Årsmelding

NSM

Cybersikkerhet

2009

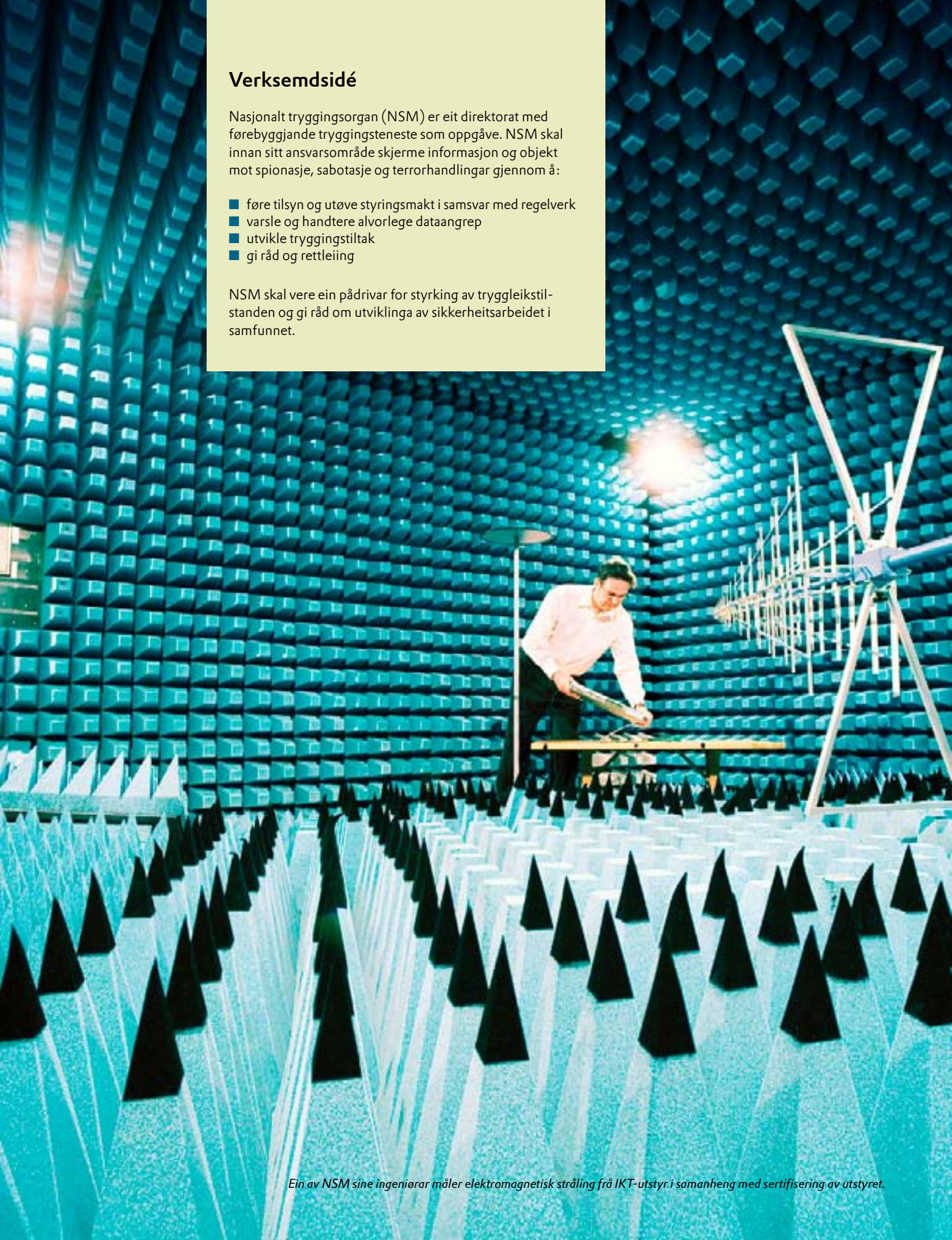
Innhold

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:

