2010

Sikkerhetskultur

NSM

Årsmelding

Nasjonal sikkerhetsmyndighet

Innhold

Verksemdsidé

Nasjonalt tryggingsorgan (NSM) er eit direktorat med førebyggjande tryggingsteneste som oppgåve. NSM skal innan sitt ansvarsområde skjerme informasjon og objekt mot spionasje, sabotasje og terrorhandlingar gjennom å:

- føre tilsyn og utøve styringsmakt i samsvar med regelverk
- varsle og handtere alvorlege dataangrep
- utvikle tryggingstiltak
- gi råd og rettleiing

NSM skal vere ein pådrivar for styrking av tryggleikstilstanden og gi råd om utviklinga av sikkerheitsarbeidet i samfunnet.

Foto: Pål Rødahl/tinagent

ORGANISASJON

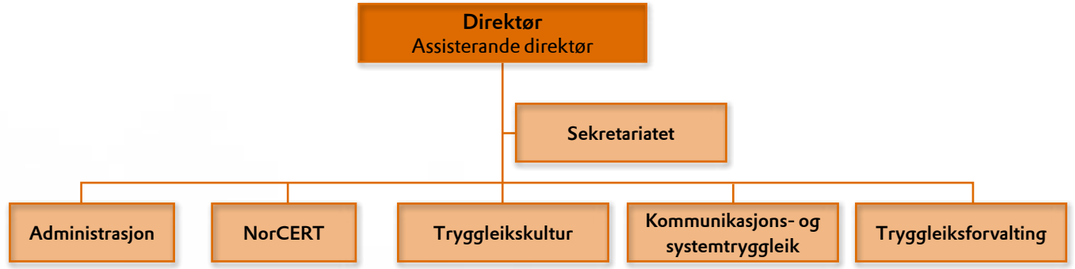
VISJON

Sikre samfunnsverdiar

VERDIAR

Vi skal vere tydelege, vi skal samhandle, og ha integritet

Foto: Pål Rødahl/tinagent



Dette er NSM:

Oppgåver, strategi og kontroll

NSM er eit direktorat for førebyggjande tryggleik som skal leggje til rette for, støtte og rapportere om gjennomføringa av defensive førebyggjande tiltak mot spionasje, sabotasje og terrorhandlingar i alle sektorar i samfunnet.

Oppgåver

NSM utøver i dag oppgåver i samsvar med følgjande lover, ordningar og avgjerder:

- Lov om forebyggende sikkerhetstjeneste (tryggingslova)
- Lov om oppfinnelser av betydning for rikets forsvar
- Lov om forsvarshemmeligheter
- Sertifiseringsordninga for IT-tryggleik i produkt og system (SERTIT)
- Nasjonal operativ varslings- og handteringskapasitet for alvorlege angrep mot samfunnsviktig IKT-infrastruktur (NorCERT), medrekna drift av Varslingssystem for digital infrastruktur (VDI)
- Sekretariatsfunksjon for Koordineringsutvalget for førebyggjande informasjonssikkerhet (KIS)
- Stønad til norsk kryptoindustri
- Det nasjonale beredskapssystemet (NBS)

Strategi

NSM vil betre tryggleikstilstanden i samfunnet ved å:

- Utvikle risikobaserte og balanserte førebyggjande tryggingstiltak
- Gi informasjon og levere tenester og produkt som når målgruppene
- Styrkje samfunnet si evne til å oppdage og reagere på sårbarheiter og tryggleikstruande hendingar
- Sikre tilliten til tryggingsarbeidet
- Forenkle og effektivisere tryggingsarbeidet
- Vere ein etterspurt bidragsytar og samarbeidspartnar nasjonalt og internasjonalt
- Vere ein attraktiv arbeidsplass med riktig kompetanse og ha ein organisasjonskultur prega av ærekjensle, heilskapstenking og innovasjon
- Sikre det økonomiske grunnlaget for verksemda

Styring og kontroll

Forsvarsdepartementet og Justisdepartementet har det overordna sektorovergripande ansvaret for førebyggjande tryggleik i militær og sivil sektor. Nasjonalt tryggingsorgan er utøvande organ for dei to departementa innan førebyggjande tryggleik. NSM er administrativt underlagt Forsvarsdepartementet, og Forsvarsdepartementet kontrollerer NSM si oppgåveløysing på vegne av Regjeringa.

EOS-utvalet er eit kontrollorgan peikt ut av Stortinget for å føre kontroll med etterretnings- og tryggingstenestene. Kontrollen er retta inn mot individuell rettstryggleik, men omfattar også ein generell kontroll med at tenestene held verksemda si innanfor dei rammer som er fastsette av lover og anna regelverk. NSM blir og kontrollert av Riksrevisjonen.

Foto: Pål Rødahl/tinagent

Informasjonssikkerhet i det offentlige:

Behov for en helhetlig tilnærming

Flere ukoordinerte regelverk regulerer informasjonssikkerheten i det offentlige i dag. Det er en svakhet, mener direktør i Nasjonal sikkerhetsmyndighet, Kjetil Nilsen. – Vi trenger en enhetlig oppfatning av hva slags sikkerhetsnivå vi bør ha, sier han.

Nasjonal sikkerhetsmyndighet har stort sett nådd hovedmålene organisasjonen satt seg i fjor, til tross for stramme rammer. Hovedoppgaver som tilsyn med etterlevelsen av sikkerhetsloven, personkontroll i forbindelse med sikkerhetsklareringer, produksjon av kryptomateriell for sikker kommunikasjon og varsling og håndtering av alvorlige dataangrep er levert til samfunnet. Men samtidig er det grunn til en fortsatt bekymring for sikkerhetstilstanden i Norge. Datasikkerheten er ikke god nok, og sikkerhetsarbeidet blir ikke prioritert.

Mange ulike krav

I fjor høst satte Aftenposten gjennom en serie artikler fokus på sikkerheten i departementene. Tilsyn fra Riksrevisjonen viste at datasikkerheten ikke var god nok, og hadde alvorlige mangler. Fornyings-, administrasjons- og kirkedepartementet ba om bistand fra Nasjonal sikkerhetsmyndighet til å gå gjennom IT-sikkerheten i departementene. Rapporten fra NSM, som er sikkerhetsgradert, bekreftet blant annet mange av funnene Riksrevisjonen gjorde. Og den bekreftet de siste årenes rapporter fra NSM om at IT-sikkerheten er for dårlig i mange virksomheter.

Kjetil Nilsen konstaterer at det er mange ulike krav til informasjonssikkerhet som forvaltningen må forholde seg til. Sikkerheten er regulert gjennom personopplysningsloven, Lov om elektronisk kommunikasjon, lover og forskrifter om informasjonssikkerhet i helsesektoren, sikkerhetsloven og så videre.

– Selv om det stilles krav, så er det sjelden formulert klare mål for sikkerheten. En annen svakhet er at offentlig forvaltning ikke har en helhetlig tilnærming til hvilke tekniske krav samfunnet skal stille. Og det er ulike oppfatninger av hvilke risikoer samfunnet ønsker å ta. Mange ulike regelverk og krav vanskeliggjør integrasjon og samarbeid, og det vanskeliggjør effektivitet og verdiskapning, sier Kjetil Nilsen.

«Mange ulike regelverk og krav vanskeliggjør integrasjon og samarbeid, og det vanskeliggjør effektivitet og verdiskaping.»

En robust grunnsikring

Hvor sikre skal systemene være? spør han. Er det individet som skal ta stilling til sikkerheten, er det virksomhetene, er det departementene, eller er det andre? Er det greit om våre dokumenter og e-poster kan leses av uvedkommende? Er det greit om dokumenter og e-poster vi mottar kan være manipulerte eller forfalsket? Er det greit at vi ikke får tilgang til kritiske systemer når vi trenger det? Er det greit om andre kan utgi seg for å være oss?

– Når vi stiller denne typen spørsmål skjønner vi risikoen vi står overfor, og hva vi er villig til å akseptere, sier Nilsen.

– Men er det en reell fare for at slike ting skjer i dag?

– Ja, det er en reell fare for dette i mange datasystemer i Norge i dag. Vårt arbeid viser at dette er mulig i mange tilfeller. Det er behov for å etablere en helhetlig robust grunnsikring basert på et definert felles sikkerhetsnivå for offentlig forvaltning og andre som eier eller drifter kritisk infrastruktur. Det er viktig for å redusere risikoen for at sensitiv informasjon kommer på avveie, eller at noen kan manipulere kritisk informasjon.

Felles standarder

– Hva mener du med et felles sikkerhetsnivå?

– Med det så mener jeg at det etableres en felles målformulering for sikkerhet med tilhørende krav. Dette kan gjøres på flere måter, og det er mange veier til målet. Vi må sørge for at de ulike regelverkene innen informasjonssikkerhet er tilstrekkelig harmoniserte til at vi har et felles sikkerhetsnivå i Norge, samtidig som særbehovene til den enkelte sektor kan bli ivaretatt.

Foto: Pål Rødahl/tinagent

Bekymret for grunnsikringen

Utgangspunktet til Nasjonal sikkerhetsmyndighet er å ha oversikt over samfunnets kritiske sårbarheter, og hjelpe virksomhetene til å motvirke eller tette sårbarhetene. De som håndterer sikkerhetsgradert informasjon i Norge i dag har relativt sikre IKT-systemer. Systemene er blant annet underlagt strenge krav i sikkerhetsloven. Men det samme gjelder ikke for alle andre.

– Vi har i flere år sagt at vi er bekymret for grunnsikringen i samfunnet, utenfor de graderte nettverkene som vi har et ansvar for. Det er fordi de ugraderte og graderte nettverkene henger mer og mer sammen. De er blant annet avhengig av den samme infrastrukturen.

Sikkerhetskultur og innsidere

– Nasjonal sikkerhetsmyndighet har i år sikkerhetskultur som tema for årsmeldingen, hvorfor det?

– Det er ofte mulig å sikre seg rent teknisk mot dataangrep. Men det er to veier til å få tak i informasjon, enten gjennom mennesket eller teknologi. Ofte bruker man begge i kombinasjon. Wikileaks-saken slik den fremstår nå tyder på at det handler om sikkerhetskultur og en innsider som har lastet ned store mengder informasjon. Noe av det farligste du kan ha er en misfornøyd medarbeider som opptrer illojalt. Sikkerhetskultur handler om holdninger og kompetanse, årvåkenhet, men også om å skaffe nok ressurser og skape prioritet rundt dette. Derfor er sikkerhetskultur viktig.

– Hva er de største utfordringene i 2011 for samfunnet når det gjelder informasjonssikkerhet?

– Det er å sikre en balanse mellom ulike hensyn som rettssikkerhet, personvern, sikkerhet, produktivitet og effektivitet. På den ene siden skal du sørge for at sikkerhetstiltakene ikke blir for inngripende, samtidig som du ikke skal la alle de andre hensynene skyve sikkerheten i bakgrunnen. Det å finne balansepunktet i det offentlige og i det private Norge mellom de ulike hensynene er en stor utfordring, sier direktør i Nasjonal sikkerhetsmyndighet, Kjetil Nilsen.

Foto: Pål Rødahl/tinagent

Viktig å få på plass en cyberstrategi

Flere land har fått på plass nasjonale strategier for cybersikkerhet. Det er nødvendig også i Norge, sier direktør i Nasjonal sikkerhetsmyndighet, Kjetil Nilsen.

Nasjonal sikkerhetsmyndighet leverte i fjor et forslag til en nasjonal strategi for cybersikkerhet til Forsvarsdepartementet og Justisdepartementet. Strategien foreslo flere konkrete tiltak for å styrke IT-sikkerheten i Norge. Strategien er nå til behandling i departementene.

– Det er viktig å få på plass en cyberstrategi for å skape den nødvendige tryggheten i ansvar, oppgaver og roller, slik at alle etater kan gå veien videre for å styrke cybersikkerheten, sier direktør Kjetil Nilsen.

Cybersikkerhet på dagsorden

Cybersikkerhet er satt på dagsorden internasjonalt i mange ulike sammenhenger i 2010. På NATOs toppmøte i Lisboa i november i fjor sa generalsekretær Anders Fogh Rasmussen i åpningstalen at cybertruslene mot kritisk infrastruktur tiltar hver eneste dag. NATOs nye strategiske konsept tar til orde for å styrke cybersikkerheten i alliansen. Cybersikkerhet blir også trukket frem i EU-kommisjonens nye strategi for intern sikkerhet, og blir beskrevet som ett av fem områder på veien mot et sikrere Europa.

Flere europeiske land har utarbeidet egne cybersikkerhetsstrategier den siste tiden. Britiske myndigheter var først ute i juni 2009. Den siste tiden har også Tyskland, Nederland og Frankrike utarbeidet egne strategier på området.

Ny teknologi gir sårbarheter

Nasjonal sikkerhetsmyndighet må være relevante også i forhold til ny teknologi, sier direktør Kjetil Nilsen.

– Vi må bli enda bedre til å spille virksomhetene gode, og hjelpe dem til å håndtere sikkerhetsutfordringene deres. Vi må finne løsninger på nye teknologiske utfordringer. Mye av teknologien som nå kommer gir nye sårbarheter og utfordringer. Det vil være umulig å nedlegge et forbud mot smarttelefoner og lesebrett. Det er et krav fra brukerne om å ta ny teknologi i bruk. Det innebærer at vi i NSM må finne løsninger på nye teknologiske utfordringer, sier han.

