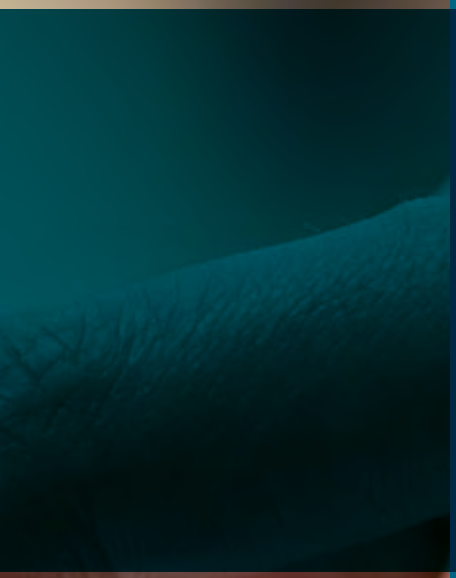
NASJONAL SIKKERHETSMYNDIGHET

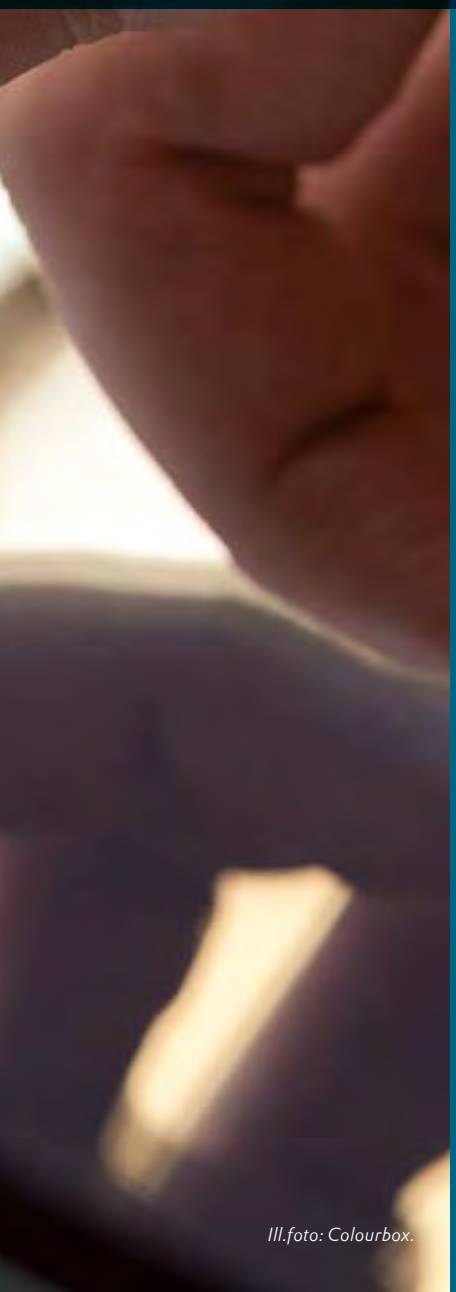
Grunnsikring

Årsmelding 2011

Nasjonal sikkerhetsmyndighet



Virksomhetsidé



Nasjonal sikkerhetsmyndighet (NSM) er et direktorat for forebyggende sikkerhetstjeneste. NSM skal innen sitt ansvarsområde beskytte informasjon og objekter mot spionasje, sabotasje og terrorhandlinger gjennom å:

- føre tilsyn og utøve myndighet i henhold til regelverk
- varsle og håndtere alvorlige dataangrep
- utvikle sikkerhetstiltak
- gi råd og veiledning

Vi skal være en pådriver for bedring av sikkerhetstilstanden og gi råd om utviklingen av sikkerhetsarbeidet i samfunnet.

Se informasjonsvideo om NSM

Ill.foto: Colourbox.

Grunnsikring handler om felles standarder, felles løsninger, og felles tillit til sikkerheten. Det gjør det mulig å samhandle mellom sektorer, sier direktør i Nasjonal sikkerhetsmyndighet, Kjetil Nilsen

Direktørens artikkel:

Samarbeid en nødvendighet

Det er onsdag etter lunsj. Direktør Kjetil Nilsen i Nasjonal sikkerhetsmyndighet har akkurat fått i seg en forsinket matbit etter en fullstappet formiddag med møter. Sola skinner inn vinduene på Kolsås, og verden ser egentlig ganske lys og vårlig ut, til forskjell fra terrorhandlingen 22. juli i fjor.

En betydelig naivitet

Den første tiden etter terrorangrepet var NSM opptatt av at alle berørte departementer sikret sine verdier. I etterkant har NSM bidratt med rådgivning i forhold til relokalisering av departementene.

– Har vi vært for naive i Norge, trodde vi at vi var trygge her i verdens utkant?

– I Norge har vi en generell tillit til hverandre. Det er bra. Men en side ved det er at vi også har en betydelig naivitet. Og det kan sette oss på prøve. Vi skal stole på hverandre, men spørsmålet er om vi noen ganger stoler for mye på hverandre, sier Kjetil Nilsen, og fortsetter:

– Jeg tror vi har en betydelig kulturell utfordring med at vi er veldig individualistiske, både som enkeltindivider og som virksomheter. Det preger oss. Og det kan gjøre det vanskelig med godt samarbeid. Vi har en tendens til å skulle løse alt selv innenfor egen virksomhet. Det er spesielt utfordrende i det digitale rom, hvor alle er avhengige av hverandre. Ingen person, virksomhet eller etat kan alene håndtere disse utfordringene. Det som må til er koordinering, samarbeid, og klar og entydig styring og ledelse, sammen med forutsigbarhet og en klar ansvarsdeling.

Fragmentert ansvar

– Har vi det i dag?

– Etter min oppfatning er det for stor usikkerhet i forhold til hvem som har oppgaver og ansvar, i alle fall når det kommer til samordning, styring og ledelse.

Kjetil Nilsens viktigste budskap det siste året har vært at ansvaret for datasikkerhet er spredt på for mange hender. Norge har for mange ukoordinerte regelverk for informasjonssikkerhet. Ulike sikkerhetsnivåer gjør det vanskelig å kommunisere med hverandre. Ansvaret er spredt på mange aktører, og det fører til fragmentert styring og kontroll. Og flere hundre offentlige datanettverk er lite effektivt, det koster samfunnet mange penger, og er lite sikkert.

> – Jeg tror vi har en betydelig kulturell utfordring med at vi er veldig individualistiske, både som enkeltindivider og virksomheter.

Derfor er tema for årsmeldingen i år grunnsikring. Grunnsikring handler både om å ha et sett minstekrav til sikring av verdier som informasjon, bygninger, objekter og mennesker. Grunnsikring dreier seg om at vi som samfunn har en felles oppfatning om sikkerhet. Grunnsikring handler om felles standarder, felles løsninger, felles tillit til sikkerheten. Det gjør det mulig å samhandle mellom sektorer, sier Kjetil Nilsen.

Ingen felles grunnsikring

– Er grunnsikringen god i Norge?

– Jeg skulle hatt lyst til å svare ja på det, men NSMs rapport om sikkerhetstilstanden viser et helt annet bilde. Vi har ikke en sektorovergripende oppfatning av hva som er god nok sikkerhet. Slik sett har vi ikke noen felles grunnsikring i Norge.

Et unntak er forskrift om objektsikkerhet, som trådte i kraft i 2011, og som skal bidra til at kritisk infrastruktur er sikret på en enhetlig måte mot terror og sabotasje. Mange sektorer er allerede godt sikret. Men arbeidet med implementeringen av forskriften vil avdekke hull og sektorer som ikke er godt nok sikret, og bidra til at objekter blir beskyttet på samme måte.

– Hvorfor er arbeidet med objektsikkerhet viktig også for datasikkerheten?

– Informasjonssikkerhet og objektsikkerhet er ofte to sider av samme sak. Et datasystem kan være et objekt, og et helt sentralt punkt i den kritiske infrastrukturen. Oppbyggingen av datasentre, som leier ut lagringsplass og tjenester, som nå foregår, signaliserer med all tydelighet at dette er objekter som må sikres både fysisk og digitalt. Men, det er ikke nok med god

– Oppbyggingen av datasentre, som leier ut lagringsplass og tjenester, som nå foregår, signaliserer med all tydelighet at dette er objekter som må sikres både fysisk og digitalt, sier Kjetil Nilsen. Foto: Pål Rødahl/tinagent

grunnsikring. Vi må også ha evnen til å håndtere hendelser når de oppstår, og det vil det, påpeker Nilsen.

Et nett uten grenser

Markedet spiller en viktig rolle i å utvikle sikrere løsninger, mener Nilsen. Staten må hjelpe markedet til å utvikle sikre løsninger gjennom å fortelle om sine behov, sier han. Ikke nødvendigvis gjennom streng regulering av informasjonssikkerhet, men med noen felles minste kjøreregler som er allment aksepterte. Markedet må komme opp med sikre løsninger, etter at det offentlige har satt krav til standardiseringer, sertifiseringer og minstekrav til sikkerhet.

Samarbeid er en nøkkel til en god grunnsikring, sier Kjetil Nilsen. I det digitale samfunnet, hvor alle er bundet sammen av datanettverk, er samarbeid helt nødvendig, både mellom offentlige etater og næringslivet. Nettet kjenner ingen grenser, heller ikke nasjonalstatens grenser. Derfor er Norge helt avhengig av andre lands myndigheter og bedrifter for å ha sikre nok nettverk.

– Thomas Kristmar, som er leder for danske GovCERT, nevner senere i denne årsmeldingen at han har stor tro på det nordiske samarbeidet. Det deler jeg med ham. Samarbeid mellom våre aller nærmeste bør være et godt sted å starte for å sikre nettverkene våre bedre.

Unik beskyttelse av kritisk infrastruktur

Verken Danmark, Nederland eller Storbritannia har lovverk til å beskytte kritisk infrastruktur på samme måte som Norge.

Forskrift om objektsikkerhet trådte i kraft i 2011, og skal implementeres frem mot 2014. Forskriften vil bety at kritisk infrastruktur i Norge blir beskyttet på en helhetlig måte mot terror og sabotasje. Verken Danmark, Nederland eller Storbritannia har tilsvarende lovverk. I Storbritannia finnes det ikke felles regelverk for objektsikkerhet for kritisk infrastruktur på tvers av sektorer, selv om enkelte sektorer som energi og vann har egne reguleringer.

– Vi er meget misunnelige på Norge, det er min personlige mening, sier Thomas Kristmar i Danmark om forskriften om objektsikkerhet som nå er under implementering i Norge. I Danmark er regelverket for kritisk infrastruktur mykere, og det er den enkelte sektoransvarlige myndighet som bestemmer sikringnivået innen egen sektor.

– Et stort skritt i riktig retning

Langtidsplanen for forsvarssektoren er et stort skritt i riktig retning for å styrke det forebyggende sikkerhetsarbeidet i Norge, sier direktør i NSM, Kjetil Nilsen.