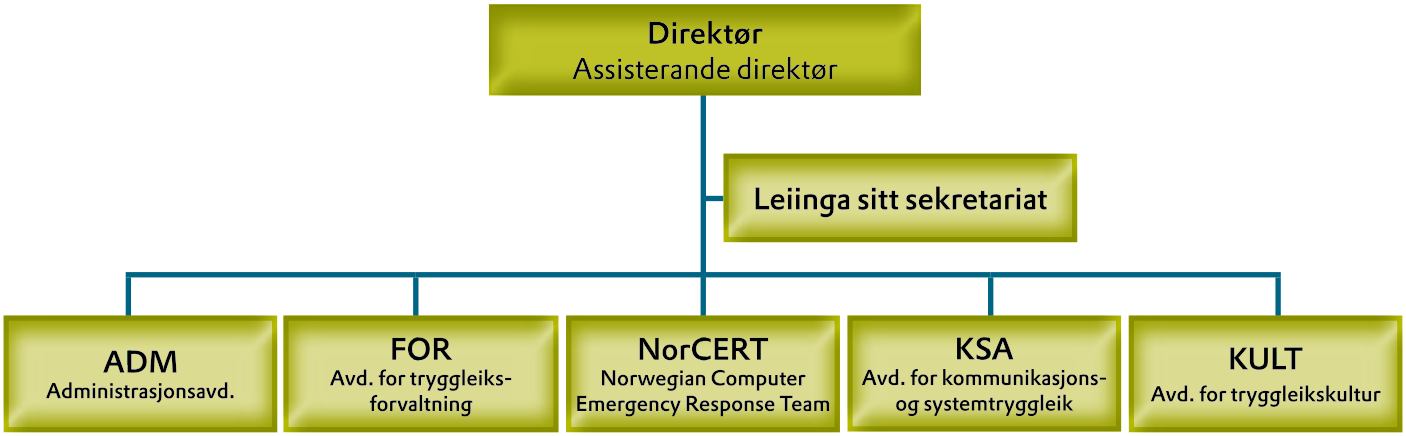
- føre tilsyn og utøve styringsmakt i samsvar med regelverk
- varsle og handtere alvorlege dataangrep
- utvikle tryggingstiltak
- gi råd og rettleiing

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



Ein av NSM sine ingeniørar måler elektromagnetisk stråling frå IKT-utstyr i samanheng med sertifisering av utstyret.

ORGANISASJON OG MEDARBEIDARAR



Dette er NSM

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 med omsyn til beredskap
- 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.

NSM sine verdiar:

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

Dei kompetente medarbeidarane

Du løyser sjeldan problem aleine. Fagfolk med spisskompetanse som kan samarbeide på tvers er nøkkelen til suksess, meiner avdelingsdirektør for Administrasjonsavdelinga, Åshild Salmela.

– Kompetanse er sjølvsagt viktig ved tilsetjing. Men det er også viktig med kompetanseutvikling av dei som er tilsette for å halde på dei gode fagfolka våre, seier ho.

NSM vil gjere dei tilsette betre rusta til å kunne samhandle og løyse oppgåva som organisasjon på ein best mogeleg måte.

– Vi vil også gi tryggleik for medarbeidarane i forhold til eiga kompetanseutvikling, slik at dei kjenner seg teke vare på, seier Åshild Salmela.

Meiningsfylte oppgåver

NSM ønskjer å vere ein attraktiv arbeidsplass. Derfor vil direktoratet systematisere og styrkje arbeidet med kompetanseutvikling. Kompetanseplanar skal byggjast opp i eit treårsperspektiv for å bidra til karriereplanar og utviklingsmoglegheiter for den enkelte medarbeidaren. Dette vil også vere bra for NSM som organisasjon.

Det sterkaste kortet til NSM er likevel at direktoratet har spennande og ikkje minst meiningsfylte oppgåver for medarbeidarane. Det er behov for både sivile og militære til ulike gjeremål. Rundt 75 % av dei tilsette har utdanningsnivå på bachelornivå eller høgare.

Etterspurd som foredragshaldarar

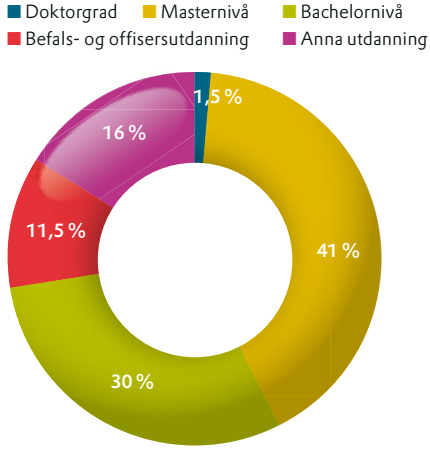
– Vi merkar etterspørselen etter kompetansen vår gjennom at vi er ønskte som foredragshaldarar. Det er tydeleg at vi i NSM sit med spisskompetanse som ingen andre har, og som andre er interesserte i å høyre om, seier Salmela.