På tilsyn i Afghanistan

Nasjonal sikkerhetsmyndighet gjennomførte i 2010 tilsyn med sikkerhetstjenesten i det norske militære styrkebidraget i Afghanistan. Tilsyn er en av hovedoppgavene i NSM, og er et viktig virkemiddel for å få bedre kunnskap og oversikt over sikkerhetstilstanden. Nærmere 600 virksomheter er underlagt sikkerhetsloven, som omfatter Forsvaret, offentlig forvaltning samt enkelte private virksomheter.

Foto: NSM

Rapport om sikkerhetstilstanden:

Sikkerhetstilstanden forverres

NSM avdekket i 2010 en rekke konkrete mangler i det forebyggende sikkerhetsarbeidet. Gapet mellom truslene og sikkerhetstiltakene øker.

NSM fører tilsyn med etterlevelsen av sikkerhetsloven, som skal legge forholdene til rette for å motvirke spionasje, sabotasje og terror. Rapport om sikkerhetstilstanden er basert på NSMs tilsyn, i tillegg til en rekke andre kilder som innrapporterte sikkerhetstruende hendelser, tekniske sikkerhetsundersøkelser, inntrengingstester, personkontroll, og NorCERTs oversikt og håndtering av hendelser på Internett. Denne rapporten viser at det er til dels alvorlige mangler i det forebyggende sikkerhetsarbeidet, og at virksomhetene har lav forståelse for at vitale nasjonale sikkerhetsinteresser må beskyttes. Blant funnene er manglende ledelsesengasjement, og manglende systemer for å varsle virksomhetsledelse om uønskede hendelser. Det har også vist seg at enkelte virksomheter ikke er kjent med at de er underlagt sikkerhetsloven.

Mange sikkerhetsmangler

I henhold til PSTs åpne trusselvurdering for 2010 er etterretningsaktiviteten mot norske interesser stadig høy. Etterretning ved hjelp av IKT, Internett, og teknisk og sosial manipulering er økende. Antall målrettede forsøk på dataspionasje øker markant hvert år. I 2010 utgjorde dataormen Stuxnet starten på en bekymringsfull utvikling, med alvorlige sabotasjeangrep mot prosesskontrollsystemer i kritisk infrastruktur og industri ved hjelp av IKT-verktøy. Metoder for avlytting og avlesning har blitt stadig mer avanserte, og markedet for avlyttingsutstyr er voksende.

Selv med en økende trussel, ser NSM mange av de samme sikkerhetsrelaterte manglene ute i virksomhetene. Dette tilsier at sikkerhetstilstanden forverres.

Fremtidsutsikter

Det må forventes en økning i alvorlige IT-hendelser i tiden som kommer. Selv robuste IKT-systemer vil ikke være fullt sikret mot ukjente tekniske trusler og de avanserte aktivitetene som utgjør de alvorligste utfordringene mot vitale nasjonale interesser. Fremveksten av skadelig programvare som angriper prosesskontrollsystemer kan i fremtiden bli en av de største sikkerhetsutfordringene som det moderne samfunnet står overfor.

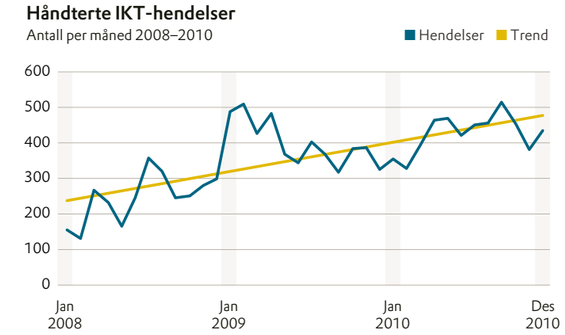
I tiden fremover er det god grunn til å holde øye med følgende trender:

- Spredning av skadevare over mobile enheter som mobiltelefoner, særlig smarttelefoner og diverse nettbrett
- Misbruk av og infisering av smartkort og smartkortlesere
- Målrettede angrep mot lukkede nett Det har vist seg at de ikke er immune, særlig med hensyn til uforsiktig bruk av minnepinner.
- Mer profesjonell utvikling av ondsinnet programvare.
- Forsøk på å infiltrere prosesskontrollsystemer.

Den ugraderte rapporten om sikkerhetstilstanden ligger i sin helhet på www.nsm.stat.no.

Blant funnene er manglende ledelsesengasjement, og manglende systemer for å varsle virksomhetsledelse om uønskede hendelser.

Stadig mer å gjøre: Grafen viser antall håndterte hendelser i operasjonssenteret til NorCERT. I 2010 ble det håndtert 5082 hendelser. I 2008 ble det til sammenligning håndtert 3091 hendelser.



IKT-hendelser i 2010:

Viktige datasystemer trolig infisert

Forsøk på spionasje mot departementer og store norske bedrifter var de mest alvorlige IKT-hendelsene NorCERT håndterte i 2010.

IKT-hendelsene er blant annet oppdaget på bakgrunn av nasjonalt og internasjonalt samarbeid, deteksjoner i Varslingssystem for digital infrastruktur (VDI), og fordi angriper begår tekniske feil eller er uforsiktig. Avanserte målrettede angrep er krevende å oppdage. Det er derfor sannsynlig at viktige datasystemer i Norge er infisert, og at informasjon er kommet på avveie.

Hendelser i 2010

Flere ulike typer IKT-hendelser har vært håndtert i 2010.

- I februar 2010 ble nettsidene til flere offentlige myndigheter, herunder Nasjonal sikkerhetsmyndighet, utsatt for et distribuert tjenestenektsangrep (DDoS). Hensikten med slike angrep er å overbelaste nettsidene slik at de blir utilgjengelige for brukerne. Flere andre nettsteder har opplevd det samme i løpet av 2010, blant annet nettsidene til aviser, bedrifter og interesseorganisasjoner.
- 7. april 2010 oppdaget en ansatt i en norsk bedrift en e-post som utga seg for å være fra en ansatt i NASA. E-posten inneholdt et dokument som forsøkte å laste ned en trojaner fra Internett. Denne trojaneren var et fjerninnloggingsverktøy som ville gitt angriperen full kontroll over kompromitterte maskiner.
- 26. april 2010 ble flere ansatte i en privat virksomhet som jobbet med et bedriftskonfidensielt prosjekt utsatt for målrettede trojanere i e-post. E-postene med trojanerne kom fra falske avsendere og ga inntrykk av å være fra personer involvert i prosjektet.
- Falske e-poster med ondsinnet programvare ble sendt til embetsmenn i andre land og ga inntrykk av at en norsk offentlig etat var avsender. Det ble sendt e-post med invitasjon til en tilstelning i juni ved etaten til personer i inn- og utland. Kort tid etter ble en ny e-post om samme sak sendt til de samme mottakerne, men fra en falsk avsender. Et vedlegg inneholdt en trojaner.
- 9. juli 2010 ble det oppdaget mistenkelig nettverkstrafikk fra en datamaskin tilhørende en ansatt i et departement. På datamaskinen ble det oppdaget flere trojanere. Den ene samlet inn alle dokumenter opprettet den siste uken og klargjorde disse til å bli sendt ut på Internett tilbake til angriperen.
- En ansatt i et departement mottok 16. november 2010 en e-post som tilsynelatende var sendt fra en internasjonal organisasjon. E-posten hadde et vedlegg som inneholdt en hittil ukjent skadevare (en ny trojaner), som gir angriperen kontroll over datamaskinen og mulighet til å stjele informasjon, uten at bruker kan oppdage dette.
- Flere departementer mottok 17. november 2010 mistenkelige e-poster som omtalte en internasjonal organisasjon. E-posten var sendt fra en forfalsket avsenderadresse, og inneholdt et vedlegg med en trojaner.
- Forsvarsbedriften Nammo oppdaget fem målrettede angrep mot seg med tro-

janere i 2010. Emnene i e-postene var relatert til forsvarsindustrien. Trojanerne var ulike versjoner av fjerninnloggingsverktøy som ville gitt angriperen full kontroll over kompromitterte maskiner.

Trojanere og ormer

Banktrojaneren Zeus er en av de mest omtalte informasjonsstjelende trojanerne i 2010. Den distribueres i stadig nye versjoner, og det er lav grad av deteksjon blant antivirusprogrammer. Det er ikke stjålet penger fra norske nettbanker i 2010, men tidlig i 2011 er det oppdaget nye trojanere som er spesialtilpasset norske nettbanker.

I 2010 dukket dataormen Stuxnet opp som en ny trussel. Dataormen kan sabotere industriprosesser og kan spres ved hjelp av forskjellige metoder, blant annet via minnepinner. Det er den første kjente skadevaren som er oppdaget på Internett som er spesifikt rettet mot slike industrisystemer. Skadevaren bruker også stjålne sertifikater fra kjente leverandører. Teknisk analyse av skadevaren viser at utviklingen av Stuxnet har krevd betydelige ressurser, herunder detaljkompetanse om proprietære styringssystemer utviklet av Siemens. Irans president Ahmedinejad innrømmet i desember at Stuxnet har påvirket landets atominstallasjoner. I Norge er det ikke registrert digitale sabotasjeangrep av denne typen. Norge er sårbart fordi vi tar raskt i bruk ny teknologi og er stor bruker av avanserte prosesskontrollsystemer blant annet innen olje, gass og vannkraft.

SIKKERHETSKULTUR

Se opp for e-poster som virker merkelige, sier Nobelinstituttet. Ansvarliggjør sjefene, sier Forsvarets sikkerhetsavdeling. Og lås PC-en når du går ut fra kontoret, sier Høyres Ine Marie Eriksen Søreide. Årets årsmelding fra Nasjonal sikkerhetsmyndighet har sikkerhetskultur som tema. Det er kort fortalt hva du og jeg gjør i det daglige for å opprettholde en god sikkerhetstilstand i samfunnet.

God lesning!

Foto: Pål Rødahl/tinagent

Jørgen Kosmo, riksrevisor.
Foto: NSM

Informasjonssikkerheten i forvaltningen:

Verre enn fryktet

– Resultatet var egentlig verre enn det vi fryktet. Det sier riksrevisor Jørgen Kosmo etter at han undersøkte informasjonssikkerheten i statsforvaltningen i fjor.

Riksrevisoren tar oss imot utenfor Riksrevisjonens solide og børstede ståldører i Pilestredet i Oslo.

– Disse dørene kostet mange penger, blant annet for å innfri sikkerhetskravene, sier han lakonisk.

Et nytt trusselbilde

Fra åttende etasje i Riksrevisjonens bygg i Pilestredet i Oslo har Jørgen Kosmo godt utsyn over forvaltningen i Kongeriket. Riksrevisjonen skal sørge for at fellesskapets midler og verdier blir brukt og forvaltet slik Stortinget har bestemt. I fjor avdekket de store svakheter i informasjonssikkerheten. Hele 11 departementer hadde vesentlige mangler i sin styring av underlagte virksomheters informasjonssikkerhet, slo Riksrevisjonen fast i Dokument 1, som ble overlevert Stortinget 19. oktober.

– Det som sjokkerte meg mest var at det var en så systematisk nedgradering av trusselbildet, til tross for at både NSM, PST og sikkerhetsrådgivere i næringslivet har vært ute og pekt på truslene, sier Jørgen Kosmo. Han beskriver et trusselbilde som har endret seg radikalt, og som har gitt en ny type kriminalitet både mot privatpersoner, mot offentligheten og mot næringsdrivende. I dag handler mange av truslene om å hente ut elektronisk informasjon om andre lands næringsvirksomhet, eller forsvars- og utenrikspolitiske dokumenter.

Informasjonssikkerhet et lederansvar

– Undersøkelsene vi gjorde viste jo at selv i de mest sentrale deler av statsforvaltningen, og da tenker jeg på Departementenes servicesenter, var bevisstheten om utfordringene man stod overfor foruroligende lav. Når bevisstheten er lav og ledelsesengasjementet ikke er til stede, blir resultatet deretter, sier Kosmo.

Han konkluderer med at informasjonssikkerhet er et ledelsesansvar. Og det er et ledelsesansvar som blir stadig viktigere. Riksrevisjonen har etterlyst større samhandling mellom ulike offentlige virksomheter, for å oppnå bedre resultater. Noe av grunnlaget for en slik samhandling ligger i utveksling av elektronisk informasjon, som for eksempel pasientjournaler. Det dreier seg om svært sensitiv informasjon om deg og meg, og enorme mengder data om enkeltmennesker som skal kunne utveksles i og mellom ulike sektorer.

– Hvis vi skal lykkes med samhandling og kommunikasjon må virksomhetene ha et kjempestort fokus på informasjonssikkerhet. Vi har ingen ambisjon om å henge ut eller sparke noen, men å skape bevissthet om og sette fokus på informasjonssikkerhet og skape et tryggere samfunn, blant annet med de råd dere i NSM kan gi.

Systematisk planlegging

Hvis ledelsen ikke har fokus på sikkerhet, åpner man for IKT-truslene som eksisterer, sier Kosmo.

– Dette er en betydelig større utfordring og burde bekymre folk mye mer enn datalagringsdirektivet, sier han.

Det er ikke bare snakk om å sette sikkerhet på agendaen, mener han. Det handler om å få på plass systemer i virksomhetene som vurderer risikoen, og da ikke bare risikoen for at du ikke klarer å gjøre det du skal, men også risikoen for trusler utenfra. Har man ikke et system for virksomhetsplanlegging og risikostyring, vil man heller ikke få til et system som ivaretar informasjonssikkerheten.