I stortingsproposisjonen heter det blant annet at regjeringen vil styrke arbeidet med forebyggende sikkerhet og IKT-sikkerhet på tvers av samfunnssektorene. Regjeringen vil i perioden 2013 – 2016 videreutvikle Nasjonal sikkerhetsmyndighet som det sentrale direktorat for beskyttelse av informasjon og infrastruktur av betydning for samfunnskritiske og andre viktige samfunnsfunksjoner.

– Vi begynner nå å se konturene av de rammer som regjeringen vil gi til det forebyggende sikkerhetsarbeidet i Norge. Det må nå følges opp av konkrete tiltak. I tillegg ser jeg frem til arbeidet med revisjonen av nasjonale retningslinjer for å styrke informasjonssikkerheten, evalueringen av sikkerhetsloven, og videreutviklingen av NSM, sier Kjetil Nilsen.

Foto: FLICKR: Magne Haagen

Tryggleikstilstanden

Tryggleikstilstanden er framleis svekka i Noreg. Forståing av risiko knytta til spionasje, sabotasje og terror er for låg.

Den største trugselen i fredstid er tjuveri av kommersielle data og intellektuell eigedom. Og den mest alvorlege trugselen kjem frå andre statar.

Tryggleikstilstanden er framleis svekka i Noreg. Forståing av risiko knytt til spionasje, sabotasje og terror er framleis for låg. Viktige tiltak som risikovurdering, styrking av kompetanse og rapportering vert ikkje gjennomført.

Rapport om tryggleikstilstanden:

Eit sårbart samfunn

Dette er blant konklusjonane i Rapport om tryggleikstilstanden, som mellom anna er basert på tilsyn med ulike verksemder underlagt tryggingslova.

Alvorlege sårbarheiter

Både statsforvaltninga, Forsvaret, og fleire private verksemder er underlagt lova. Rapporten viser at viktige IKT-system ofte ikkje er godt nok sikra. Konsekvensen kan mellom anna vere at spionasjeoperasjonar med potensielt store konsekvensar kan gjennomførast i Noreg utan at dei vert oppdaga. Også såkalla inntrengingstesting, som er kontrollerte dataåtak som vert nytta for å teste motstanden i eit datasystem, har avdekka svært alvorlege sårbarheiter. Sårbarheitene kan gi tilgang til å manipulere, endre og slette både sensitiv informasjon og høgt tryggleiksgradert informasjon. Testane syner at det kostar lite å bryte seg inn i mange kritiske datasystem.

Store utfordringar

NSM har også registrert alvorlege sårbarheiter hos verksemder som leverer samfunnskritiske tenester. Desse sårbarheitene kan verte, og har vorte, avdekka og utnytta på ein måte som kan få store tryggleikspolitiske og/eller økonomiske konsekvensar. NSM er også bekymra for utviklinga når det kjem til grunnleggjande kryptoinfrastruktur. Held den negative utviklinga fram, er det risiko for at høgt gradert informasjon, spesielt i forsvarssektoren, vert kompromittert og dermed utsett for utnytting av framand etterretning. I tillegg eksisterer det store utfordringar rundt tryggleiksklarering av personar og verksemder, og manglande rapportering om eigen tryggleikstilstand.

Eit aukande gap

NSM har tidlegare rapportert om eit aukande gap mellom trugsel og implementerte tryggleikstiltak. Trenden er at dette gapet framleis aukar.

I tida framover er det god grunn til å halde auge med:

- Ei fortsatt auke i alvorlege IKT-hendingar
- Meir profesjonell utvikling av ondsinna programvare gjennom
  – målretta åtak mot lukka nett
  – forsøk på å infiltrere prosesskotroll system
- Spreiing av skadevare over mobile einingar
- Misbruk av og infisering av smartkort og smartkortlesarar
- Sårbarheiter i leverandørkjeda av IKT-utstyr
- Auka førespurnad etter klarering av personell med tilknyting til andre statar

> – NSM har tildlegare rapportert om eit aukande gap mellom trugsel og implementerte tryggleikstiltak.

Fleire tiltak

Fleire prosessar kan påverke det førebyggjande tryggleiksarbeidet i Noreg, mellom anna:

- Ny langtidsplan for forsvarssektoren
- Ny stortingsmelding om samfunnstrygggleik frå Justis- og beredskapsdepartementet
- 22. juli-kommisjonen sine konklusjonar og anbefalingar
- Evaluering av tryggingslova
- Prosjekt for evaluering og vidareutvikling av Nasjonalt tryggingsorgan
- Reviderte nasjonale retningslinjer for informasjonstryggleik. NSM sitt forslag til nasjonal strategi for cybertryggleik inngår som ein del av arbeidet
- Forskrift for objekttryggleik vert implementert fram mot 2014
- Forsvarssektoren sine retningslinjer for informasjonstryggleik og cyberoperasjonar

Foto: FLICKR: Magne Haagen

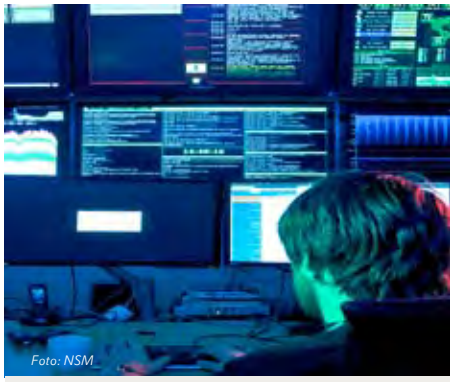


Foto: NSM

Tredobla på fire år

Talet på saker som vert handsama av NSM si avdeling NorCERT er tredobla dei siste fire åra.

I 2011 handsama avdelinga over 20 saker som vert vurdert som særskilt alvorlege. Desse har i all hovudsak vore målretta dataspionasjeåtak mot norske industriselskap som utviklar og produserer avansert teknologi. Olje- og gassektoren og forsvarssektoren er særskilt utsett. Men mørketala er truleg store, og det er grunn til å tru at fleire sektorar er ramma.

Ill. foto: Colourbox

Kunne ha tapt fleire titalls millionar kroner

Eit norsk høgteknologisk selskap som stadig blir utsett for dataåtak, har rekna på kor mykje ei hending kan koste.

Eit søsterselskap fekk store delar av sitt interne nett kompromittert. Verksemda kom fram til at ei liknande hending ville kosta fleire titalls millionar kroner i direkte tap. Dersom hendinga hadde vorte kjent, ville dei tapt langt større summar.

Ill. foto: Colourbox

Tapte fleire hundre millionar kroner

Ei norsk verksemd har estimert sitt tap på grunn av dataspionasje til fleire hundre millionar kroner.

I tilknyting til ei kontraktsforhandling om eit prosjekt i utlandet vart verksemda utsett for eit dataåtak. Virus infiserte maskinane til nøkkelpersonell i ei kritisk fase i forhandlingane. Ein e-post, tilsynelatande frå sjefen, refererte til eit internt prosjekt som berre få tilsette var informert om. Fleire opna e-postvedlegget, og fleire maskinar vart infisert. Verksemda tapte kontraktsforhandlingane. Infeksjonen vart fyrst oppdaga i etterkant av den kritiske fasen i forhandlingane. Den tapte posisjonen til verksemda i kontraktsforhandlingane er anslått til fleire hundre millionar kroner.

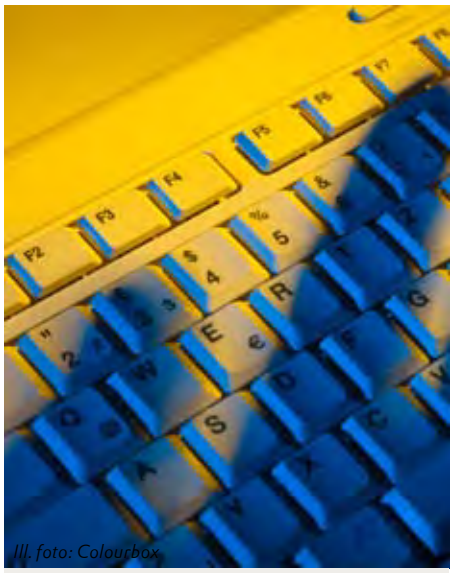
– Mange kritiske IKT-system er ikkje tilstrekkeleg sikra mot spionasje og anna alvorleg IKT-relatert kriminalitet.

Ill.foto: Colourbox.

Dei mest alvorlege og avanserte trugslane mot Noreg kjem frå andre statar som ønskjer å bruke IKT til etterretningsverksemd. Den største trugselen i fredstid er tjuveri av kommersielle data og intellektuell eigedom.

IKT-risikobiletet:

Ei strategisk utfordring



Ill. foto: Colourbox

I 2008 vart det etablert ei koordineringsgruppe mellom Etterretningstenesta, Politiets tryggingsteneste (PST) og Nasjonalt tryggingsorgan (NSM) for å oppnå meir heilskapleg forståing og vurdering av IKT-risikobiletet. Koordineringsgruppa har etablert eit betydeleg samarbeid. Gjennom samarbeidet har det vorte avdekka store utfordringar.

Nokre av desse utfordringane vert forsterka ved at norsk næringsliv og offentlege verksemder i aukande grad etablerer tilgang til eigne datasystem frå utlandet. Dei tenesteutset også oppgåver til aktørar i utlandet og lagrar informasjon i nettskyer som ofte ligg på utanlandske serverar. På denne måten svekkast ikkje berre vernet som norsk jurisdiksjon kan gi norske interesser. Det eksponerer også norske data-nettverk for uønskt avlytting og avlesing.

Sensitiv informasjon

Stadig større mengder av sensitiv og kritisk informasjon vert gjort tilgjengeleg over IKT-system og på Internett. Standardsystem som operativsystem og applikasjonar med global utbreiing vert nytta i aukande grad. Sårbarheitene i systema vert dermed meir kjent og utnytta. Dette kan også gjelde system som styrer drifts- og produksjonsprosessar, mellom anna innan olje- og gassektoren og kraftsektoren. Hendingar som rammar ei verksemd eller ein sektor vil raskt kunne påverke andre sektorar eller system i andre land. Utbreiinga av flyttbare mediar forsterkar dette biletet.

Sårbarheitene vert forsterka av at mange verksemder synast å ha manglande vilje og/eller evne til å prioritere IKT-tryggingsarbeidet. Kommersielle omsyn gjer at mange veljer billigare og mindre sikre løysningar. Kompetanse om IKT-tryggleik er mangelfull og reduserer evna til å oppdage og reagere på uønskte hendingar. Mange kritiske IKT-system er ikkje tilstrekkeleg sikra mot spionasje og anna alvorleg IKT-relatert kriminalitet.