Set leiarskap i fokus

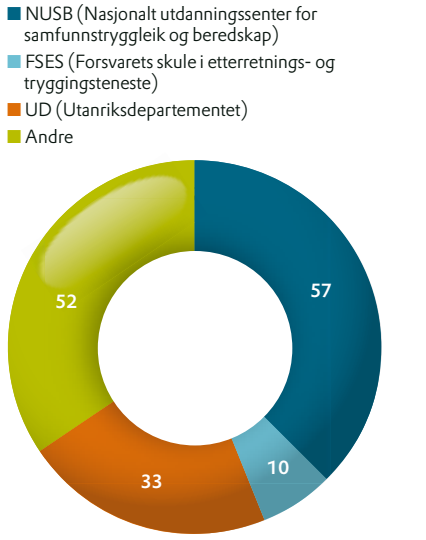
NSM har også eit viktig ansvar i forhold til mandatet sitt om å vere medviten i alt direktoratet gjer som organisasjon, og i alt den einskilde gjer som ambassadør for verksemda. NSM har gjennom fleire år arbeidt med haldningar, etikk og leiing. Dette er av stor verdi for heile organisasjonen, og bidrar til å tydeleggjere integriteten til NSM som organisasjon.

– Vi set leiarskap i fokus, noko som eigentleg handlar om å bevisstgjere medarbeidarar og leiarar på samspelet dei i mellom. Det er sett i system gjennom å skape eit fellesskap i form av samlingar, og vi har teke i bruk eit nytt verkty for medarbeidarsamtale. Men nye kollegaer kjem til, og det er derfor viktig å innsjå at dette også er ein kontinuerleg prosess, avsluttar Åshild Salmela.

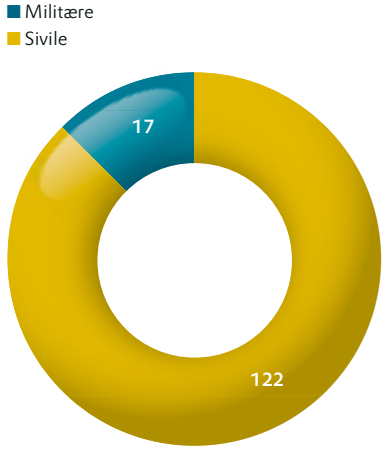
Høgaste utdanning
Per 31. desember 2009



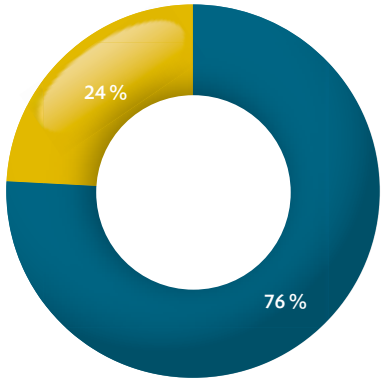
Foredragsverksemd
Timer per oppdragsgivari 2009



Tal på tilsette
Per 31. desember 2009



Kjønnsfordeling
Tilsette per 31. desember 2009



Utviklar leiarane

NSM utvikla i fjor eigne leiarkriterier for å byggje opp under ein høg etisk standard og sikre gode avgjerder.

Alle tilsette i forsvarssektoren er omfatta av ein eigen handlingsplan der det blir skapt medvit rundt haldningar og etikk. Nasjonalt tryggingsorgan har eit spesielt ansvar for at eigne handlingar er prega av integritet, openheit og høy etisk standard. Dette er eit av mange tema i leiarutviklingsprogrammet i NSM, der alle leiarnivå har delteke. Utviklingsprogrammet er eit langsiktig arbeid som blir vidareført i 2010, og skal vere med på å byggje opp under høg etisk standard og sikre gode avgjerder.