Fortsetter neste side >>

«Man sier dette er så dyrt. Ja, det er dyrt. Men hva er alternativet?»

Ill.foto: Colourbox

Er du en sikker leder?

Virksomhetens leder har det endelige ansvar for utøvelse av forebyggende sikkerhetstjeneste i henhold til sikkerhetsloven. Ansvaret omfatter også sikkerhetsoppgaver utført av andre for virksomheten, og forebyggende sikkerhetstjeneste i underlagte virksomheter. Ansvaret oppfylles gjennom:

- Kunnskap om regelverket
- Forståelse for risiko
- Etablering av forebyggende sikkerhetstjeneste
- Oppfølging av forebyggende sikkerhetstjeneste

>>

Sikkerhet gir tillit

Riksrevisjonen selv har et sterkt fokus på informasjonssikkerhet internt, sier han.

- Vi gjør noe hele tiden. Tenk på alt materialet vi får inn i forbindelse med tilsyn og revisjoner. Hvis vi skal ha tillit i forvaltningen til å få informasjonen vi trenger, må de føle trygghet for at det er sikkerhet her. Derfor har vi et kjempefokus på informasjonssikkerhet. Det gjelder både datasystemer og papirhåndtering.

– Det kan være vanskelig å få til endring i store organisasjoner som staten, hvordan skal vi få til dette i Norge?

– Først og fremst er det snakk om å ha et overordnet fokus. Har departementer og direktorater et overordnet fokus på informasjonssikkerhet, vil lederne forstå ansvaret de har. Men det å ikke ivareta ansvaret man har må ha konsekvenser. Der har du mange reaksjonsmåter, fra å bruke statens lønnssystem og personlige tillegg, til å be folk finne seg en annen jobb. Hvis lederne ikke er villige til å følge den overordnede politiske styringen, må det ha konsekvenser. Lederne må rett og slett måles på informasjonssikkerhet, sier Jørgen Kosmo.

Og etater som Nasjonal sikkerhetsmyndighet, som driver tilsyn med sikkerhetsloven, må reagere når de ser vesentlige sikkerhetsbrudd, mener han.

– Det er forskjell på litt slurv, og systematisk mangel og fokusering på informasjonssikring. Man sier dette er så dyrt. Ja, det er dyrt. Men hva er alternativet?

NSM hjalp departementene med datasikkerheten

Nasjonal sikkerhetsmyndighet hjalp Fornyings-, administrasjons- og kirkedepartementet (FAD) med sikkerheten etter Riksrevisjonens kritikk i fjor høst. NSM foretok undersøkelser rundt datasystemene i Departementenes servicesenter, og leverte en rapport til departementet rett før jul.

– NSM sin gjennomgang gir FAD og Departementenes servicesenter (DSS) et veldig godt grunnlag for å arbeide videre med å forbedre sikkerheten på datasystemene, sa fornyingsminister Rigmor Aasrud i en pressemelding 10. januar 2011.

Avdekket sikkerhetssvikt i departementene

Aftenposten satte i fjor høst fokus på informasjonssikkerheten i departementene i en rekke artikler etter Riksrevisjonens årsrapport. Artiklene handlet både om datasikkerheten i Departementenes servicesenters ugraderte nettverk, og tilsyn fra NSM som viste manglende samsvar med bestemmelser i, eller i medhold av, sikkerhetsloven.

– I dag er sikre digitale informasjonssystemer like viktig for landets trygghet og borgernes beskyttelse som velfungerende forsvar og politi, skrev Aftenpostens kommentator Håvard Narum i en kommentar 22. oktober.

Nobelinstituttets 3 råd om e-poster

Her er IT-ansvarlig Bjørn Helge Vangens 3 råd om hvordan du unngår skadelig programvare fra e-poster:

1. Sett e-posten i sammenheng: Henger innholdet og avsender sammen, eller er det noe du stusser på?
2. Det er ikke nødvendig å åpne alle e-poster og vedlegg.
3. Si fra til dataansvarlig hvis det er noe du synes virker merkelig med e-posten.

Sikkerhetskultur på Nobelinstituttet:

Angrep styrket sikkerheten

De opplevde et av fjorårets mest omtalte dataangrep. Det har ført til en større bevissthet rundt sikkerhetskulturen på Nobelinstituttet.

– Vi lever i en tid og har en profil som gjør at vi kan tråkke andre på tærne. Dataangrepene var en kraftig vekker på IT-sikkerhet. Vi tenker mer på det.

Det sier Bjørn Helge Vangen, som er bibliotekar og IT-ansvarlig på Nobelinstituttet. Prisutdelingen i fjor til kinesiske Liu Xiaobo gikk ikke upåaktet hen. I oktober la noen inn skadevare, en såkalt trojaner, på nettsiden til Nobelinstituttet. Det gjorde at alle som gikk inn på sidene med nettleseren Firefox ble infisert. Hva som var motivet kan man bare spekulere på.

Angrep økte bevisstheten

– Vi fikk en telefon fra NSM om at det var noe på nettsidene våre. Det gikk 40 minutter fra vi fikk telefonen til det var borte, det er vi litt fornøyd med, sier Vangen.

Så begynte e-postene å komme. Etter det første angrepet kom opp mot 8 forskjellige forsøk på å trenge seg inn i datasystemene. Direktør Geir Lundestad fikk e-poster hvor noen prøvde å lure ham til å oppgi brukernavn og passord på e-postkontoene.

– Vi hadde lagt oss på det vi opplevde som et bra nivå på informasjonssikkerhet. Det er menneskelig å tro at det går bra når ingen ting har skjedd. Men når man får så spesifikke angrep øker det bevisstheten, sier IT-ansvarlig Vangen.

Det er ikke nødvendig å åpne alle e-poster, og det er ikke nødvendig å åpne alle vedlegg, mener han. Og det er faktisk mulig ut fra sammenhengen i en e-post å se om den kan inneholde skadevare eller ikke. Hvis det er en norsk avsender, hvorfor skriver han eller hun på engelsk, eller på dårlig norsk? Hvorfor sender en ansatt i et større selskap e-poster fra en Yahoo-adresse? Henger innholdet, avsender og sammenhengen sammen? Det er ingen grunn til å åpne alle e-poster og lese alt, man må ikke alltid være hjelpsom, sier Bjørn Helge Vangen.

Boksekamp med usynlig fiende

– Jeg følte dette nærmeste som en slags boksekamp med en du kanskje visste hvem var, men som du ikke var helt sikker på. Vedkommende fikk jo inn en del slag på oss, selv om jeg følte vi vant kampen til slutt. Når vi har mestret dette godt, er det dels fordi vi har kompetanse, og dels fordi det var mange som ville hjelpe oss, blant annet dere i Nasjonal sikkerhetsmyndighet, sier direktør ved Nobelinstituttet Geir Lundestad. Og sikkerhetskulturen er blitt bedre, sier han.

– Absolutt. Disse episodene vi hadde ganske mange av gjorde at vi alle sammen etter hvert ble veldig nøye på hva vi åpnet av e-post, og særlig vedlegg til e-poster. Vi har fått en høyere beredskap og bedre rutiner, sier Lundestad.

Bjørn Helge Vangen og Geir Lundestad. Foto: NSM

Har rutiner for e-post

Nobelkomiteen har strenge rutiner for hvordan de bruker e-post for å unngå lekkasjer.

– Vi ønsker ikke å ha lekkasjer. Da er første bud at vi ikke bruker e-post i korrespondansen mellom komitemedlemmene når det gjelder spørsmål om utvelgelse av prisvinnere. Det har vært rutine i flere år, sier direktør Geir Lundestad. Også innkommende e-post er gjenstand for strenge rutiner på Nobelinstituttet.

– Hvis vi er i det minste tvil om e-posten er infisert sender vi den over til dataansvarlig, sier Lundestad.

«Dataangrepene var en kraftig vekker på IT-sikkerhet.»

På nett uten sikring

– De mest alvorlige sakene vi har håndtert i NorCERT i 2010 har vært forsøk på spionasje. Det handler om å få noen til å åpne et dokument. Og det handler om å lure brukeren, sier avdelingsdirektør i Nasjonal sikkerhetsmyndighet, Christophe Birkeland.

Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd. Det er definisjonen Nasjonal sikkerhetsmyndighet bruker på sikkerhetskultur. Kort fortalt dreier det som om hva du og jeg gjør i det daglige for å vedlikehold eller forbedre sikkerhetstilstanden.

For liten kompetanse

I takt med at antivirus og brannmurer og andre tekniske tiltak har blitt stadig bedre, øker fokuset på oss brukere av datasystemer. Kriminelle retter i økende grad spionasjeforsøk og andre former for dataangrep mot det svakeste leddet, som i mange tilfeller er oss som sitter ved datamaskinene, sender e-post på mobilen, eller legger ut meldinger på Facebook og Twitter.

I NSM-avdelingen NorCERT håndterer avdelingsdirektør Christophe Birkeland en stadig økende mengde alvorlige dataangrep. De er rettet mot et fåtall personer. Han mener at sikkerhetskulturen kan styrkes i mange norske virksomheter.

– Kompetanse er det største problemet hos alle. Selvsagt gjelder det for folk som jobber med IT. Men det handler også om kompetanse hos vanlige brukere. Du klikker ikke på en hvilken som helst side på nett. Du åpner ikke et hvilket som helst vedlegg. Du svarer ikke på e-poster som oppfordrer deg til å oppgi brukernavn og passord. Du videresender ikke kjedebrev, det vil si e-poster med melding om at Internett går ned hvis du ikke sender meldingen videre til minst ti personer du kjenner. Men folk flest gjør nettopp det, og derfor er det kort vei mellom kompromitterte datasystemer og dårlig sikkerhetskultur.

Godtroende nordmenn

– Jeg tror nok vi er litt godtroende. Vi har kanskje en litt naiv holdning til en del ting? Spørsmålet kommer fra Hans Marius Tessem, som har jobbet med holdningsskapende arbeid mot kommuner og små og mellomstore bedrifter gjennom Norsk senter for informasjonssikring, NorSIS. Et av godene ved det norske samfunnet er at vi stoler på og har tillit til hverandre. Men det kan samtidig gjøre oss til lette mål, mener han. Når vi kobler oss til Internett er vi en del av ett av de mest kriminelle miljøene i verden. Det er kanskje lett å glemme når du er på kontoret eller i stua.

– Hvis en person som har tilgang til mye kritisk informasjon blir lurt, kan jo konsekvensen være at han eller hun mister informasjonen, eller at et datasystem blir ødelagt, sier han.

For mye teknikk

Roar Thon i Nasjonal sikkerhetsmyndighet har jobbet i mange år blant annet med informasjon om sikkerhetskultur og sikkerhet i sosiale medier. Han ser at det jobbes mye med sikkerhetskultur i norske virksomheter, og at det får mer og mer fokus.

– Men basert på enkelthendelser vi ser kan det fortsatt stilles spørsmål ved hvorvidt det finnes god nok sikkerhetskultur og atferd i flere virksomheter. Mange snakker om sikkerhet som noe man har egne folk til å håndtere, og tar ikke inn over seg at hver og en må bidra. Dette gjelder spesielt ledere, sier han.

Han mener at norske virksomheter i dag fokuserer mye på de tekniske løsningene, og at de ofte glemmer at man er avhengig av å manipulere mennesker for å lykkes med spionasjeforsøk.

Og kompetanse er viktig, sier Christophe Birkeland i NorCERT.

– I 2011 burde arbeidsgivere stille krav til brukerne i virksomhetene når det gjelder datasikkerhet. Hvor mange virksomheter gir nødvendig opplæring i sikker bruk av virksomhetens datasystemer? Og hvordan kontrolleres dette? spør han til slutt.

«Kompetanse er det største problemet hos alle.»

Kommuner mangler sikkerhetskultur

Norske kommuner mangler en god sikkerhetskultur, og de minste er verst.

Det viser rapporten «Informasjonssikkerhet i nordiske kommuner og fylkeskommuner», som er utført av NorSIS i samarbeid med organisasjonen Kommunal informasjonssikkerhet (KINS).

Rapporten viser blant annet at den hyppigste årsaken til sikkerhetsbrudd er medarbeiderenes atferd. (Computerworld 28. september 2010).

I 2011 burde arbeidsgivere stille krav til brukerne når det gjelder datasikkerhet, mener Christophe Birkeland i NSM. Foto: Pål Rødahl/tinagent

Mange snakker om sikkerhet som noe man har egne folk til å håndtere, og tar ikke inn over seg at hver og en må bidra, sier Roar Thon i NSM. Foto: Håvar Haug

Når vi kobler oss til Internett er vi en del av ett av de mest kriminelle miljøene i verden, sier Hans Marius Tessem i NorSIS. Foto: Ida Hjerkinn

Brukeratferd avgjørende for sikkerheten

Mange nordmenn er uforsiktige eller lar seg lure. Resultatet er at tusenvis av norske datamaskiner blir infisert av ondsinnet eller uønsket programvare, skriver Microsoft Norge i en pressemelding fra november i fjor.

Bedre programvare og økt bruk av automatiske oppdateringer gjør at datakriminelle i stadig større grad tyr til sosial manipulering for å lure ondsinnet programvare inne i brukernes datamaskiner, skriver Microsoft i pressemeldingen, som er basert på verdens mest omfattende rapport om datasikkerhet, Microsoft Security Intelligence Report (SIR).

