJONAL SIKKERHETSMYNDIGHET I 2014?

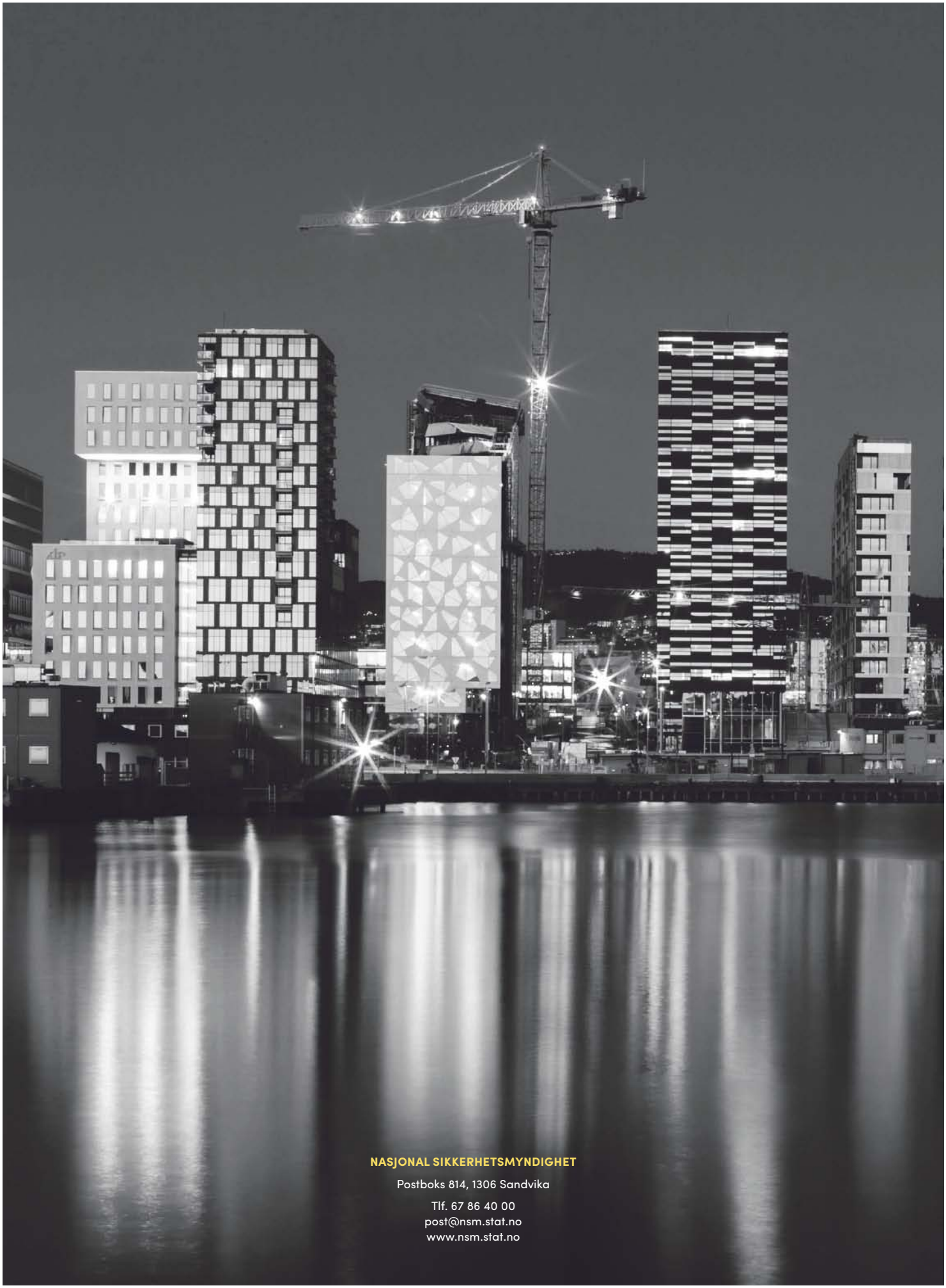
Nasjonal sikkerhetsmyndighet skal i 2014 særlig prioritere å:

- videreutvikle NSM som det nasjonale fagmiljøet for IKT-sikkerhet i Norge
- styrke NorCERT-funksjonen, spesielt med hensyn til koordinering av håndteringen av potensielt alvorlige dataangrep
- styrke NSMs rådgivnings- og veiledningskapasitet, særlig på objektsikkerhetsområdet
- styrke NSMs tilsyn og kontrollaktivitet, inkludert øke aktiviteten innenfor inntrengingstesting og tekniske sikkerhetsundersøkelser
- videreutvikle og styrke kompetansemiljøene i forebyggende sikkerhetsarbeid, internt og eksternt
- gjennomføre kompetansereformen, herunder bistå i den konkrete operasjonaliseringen av Meldt. ST. 14 «Kompetanse for ny tid».
- Det forventes at NSM er proaktive innenfor sitt ansvarsområde og følger opp avvik som avdekkes, for å bidra til å bedre sikkerhetstilstanden.

NSM ORGANISASJON

NSMs ledergruppe: Morten Hatlem, avd.dir. HR, Hans Robert Bjørnaas, avd.sjef Teknologi, Hans Christian Pretorius, avd.dir. Operativ, Vigdis Grønhaug, avd.dir. Kontroll, Knut Bjørn Medhus, avd.sjef Plan og Strategi, ass. direktør Annette Tjaberg, Per Christensen, spesialrådgiver, direktør Kjetil Nilsen, Vidar Bottolvs, sikkerhetssjef, Bente Hoff, avd.dir. Informasjonsforvaltning, Carsten rapp, avd.dir. Sikkerhetsstyring og Mona Strøm Arnøy, avd.dir. Kommunikasjon





NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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