Leiarkriteria til NSM er:

- Ein leiar skal ta ansvar – skape felles forståing for målet til organisasjonen
- Ein leiar skal vere målretta – prioritere, planleggje, stille krav og følgje opp leveransar
- Ein leiar skal motivere – kommunisere tydeleg, skape trivsel, gi stønad og skape lagånd

Leiinga til NSM

Leiinga i Nasjonalt tryggingsorgan (f.h):

- **Kjetil Nilsen**, direktør, er politiutdanna, jurist, og har ein mastergrad i leiing, samt NATO Defence College.
- **Geir A Samuelsen**, assisterande direktør, er sivilingeniør og har ein mastergrad i økonomi og leiing, samt Forsvarets høgskule.
- **Tore Gustafsson**, kommandør og avdelingssjef for Avdeling for tryggleikskultur, er utdanna på Sjøkrigsskulen og Forsvarets stabsskule.
- **Hans Robert Bjørnaas**, oberst og avdelingssjef for Kommunikasjons- og systemtryggleiksavdelinga, er utdanna på Luftkrigsskulen og Forsvarets stabsskule.
- **Åshild Salmela**, avdelingsdirektør for Administrasjonsavdelinga, har utdanning innan økonomi og leiing.
- **Vigdis Grønhaug**, avdelingsdirektør for Avdeling for tryggleiksforvaltning, har militær befalsutdanning, er høgskuleingeniør og bedriftsøkonom.
- **Christophe Birkeland**, avdelingsdirektør for NorCERT, har ein doktorgrad frå NTNU og Forsvarets høgskule.

DIREKTØREN SIN ARTIKKEL

Mottok strategi for cybertryggleik

Forsvarsminister Grete Faremo og justisminister Knut Storberget fekk overlevert NSM sitt utkast til ein nasjonal strategi for cybertryggleik på Akershus festning 18. januar.

Cybertryggleik:

Mange sårbarheiter i cyberspace

Kva gjer du som sjef for ei samfunnskritisk verksemd den dagen systema ikkje får tilgang til den internettkoplinga dei er avhengig av? Eller kva gjer du når du blir klar over at sensitiv informasjon er stolen? Aksepterer du det?

22. desember i fjor blei NSM sitt forslag til ein nasjonal strategi for cybertryggleik sendt Forsvarsdepartementet og Justisdepartementet. Strategien skal gi ei betre førebygging og handtering av IKT-hendingar med store skadefølgjer for samfunnet. Strategien er no på høyring. Cybertryggleik er viktig. Det omfattar alle fagområda frå kryptering, tryggleiksgodkjenning av IKT-system, til tryggleikskultur, tryggleiksadministrasjon og leiing. Derfor er cybertryggleik tema for årsmeldinga til NSM i år.

Vi er blitt meir sårbare

– Samfunnet har endra seg raskt dei seinare åra. Vi har blitt eit nettverksbasert samfunn. Det inneber at sektorar, verksemder og funksjonar som tidlegare var uavhengige av kvarandre i dag har blitt gjensidig avhengige, og Internett bind dei saman. Det har gjort oss meir sårbare. IKT-systema er derfor paradoksalt nok både ein berebjelke og ein akilleshæl.

Det seier direktør i Nasjonalt tryggingsorgan, Kjetil Nilsen. Han er politimannen og juristen som tidlegare blant anna var ansvarleg for PST si operative avdeling, og som kom til NSM som ny direktør i mars i 2009. Han kom til eit høgteknologisk miljø med tryggingsekspertar på ei lang rekkje ulike fagområde, som jobbar med alt frå laboratorietesting av nettverkskomponentar, til tryggleiksklareringar og tilsyn. Nasjonalt tryggingsorgan har fokus på dei mest kritiske strukturane, seier Nilsen.

Omfattande tiltak

– Vi må hugse på at det vi skal skjerme ikkje er kva som helst. Det er snakk om statsløyndomar, sabotasje- og terrormål. Det er ein viss forskjell på å verne dette, og verne familiebilete og private personopplysningar. Derfor vil tiltaka til NSM alltid vere noko meir omfattande, noko meir inngripande, og noko meir kostbare enn andre tiltak. Men det som blir meir og meir tydeleg er at utfordringa også er nett alt dette som ligg

> «IKT-systema er paradoksalt nok både ein berebjelke og ein akilleshæl».

rundt. Alt heng saman i det nettverksbaserte samfunnet. Ei svakheit i nokre delar kan få følgjer for andre delar. Vi er alle i same båt, alle treng energi og telekommunikasjon. Vassdammar for energiforsyning blir ikkje lenger styrde med spakar av ein lokal operatør. Dei blir fjernstyrde, på same måte som togstasjonar og oljeinstallasjonar. Minibankar fungerer ikkje utan straum, og færre og færre system har ei manuell reserveløysing som ikkje er avhengig av tele og energi.