Sikkerhet et ledelsesansvar

– Vi må få på plass en sikkerhetskultur, sa fornyingsminister Rigmor Aasrud i en pressemelding i fjor høst.

– Alle i samfunnet – enten vi snakker om myndigheter, virksomheter eller privatpersoner – må ta inn over seg hvilke sikkerhetsutfordringer vi står overfor. Derfor må sikkerhetsarbeid være en del av den daglige driften, sier statsråden, som er klar på at sikkerhetsarbeid er et ledelsesansvar som må på dagsordenen i norske styrerom.

Hans Kristian Herland, sjef for Forsvarets sikkerhetsavdeling.
Foto: Forsvarets mediesenter

Sikkerhetskultur i Forsvaret:

Til soldatenes beste

– Vi har ikke strenge sikkerhetskrav i Forsvaret for å være vanskelige og vriene. Det er fordi soldatene våre i Afghanistan og ellers hvor de måtte tjenestegjøre skal komme hjem igjen uskadd, og for at de skal ha best mulig forutsetninger for å løse sine oppdrag. Det er derfor vi jobber med sikkerhet, sier sjefen for Forsvarets sikkerhetsavdeling, FSA, Hans Kristian Herland.

Kommandør Herland holder til i tidligere forsvarssjefers kontorer ytterst mot sjøen og Vippetangen på Akershus festning. Her skal en stab på noen titalls personer sørge for at over 20 000 ansatte i Forsvaret, i alle aldre og ulike yrkesgrupper, nasjonalt og internasjonalt, har en sikkerhetskultur som gjør at sikkerhetsgradert informasjon ikke lekker ut.

Mer avhengig av teknologi

– Forsvaret er en stor og mangslungen organisasjon med mange profesjoner, alt fra yrkesbefal til vernepliktige og sivile. Det er et veldig spenn i bakgrunn og kompetanse. Det å få alle disse til å gå i samme retning og ha en felles sikkerhetsforståelse er en stor utfordring, sier Herland.

Teknologiutviklingen preger samfunnsutviklingen, og vi blir stadig mer avhengig av teknologi og kritisk infrastruktur. Konsekvensene når noe svikter viser seg ofte å bli alvorlige. Også selve forsvarsstrukturen er endret siden den kalde krigen. Den er blitt mindre redundant og mer teknologiavhengig, og konsekvensene ved sikkerhetstruende hendelser kan bli svært alvorlige for selve forsvarsevnen. Sett i statssikkerhetsperspektivet er det derfor avgjørende at det er en proaktiv gjennomgående sikkerhetstjeneste i Forsvaret, mener Herland. Beskyttelse av forsvarets operative evne er derfor FSAs virksomhetsgrunnlag og hovedfokus.

Satser på sjefene

I fjor høst kjørte FSA et sikkerhetsseminar rettet mot sjefene i Forsvaret, og viste blant annet hvor lett en mobiltelefon kan avlyttes. Det ga et helt annet utgangspunkt for forståelsen for sårbarheten, og dermed risikoen, ved bruk av mobiltelefon. Oppmerksomheten rundt sikkerhetssaker i media både rundt Wikileaks og datasikkerhet har bidratt til å løftet sikkerhetsarbeidet, mener Herland.

Men i Forsvaret ser de at holdningen til sikkerhet i stor grad står og faller med sjefens holdning til sikkerhet. Derfor har FSA fokusert på å jobbe mer mot sjefene i Forsvaret fremover.

– Vi søker å ansvarliggjøre sjefene i større grad enn tidligere, og jobber både mot sjefsnivået, mot sikkerhetsledere og mot avdelingssikkerhetsoffiserer. Vi skal også fremover jobbe med utdanningsstrukturen i sikkerhetsarbeidet, det er en veldig mangfoldig kompetanse som trengs i dag. Og alle behøver trolig ikke ha samme kompetanse. Det er hele tiden snakk om å finne ut hva som er «godt nok» og «målrettet» mot den enkeltes rolle i sikkerhetsarbeidet, sier Herland, som er opptatt av å motivere.

– Jeg tror på de gode eksemplene, og å trekke disse frem, mer enn paragrafer og pekefingre. Alt sikkerhetsarbeid i Forsvaret er basert på operative behov. En god sikkerhetskultur gir oss operativ effekt. Hvis vi klarer å holde gradert informasjon hemmelig, er motstanderens evne til å finne ut hvor vi er, hva vi skal gjøre, og hvordan de kan angripe oss, vanskeligere. Det gjør det lettere for oss å operere slik vi vil, ta vare på soldatene, og løse våre oppdrag, sier Hans Kristian Herland.

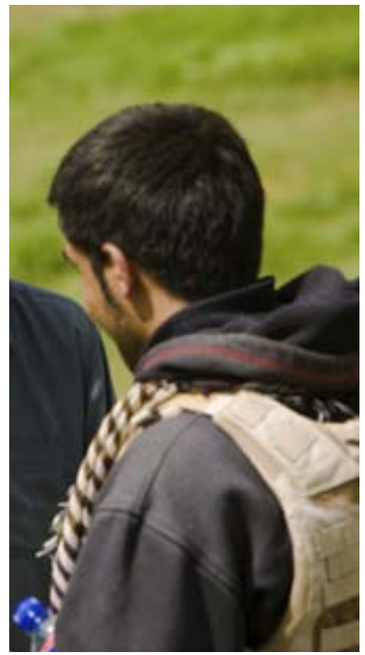


Foto: Forsvarets mediesenter

Hans Kristians 3 råd for god sikkerhetskultur

1. Du må være systematisk.
2. Trekk frem de gode eksemplene, vær konkret, få frem den positive siden og fokuser på den operative effekten ved å drive sikkerhetsarbeid.
3. Du må kontinuerlig arbeide med etikk og holdninger hos alle som jobber i organisasjonen.

«Vi søker å ansvarliggjøre sjefene i større grad enn tidligere.»

Lite sikkerhetsopplæring

Bare en tredel av virksomhetene har kontinuerlig sikkerhetsopplæring av de ansatte, og under halvparten har sikkerhetsopplæring av nyansatte.

Det viser Mørketallsundersøkelsen fra Næringslivets sikkerhetsråd, som blir gjennomført i private og offentlige virksomheter annet hvert år. Undersøkelsen viser også at opp mot halvparten av gjerningsmennene bak datakriminalitet er egne ansatte eller innleide konsulenter. Det er nødvendig at kunnskapsformidlingen om sikkerhet må fortsette med fokus på de små og mellomstore virksomhetene, er en av hovedanbefalingene i rapporten.

Erik Lund-Isaksen, departementsråd i Forsvarsdepartementet. Foto: NSM

Lekkasjene

2010 har vært året for de store lekkasjene, blant annet gjennom Wikileaks. Lekkasjesaker svekker omdømmet, og skader forholdet mellom kollegaer, sier departementsråd Erik Lund-Isaksen i Forsvarsdepartementet.

– Det at noen lekker, og særlig hvis det er en bevisst lekkasje, gir utrolig dårlige signaler.

Departementsråd Erik Lund-Isaksen er den øverste administrative leder i Forsvarsdepartementet. Han er sjef for den sektoren som forvalter desidert mest sikkerhetsgradert informasjon i Norge. Likevel hender det at det lekker, og at gradert informasjon eller dokumenter finner veien til pressen.

Straffbart å lekke

– Det ene perspektivet på bevisste lekkasjer er at personer selv blir privatpraktiserende i forhold til å avgjøre når de vil bryte loven. Det er jo straffbart å lekke. Det betyr det samme som om en person selv avgjør om det er legitimt å stjele, om det er greit å kjøre for fort og så videre. Det andre perspektivet er arbeidsmiljø. Det at noen velger å lekke skaper usikkerhet hos kollegaer. Det fører til spørsmål om hvem folk kan stole på og ikke. All erfaring viser at det er dårlig for arbeidsmiljøet. Det rammer ikke bare virksomheten du jobber i, men også kollegaene. Og så er det omdømmeperspektivet. Noen tror at de får anerkjennelse hvis de lekker, og at det er noe folk setter pris på. Den langsiktige virkningen er det motsatte. En organisasjon som lekker taper på omdømme. Det vil sakte men sikkert danne seg et bilde av en organisasjon uten kontroll, uten lojalitet, og det er i det lange løp veldig negativt. Den som bevisst lekker skaper veldig mange dårlige konsekvenser, sier Lund-Isaksen.

– Er det en lekkasjekultur i Forsvaret?

– Jeg vil ikke si det er en lekkasjekultur. Når du ser på den totale mengden gradert informasjon vi håndterer, er det snarere unntaket enn regelen at gradert informasjon kommer ut. Men det betyr ikke at vi ikke har et problem med at noen i enkelte tilfeller synes det er legitimt å lekke.

Sterk tilhørighetskultur

– Forsvaret totalt sett kommer sjelden godt ut av lekkasjesaker.

Det sier sjef for Forsvarets sikkerhetsavdeling, kommandør Hans Kristian Herland. Han beskriver Forsvaret som en organisasjon med sterk tilhørighetskultur. Personellet identifiserer seg veldig sterkt med sin egen avdeling, og det er tendenser til en økt tilbøyelighet til å kjempe for at avdelingen deres får den plass og oppmerksomhet de mener den fortjener. Lekkasjer skjer spesielt i omstillingsprosesser, sier han. Eller for eksempel i diskusjoner rundt innkjøp av utstyr og materiell, som i saken rundt det pansrede kjøretøyet Dingo 2. Forsvaret innledet i fjor etterforskning etter at detaljer rundt det pansrede kjøretøyet som brukes i Afghanistan kom ut i media.

– Det er veldig uklokt å fortelle at slike kjøretøyer har noen svakheter, og hva svakhetene er. Det er illjoalt overfor dem som skal benytte kjøretøyet og kan sette personell i fare, sier Herland.

Wikileaks satte for alvor temaet på dagsorden i 2010, med sine lekkasjer av hundretusenvis av amerikanske sikkerhetsgraderte dokumenter. Blant de få som har skaffet seg full tilgang til informasjonen er Aftenposten.

Media har et stort ansvar

– Når vi sitter med informasjon som er knyttet til rikets sikkerhet har vi et stort ansvar. Det tar vi veldig alvorlig.

Hilde Haugsgjerd er sjefredaktør i Aftenposten, som har fått tilgang til 250 000 hemmeligstemplede Wikileaks-dokumenter. Hun forteller at de tar en nøye vurdering på hva slags dokumenter de legger ut.

– Vi legger bare ut ting vi selv har gått grundig gjennom og vurdert, og som vi er trygge på at ikke setter menneskers liv i fare, er uetisk eller uansvarlig å offentliggjøre, sier hun.

Men det kan være ulike vurderinger av hva som knytter seg til rikets sikkerhet. Det er et langt spenn fra konkrete opplysninger knyttet til steder eller navngitte personer i utsatte posisjoner, til overordnede politiske vurderinger av en konflikt eller en utenriks-politisk situasjon, mener Haugsgjerd. Den øverste forsvars- og utenriksledelse vil ikke så sjelden ha en oppfatning av rikets sikkerhet som kan være høyst diskutabel. Det ligger i politikkens og lederskapets mekanismer å ønske seg størst mulig kontroll over informasjonsflyten, sier hun.

Et etisk spørsmål

– Hva slags vurderinger gjør dere i forhold til sikkerheten?

– Tre millioner amerikanske diplomater og forsvarsansatte har trolig allerede hatt tilgang til Wikileaksdokumentene. Da er det lite trolig at de inneholder farlige militære opplysninger. Men det er ting knyttet til enkeltpersoners sikkerhet og jobbsituasjon, for eksempel i Kina, som gjør at vi ikke har publisert opplysninger. Vi gjør vurderinger etter beste skjønn, søker råd, og er vi i tvil publiserer vi ikke.

– Er det greit å lekke gradert informasjon?

– Det spørs hva slags informasjon det dreier seg om. Mediene har til alle tider benyttet seg av taushetsbelagt informasjon. Avsløringer som har ført til vesentlige, positive endringer i samfunnet har vært basert på at folk av ideelle hensyn har lekket til mediene. Det er umulig å svare generelt på når det er etisk akseptabelt å offentliggjøre taushetsbelagt informasjon. Det avhenger av hva som lekkes, til hvem, hvorfor. Det er ikke greit å gjøre det av økonomisk vinnings hensikt for eksempel, sier Hilde Haugsgjerd.

«Vi kan ha så mange brannmurer vi vil, men det er holdningene til de som jobber i systemet som er den store faktoren.»

For mye hemmelighold

Hun sier media har et selvstendig faglig og etisk ansvar for å vurdere publisering av informasjon som er beskyttet av hensyn til rikets sikkerhet. Pressen må vurdere både vesentlighet, den samfunnsmessige betydningen av informasjonen, og om publisering kan innebære en risiko for menneskers liv og helse.

– Det er ikke slik at det er greit for oss å publisere hemmeligstemplet eller taushetsbelagt informasjon selv om kilden sier det, sier Haugsgjerd. Men hun mener det er for mye hemmelighold av informasjon i forvaltningen.

– Hvis vi holder oss utenfor det som har med militæret og samfunnssikkerheten å gjøre, og ser på stats- og kommuneforvaltningen, er det for mye informasjon som holdes utenfor offentligheten av bekvemmelighetshensyn, sier Hilde Haugsgjerd.