Ei strategisk utfordring

Fordi det norske samfunnet er digitalisert, har avhengigheita av IKT og Internett vorte ei strategisk utfordring. I fredstid er den største trugselen mot norske interesser tjuveri av kommersielle data og intellektuell eigedom. Dette kan for eksempel påverke våre konkurransefortrinn, konkurranseevne, forhandlingskort, avgjerder, børsverdiar, industri og infrastruktur. Aktørar kan også plante skadevare som kan brukast i ei krise eller konflikt for å forstyrre eller øydeleggje system og prosessar for å redusere handlingsrommet til norske styresmakter. Fleire statar har utvikla offensive kapasitetar som i ein krisesituasjon kan øydeleggje kritiske samfunnsfunksjonar og kritisk infrastruktur. Politiske og økonomiske avgjerdsprosessar, samt forsvaret av landet, kan derfor påverkast gjennom dataåtak.

Andre statar

Mange ulike aktørar kan true Noreg og norske interesser. Dei mest alvorlege og avanserte trugslane kjem frå andre statar som ønskjer å utnytte IKT til etterretningsverksemd. Dei samlar inn informasjon for å understøtte eigne styresmakter, og eige næringsliv og forsvar. Fleire statar har dessutan etablert eller bygd opp såkalla militære cyberkommandoar, nasjonale cybersentre og dedikerte einingar.

Kven står bak?

Det digitale rom er ein egna arena for aktørar som vil skjule opphavet til ondsinna handlingar. Det gjer det vanskeleg å stille nokon til ansvar for denne type aktivitet. Dermed vert det førebyggande tryggleiksarbeidet desto viktigare, i tillegg er det viktig å fokusere på kva som bør sikrast.

Kven vert ramma?

I 2011 vart tunge næringslivsaktørar, bedrifter med spisskompetanse, Forsvaret, sentrale departement, forskingsverksemder og finansnæringa ramma av forsøk på elektronisk utnytting. Det vert oppdaga eit aukande tal avanserte operasjonar mot mål av høg verdi for samfunnet.

IKT-risikogruppa: Roller og ansvar

Etterretningstenesta har ansvaret for vurderinga av utanlandske aktørar sine intensjonar og kapasitetar. NSM har ansvaret for å førebygge defensivt mot spionasje, sabotasje og terror, og støtte ramma verksemder med å identifisere og handsame uønska IKT-hendingar. Politiets tryggingsteneste skal førebygge og etterforske hendingane der det er mistanke om at framande statar står bak, og i tillegg vurdere trugselen mot Noreg og norske interesser.

Grunnsikring

Flere store prosesser er i gang for å styrke grunnsikringen i Norge. – Det er avgjørende med permanente sikringstiltak rundt viktige samfunnsfunksjoner, mener tidligere Veritas-direktør Sven Ullring. Men hva gjør de i utlandet for å styrke grunnsikringen? Vi dro til Storbritannia, Nederland og Danmark for å høre hvordan de løser utfordringene, spesielt i forbindelse med de digitale nettverkene.

Ill.foto: Colourbox.

– Sikkerhet er god forretning, det lønner seg. I oljeindustrien har man lært at katastrofer er svært kostbare.

Ill.foto: Colourbox.

Det må ofte en alvorlig hendelse eller et alvorlig angrep til for at sikkerhet skal bli satt på dagsorden, sier tidligere konsernsjef i Veritas, Sven Ullring.

Gjesteintervjuet:

– Synes du sikkerhet er dyrt, prøv en katastrofe

Se intervju med Sven Ullring

Han stod bak utredningen NOU 2006:6 «Når sikkerheten er viktigst» som kom i 2006, og som handlet om beskyttelse av landets kritiske infrastruktur og samfunnsfunksjoner. Kritisk infrastruktur er i følge utredningen «de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner, og som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse».

Flere tiltak er realisert etter utredningen. Forskriften om objektsikkerhet, som skal styrke sikkerheten rundt bygg, anlegg og andre objekter mot terror og sabotasje, er trådt i kraft. NorCERT i Nasjonal sikkerhetsmyndighet er etablert og videreutviklet. Justis- og beredskapsdepartementet har fått en tydeligere rolle i sikkerhets- og beredskapsarbeidet. Men innføringen av tiltakene har gått for langsomt, sier Ullring, og fremdeles mangler det en overordnet beredskapslov.

En helhetlig grunnsikring

Terrorangrepet 22. juli viste oss at trusler kan oppstå uten forvarsel. Neste katastrofe kan like gjerne være et cyberangrep mot kritisk infrastruktur. Derfor er det avgjørende med permanente sikringstiltak rundt viktige samfunnsfunksjoner som kan være terrormål, mener Ullring.

– Denne grunnsikringen må være helhetlig, den må omfatte fysiske sikringstiltak, personellmessige sikringstiltak, datasikkerhetstiltak og så videre.

Ullring har lang fartstid i norsk og utenlandsk næringsliv. Han bygget vannkraftverk, flyplasser, sykehus med mer rundt om i verden bl.a. som utenlandssjef i Skanska, og var i en årrekke konsernsjef i Det Norske Veritas. I tillegg har han hatt en rekke tillitsverv i Storebrand, Hydro, Schlumberger, NHO osv. Samfunnet kan lære mye av både oljeindustrien og bygningsbransjen, sier han.

Sikkerhet lønner seg

– Sikkerhet er god forretning, det lønner seg. I oljeindustrien har man lært at katastrofer er svært kostbare. Se bare på katastrofer som Piper Alfa eller oljeutslippet i Mexicogulfen, sier Sven Ullring.

– Men skjønner du at bedrifter ikke bruker tid og krefter på sikkerhet? Det er ofte vanskelig å se den umiddelbare gevinsten av å bruke penger på sikkerhetstiltak?

– Nei, jeg skjønner det ikke, og jeg forstår det ikke. La meg si det på denne måten: På 70-tallet var vi alle veldig opptatt av kvalitet. Vi så at det var store penger å tjene på å gjøre tingene riktig med en gang, og ikke bruke tid og penger på reklamasjoner. I dag er det en selvfølge at man bygger kvalitet. Firmaene har ISO-standarder og diplomer med sertifiseringer på veggene. Så kom miljøsatsningen. I dag må alle forstå at det er viktig at bedriften ikke forurenser. Nå er vi opptatt av helse, miljø og sikkerhet, som er kommet på plass. Det neste nå er å forstå at sikkerhetsbegrepet omfatter mer enn å operere på en sikkerhetsmessig god måte. Vi må inkludere beredskap mot naturkatastrofer, terrorangrep og cyberangrep i sikkerhetsbegrepet. Jeg har vært med på dette en god stund. Til slutter faller tingene på plass.

– Som jeg alltid har sagt, sier Sven Ullring til slutt, synes du sikkerhet er dyrt, prøv en katastrofe.

Foto: NSM.

En ny lov skal hjelpe danskene med å stoppe alvorlige dataangrep. I fjor ble arbeidet med informasjonssikkerhet omorganisert, og et nytt IT-sikkerhetssenter er under planlegging. – Det finnes ikke den politiker med respekt for seg selv som ikke snakker om IT-sikkerhet, sier sjefen for det danske varslingssentret for internettrusler.

Satser på datasikkerhet:

Danskene tar grep

Se intervju med Thomas Kristmar

Store dataskjermer i hopetall og diverse kommunikasjonsutstyr fyller kontoret til Thomas Kristmar, sjefen for danske GovCERT, som ligger et lite steinkast unna danskebåten i København.

– Vi har nettopp hatt en øvelse med mitt kontor som situasjonssenter, og har ikke rukket å rydde vekk utstyret ennå, sier han. GovCERT er statens varslingssenter for internettrusler. Det er et senter som kan forvente stor utvikling i tiden som kommer.

– Alt som er relatert til IT-sikkerhet er nå et hett politisk tema, sier han.

IT-sikkerhet og politikk

Ting skjer raskt i Danmark. Da den nye regjeringen med statsminister Helle Thorning-Schmidt i spissen tok over makten i oktober i fjor, la den umiddelbart ned IT- og telestyrelsen, og overførte ansvaret for beskyttelse av kritisk IT-infrastruktur til Forsvarsministeriet. Et nytt IT-sikkerhetssenter er under planlegging, og er omtalt i regjeringsgrunnlaget «Et Danmark der står sammen». Det tok kun ett år fra ideen til en egen lov for varslingstjenesten GovCERT ble unnfanget, til den var vedtatt av Folketinget. Hvorfor tok danskene grep?

– Det siste året har det kommet en voksende erkjennelse av vår avhengighet av sikkerhetsnivået i samfunnet. Det som har vært til nå er ikke godt nok, sier Kristmar. Han viser blant annet til at Danmark har en sentral digital infrastruktur, og en digital signatur for banker som kan brukes til alle offentlige tjenester. I tillegg er det laget en lov som sier at all kommunikasjon mellom stat og borger skal være digital fra 2015.

Innsyn i e-poster

I fjor fikk også den danske statens varslingstjeneste for internettrusler lovfestet anledning til å registrere, analysere og oppbevare inn- og utgående trafikk- og pakkedata. Det betyr at GovCERT også kan lese innholdet i internettbasert kommunikasjon ved mistanke om sikkerhetshendelser. Danmark er trolig alene i Europa om en slik lovgivning.

– Det vi har lært er at du trenger tilgang til innholdet i internettkommunikasjonen for å gjøre jobben som et varslingssenter på en god nok måte, sier Kristmar.

I planleggingen av senteret kom de frem til at de trengte en sikker juridisk forankring for å kunne ha tilgang til innholdet i internettkommunikasjonen. For det første ønsket de å være på trygg grunn juridisk. Men de ønsket også å operere med absolutt åpenhet rundt sin egen virksomhet. Dessuten ønsket senteret å ha maksimum sikkerhet rundt dataene de samler inn.

– Det sentrale er at loven spesifiserer at GovCERT hos sine kunder kan se all kommunikasjonen til og fra virksomhetene, sier Kristmar. Loven sier klart at innhold kun kan gis videre i to tilfeller, enten til dansk politi ved alvorlig hackerkriminalitet, eller til MILCERT som ledd i beskyttelsen av kritisk infrastruktur. Og organisasjonen får kun se på data hvis det er snakk om en sikkerhetshendelse.

Foto: NSM.

Kontoret til Thomas Kristmar ligger et steinkast fra danskebåten i København.

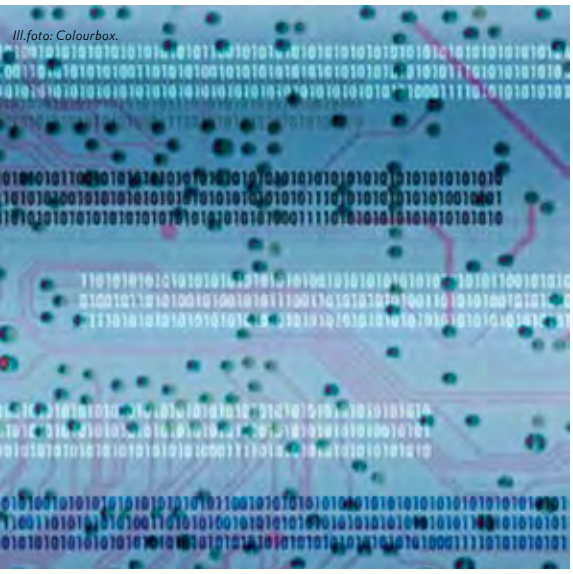

Ill.foto: Colourbox.