Har for lita oversikt

– Klarer ikkje offentlege og private verksemder sjølv å ta vare på sin eigen tryggleik?

– Verksemdene har primæransvaret.Og ja, langt på veg klarer dei det. Vår uro er at tilnærminga i for stor grad er fragmentert, sektorbasert, og at det ikkje er ei felles oppfatning av kva som bør vere den nødvendige grunnsikringa. Tryggleiken blir sjeldan betre enn det svakaste leddet i kjeda. Når dei mest kritiske systema er avhengig av at alt anna fungerer, har vi eit ansvar til å peike på dette, og sørgje for ei skikkeleg vurdering, som i cybertryggleiksstrategien som no er sendt på høyring.

– Så vi har for lita oversikt?

– Ja, vi veit for lite om tryggleikstilstanden.

Må auke kompetansen

Betre situasjonsforståing og oversikt over kva som skjer på Internett er blant tiltaka som står på resepten til NSM

– Vi må auke kompetansen. Vi må betre samordninga. Vi må utvikle evna til å handtere ei hending når ho oppstår. Det er også på sin plass å nemne endringane i regelverket rundt objekttryggleik. Den nye objekttryggingsforskrifta vil føre til at kritisk infrastruktur blir kartlagd på ein betre måte. Vi veit for lite om dei kritiske punkta. Ei ulukke i éin sektor kan få store ringverknader i ein annan, utan at vi veit kva slags, seier Kjetil Nilsen.

– NSM foreslår i strategien tiltak som vil koste pengar, kvifor er arbeidet med cybertryggleik viktigare enn andre typar tryggleik?

– Vi seier ikkje at det er viktigare enn annan type tryggleik. Men vi seier at det er viktig. Truslar kan ha sitt opphav både i uhell, naturkatastrofar, og ønskte, gjennomtenkte handlingar som for eksempel kriminalitet og sabotasje. Men om telenettet fell ut som følgje av det eine eller det andre vil det ofte ha dei same konsekvensane. Tiltaka vi foreslår vil kunne ha positiv verdi, same kva årsaka er, seier Nilsen.

Utfordringar i krise og krig

– Men er det verkeleg fare for at tele eller straum skal falle ut som følgje av eit angrep?

– Den norske infrastrukturen er robust. Risikoen er ikkje stor. Men det kan ikkje utelukkast, særleg om ein tek høgde for dei mest kompetente trusselaktørane. Det er gjort mykje for å skape redundans i det norske samfunnet. Men konsekvensane av ein slik situasjon vil vere overveldande.

– Då seier du på ein måte to ting – at vi er veldig sårbare, men også robuste.

– Vi er av dei meir robuste, men dette er ei kontinuerleg utvikling der det kjem nye sårbarheiter med den nye teknologien. Vi må minimalisere sårbarheitene. Og dersom ein situasjon oppstår, må vi ha evne til å handtere den.

Det globale nettverkssamfunnet stiller oss overfor store utfordringar når det gjeld beredskap, krise og krig.

– Ein må ha eit gjennomtenkt forhold til tryggleik og leveransedyktigheit i krise og krig. Men også i fredstid stiller dei digitale nettverka oss overfor store utfordringar, for eksempel i forhold til spionasje.

– Krise og krig, sabotasje og spionasje – skjønner du at det kan liggje litt langt unna folk flest når vi lever i eit trygt og demokratisk samfunn, der det er langt mellom dei nasjonale krisene?

– Det er lett å forstå at det kjem i bakgrunnen i dagliglivet. Vi er så vand med at alt fungerer. Men med ein gong noko ikkje fungerer, den dagen du ikkje får tilgang til internettkoplinga di på jobben, eller heime, kva gjer det med deg? Får du gjort det du skulle gjere? Kan du klare deg utan? Eg trur alle som har kjent på kva det inneber at systema ligg nede vil kunne forstå at dette kan få stor betydning, seier Kjetil Nilsen.