Ledelse og holdninger viktig

Hva skal man så gjøre med lekkasjekulturen? Forsvarsdepartementet politianmelder lekkasjer av gradert informasjon.

– Vi som regjeringskontor kan ikke sitte å se på at loven brytes uten å reagere. Vi kan ikke være fristilt i forhold til juss. Vi synes det er viktig å opptre ordentlig. Vi kommer fortsatt til å politianmelde lekkasjer. Så får vi heller ta kjeften med at vi forfølger våre egne, sier Lund-Isaksen.

Samtidig er ledelsen ansvarlig for å skape minst mulig grobunn for lekkasjer. Lekkasjer kan være resultatet av noe du ikke får tilfredsstilt i interne diskusjoner. Det er et lederansvar å sørge for at folk føler de har vært med i de viktige debattene. Samtidig må ledelsen lage en kultur for at folk får være med i viktige debatter uten å lekke, eller lage en alternativ diskusjon.

– Hvordan kan man unngå at informasjon lekker?

– Det er snakk om den menneskelige faktoren. Vi kan ha så mye brannmurer vi vil, men det er holdningene til de som jobber i systemet som er den store faktoren. Hvis du mangler lojalitet og forståelse, har du en risikofaktor du ikke har kontroll på.

– Er ikke lojalitet et veldig gammeldags ord?

– Jeg håper inderlig ikke det. Jeg har veldig sjelden møtt folk som ikke sier at de føler noe for arbeidsplassen de jobber i, sier Erik Lund-Isaksen.

Arne Røed Simonsen, seniorrådgiver NSR. Foto: Morten Brakestad, Propix

De ubevisste lekkasjene

Ikke alle lekkasjer er bevisste. Det mener seniorrådgiver Arne Røed Simonsen i Næringslivets sikkerhetsråd.

NSR jobber aktivt for å bekjempe kriminalitet i og mot næringslivet. Det er en bevisstløs lekkasjekultur både i næringslivet og forvaltningen, mener han.

– Noen ganger ønsker kanskje ansatte å vise at de er flinke og vet mye. Da forteller du kanskje mer enn du burde gjøre. Man bør bevisstgjøre folk om hva de snakker om, hvor, med hvem, enten det dreier seg om sosiale medier, eller hva du snakker om på bussen eller på flyet. Jeg har sittet på fly opptil flere ganger og hørt byråkrater fra departementer snakke sensitivt, sier han.

Hilde Haugsgjerd, sjefredaktør i Aftenposten. Foto: Aftenposten

Soner Sevin og Marte Lerberg Kopstad i Utenriksdepartementet. Foto: NSM

Sikkerhetskampanjene

Én ansatt med én minnepinne kan forårsake at alle sikkerhetsmekanismene i organisasjonen din blir null verdt, sier datasikkerhetsleder i Utenriksdepartementet, Soner Sevin.

– Her sitter utenriksministeren, og her borte sitter utenriksråden. Datasikkerhetsleder i Utenriksdepartementet Soner Sevin viser rundt i korridorene over 7. juniplassen i Oslo. Det er korridorer som trolig svært mange gjerne skulle hatt tilgang til.

– Hvis du tenker på sannsynligheten for å bli utsatt for dataangrep er nok Utenriksdepartementet langt fremme. Vi forvalter sensitiv informasjon. Vi reiser mye. Vi opererer i utlandet, og i områder vi ikke har kontroll over, sier Sevin.

Plakater og brosjyrer

I fjor stod hans seksjon, med god hjelp fra kommunikasjonsbyrået Miksmaster, bak en kampanje for sikkerhetskultur som er blitt lagt merke til. Kampanjen rettet seg mot alle de ansatte i Oslo, og er nå sendt ut til alle utenriksstasjonene, fra Kina til Washington. Mannshøye «trojanske hester» ble satt ut i resepsjonen, som symbol på spionprogrammer som kan smugles inn i datasystemene via minnepinner. Ansatte ble minnet om at navnet på båten eller favorittfilmen din er et dårlig passord, om å låse PC-en når du tar lunsj, og tenke på hva du laster ned på vedlegg på e-post. Plakater ble satt opp i heisene, på speilene på toalettene, og over makuleringsmaskinene. Brosjyrer med IKT-retningslinjer ble hengt opp på hver enkelt PC.

– Vi har brukt humor og nysgjerrighet bevisst for å få brukernes oppmerksomhet, sier Sevin.

«Sikkerhetskultur og sikkerhetsbevissthet er utrolig viktig.»

Store utfordringer

Han beskriver store utfordringer som ikke løses med tekniske tiltak alene. Definitivt.

– Hele den tekniske muren er null verdt hvis det kommer en trådløs enhet inn på nettverket og sender informasjon ut, som for eksempel en mobiltelefon. Alle bruker minnepinner eller ulike USB-enheter nå. Det tar sekunder å laste ned informasjon fra PC-en. Vi reiser mye rundt om i verden. Hvis du kjeder deg på en flyplass tar du kanskje opp laptopen og surfer på aviser, og velger det nærmeste og billigste trådløsnettverket, som lett kan avlyttes. PC-er på hotellrom kan tømmes utrolig fort. Delegasjoner får minnepinner i gave som kan inneholde virus. UD er en global organisasjon, og du kan koble deg inn i systemet fra alle kanter av verden. Sikkerhetskultur og sikkerhetsbevissthet er utrolig viktig, sier Sevin.

Falske e-poster

– Som høyteknologisk bedrift er Nammo et interessant mål for industrispionasje.

Noen vil stjele hemmelighetene i bedriften til IT Manager Ole Ingarth Karlsen. Forsvarsprodusenten Nammo omsetter for 3,5 milliarder kroner i året, har 2000 ansatte i sju forskjellige land og 18 produksjonssteder. I fjor opplevde bedriften fem målrettede spionasjeforsøk mot datasystemene på hovedkontoret, blant annet gjennom falske e-poster med infiserte vedlegg. Bedriften er nå godt i gang med en ny sikkerhetskulturkampanje som omfatter alle ansatte i de ulike landene.

– Vi hadde en erkjennelse av at vi ikke ville kunne klare å beskytte bedriften med IT-sikkerhetssystemer alene. Vi måtte ha de ansatte med på laget, sier Karlsen.

Foto: Miksmaster as - www.miksmaster.no

Han ønsker først og fremst at de ansatte skal være svært varsomme med å åpne lenker og vedlegg i e-post fra personer de ikke kjenner, i tillegg til å tenke gjennom en rekke andre IT-sikkerhetsutfordringer både på jobb og hjemme. Symbol for kampanjene har vært «spionfluer», som et bilde på noe lite og nesten usynlig som kan komme inn i datasystemene og se og høre alt du gjør. «Fly on the wall» er et begrep som er kjent i landene de opererer i.

– Brukerne har vært flinke og er helt klart blitt mer oppmerksomme og varsomme, sier han.

Mer oppmerksomme

Og også i Utenriksdepartementet har kampanjen hatt effekt.

– Folk snakker fortsatt om kampanjen, etter at vi har tatt ned plakatene. Det er utrolig positivt, sier Soner Sevin.

– Vi har blitt oppmerksomme på en del ting vi egentlig vet, men som vi kanskje ikke har like stor oppmerksomhet på hele tiden. Jeg var nylig på reise i utlandet etter at kampanjen startet, og da var jeg veldig forsiktig, sier kommunikasjonsrådgiver Marte Lerberg Kopstad.

(Soner Sevin har siden artikkelen ble skrevet begynt i ny jobb i en annen virksomhet.)

Soners 3 råd om kampanjer for sikkerhetskultur

1. Keep it simple! Hvis du ønsker å nå sluttbrukerne må budskapet være enkelt.
2. Lag dine egne anbefalinger. De må tilpasses trusselbildet organisasjonen er utsatt for. Det er viktig at sluttbrukerne kjenner seg igjen.
3. Tenk nytt, vær kreativ, bruk farger og illustrasjoner for å gjøre budskapet mer treffsikkert.

Ole Ingarths 3 råd om kampanjer for sikkerhetskultur

1. Søk råd hos noen som har gjort dette tidligere, så slipper du å finne opp kruttet på nytt.
2. Viktigheten blir ofte understreket når også toppledelsen snakker om betydningen av god IT-sikkerhet.
3. Gjenta budskapet, det kan ikke sies mange nok ganger.

Sikkerhetskultur på Stortinget:

Tar oppgjør med bevisstløsheten

Ine Marie Eriksen Søreide bruker nesten aldri minnepinner, har ikke Facebook- eller Twitter-konto, og blir veldig skeptisk når hun får e-poster fra folk hun ikke kjenner til. – Man tenker ofte at «jeg har ikke noe hemmelig», men hvis du ikke er forsiktig handler det i realiteten om å gi folk tilgang til et helt system av informasjon, sier lederen av Utenriks- og forsvarskomiteen.

På Løvebakken må jakker, nøkler og lommebøker gjennom scanneren ved inngangen før du slipper inn. Strenge vakter sørger for kontroll på alle besøkende. Minnepinner med virus eller vedlegg på e-post kan det være vanskeligere å ha full kontroll med.

– Jeg tror det er veldig variabelt med hvor oppmerksomme vi politikere er på informasjonssikkerhet. Jeg satt åtte år i Utdanningskomiteen, og hadde alle mine foredrag på en minnepinne som jeg stappet inn i så å si alle PC-er, inkludert min egen.

Bør ha stor bevissthet

Ine Marie Eriksen Søreide fra Høyre leder Utenriks- og Forsvarskomiteen på Stortinget. Hun fikk en a-ha-opplevelse da hun gikk inn i komiteen i 2009, og fikk orienteringer fra blant andre Politiets sikkerhetstjeneste om informasjonssikkerhetstruslene, e-poster med spionvedlegg og så videre.

– På utenriks- og forsvarsfeltet får man veldig fort forståelsen av at man håndterer informasjon som er langt mer interessant for utenforstående enn den man tidligere har hatt. Og det er jo ingen grunn til at man bør begrense det til dem som holder på med utenriks- og forsvarspolitikk. Tvert i mot. Vi bør ha en stor bevissthet i hele systemet her, sier hun.

Det er lett å tenke at man selv ikke er et spesielt interessant mål for noe som helst. Den tanken gjelder det å løsrive seg fra, mener Eriksen Søreide.

«Jeg er blitt veldig oppmerksom på hva jeg får av gaver, for eksempel minnepinner.»

Naive nordmenn

– Det er jo ofte den informasjonen og menneskene du har tilgang til som er potensielt interessant, og da må du agere på en spesiell måte for å beskytte den og de. Det er det som er kjernen, sier hun, og forteller blant annet at hun nesten aldri bruker minnepinner lenger, og blir veldig oppmerksom på e-poster fra navn hun ikke kjenner til, blant annet på grunn av alle de dataangrepene som kan komme inn i systemet via falske e-poster.

Gaver går rett til skanning.

– Jeg er blitt veldig oppmerksom på hva jeg får av gaver, for eksempel minnepinner. Hva som helst kan jo være på de minnepinnene, sier hun.

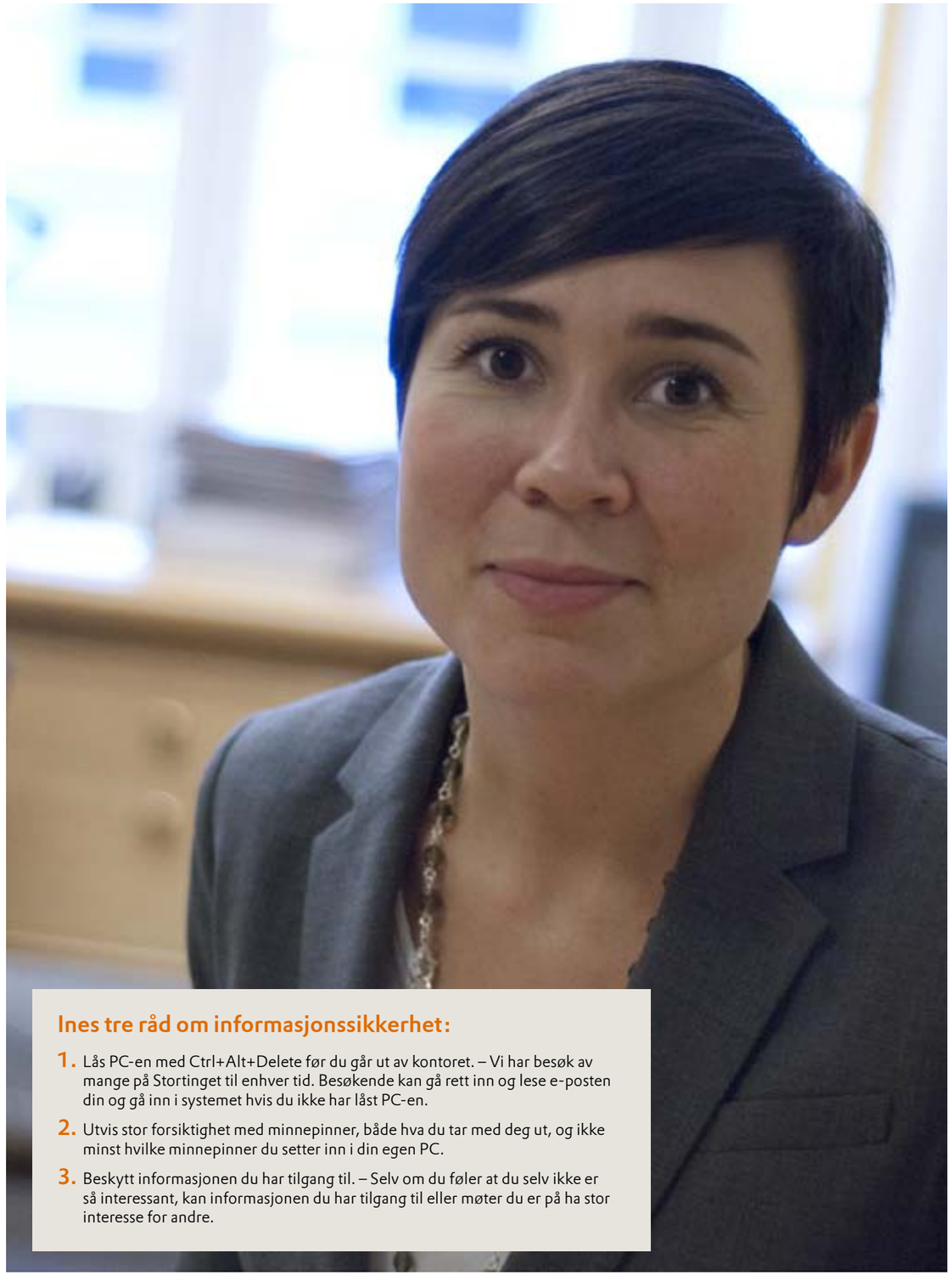
Og nordmenn kan være litt naive, tror Ine Marie Eriksen Søreide.