Foto: NSM.

De nordiske landene har samme infrastruktur, og samme trusler, sier sjef for GovCERT i Danmark, Thomas Kristmar.

Lever av tillit

– Vi skal vite at det er noe galt før vi ser på innholdet, sier Thomas Kristmar, som i forarbeidet til loven gikk åpent ut, og fikk det danske datatilsynet og viktige interessentgrupper med på laget.

– Vi lever av tillit. Hvis noen begynner å tro at vi går på fisketur i data, leser folks private e-post, deler dataene ut til høyre eller venstre, er det ingen som vil bruke oss, sier Kristmar, som også forteller at det ikke har vært noen høylydt debatt om lovforslaget.

Samme trusselnivå

Han mener danskene har akkurat det samme IKT-trusselnivået som Norge, og viser til rapporten som ble utarbeidet av tidligere utenriksminister Thorvald Stoltenberg i 2009. Rapporten inneholdt blant annet et forslag om samarbeid mellom de nordiske landenes sentre for varsling og håndtering av dataangrep, CERT-ene. Den har blant annet ført til oppbyggingen av en felles, sikkerhetsgradert kommunikasjonsplattform.

– Stoltenbergrapporten er en erkjennelse av at vi har det samme trusselnivået. Vi deler infrastrukturen. Norges nettforbindelser går gjennom Danmark. Danmark er avhengig av teleforbindelser i Sverige. Vi har felles nordiske banker. Vi har samme infrastruktur, samme trussel, og det er behov for at vi jobber tettere om dette, sier Kristmar, som for øvrig skryter av NorCERT i Nasjonal sikkerhetsmyndighet.

– Norge er i den europeiske superliga. Dere har historikk, dere har et godt samarbeid med deres kunder, som gjør at de proaktivt henvender seg til dere, dere har tillit, og dere har også sterk teknisk kompetanse, sier han.

Dette gjør danskene

- Overførte i fjor ansvaret for beskyttelse av kritisk IT-infrastruktur til Forsvarsministeriet
- Fikk i fjor også ny lov for behandling av personopplysninger i forbindelse med alvorlige IT-hendelser
- Planlegger nytt, nasjonalt IT-sikkerhetssenter

– Innenfor det siste året har det kommet en voksende erkjennelse av vår avhengighet av sikkerhetsnivået i samfunnet. Det som har vært til nå er ikke godt nok.

– Nederland er et lite land. Derfor må vi samarbeide, sier direktør for det nye cybersentret i Nederland, Wil van Gemert. På bare ett år har nederlenderne satt i gang flere tiltak for å styrke informasjonssikkerheten.

Nytt cybersenter i Nederland:

I samarbeidets ånd

Se intervju med Wil van Gemert

I 19. etasje i det nederlandske innenriksdepartementet sitter sjefen for det nye cybersentret i Nederland, som ble opprettet i januar. Etter hvert skal nye kontorer i det nederlandske sikkerhets- og justisdepartementet innredes. En rundt 10 minutters biltur unna er det nye cybersenteret, som ble åpnet i januar, i full gang.

Et topprioritert område

Sentret ble opprettet som en del av nederlendernes nye cyberstrategi som kom i fjor. Både strategien og flere IKT-hendelser har gjort at nederlandske politikere har IT-sikkerhet som et topprioritert område. I fjor ble blant annet det nederlandske selskapet DigiNotar, som utstedte digitale sertifikater både til privat og offentlig sektor, hacket. Tilliten til sertifikatene forsvant, og selskapet gikk konkurs. I slutten av januar i år ble et nasjonalt telefonselskap utsatt for dataangrep, og kundene stod i fare for å miste fasttelefonen. Store lekkasjesaker skapte overskrifter. Og en hacker skapte store diskusjoner da han viste hvordan det var mulig å hacke seg inn i pumpen til en av de store innsjøene i Nederland. Hvis den tørket inn, ville Nederland fått problemer med dikene som holder nederlenderne tørre på bena, i hvert fall i følge media.

– Jeg tror at regjeringen innså at et av de store spørsmålene for fremtiden var å skape et sikkert miljø, ikke bare når du går rundt på gaten, men også virtuelt, sier van Gemert.

Den nederlandske måten

Nederland har bare i løpet av ett år tatt flere skritt for å styrke IT-sikkerheten. Arbeidet har vært basert på fire pilarer. En ny strategi for cybersikkerhet, laget i nært samarbeid mellom flere departementer, har angitt retningen de skal gå for å styrke sikkerheten. Et eget råd for informasjonssikkerhet med offentlige og private deltakere er opprettet.

– Det er en typisk nederlandsk måte å jobbe sammen på, for å finne en løsning hvor alle kan enes om noe, sier van Gemert.

– Vi har professorer, men også representanter fra finanssektoren, fra energisektoren, fra den nasjonale etterretningen og fra militæret i dette rådet.

Arbeidet med å publisere årlige trusselvurderinger er i gang. Og et eget senter for cybersikkerhet ble åpnet i januar av den nederlandske sikkerhets- og justisministeren.

En hacker skapte store overskrifter tidligere i år da han viste hvordan det var mulig å hacke seg inn i pumpene til en av de store innsjøene i Nederland. Foto: http://commons.wikimedia.org/wiki/File:Oosterscheldekering-pohled.jpg

Foto: NSM

– 80 prosent av infrastrukturen i Nederland er eid av privat sektor. Vi er helt avhengig av deres deltakelse , ellers kan du ikke sikre samfunnet, sier direktør Wil van Gemert. Douwe Leguit til venstre er sjef for utvikling og programmer i det nasjonale cybersentret. Foto: NSM.

Nasjonalt sikkerhetssenter

Senteret skal varsle om trusler og håndtere nasjonale IKT-kriser, i tillegg til å gi råd om utviklingen, trusler og trender.

– Ambisjonen til regjeringen er å bringe dette videre, og senteret vil doble kapasiteten. Det er nødvendig, for det er mange forventninger til oss, både i forhold til hva slags rolle senteret skal spille, hva vi skal publisere og så videre, sier Wil van Gemert, som har bakgrunn som nasjonal koordinator for kontraterrorisme og sikkerhet i Nederland.

Den nederlandske regjeringen er helt avhengig av deltakelse fra privat sektor, sier han.

Privateid infrastruktur

– 80 prosent av IKT-infrastrukturen i Nederland er eid av privat sektor. Vi er helt avhengig av deres deltakelse, ellers kan du ikke sikre samfunnet.

Strategien foreslår en rekke tiltak, blant annet oppdatering av lovverk, minstestandarder knyttet til IT-sikkerhet, et rammeverk for informasjonssikkerhet for nasjonale statlige tjenester, målrettede nasjonale kampanjer, en egen plan for IT-kriser, et utdanningssenter for IT-sikkerhet og så videre.

Alle har et ansvar

Nå går diskusjonen om hva slags myndighet og makt regjeringen skal ha for å reagere på IT-hendelser, for eksempel om det trengs lovgivning som kan pålegge selskaper å rapportere til regjeringen dersom de blir hacket.

Og nettet utfordrer vår måte å organisere oss på for å skape sikkerhet, sier van Gemert. – I den virkelige verden har vi levd i tusenvis av år, og etter hvert funnet en måte å organisere oss på. Vi har veier, men du kan ikke kjøre på veien hvis du ikke har sertifikat eller en bil som ikke oppfyller sikkerhetskrav. Dette har vi ikke på Internett, du kan bruke nettet uten beskyttelse. Utfordringen for fremtiden er å finne en modell hvor alle sivile, private og offentlige er lenket sammen, og hvor alle tar sitt ansvar, sier Wil van Gemert.

– Jeg tror at regjeringen innså at et av de store spørsmålene for fremtiden var å skape et sikkert miljø, ikke bare når du går rundt på gaten, men også virtuelt.

Ill.foto: Colourbox.

Dette gjør nederlenderne

Nederlenderne har satt i verk en rekke tiltak i strategien for cybersikkerhet som ble vedtatt i fjor, blant annet:

- Opprettet et nasjonalt sikkerhetssenter for cyberspace som skal samle offentlige og private aktører
- Opprettet et råd for informasjonssikkerhet med medlemmer fra offentlige og private virksomheter og akademia
- Oppdaterer flere regelverk for informasjonssikkerhet
- Etablerer ett rammeverk for informasjonssikkerhet for statsforvaltningen
- Opprettet en nasjonal kriseplan for nasjonale IT-kriser
- Fortsetter å utvikle målrettede kampanjer for informasjonssikkerhet

Før var det IT-nerdene som var opptatt av informasjonssikkerhet. Nå er det blitt et politisk spørsmål, og et av statsminister David Camerons hovedsatsningsområder. Hva skjedde?

Informasjonssikkerhet i Storbritannia:

En politisk sak

Se intervju med Mark Phillips

– En av grunnene var en stor gjennomgang av forsvarsbudsjettet.

Det sier strategisjef i Cabinet Office i London, Matthew Erikson. Han har fått presset inn en kaffeavtale i en travel kalender i lokalene på adressen 70 Whitehall, som ligger rundt 20 meter fra Downing Street, og et par minutters gange fra det britiske Underhuset. Midt i britenes ærverdige og politiske sentrum er informasjonssikkerhet blitt et høyt profilert politisk tema det siste året. En ny strategi for informasjonssikkerhet ble publisert i fjor, og 6 milliarder kroner (650 millioner pund) er satt av til arbeidet med informasjonssikkerhet over en fireårsperiode.

For stor risiko

Det var nok av grunner, sier Erikson. Forsvarsutgiftene var for store. David Camerons regjering trakk forsvar og sikkerhet sammen til et område, opprettet et nasjonalt sikkerhetsråd, og gjennomførte en storstilt gjennomgang av alle sikkerhetstrusler og farer som kunne ramme Storbritannia. Resultatet var blant annet en stor satsning på informasjonssikkerhet på tvers av sektorer. Risikoen for at noen skulle klare å bryte seg inn i datanettverkene og påføre britisk økonomi stor skade var rett og slett for stor.

– Det var nok av bevis for at vi måtte gjøre noe. Det var Stuxnet-ormen som kom i 2010, det var høyprofilerte datalekkasjer både innenfor og utenfor regjeringen, og du hadde cyberangrepene under Georgia-krigen og et stort dataangrep i Estland. Privat sektor ble også berørt av datalekkasjer, sier han.

Økonomisk suksess

Tvers overfor Cabinet Office sitter forsker Mark Phillips i den over 150 gamle tenketanken Royal United Services Institute, RUSI. Bordet vi sitter ved ble brukt av britiske og tyske militære i forhandlingsfasen etter første verdenskrig. Mark Phillips var stabssjef for tidligere sikkerhetsminister baronesse Pauline Neville-Jones både før og etter valget, og assisterte henne tett i jobben som sikkerhetsminister.

Gjennomgangen som ble gjort viste at sannsynligheten for dataangrep og svikt i datasystemene var stor, og førte til at det automatisk ble et topprioritert område for regjeringen.

– Regjeringen ble i stand til å vise at cyber ikke bare er et tradisjonelt forsvars- eller sikkerhetsspørsmål som kan overlates til etterretningsorganisasjonene eller Forsvarsdepartementet. Det ble samlet empiri for å vise at et sikkert og motstandsdyktig cyberspace er veldig viktig for økonomisk suksess og vekst for Storbritannia, og at andre departementer og privat sektor derfor måtte involveres i å utvikle løsninger på utfordringene, sier Mark Phillips.

Økt bevissthet

Den nye cyberstrategien har økt bevisstheten om cyberspace på tvers av regjeringen, og den har også økt den offentlige interessen.

Og også i Storbritannia er offentlig-privat samarbeid en nøkkel for å lykkes. Det er utfordrende. Cyberspace har gjort definisjonen av kritisk infrastruktur langt bredere. Derfor må regjeringen finne ut hvordan den kan komme i inngrep med

Ill.foto: Colourbox.

Dette gjør britene

- Bruker 6 milliarder norske kroner på et fire år langt program for informasjonssikkerhet.
- Publiserte i fjor en nasjonal strategi for cybersikkerhet.
- Strategien inneholder en rekke tiltak, blant annet et nytt nasjonalt cyberkrimsenter, internasjonalt samarbeid på regjeringsnivå, bevissthetskampanjer, utdanningstiltak mm.

– Regjeringen ble i stand til å vise at cyber ikke bare er et tradisjonelt forsvars- eller sikkerhetsspørsmål som kan overlates til etterretningsorganisasjonene eller Forsvarsdepartementet.

Foto: NSM.

Ill.foto: Colourbox


Ill.foto: Colourbox

et langt større antall ulike private selskaper, små og store, for å sikre infrastrukturen godt nok. Informasjonsdeling er et nøkkelspørsmål. Men informasjonsdeling er også utfordrende, sier Mark Phillips.

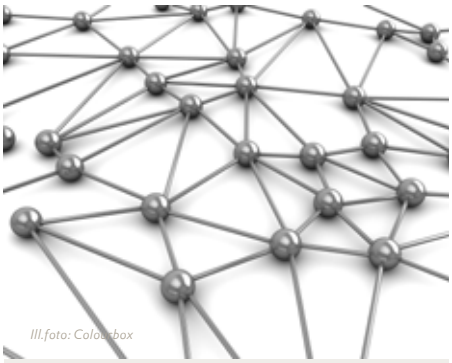
– Det er mye snakk om «partnerskap» mellom staten og privat sektor, spesielt med tanke på informasjonsdeling, sier han.

– Men hva er formålet med samarbeid og informasjonsdeling? Er det å forbedre kunnskapen om trusler og sårbarheter, er det å utvikle en felles situasjonsforståelse, handler det om å utvikle råd og retningslinjer for informasjonssikkerhetsstandarder, eller har det med å styrke hendelseshåndteringen å gjøre? Dette er noen av spørsmålene vi har behov for å finne ut av, sier han.

Han fremhever også spesielt mangelen på kompetanse på IT-sikkerhet i Storbritannia. Store, nasjonale kampanjer er blitt satt i gang for å øke oppmerksomheten om IT-sikkerhet som fag.

– For øyeblikket mangler kapasitetene, i form av tekniske ferdigheter, til å møte det vi trenger av kompetanse, sier Mark Phillips ved RUSI.

– Det er behov for mye større og raskere investeringer til utdanning og kursing, sier han.


Ill.foto: Colourbox

Bygger offentlig supernett

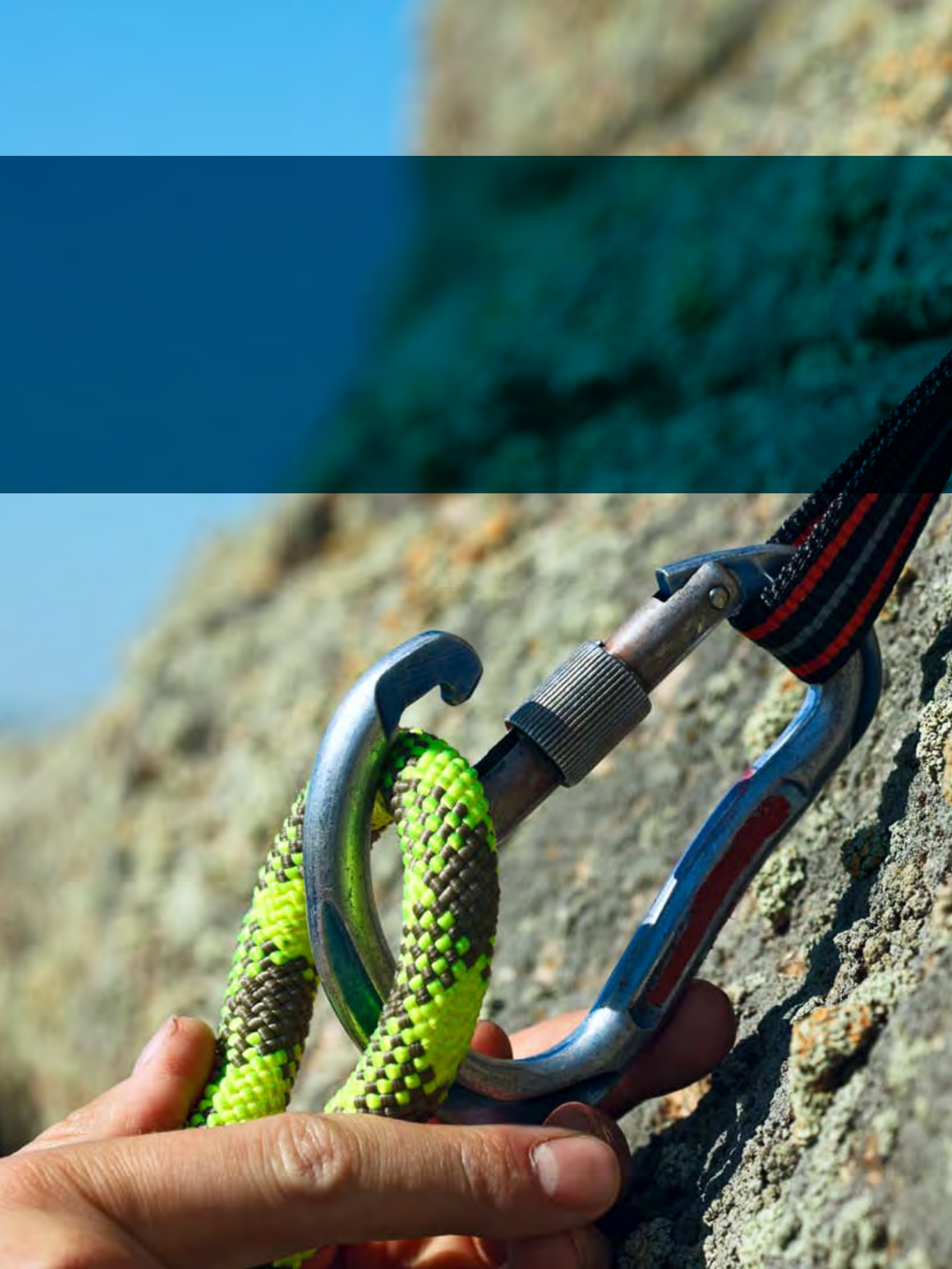
Britene er godt i gang med å bygge et offentlig supernettverk som kan skape store besparelser for offentlig sektor.

I følge Cabinet Office vil nettverket føre til besparelser på 150 milliarder kroner i årlige utgifter. Public Service Network (PSN) vil bli et «nettverk av nettverk», basert på standarder, og vil gi tilgang til et bredt utvalg av nettverkstjenester med garantert sikkerhet og integritet. Nettverket vil bli svært viktig for offentlig sektor, blant annet for å dele informasjon på tvers av sektorgrenser.

– En av de store ideene har vært å trekke sammen alle IT-strukturene i stedet for ti ulike IT-avdelinger. Det gjør det billigere, og også enklere, hvis vi gjør det riktig, sier Matthew Erikson ved Cabinet Office.

– Gjennomgangen som ble gjort viste at sannsynligheten for dataangrep og svikt i datasystemene var for stor, og førte til at det automatisk ble et topprioritert område for regjeringen.

Ill.foto: Colourbox



NSM i 2011 og 2012

NSM står overfor mange store utfordringer fremover. Her kan du lese om hva vi gjorde for å sikre samfunnsverdier i 2011, og hva som er de største utfordringene for oss å ta tak i.

Ill.foto: Colourbox.

Nasjonal sikkerhetsmyndighet opplever stor pågang etter både råd og veiledning, hjelp til håndtering av dataangrep, gjennomføring av inntrengingstesting og på flere andre fagområder. Rekruttering er fremdeles en utfordring. Men turnoveren har gått ned, samtidig som kvinneandelen har gått opp.

Rapport for 2011 :

Stor pågang etter tjenester

NSM hadde i fjor et mindreforbruk på 5.9 millioner kroner, noe som tilsvarer 4 prosent av den totale budsjettrammen. Mindreforbruket skriver seg blant annet fra relokalisering av NorCERT og forsinkelsen i sluttoppgjør knyttet til denne.

Prioriterte objektsikkerhet

Tilsynsvirksomheten er sentral for direktoratet. Resultatene fra tilsynet danner kjernen i den årlige rapporten om sikkerhetstilstanden. Erfaringene fra tilsynet trekkes systematisk inn i utviklingsarbeidet både når det gjelder regelverksutvikling og utarbeidelse av veiledninger og utvikling av tekniske tiltak. I 2011 har NSM hatt utfordringer med å gjennomføre et tilstrekkelig antall tilsyn. Dette grunnet den nødvendige prioritering av støtte til objektsikkerhetsarbeidet i sektorene og ikke minst oppfølgingen av råd og veiledningsvirksomhet på sikkerhetsområdet etter terrorhandlingene 22. juli. Det har likevel vært lagt vekt på å gjennomføre tilsyn ved et representativt utvalg tilsynsobjekter.

Stor pågang

Også i 2011 har det vært stor pågang utenfra etter foredragsholdere fra direktoratet. Den årlige sikkerhetskonferansen i regi av NSM var meget godt besøkt og deltakerne ga generelt gode tilbakemeldinger. I 2011 ble det i alt holdt 72 foredrag og kurs om sikkerhetskultur og brukeratferd. Når det gjelder den mer strukturerte undervisningen rettet inn mot det praktiske sikkerhetsarbeidet i virksomhetene er denne dessverre redusert både i Forsvaret som sivilt. NSM har derfor startet et arbeid med kompetanseplaner og ser selv på muligheten for å gjennomføre slik undervisning i større grad. Dette arbeidet videreføres i 2012.