– Jeg tror nok vi i Norge har en litt naiv forestilling om at det ikke er noen som vil Norge noe vondt, det at det ikke er noen som ønsker å spionere på oss. «Så ille er det vel ikke?» Jeg tror vi bare må kvitte oss med de tankene, og legge til grunn at informasjon om sentrale samfunnsområder i Norge er interessant for andre, sier hun.

Besøkte NSM

Utenriks- og forsvarskomiteen besøkte før jul Nasjonal sikkerhetsmyndighet for å få mer informasjon om virksomheten og fagområdene NSM jobber med.

– Besøket var en nyttig påminner for mange om at den største utfordringen for alle er ens egen litt ubevisste atferd, sier leder av komiteen, Ine Marie Eriksen Søreide.



Ines tre råd om informasjonssikkerhet:

1. Lås PC-en med Ctrl+Alt+Delete før du går ut av kontoret. – Vi har besøk av mange på Stortinget til enhver tid. Besøkende kan gå rett inn og lese e-posten din og gå inn i systemet hvis du ikke har låst PC-en.
2. Utvis stor forsiktighet med minnepinner, både hva du tar med deg ut, og ikke minst hvilke minnepinner du setter inn i din egen PC.
3. Beskytt informasjonen du har tilgang til. – Selv om du føler at du selv ikke er så interessant, kan informasjonen du har tilgang til eller møter du er på ha stor interesse for andre.

Ine Marie Eriksen Søreide (H).
Foto: NSM

NSM I 2010

NSM når målene direktoratet har satt seg, med et godt, men stramt budsjett. Viktige saker i løpet av året har vært ny forskrift om objektsikkerhet, og en ny blankett for de over 25 000 personene som årlig sikkerhets-klareres i Norge. En av NSMs utfordringer er rekruttering. Og det er mange engasjerte mennesker i Nasjonal sikkerhetsmyndighet, forteller Lena Bjørgum og Runa Skimten.

Foto: Pål Rødahl/tinagent

NSMs ledelse (f.h.)

- **Kjetil Nilsen**, direktør, er politiutdannet, jurist, har en mastergrad i ledelse, samt NATO Defence College.
- **Åshild Salmela**, avdelingsdirektør for Administrasjonsavdelingen, har utdanning innen økonomi og ledelse.
- **Tore Gustafsson**, kommandør og avdelingssjef for Avdeling for sikkerhetskultur, er utdannet på Sjøkrigsskolen, Forsvarets stabsskole, og har i tillegg gått på Forsvarets Høgskole.
- **Christophe Birkeland**, avdelingsdirektør for NorCERT, har en doktorgrad fra NTNU og har gått på Forsvarets høgskole.
- **Hans Robert Bjørnaas**, oberst og avdelingssjef for Kommunikasjons- og systemsikkerhetsavdelingen, er utdannet på Luftkrigsskolen og Forsvarets stabsskole.
- **Vigdis Grønhaug** (ikke til stede da bildet ble tatt), avdelingsdirektør for Avdeling for sikkerhetsforvaltning, har militær befalsutdanning, er høgskoleingeniør og bedriftsøkonom.

Tall i millioner kroner	**Budsjett 2010**	**Regnskap 2010**	Regnskap 2009	Regnskap 2008	Regnskap 2007	Regnskap 2006
Lønnsutgifter	*78,9*	***78,2***	*77,9*	*71,5*	*66,0*	*62,0*
Utgifter til varer og tjenester	*38,3*	***47,6***	*41,5*	*44,5*	*49,6*	*51,5*
Sum driftsutgifter	117,2	**125,9**	119,4	116,0	115,6	113,5
Inntekter og refusjoner	2,9	**12,3**	11,4	9,9	10,6	14,4
Netto	**114,2**	**113,6**	108,0	106,1	104,9	99,1

ÅRSKAVALKADE

18. januar: Justisministeren og Forsvarsministeren mottok NSMs forslag til en nasjonal strategi for cybersikkerhet på NorCERT. Slik NSM ser det er det nå behov for en sektorovergripende tilnærming for å sikre de viktigste informasjonsressursene mot de mest alvorlige hendelsene.

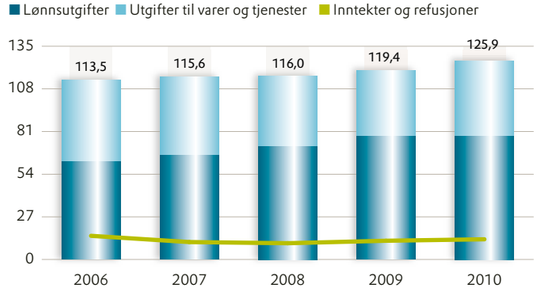
28. februar: Det nederlandske firmaet Brightsight BV ble godkjent av sertifiseringsordningen for IT-sikkerhet, SERTIT, som ligger under NSM. Firmaet spesialiserer seg på chip-evalueringer.

02. mars: ITAKT-prisen for 2009 ble utdelt til NSMs avdelingsdirektør Christophe Birkeland, sjef for NorCERT. Prisen fikk han for hans mangeårige innsats for å spre kunnskap om utviklingen av IKT-risikobildet.

16. mars: NorSIS og NSM arrangerte sammen den første sikkerhetskulturkonferansen Sikker.info på Lillehammer 16. – 17. mars. Maihaugen var en verdig ramme rundt arrangementet som hadde 65 deltakere fra så vel offentlig som privat sektor.

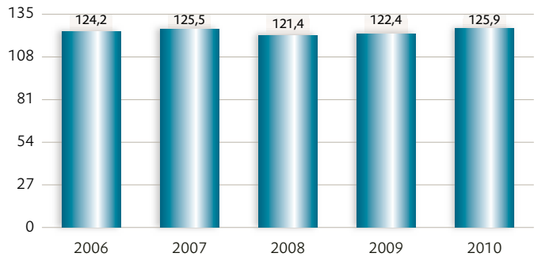
Driftsregnskap 2006–2010

Tall i millioner kroner



Sum driftsutgifter 2006-2010

Faste 2010-kroner i millioner



NSM i 2010:

Når målene

NSM har i 2010 hatt et godt, men stramt budsjett. Direktoratet har i stor grad nådd årets mål, både når det gjelder strategiske initiativ og løpende produksjon. Det økonomiske resultatet for driften viser et samlet mindreforbruk på 0,6 mill kr, som tilsvarer 0,5 % av bevilgningen.

NSM er en kunnskapsbasert virksomhet, med stor grad av spesialistkompetanse innen et bredt oppgavespekter. Rekruttering og vedlikehold av kompetansen er viktige virkemidler for å ivareta direktoratets oppgaver. Faren for svikt i den faglige kompetansen er et av de risikomomenter som negativt kan innvirke på måloppnåelsen.

Utvikler sikkerhetstiltak

Tilsynsvirksomheten er en sentral del av NSM, og det legges særlig vekt på å trekke erfaringer fra tilsynsvirksomheten og analyser av sikkerhetstilstanden inn i videreutviklingen av sikkerhetstiltak. Virksomheten har ikke blitt gjennomført i ønsket omfang i løpet av 2010. I denne situasjonen har det vært lagt ekstra vekt på organisere aktiviteten slik at det likevel er skaffet tilveie et godt grunnlag for utviklingsarbeidet.

Når målgruppene

Pågangen etter foredragsbistand fra NSM er på et stabilt høyt nivå, og direktoratet har bidratt med både generell og spesiell informasjon overfor en rekke oppdragsgivere. Sikkerhetskonferansen og andre konferanser og kurs direktoratet arrangerer har høye deltakerantall, og får gode tilbakemeldinger. Trafikken på NSMs nettsider viser en økende trend, og er en enkel måte å få gitt relevant informasjon til målgruppene på. Her publiseres også en overordnet beskrivelse av IKT-trusselbildet to ganger i året. Det er utviklet et nytt konsept for rapport om sikkerhetstilstanden, som innebærer en mer spisset rapport i forhold til virksomhetenes oppfølging av sikkerhetsloven.

Styrker samfunnets evne til å oppdage og reagere

Aktiviteten og operativiteten i NorCERT øker. En VDI-sensor med stor trafikk ble koblet fra i september, noe som medførte nedgang i den totale datamengden som analyseres. Justert for dette viser imidlertid trenden fortsatt økning i trafikken.

Inntrengingstesting har i løpet av 2010 vist seg som et godt virkemiddel for å motivere og ansvarliggjøre virksomhetene til å styrke sikkerheten i egne systemer.

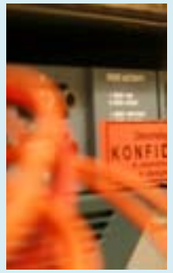
Analyse av skadelig programvare, malwareanalyse, er av betydning for nasjonal suverenitet og vår internasjonale posisjon i cyberrommet. Men malwareanalyse er en svært konkurranseutsatt kompetanse som det er for lite av i Norge, noe som også er en utfordring for NSM.

Forslaget til cyberstrategi er et annet område som involverer og engasjerer NSMs fagmiljøer. Direktoratet ser frem til å bistå departementet i arbeidet med å bearbeide forslaget.

02. juli: Inntrengingstesting (pentest) i graderte systemer er en oppgave for NSM, hjemlet i sikkerhetsloven. NSM har blitt gitt et utvidet mandat til også å gjennomføre slike tester i ugraderte, men kritiske systemer i virksomheter omfattet av loven.

09. juni: NSMs årsmelding for 2009 med tittelen «Cybersikkerhet» ble utgitt. Årsmeldingen inneholdt som vanlig vår årlige rapport om sikkerhetstilstanden. Hovedkonklusjonen i denne er at våre nasjonale hemmeligheter er for dårlig sikret.

15. juni: Elektromagnetisk stråling fra informasjonssystemer er en alvorlig sårbarhet som kan resultere i kompromittering av gradert informasjon om den ikke håndteres. NSM satte fokus på denne utfordringen i et vel besøkt seminar på Oscarsborg festning 15. – 18. juni. Både teknisk personell og ledere deltok.



20. august: NSM sender ut sikkerhetsvarsel om dataormen Stuxnet som er rettet mot industrisystemer. NSM har i flere år advart mot at industrisystemer kan bli utsatt for dataangrep. Stuxnet representerer en alvorlig utvikling i IKT-risikobildet.

Fornøyde brukere

NSMs brukere er stort sett fornøyd med informasjonen de får. I en informasjonsundersøkelse direktoratet gjennomførte før jul fikk nettstedet karakteren 4,48 på en skala fra 1 til 6, hvor 1 var meget dårlig og 6 var meget bra. NSMs veiledninger fikk 4,88, brosjyrer som «Sikrere bruk av minnepinner» fikk karakter 4,92, og NSMs mediebrief fikk karakteren 5,15.

Sikrer tilliten, forenkler og effektiviserer sikkerhetsarbeidet

Det er avgjørende for NSM å ha tillit i samfunnet. EOS-utvalget har i sin årlige rapport ikke hatt merknader til NSMs arbeid. Direktoratet anser dette som et uttrykk for tillit. Vurderingen av oppslag i media om NSM viser at direktoratet i hovedsak fremstilles på en positiv måte. NSM har i 2010 begynt på et utviklingsarbeid knyttet til internkontroll, og satsningen på dette området vil forsterkes i 2011. Implementering av forsvarssektorens handlingsplan for holdning, etikk og ledelse (HEL) er også et område som er viet fokus.

Saksbehandlingstid er en viktig parameter for måling av brukertilfredshet knyttet til effektiviteten i sikkerhetsarbeidet. For personkontroll er saksbehandlingstiden noe økt fra 2009, men fortsatt innenfor definert målsetting. Saksbehandlingstiden for klareringssaker i førsteinstans og klagebehandling av klareringssaker er begge redusert i 2010.