Håndterte krevende saker

Også i 2011 har den operative aktiviteten i NorCERT vært økende. Et antall krevende og alvorlige saker hvor man har støttet politiet og PST har opptatt store deler av tiden. Konsekvensen av dette har vært at et større antall saker av mindre betydning, men hvor NorCERTs kompetanse kunne ha representert en positiv forskjell, har måttet nedprioriteres eller avvises. NorCERT har bistått flere sektormyndigheter med å forberede etablering av sentrale responsmiljøer i sektorene, herunder i helsesektoren og justissektoren. NorCERT flytter i 2012 inn i nye lokaler, og vil fremover befeste sin nasjonale koordinerende rolle i nært samspill med de enkelte samfunnssektorene, EOS-tjenestene og politiet.

Etterspurte tjenester

Kapasiteten for inntrengningstesting, som er kontrollerte dataangrep som kan teste motstandsdyktighetene til datasystemer, er sterkt etterspurt. Det har i 2011 ikke vært mulig å etterkomme alle anmodninger og det var venteliste ved årsskiftet. NSM kan også på forespørsel kontrollere om virksomheter lagrer, behandler eller transporterer skjermingsverdig informasjon på informasjonssystemer som ikke er godkjent for dette gjennom såkalt monitoring. NSM vil motivere sektormyndigheter og virksomhetsledere til å ta dette hjelpemiddelet i større bruk fremover. Aktiviteten innen fagområdet tekniske sikkerhetsundersøkelser (TSU), som motvirker og avdekker forsøk på avlytting og innsyn, har i 2011 vært på et jevnt og høyt nivå.

Den frivillige sertifiseringsordningen (SERTIT) har i 2011 vært benyttet av flere utenlandske produsenter.

NSM har et godt samarbeid med en rekke toneangivende land på sikkerhetsområdet, og opplever at NSMs kompetanse er etterspurt.

Utvikler personellsikkerhetstjenesten

Nasjonal sikkerhetsmyndighet utfører et betydelig arbeid med å innhente personopplysninger til sikkerhetsklareringssaker. I fjor ble det innhentet opplysninger til over 20.000 ulike saker. Saksbehandlingstiden for personkontrollen er innenfor den målsettingen som er satt. Utviklingen når det gjelder saksbehandlingstid i klagesaker ble

– NSM er en kunnskapsvirksomhet med mye spesialistkunnskap innenfor et bredt oppgavespekter.

NSM utfører jevnlig tilsyn i andre land, blant annet i Afghanistan, som her ved den norske ambassaden i Kabul.

Foto: NSM.

redusert i 2011, mens den gikk noe opp når det gjelder klareringssaker i 1. instans. Dette reflekterer at ressursene på området totalt sett er i minste laget. Det har i 2011 vært arbeidet med å etablere grunnlag for et nytt helelektronisk saksbehandlerverktøy innen personellsikkerhet til erstatning for dagens system (kalt TUSS) som er en blanding av teknisk løsning og papirbaserte arkiver. I 2011 ble det utgitt en revidert personopplysningsblankett til bruk ved personkontroll.

NSM etablerte også i 2011 et prosjekt for å ta frem en bedre prosess for gjennomføring av sikkerhetsgodkjenning av informasjonssystemer som skal håndtere skjermingsverdig informasjon iht. sikkerhetsloven.

Rekruttering en utfordring

NSM er en kunnskapsvirksomhet med mye spesialistkunnskap innenfor et bredt oppgavespekter. 48 prosent av de ansatte har mastergrad eller hovedfag, mens 29 prosent har bachelorgrad eller lignende. Det er en utfordring å holde på og rekruttere den nødvendige spesialistkunnskap,

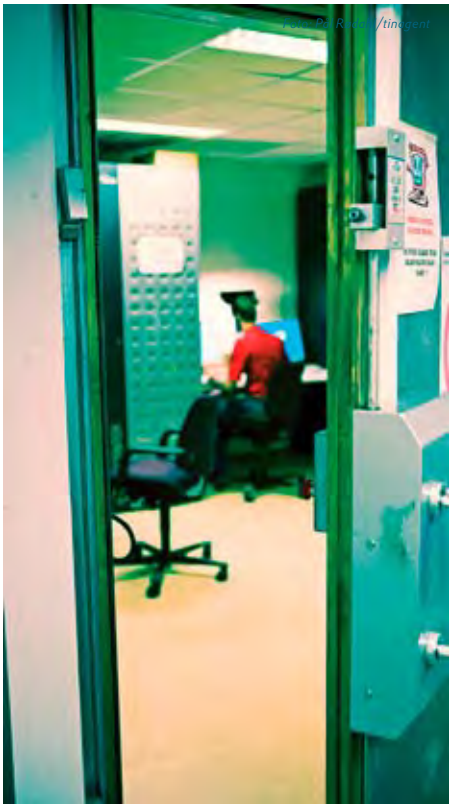


Foto: Per Rune Ytterdal/tinagent

Foto: NSM.

Fornøyde brukere

NSMs årlige sikkerhetskonferanse får svært gode tilbakemeldinger fra deltakerne. 78 prosent av de som svarte gav terningkast 5 eller 6 til at konferansen svarte til forventningene.

77 prosent gav terningkast 5 eller 6 til at de kommer til å anbefale konferansen til andre. Konferansen samlet over 300 sikkerhetseksperter fra offentlige og private virksomheter i Norge, og ble åpnet av forsvarsminister Espen Barth Eide og justisminister Grete Faremo.

Tall i millioner kroner	**Budsjett 2012**	**Regnskap 2011**	Regnskap 2010	Regnskap 2009	Regnskap 2008	Regnskap 2007	Regnskap 2006
Lønnsutgifter	*83,2*	*81,5*	78,2	77,9	71,5	66,0	62,0
Utgifter til varer og tjenester	*75,9*	*70,7*	47,6	41,5	44,5	49,6	51,5
Sum driftsutgifter	159,1	**152,2**	125,9	119,4	116,0	115,6	113,5
Inntekter og refusjoner	8,2	**9,1**	12,3	11,4	9,9	10,6	14,4
Netto	**150,9**	**143,1**	113,6	108,0	106,1	104,9	99,1

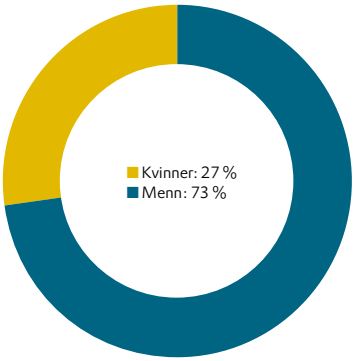
Ill.foto: Colourbox

Foto: Pål Rødahl/Imagent

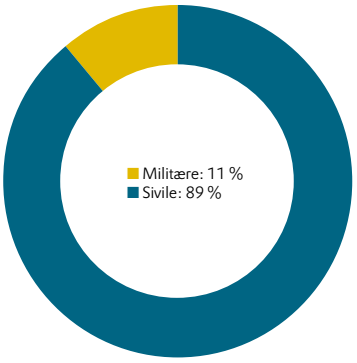
særlig innenfor IKT-feltet. Likevel er turnoveren i direktoratet gått ned fra 11 prosent i 2010 og til 6.3 prosent i 2011. Sikkerhetsarbeid er en mannsdominert bransje. Derfor er det positivt at kvinneandelen i NSM har økt i løpet av fjoråret, fra 23 til 27 prosent. NSM oppfordrer fortsatt kvinner til å søke på utlyste stillinger, og det er fortsatt et uttalt mål å øke kvinneandelen.

NSM skal sikre tilliten til sikkerhetsarbeidet som blir gjort i Norge. Verken Stortingets kontrollorgan for etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-utvalget), eller klagenemda for offentlige anskaffelser (KOFA), hadde merknader til NSM i 2011.

Kjønnsfordeling
Ansatte per 31. desember 2011



Fordeling sivilt/militært ansatte
Per 31. desember 2011



Dette gjør NSM

Her er noen nøkketall fra fjoråret.

- Håndterte 5800 IKT-hendelser i NorCERT, som varsler og håndterer alvorlige dataangrep. Over 20 av sakene blir karakterisert som alvorlige.
- Innhentet personopplysninger til 28 000 klareringssaker
- Gjennomførte 28 tilsyn hos virksomheter underlagt sikkerhetsloven. Har siden 2008 i alt gjennomført 50 tilsyn i tre verdensdeler
- Gjennomførte 72 foredrag og kurs om sikkerhetskultur, og totalt 149 undervisningstimer
- Produserte og reviderte totalt 10 veiledninger og brosjyrer
- Utstedte 131 sikkerhetsgodkjenninger og brukstillatelser til sikkerhetsgraderte informasjonssystemer
- Samlet over 300 deltakere til den årlige sikkerhetskonferansen
- Fortsatte arbeidet med forskning på høyt graderte prosjekter som får internasjonal anerkjennelse

De håndterer stadig flere IKT-hendelser, og norske virksomheter står i kø for å bli medlem i samarbeidet om å oppdage dataangrep gjennom sensorsystemet VDI. – I 2012 vil vi høyst sannsynlig få med sektorer som tidligere var dårlig representert. Det er svært gledelig og vitner om samfunnsansvar, sier avdelingsdirektør Eiliv Ofigsbø.


Foto: NSM

NorCERT:

Stadig mer å gjøre

Han overtok som avdelingssjef for NorCERT i fjor høst, og har tilbrakt de siste fire årene som oberst og såkalt «branch chief» i NATO i Brussel.

– Vi har sett et jevnt økende antall håndterte hendelser i NorCERT siden avdelingen ble etablert i 2006, sier Ofigsbø.

– I snitt øker antall saker med 30 prosent i året, med ny rekord i fjerde kvartal 2011. Dette er ikke en eksakt størrelse, men mer en trendutvikling. Økningen i antall saker og kompleksitet har gjort at NorCERT i mange tilfeller har måttet prioritere strammere enn hva vi strengt tatt ønsker.

Et viktig samspill

Like sentralt som det å håndtere hendelser er å oppdage dem. Dette skjer ved at NSM mottar informasjon fra internasjonale og nasjonale samarbeidspartnere, deteksjon gjennom vårt eget VDI-system og ikke minst tips fra oppmerksomme brukere og IT-sikkerhetspersonellet i virksomhetene.

– Spesielt viktig er samspillet og informasjonsutvekslingen med våre medlemmer og partnere, understreker Ofigsbø. – Det er derfor gledelig å konstatere at deres antall har vært relativt stabilt gjennom året, og at vi nå har flere i prosess med å bli medlemmer hos oss. For NorCERT er det ikke en hovedmålsetting at vi nødvendigvis har et veldig høyt antall medlemmer, men det er viktig at vi har et representativt utvalg virksomheter som har en samfunnsviktig eller samfunnskritisk funksjon. I 2012 vil vi høyst sannsynlig få med sektorer som tidligere var dårlig representert. Dette er svært gledelig, fremholder Ofigsbø.