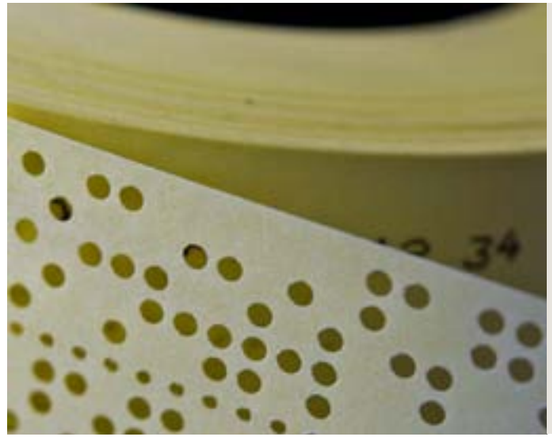
I desember lanserte NSM ny personopplysningsblankett til bruk ved anmodning om sikkerhetsklarering, og veileder til utfylling av blanketten. Det er første gang det gis ut en slik veileder. Den nye blanketten gjenspeiler de lov- og samfunnsmessige endringer som har skjedd siden forrige revisjon i 2000. Blanketten er tatt i bruk fra årsskiftet.

En etterspurt bidragsyter og samarbeidspartner

NSM opplever stor etterspørsel fra samarbeidspartnere både nasjonalt og internasjonalt. Med utgangspunkt i direktoratets oppgaveløsning etter sikkerhetsloven og NorCERT står PST og Etterretningstjenesten naturlig nok i en særstilling. Det legges ned betydelig innsats for å vedlikeholde samarbeidet som er bygget opp over mange år med utenlandske samarbeidspartnere. I og med at andre land ikke er organisert på samme måte på etterretnings- og sikkerhetsområdet som Norge, er det nødvendig at NSM opprettholder kontakt med flere etater i de enkelte land.

Fokus på økonomi

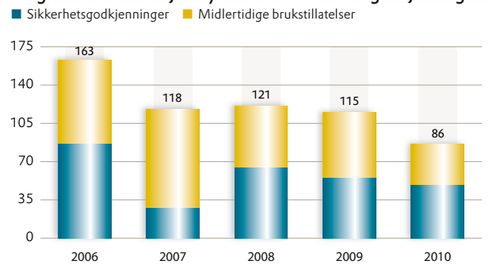
NSM har løpende fokus på effektiv ressursutnyttelse, kostnadseffektiv myndighetsutøvelse og kostnadseffektiv utvikling av sikkerhetstiltak. I henhold til krav fra departementene er det gjennomført interneffektivisering tilsvarende 0,5 prosent av budsjettet. Kundefinansiert aktivitet er i 2010 videreført på nivå med foregående år. NSMs inntektsside består i stor grad av refusjoner til dekning av tilsvarende merutgifter.



Mister summetonen uten NSM

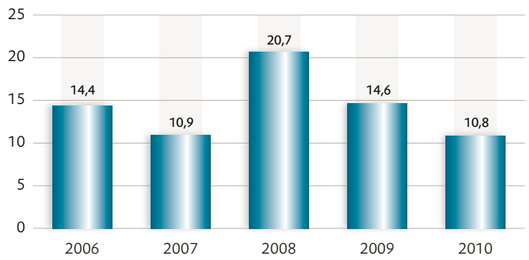
Uten kryptonøkler fra NSM mister Forsvaret, utenrikstjenesten og offentlig forvaltning det graderte sambandet og summetonen i titusenvis av telefoner. NSM produserer og distribuerer kryptonøklene som er nødvendig for det sikre sambandet i telenettet, mellom datamaskiner, og i nettverk og systemer. I fjor ble det produsert rundt 22 000 kryptonøkler. Antall telefonhenvendelser til kryptosupport var på rundt 3000. I tillegg hadde NSM 13 ukelange kureroppdrag for å frakte kryptonøkler sikkert frem dit de skal.

Antall sikkerhetsgodkjenninger og midlertidige brukstillatelser for graderte informasjonssystemer hvor NSM er godkjenningsansvarlig



Utgifter til FoU og materiellinvesteringer 2005-2010

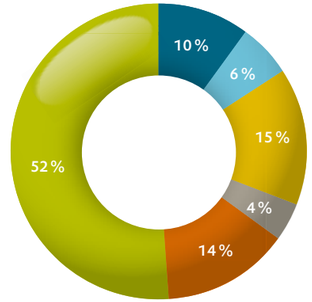
Faste 2010-kroner i millioner



Figuren viser utviklingen i NSMs utgifter til forskning og utvikling og materiellinvesteringer ført på kapittel 1760 i perioden 2006-10 korrigert for prisvekst.

Foredragsvirksomhet

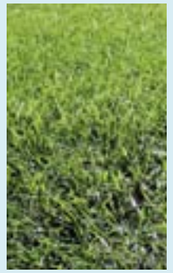
Fordelt på oppdragsgiver i 2010



August: NSM innfører i august en endring av praksis for kontroll med luftfotografering og produksjon av kartmateriale. Gjennom depixellering kan skjermingsverdige objekter nå sees på foto, men ikke detaljene.

August: En ny bølge med «wikileaks» skyller inn over verdenssamfunnet. Denne gangen omfatter lekkasjene amerikanske diplomatiske dokumenter som også omfattet norske forhold. Mange kommentatorer og eksperter drøfter konsekvenser for diplomatisk arbeid og utfordringer for sikkerhetstjenesten.

01. september: PST, POD og NSM utga sammen en veileder i sikkerhets- og beredskapstiltak mot terrorhandlinger. Veilederen retter seg mot offentlige og private virksomheter.



15. september: Direktorater som vil følge med i tiden må være til stede der det skjer. NSM startet derfor sikkerhetsbloggen som et prøveprosjekt. Målgruppen er folk som jobber med informasjonssikkerhet til daglig, sikkerhetsledere i offentlige og private virksomheter, og andre som er opptatt av informasjonssikkerhet.

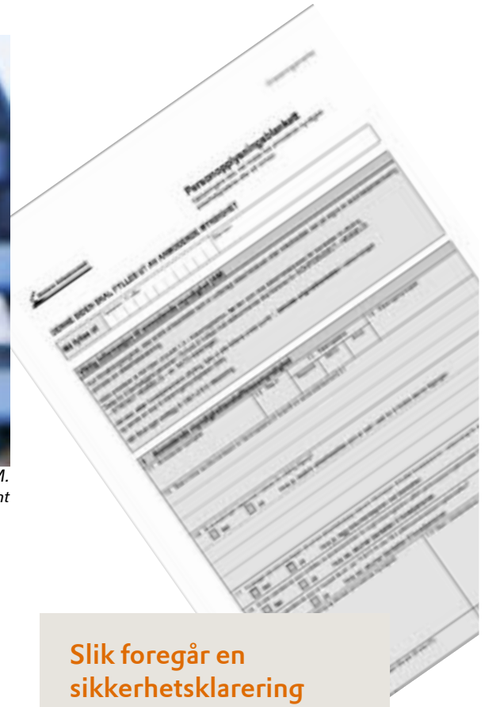
22. oktober: En milepæl blir passert. Objektsikkerhetsforskriften blir vedtatt i statsråd. Dette legger til rette for en tverrsektoriell tilnærming for egenbeskyttelsen rundt potensielle terror- og sabotasjemål i samfunnet.

Oktober: NSM får i oppdrag av Fornyings-, administrasjons- og kirkedepartementet å foreta en tilstandsvurdering av det ugraderte nettet i departementene. Bakgrunnen er Dokument 1 fra Riksrevisjonen, som hadde en rekke kritiske merknader til informasjonssikkerhetsarbeidet i statsforvaltningen.

09. november: NSM arrangerte sin årlige nasjonale sikkerhetskonferanse i Oslo 9. - 10. november. Årets tema var Sikker ledelse og cybersikkerhet. Justisministeren og Forsvarsministeren hilste konferansen fra kinoleretet. Det var ny rekord i oppslutningen med ca 380 eksterne deltakere.

09. desember: Revidert personopplysningsblankett ble lansert på seminar i Oslo sentrum. Blanketten er det av NSMs produkter som «treffer» flest nordmenn, ca. 25 000 i året, i forbindelse med sikkerhetsklarering.

Hanne Mauseth, saksbehandler i NSM.
Foto: Pål Rødahl/tinagent



Ny personopplysningsblankett:

Selvangivelsen

De aller fleste må fylle ut mindre informasjon i den nye personopplysningsblanketten som Nasjonal sikkerhetsmyndighet utarbeidet i fjor. Blanketten er den sikkerhetsmessige selvangivelsen du og jeg må levere inn for å få sikkerhetsklarering.

Alle som skal sikkerhetsklareres i Norge må fylle ut en personopplysningsblankett. I blanketten redegjør de blant annet for statsborgerskap, sivil status og familieforhold, strafferettslige forhold og sitt forhold til rus og alkohol. Blanketten er kort og godt den sikkerhetsmessige selvangivelsen alle og enhver må fylle ut for å få sikkerhetsklarering.

Vurderer sikkerhetsklarering

– Den første indikasjonen man får på en persons sikkerhetsmessige skikkethet er gjennom personopplysningsblanketten, sier saksbehandler Hanne Mauseth i Nasjonal sikkerhetsmyndighet.

Hvis det er store forskjeller mellom informasjonen den enkelte har fylt ut i blanketten kontra det som avdekkes i personkontrollen, vil det vurderes om sikkerhetsklarering kan gis.

I fjor utarbeidet Nasjonal sikkerhetsmyndighet en ny blankett for personopplysninger til bruk i forbindelse med sikkerhetsklarering og autorisasjon.

Mindre å fylle ut

Selv om personopplysningsblanketten nå er på hele 11 sider, må de aller fleste fylle ut færre opplysninger enn tidligere.

Hovedregelen er at alle som skal klareres for KONFIDENSIELT eller HEMMELIG nå slipper å føre opp personopplysninger på foreldre, barn og søsken. Den nye blanketten inneholder også spørsmål om hva slags tilknytning folk har til andre land, etter at endringer i sikkerhetsloven i 2006 førte til at også utenlandske statsborgere i større grad kunne klareres.

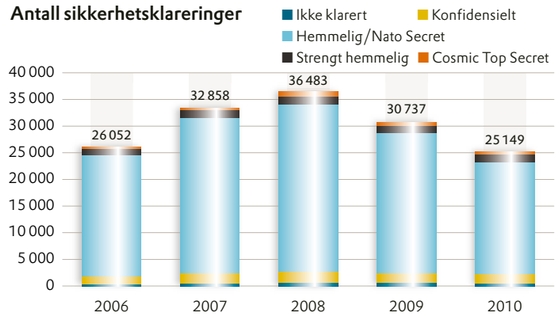
Innhenter personopplysninger

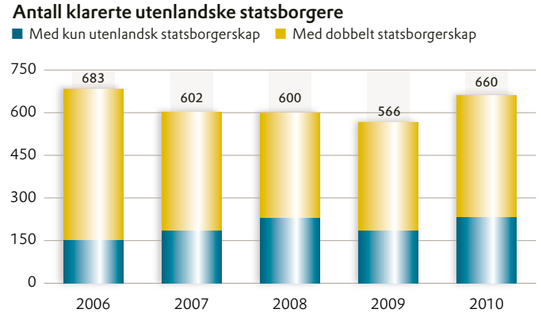
I Norge er det 44 klareringsmyndigheter som sikkerhetsklarerer personer som skal ha tilgang til sikkerhetsgradert informasjon. Forsvarets sikkerhetsavdeling (FSA) er den største, og rundt 85 prosent av sikkerhetsklareringene blir gjort der. Det er imidlertid Nasjonal sikkerhetsmyndighet som innhenter personopplysninger om de som skal klareres, blant annet fra strafferegistre, kredittregistre og så videre.

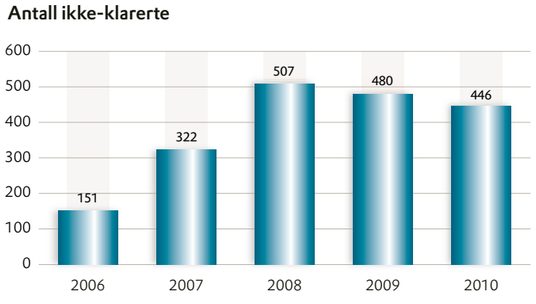
NSM skal også utarbeide tiltak for å forhindre at personer som kan utgjøre en sikkerhetsrisiko får tilgang til gradert informasjon.