– I 2011 har vi hatt høy aktivitet både mot nasjonale og internasjonale samarbeidspartnere. Jeg vil i forhold til internasjonale arenaer særlig trekke frem det gode arbeidet som gjennomføres innen rammen av European Government CERT Group (EGC).

Nye lokaler

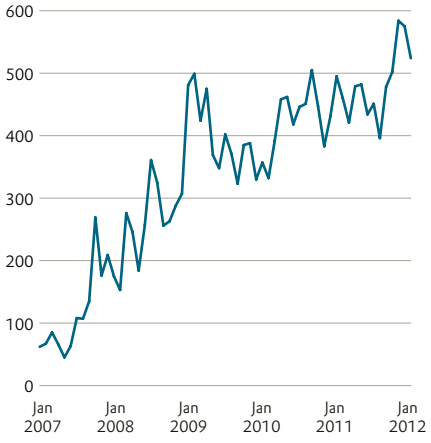
2012 blir en milepæl for NorCERT. Da flytter avdelingen ut av de svært trange men historiske lokaler på Akershus festning og inn i moderne behovstilpassede fasiliteter i nærheten av Helsfyr. Avdelingssjefen lover at man skal være operative der før sommerferien. Nye lokaler vil gi bedre operativitet og stabilitet.

En av NorCERTs hovedoppgaver er å ha kontinuerlig oversikt over det såkalte IKT-risikobildet. I dette arbeidet samarbeider NSM tett med PST og E-tjenesten.

Økt kompetanse

– Vi samarbeider godt, og vil fremdeles ha høyt fokus på dette arbeidet. Det er imidlertid stadig viktigere å kommunisere IKT-risikobilet på en god måte til relevante samfunnsaktører slik at vi øker kompetansen og forståelsen for IKT-sikkerhetsarbeidet. Der ligger nøkkelen til at vi som samfunn kan lykkes med å forebygge, avslutter avdelingsdirektør Ofigsbø.

Håndterte IKT-hendelser
Antall per måned 2007 – 2012



– Vi har sett et jevnt økende antall håndterte hendelser i NorCERT siden avdelingen ble etablert i 2006.

Ill.foto: Colourbox.

De leverer titusenvis av kryptonøkler til statsforvaltningen i året, sikrer møterom mot avlytting, og forsker både på trådløse nettverk, krypto og elektromagnetisk stråling. – Forskning og utvikling har vært viktig i 2011, sier avdelingssjef for Kommunikasjons- og systemsikkerhetsavdelingen (KSA), oberst Hans Robert Bjørnaas.

Kommunikasjons- og systemsikkerhetsavdelingen:

Forskning blir stadig viktigere

– Forskning er en forutsetning for å møte sikkerhetsutfordringene i det moderne samfunnet. Det er viktig både for å forstå ny teknologi med de sårbarhetene som følger med, og for å etablere mottiltak. I 2012 har vi fått til en betydelig kraftsamling om forskning- og utvikling i NSM. Det er viktig for samfunnets evne til å beskytte seg mot sårbarheter som datateknologien fører med seg, sier Bjørnaas.

Ny teknologi

Flere forskningsprosjekter er i gang. Ett prosjekt handler om svakheter ved trådløs teknologi. Et annet prosjekt handler om elektromagnetisk stråling, og et tredje prosjekt handler om forskning på tekniske sikkerhetsundersøkelser. Det siste har med hvordan man kan sikre blant annet møterom mot avlytting. Nasjonal sikkerhetsmyndighet jobber også kontinuerlig med forskning på ny kryptoteknologi for å utvikle neste generasjons kryptoutstyr.

– Jeg er også veldig stolt av det vi har oppnådd på området inntrengningstesting. Fjoråret var et oppbyggingsår, og kapasiteten er nå veldig etterspurt.

Inntrengingstesting

Den teknologiske utviklingen tvinger avdelingen til å tenke nytt, sier Bjørnaas.

– Vi har tradisjonelt fokusert på det høygraderte området, og der er de konkrete tiltakene meget sensitive – naturlig nok. De konkrete tekniske tiltakene for sikring av HEMMELIG- eller STRENGT HEMMELIG-informasjon er ikke trivialiteter. De skal stå i mot sofistikerte angrep fra aktører med store ressurser og mye kunnskap. Skjerming av disse tiltakene er en del av vår strategi. Fremover vil vi imidlertid måtte engasjere oss mer på det lavgraderte området og kanskje også på områder utenfor det som i dag omfattes av sikkerhetsloven.

Sikring av skytjenester

– Noe som har blitt særlig tydelig for oss på teknisk side i 2011 er at vi må bevege oss fra grunnholdningen «vi vil se på løsninger om en bruker presenterer et behov» til et mer proaktivt «hvilke løsninger bør vi tilby gjennom å sette oss i fremtidige brukeres sted». På kort sikt medfører dette selvsagt et økt ressursbehov i NSM, men på sikt vil det bety besparelser for samfunnet. Sikring av skytjenester er et eksempel på et område hvor vi ikke kan avvente at noen kommer til oss, presenterer behov og gir oss penger, sier Bjørnaas.

Foto: NSM.

– Forskning er en forutsetning for å møte sikkerhetsutfordringene i det moderne samfunnet.

Du trenger solid kompetanse for å sikre datasystemer og infrastruktur mot angrep. – 2011 har vært et kompetanseår, sier avdelingsdirektør for Administrasjonsavdelingen (ADM), Åshild Dikkanen Salmela.

Administrasjonsavdelingen:

Et kompetanseår

– Vi har særlig prioritert lederkompetansen på avdelingssjefs- og seksjonsledernivå. På ledersamlinger har vi fokusert på praktiske og juridiske forhold knyttet til det å være en leder i det daglige – såkalt hverdagsledelse. Eksempler på områder har vært hovedavtalen og annet regelverk, samt sykefraværsproblematikk. Vi har trukket inn eksterne forelesere. Representanter for fagorganisasjonene og andre nøkkelpersoner har også fått være til stede.

Mye kursing

– Vi har videre sørget for å kurse opp i spes-ielle stillinger innen AKAN-området (Arbeidslivets komité mot alkoholisme og narkomani) og vi har hatt opplæring av våre representanter i Arbeidsmiljøutvalget (AMU). Vi har dessuten fått på plass et grunnkurs for sikkerhet for egne ansatte. Alle medarbeidere har også gjennomført e-læring om det som i forsvarssektoren omtales som «HEL», holdninger, etikk og ledelse.

2011 var også et år med betydelig planlegging av nye systemer som intranett og dokumenthåndteringssystem.

– Vi har lært utrolig mye gjennom året. Jeg vil særlig fremheve lærdommen om tidlig å sette av nok ressurser til gjennomføring av så store prosjekter. Utfordringen fremover blir imidlertid å ta systemene og mulighetene i bruk på en god måte, fremholder hun.

Intern kontroll

Ordene internkontroll og internrevisjon har vi hørt nevnt mye i NSM de siste årene.

– 2011 var året hvor vi fikk på plass en person dedikert til internkontroll. Det er bra med tanke på å få bedre dokumentasjon av rutiner og systemer, og se til at disse følges. Jeg ser også frem til at vi iht. avtale med Forsvarsdepartementet har fått på plass en egen internrevisjon til støtte for Sjef NSM.

Gode ansettelser

Hele 26 ansettelser ble gjennomført i fjor, med en stor mengde kvalifiserte søkere.

– Fremover vil vi fokusere på å få rekrutteringsprosessen enda mer strømlinjeformet, noe som er viktig for å få ansatt den riktige kompetansen vi trenger, sier Åshild Dikkanen Salmela.


Foto: NSM

Foto: NSM

– Vi har særlig prioritert lederkompetansen på avdelingssjefs- og seksjonsledernivå.

Foto: Pål Rødahl/tinagent

Retningslinjene for å autorisere personer som skal få tilgang til statshemmeligheter er blitt tydeligere, sier avdelingssjef for Avdeling for sikkerhetskultur (KULT), kommandør Tore Gustafsson.

Avdeling for sikkerhetskultur:

Mer brukerrettet i 2011

– Det er særlig to produkter med vidt nedslagsfelt som har vært viktige for oss i 2011, sier Gustafsson.

– Revideringen av personopplysningsblanketten har bragt denne i tråd med regelverket og gjort den mer brukervennlig. Blanketten er det produktet fra NSM som når flest alminnelig mennesker i samfunnet. Vi må derfor legge betydelig vekt på hvordan den er utformet.

– Det andre produktet er den reviderte håndboken for autorisasjonsmyndighetene. Denne er arbeidsverktøyet for alle de som ute i den enkelte virksomhet bestemmer om vedkommende skal kunne settes til å håndtere våre statshemmeligheter.

Mange seminarer

– Blanketter og dokumenter er vel og bra. Hvordan sørger dere for at de blir brukt?

– Vi valgte i 2011 å kjøre regionale seminarer for autorisasjonsmyndighetene om begge produkter. Vi traff og motiverte over 300 nøkkelpersoner i dette arbeidet i Oslo, Stavanger, Bergen, Trondheim og Bodø. Både sivile og militære myndigheter var med i tillegg til kommunesektoren.

Gode tilbakemeldinger

Tilbakemeldingene har vært veldig gode, og vi vil følge opp dette videre i 2012.

KULT har alltid lagt vekt på undervisning og informasjon som virkemiddel, og gjennomfører en rekke kurs i løpet av året.

– Avdelingen har også i 2011 holdt en rekke foredrag om sikkerhetskultur og særlig utfordringene som følger av de sosiale medier. Her føler jeg at NSM virkelig har vært i forkant og frontet et tema som faktisk har blitt satt på dagsorden i samfunnet. Det er gledelig at virksomhetene selv tar dette på alvor, følger opp og setter det på agendaen.

Avdelingssjefen har mye på hjertet når høydepunktene i 2011 skal listes.

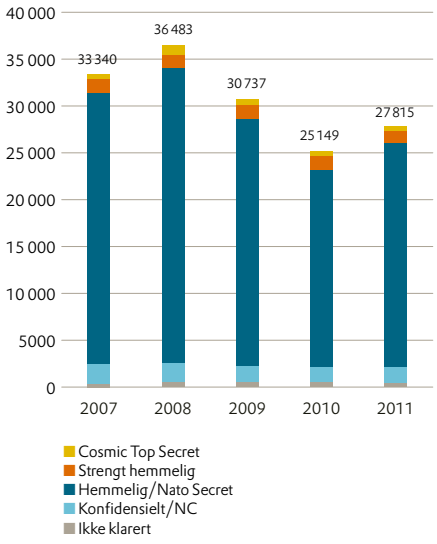
Ny veiledning

– Vi har utgitt ny veiledning til bruk av landvurderingene i 2011. Dette for å gi klareringsmyndighetene bedre grunnlag for vurderinger av saker med såkalt utenlandstilknytning. Avdelingen gjennomførte også tilsyn med syv klareringsmyndigheter for å vurdere hvordan man behandlet nettopp slike saker. Hovedinntrykket var at det generelt ble gjennomført for få samtaler, sakene ble for dårlig belyst og det var vanskelig å finne grunnlaget for avgjørelsene. Dette går først og fremst på kompetanse. Vi har også utvidet listen over landvurderinger som er tilgjengelig for klareringsmyndighetene.

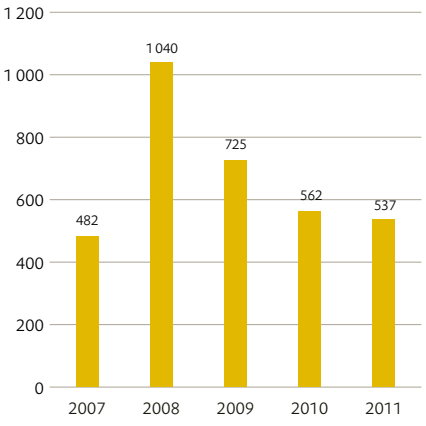
– Opp i alt dette utrednings- og utviklingsarbeidet er det viktig ikke å glemme den løpende saksbehandlingen som skjer år etter år, understreker Gustafsson.

Foto: NSM.

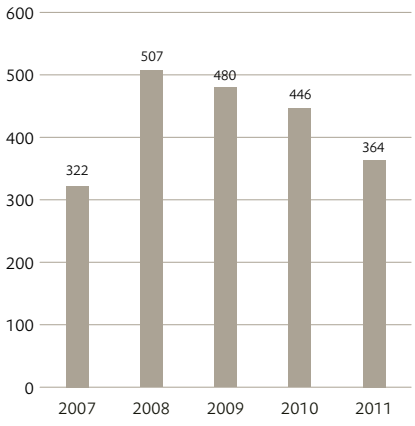
Antall sikkerhetsklareringer



Antall klareringer for Cosmic Top Secret



Antall ikke-klarerte



– Vi valgte i 2011 å kjøre regionale seminarer for autorisasjonsmyndighetene om begge produkter. Vi traff og motiverte over 300 nøkkelpersoner i dette arbeidet i Oslo, Stavanger, Bergen, Trondheim og Bodø.

Norske bygg og installasjoner skal sikres bedre mot terror og sabotasje. Sikkerhetsgodkjenning av datasystemer skal legges om. Og bakkestasjonene i det europeiske satellittprosjektet Galileo skal sikkerhetsgodkjennes av NSM og Avdeling for sikkerhetsforvaltning (FOR). – Det er nok å gjøre, sier avdelingsdirektør Vigdis Grønhaug.

Avdeling for sikkerhetsforvaltning:

Styrker objektsikkerheten

Hun fremhever spesielt arbeidet med objektsikkerhet som svært viktig i 2011.

– Etter å ha ligget på vent i mange år ble regelverksendringen gjort gjeldende fra 1. januar i 2011. Vår oppgave har nå vært å utforme en veiledning i objektsikkerhet og følge opp med rådgiving til berørte departementer og virksomheter. I tillegg bidro vi med råd og veiledning etter terrorangrepet 22. juli. Sammenfattende, en meget krevende situasjon, understreker avdelingsdirektøren.

– At vi greide å få ut en veiledning i objektsikkerhet til 1. september og samtidig har vært tilgjengelige for rådgiving, skyldes at vi omprioriterte nokså kraftig i NSM og løftet i flokk.

Økt risikoforståelse

Noe som alltid er viktig for avdelingen er å jobbe frem NSMs årlige Rapport om sikkerhetstilstanden. I år peker den spesielt på at det er manglende risikoforståelse på alle nivåer i samfunnet. Derfor vil det være viktig å jobbe for økt risikoforståelse for eksempel ved informasjonskampanjer, holdningskampanjer og utdanning, sier Vigdis Grønhaug.


Foto: NSM.

– Å etablere et bedre undervisningstilbud innen forebyggende sikkerhet vil være kjempeviktig fremover. Tilsyn viser at folk mangler kompetanse, det gjelder både vanlige brukere, sikkerhetsledere og virksomhetsledere. Det finnes nesten ikke kurs innen fagområdet forebyggende sikkerhet i dag.

Sikkerhetsgodkjenninger

Også ordningen med sikkerhetsgodkjenning av informasjonssystemer, hvor det til nå har vært store utfordringer, har tatt mye tid.

– Sikkerhetsgodkjenning av informasjonssystemer er en stor oppgave for NSM. Jeg er veldig glad for at vi nå har etablert et eget prosjekt utenfor linjen for å ta frem forslag til løsning, sier hun.

Apropos godkjenning. NSM har i noen år støttet Norsk Romsenter på sikkerhetssiden i forbindelse med det norske engasjementet inn mot Galileo-prosjektet. Aktiviteten berører flere avdelinger og elementer i NSM.

Europeisk romfart

– Min avdeling blir berørt i betydelig grad, særlig knyttet til sikkerhetsgodkjenning av viktige bakkeinstallasjoner for rominfrastrukturen. Det er et betydelig arbeid forbundet med forberedelsene til de formelle akkrediteringene fra den europeiske romfartsorganisasjonen ESA. Dette arbeidet tar mye tid. Men – det er også spennende. Det er ikke alle statsansatte som i jobben får gleden av å komme til Svalbard, Jan Mayen og Antarktis, avslutter avdelingsdirektøren.

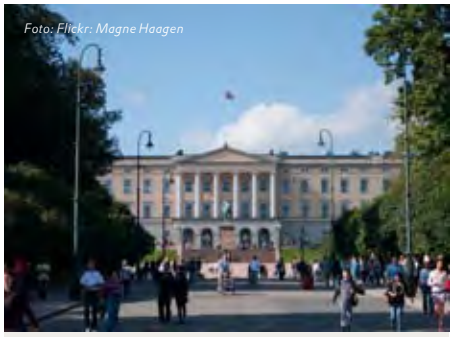


Foto: Flickr: Magne Haagen

Ny forskrift om objektsikkerhet

Arbeidet med å identifisere bygg og installasjoner som må sikres mot terror og sabotasje er nå i gang.

Forskrift om objektsikkerhet vil styrke Norges sikring mot terror, sabotasje og spionasje. Forskriften og identifiseringen av skjermingsverdige objekter vil føre til at vi for første gang får en nasjonal oversikt over kritisk infrastruktur i Norge. Forskriften skal være ferdig implementert i 2013. Nasjonal sikkerhetsmyndighet følger opp arbeidet, gir råd og veiledning i prosessen, og skal føre tilsyn med forskriften når den er ferdig implementert.

– Ansatte i NSM skal være tydelige, samhandlende og ha integritet.

Foto: NSM.

NSMs hovedbygg ligger under Kolsåstoppen i Bærum. På taket ser vi fra venstre: Vigdis Grønhaug, Hans Robert Bjørnaas, Åshild Salmela, Kjetil Nilsen, Eiliv Ofigsbø, Tore Gustafsson og Annette Tjaberg.

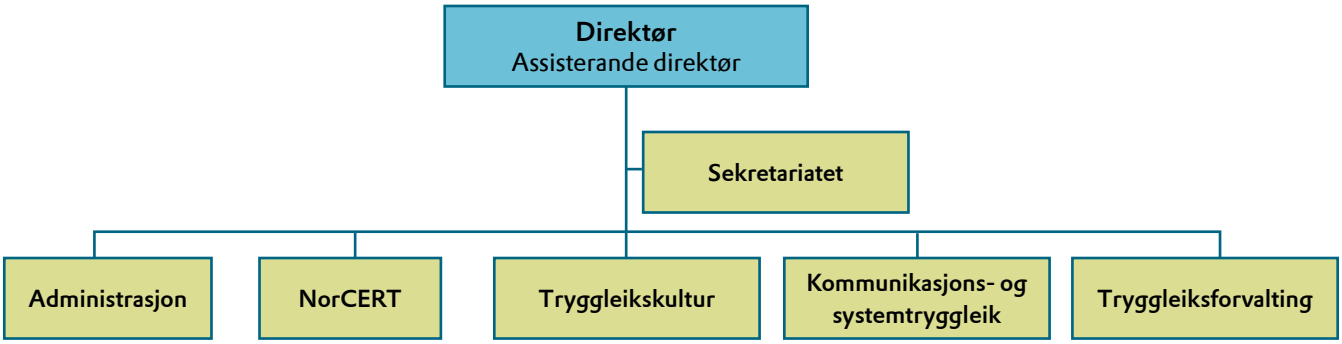
NSMs ledelse

- **Kjetil Nilsen,** direktør, er politiutdannet, jurist, har en mastergrad i ledelse samt NATO Defence College.
- **Annette Tjaberg,** assisterende direktør, er utdannet handelsøkonom. Hun har også gått på Forsvarets høgskole.
- **Åshild Salmela,** avdelingsdirektør for Administrasjonsavdelingen, har utdanning innen økonomi og ledelse fra BI.
- **Eiliv Ofigsbø,** avdelingsdirektør for NorCERT, er utdannet som cand.scient. i informatikk fra Universitetet i Oslo, og har i tillegg militær utdanning.
- **Tore Gustafsson,** kommandør og avdelingssjef for Avdeling for sikkerhetskultur, er utdannet på jøkrigsskolen, Forsvarets stabsskole, og har gått på Forsvarets høgskole.
- **Hans Robert Bjørnaas,** oberst og avdelingssjef for Kommunikasjons- og systemsikkerhetsavdelingen, er utdannet på Luftkrigsskolen og Forsvarets stabsskole, og har gått på Forsvarets høgskole.
- **Vigdis Grønhaug,** avdelingsdirektør for Avdeling for sikkerhetsforvaltning, er utdannet som høgskoleingeniør innen elektronikk, er bedriftsøkonom, og har i tillegg militær utdanning.

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

Dette er NSM:

Oppgåver, strategi og kontroll



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)
- Støtte til norsk kryptoindustri

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 Justis- og beredskapsdepartementet har det overordna sektorovergripande ansvaret for førebyggjande tryggleik i militær og sivil sektor. Nasjonalt tryggingsorgan er utøvande organ for dei to departementa innan feltet. NSM er administrativt underlagt Forsvarsdepartementet, som igjen kontrollerer NSM 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 kontroll med at tenestene held seg innanfor fastsette lover og anna regelverk. NSM blir og kontrollert av Riksrevisjonen.

Foto: Pål Rødahl/tinagent

Årsmelding for 2011

Utgitt mai 2012
Ansvarlig redaktør: Kjetil Nilsen
Redaktør: Kjetil Berg Veire
Redaksjon: Liv Nodeland, Anders Bjønnes
Grafisk design: Haugvar Kommunikasjon & Design/NSM
Forsidefoto: Colourbox.com

Nasjonal sikkerhetsmyndighet

Postadresse:
Postboks 14
NO-1306 Bærum Postterminal

Besøksadresse:
Rødskiferveien 20, Kolsås

Telefon: 67 86 40 00
Telefaks: 67 86 40 09

www.nsm.stat.no