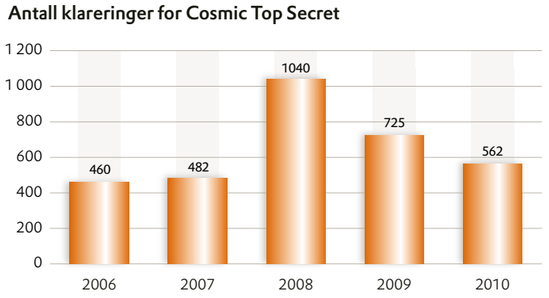
Slik foregår en sikkerhetsklarering

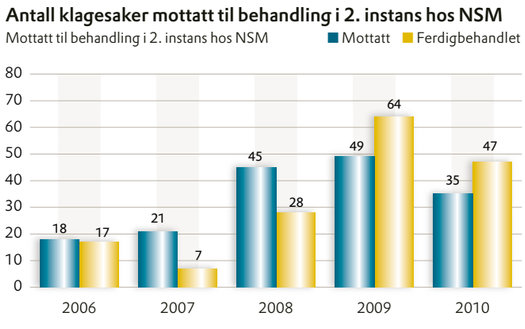
1. Du er aktuell for en stilling eller en tjeneste som gir tilgang til sikkerhetsgradert informasjon.
2. Din overordnede ber deg derfor fylle ut en personopplysningsblankett.
3. Den kontrolleres og sendes til Nasjonal sikkerhetsmyndighet (NSM).
4. NSM iverksetter personkontroll med informasjon fra flere ulike kilder, blant annet Bøteregistret, Straffesaksregistret, Politiets sikkerhetstjeneste (PST), Det sentrale folkeregister og private kredittopplysningsregistre.
5. Resultatet sendes til din klareringsmyndighet.
6. Klareringsmyndigheten fatter sin avgjørelse, med fire mulige utfall: Klarering som anmodet, klarering med vilkår, nedsatt klarering eller ingen klarering.
7. Klareringsbevis sendes virksomheten
8. Hvis du ikke får klarering som anmodet, får du beskjed og kan klage











Hva påvirker en sikkerhetsklarering?

Klareringsavgjørelser beror alltid på en konkret vurdering av den enkelte sak, og er sammensatt. Her er noen forhold som kan påvirke klareringsavgjørelsen.

- En økonomisk situasjon som øker faren for press
- Psykiske problemer og annen sykdom som påvirker dømmekraft
- Misbruk av rusmidler
- Under politietterforskning
- Tidligere straff, herunder for gjentatte mindre forseelser
- Manglende personhistorikk, for eksempel som følge av utenlandsopphold i land Norge ikke har sikkerhetsmessig samarbeid med
- Å nekte å oppgi opplysninger om seg selv
- Å gi uriktig informasjon i personkontrollskjemaet eller ved sikkerhetssamtaler

Foto: ESA - P. Carril,2010

Sikrar Europa sitt nye navigasjonssystem:

Sikkert på bakken

Galileosystemet vil bestå av rundt 30 satellittar, og ein verdsomspennande bakkeinfrastruktur til bruk for kontroll av satellittane og ytinga til systemet. Svalbard kan bli ein av dei første bakkestasjonane i det storstilte satellittprosjektet som vert tryggleiksgodkjent. Nasjonalt tryggingsorgan (NSM) er ansvarleg for at tryggleiken vert teke hand om i samband med bakkestasjonar på norsk jord.

Tryggleiksgodkjenninga betyr at bakkestasjonen er førebudd for operativ status, og inneber at nødvendige tryggleikstiltak for å ta hand om integriteten og tilgjengelegheiten til systemet er på plass. Nasjonalt tryggingsorgan koordinerar implementeringa av tryggleiksstiltaka, mens KSAT har det operative ansvaret i Noreg. NSM er også ansvarleg for at operatørar har nødvendig leverandørklarering. Direktoratet jobbar også saman med EU og European Space Agency om å utarbeide lokale tryggleiksprosedyrar for bakkestasjonar på norsk jord.

Mykje koordinering

Galileoprosjektet er det største, og første, felles infrastrukturprosjektet i EU. Galileo er EU sitt eige uavhengige system for navigasjon, og skal kunne brukast saman med amerikanske GPS. Bakkestasjonane har ei rekke operative oppgåver. Dei styrer antenner for å få best mogleg signal, og sender korreksjonar til satellittane. I Noreg er det planlagt tre stasjonar, utanfor Longyearbyen på Svalbard, på Jan Mayen, og på den norske Troll-stasjonen i Antarktis. Prosjektet startar oppskytinga av satellittar i år.

- I prosjekt som Galileo er det mykje arbeid som skal utførast. Det er store mengder med dokument som skal gjennomgåast, og kravsett som skal tilpassast norske forhold. Nasjonalt tryggingsorgan har eit nært samarbeid med Norsk Romsenter, og deltar også i arbeidsgrupper i EU som har ansvaret for tryggleiken i programmet. Det er mykje møteverksemd, og mykje koordinering både nasjonalt og internasjonalt som skal gjerast, seier seksjonssjef Øivind Christophersen i NSM.

Foto: NSM

Ill.foto: Colourbox

Fleire kan bli lagt under tryggingslova

Forskrifta om objekttryggleik kan innebere at fleire private verksemder vert underlagt tryggingslova. Det er ikkje usannsynleg at det vert identifisert skjermingsverdige objekt i private verksemder som i dag ikkje er underlagt lova. Ei endeleg avgjerd om at tryggingslova skal gjerast gjeldande for ein bestemt verksemd vert gjort av Forsvarsdepartementet etter ei grundig saksbehandling.

Objekttryggleik:

Nytt regelverk styrkjer tryggleiken

I fjor haust vart forskrift om objekttryggleik vedteke av regjeringa. Forskrifta inneber at tryggleiken rundt bygg, anlegg og andre objekt blir styrkt mot terror, sabotasje og spionasje.

- I forskrifta vert det gjeve nærare bestemmingar om utpeiking, klassifisering og vern av det som kallast skjermingsverdige objekt. Det er objekt som er så viktige at det kan skade riket sitt sjølvstende og tryggleik eller andre vitale nasjonale tryggleiksinteresser dersom dei blir utsett for terror- og sabotasjeåtak. Gjennom dette regelverket etablerast eit felles tryggleiksnivå for desse objekta. Det seier underdirektør og seksjonssjef i Nasjonalt tryggingsorgan, Dagfinn Buset.

Kritiske nodar

Mange bygg og anlegg og andre objekt er i dag godt verna mot terror, sabotasje og spionasje i Noreg. Men det finnast ingen heilskapleg oversikt over kva som er beskytta, og korleis det er beskytta. Den nye forskrifta inneber ei overordna koordinering av det førebyggjande tryggleiksarbeidet på dette området, og vil sikre at avhengigheiter på tvers av sektorar i samfunnet vurderast med omsyn til behov for vern.

- Kva kan eit typisk objekt vere?

- Det kan til dømes vere ein stor datasentral, ein kritisk node i kraftinfrastrukturen eller olje- og gassinfrastrukturen, kommandosentralar, store lager av ekstremt farlege stoff, symbolbygningar og så vidare, seier Dagfinn Buset.

Mange spørsmål

Det er departementa som har ansvar for å peike ut dei skjermingsverdige objekta innan sine ansvarsområde. Deretter skal objekta klassifiserast som VIKTIG, KRITISK eller MEGET KRITISK. NSM utarbeider no ei rettleiing om korleis det nye regelverket skal implementerast.

- Det er mange verksemder som har spørsmål om korleis regelverket skal settast ut i praksis. Ei rettleiing vil vere eit viktig verktøy. NSM kommer også til å gjennomføre ein møteserie i 2011 for å sjå til at identifiseringa og klassifiseringa av skjermingsverdige objekt skjer i alle sektorar, seier underdirektør Dagfinn Buset.

«Det er mange verksemder som har spørsmål om korleis regelverket skal settast ut i praksis.»

Dagfinn Buset, seksjonssjef i NSM.
Foto: Pål Rødahl/tinagent

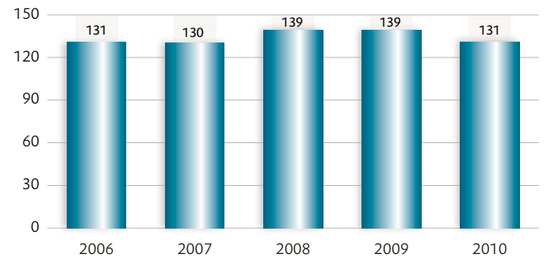
Kva må skjermast?

Typiske objekt som bør skjermast mot terror og sabotasje kan vere:

- Produksjonsanlegg
- Infrastrukturnodar
- Datasentralar og serverrom
- Kommandosentralar
- Arkiv
- Opphaldsstader for nøkkelpersonell
- Lager av ekstremt farlege stoff
- Symbolbygningar

F.v.: Lena Bjørgum og Runa Skimten i NSM.
Foto: Pål Rødahl/tinagent

Antall årsverk
Totalt per 31. desember



Jobb i NSM:

Mange engasjerte mennesker

Mange mennesker, sterke meninger: Nasjonal sikkerhetsmyndighet er en spennende arbeidsplass, sier Lena Bjørgum og Runa Skimten.

Lena Bjørgum er nyutdannet statsviter, med en master i administrasjon og organisasjonsvitenskap. Masteroppgaven hennes handlet i hovedsak om samordning på samfunnssikkerhetsfeltet, forteller hun. Jobben i NSM er hennes første jobb etter utdannelsen.

– Jeg fungerer som en inngangsportal for henvendelser om personellsikkerhet i min avdeling, Avdeling for sikkerhetskultur. En typisk utfordring for meg som nyansatt er sammenhengen mellom teori og praksis. I masteroppgaven hadde jeg en overordnet tilnærming til samfunnssikkerhet, mens jeg nå jobber med et spesifikt fagfelt, som er personellsikkerhet.

Ingen dag er lik

– Hvordan er det å jobbe i NSM?

– NSM er uten tvil en spennende arbeidsplass. Ikke bare har jeg kontakt med interessante mennesker, men som koordinator har jeg også kontakt med eksterne på fagfeltet. Selv om mye av arbeidet gjøres på kontoret, har vi likevel en del møtevirksomhet, og ingen dag er lik. Det er også en god blanding av å jobbe individuelt og i grupper. Miljøet er preget av mennesker med ulik og spennende bakgrunn, som alle brenner for faget sitt, forteller hun.

– Jeg møter daglig motiverte og engasjerte mennesker på jobb, som alle bidrar til et positivt og veldig hyggelig miljø. Jeg har til den dag i dag ikke kjedet meg et sekund på jobb!

Faglig utvikling

Runa Skimten har IT-faglig bakgrunn fra høyskole og universitet og har tidligere også jobbet som konsulent i noen år.

- Jeg jobber nå innen fagområdet nettverkssikkerhet. Det handler om å utvikle sikkerhetskrav og tiltak, skrive veiledninger, og jobbe med teknologier i lab. Rådgivningsarbeid mot prosjekter og virksomheter er også en viktig del av jobben min.

– Hvorfor valgte du NSM som arbeidsplass?

– NSM tilbyr meg den fortsettelsen på utdannelsen som jeg ønsker. Som sentral aktør på samfunnssikkerhetsfeltet er NSM en veldig spennende plass å jobbe. Det legges til rette for faglig utvikling, og mulighetene er mange. I tillegg til dette har vi jo også goder som trening i arbeidstiden og sosiale sammenkomster.

Variert arbeid

– Hvordan er det å jobbe i NSM?

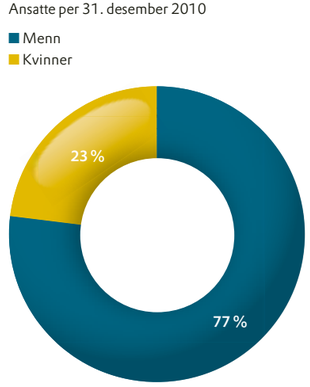
– NSM er nok litt annerledes enn mange andre arbeidsplasser. Tatt i betraktning vår rolle i samfunnet kan arbeidsomfanget være veldig variert, og omfatte både nasjonalt og internasjonalt arbeid. Det å kunne representere Norge i internasjonale fora var for meg en ny og lærerik opplevelse, noe jeg så klart synes er interessant. Ellers har jeg begynt å jobbe mer teknisk igjen enn jeg gjorde en periode, og det gir nye utfordringer. Men jeg har en gruppe dyktige kollegaer rundt meg og vi har et fint samarbeid.

Samtidig påpeker Runa at hun synes NSM har mange utfordringer, og at en av dem er omfanget av alt vi skal gjøre i kraft av den rollen vi har.

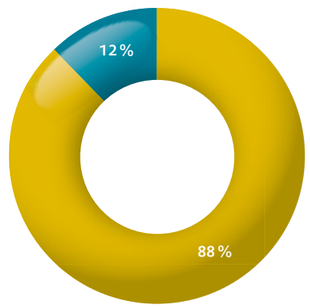
– Ideelt sett burde vi vært mange flere enn vi er. Ergo må vi prioritere hva, og hvordan, vi gjør ting. I NSM er det mange mennesker med engasjerte og sterke meninger, noe som gjør at dialog og diskusjon alltid får en interessant vri. Enden på visa er at når et produkt har kommet igjennom kverna, så er som regel resultatet ganske så bra!

«Som sentral aktør på samfunnssikkerhetsfeltet er NSM en veldig spennende plass å jobbe.»

Kjønnsfordeling
Ansatte per 31. desember 2010



Fordeling sivilt/militært ansatte
Per 31. desember 2010



Nasjonal sikkerhetsmyndighet
Postboks 14
NO-1306 Bærum Postterminal

Besøksadresse: Rødskiferveien 20, Kolsås
Telefon: 67 86 40 00
Telefaks: 67 86 40 09

www.nsm.stat.no

Årsmelding for 2010

Utgitt april 2011
Ansvarlig redaktør: Kjetil Nilsen
Redaktør: Kjetil Berg Veire

Redaksjon: Liv Nodeland, Anders Bjønnes
Grafisk design: Håvar Haug, Marit Sylstad/NSM
Forsidefoto: Pål Rødahl/tinagent