Nasjonal strategi for cybertryggleik

I NSM sitt forslag til ein nasjonal strategi for cybertryggleik blir det foreslått 22 tiltak for å styrkje Noreg si evne til å førebyggje og handtere alvorlege IKT-hendingar. Hovudmåla til strategien er å:

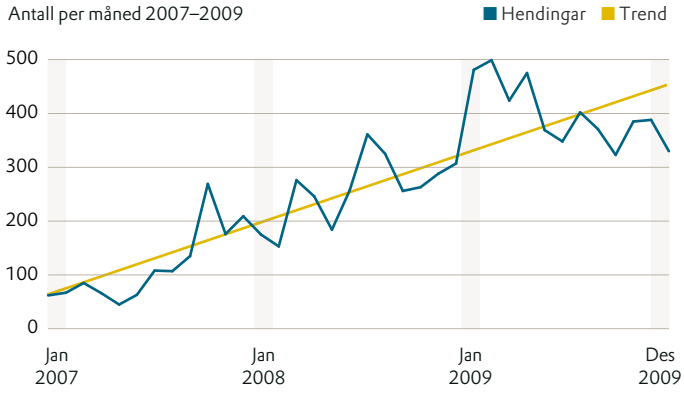
- Etablere ei felles situasjonsoversikt og forståing
- Byggje og oppretthalde robuste og sikre IKT-system
- Bevisstgjere, opplyse og påverke
- Styrkje evna til å oppdage, varsle og handtere IKT-hendingar
- Motarbeide og etterforske IKT-hendingar
- Styrkje samordninga av cybertryggleiksarbeidet

Kraftsamling rundt nytt cybersenter

Strategien foreslår å opprette eit nasjonalt cybersenter underlagt NSM, som ei vidareutvikling av NorCERT, i tett samarbeid med PST og E-tenesta. Måla for senteret vil vere å styrkje Noreg si evne til effektivt å handtere og respondere på alvorlege IKT-hendingar og situasjonar, betre og meir samanfallande forståing av tryggleiksutfordringane, betre utnytting av kritisk kompetanse, synleggjering av nasjonal innsats og tilrettelegging for internasjonalt og nasjonalt samarbeid. Dette inkluderer vidareutvikling av modellar for operativt samarbeid mellom offentlege styresmakter og private verksemder.

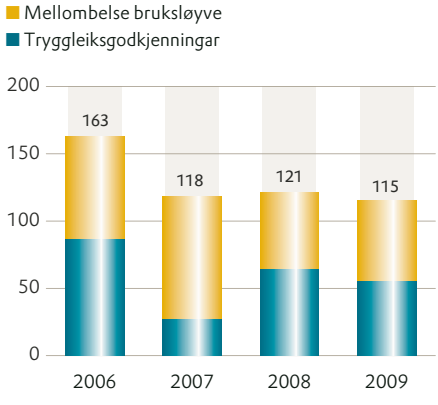
Nokre sentrale tal

Handterte IKT-hendingar
Antall per måned 2007–2009



Stadig meir å gjere: Grafen viser talet handterte hendingar i operasjonssenteret til NorCERT. Mengda saker er meir enn tredobla i perioden 2007 til 2009. I 2009 blei det handtert 4795 hendingar.

Tal på tryggleiksgodkjenningar og mellombelse bruksløyve for graderte informasjonssystem der NSM er godkjenningsansvarleg



Tal på godkjende system
Per sektor i 2009

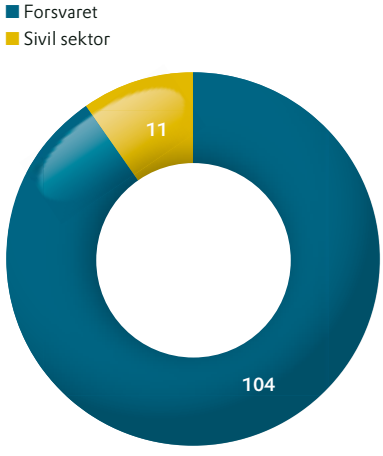


Diagram over:
Oversikta skil ikkje mellom omfang og kompleksitet i dei ulike sakene. Det er stor variasjon i dette mellom dei ulike systema. Tala kan såleis ikkje samanliknast direkte frå år til år, men gir likevel eit bilete av aktivitetsnivået.

NATO og USA uroleg for cybertryggleiken

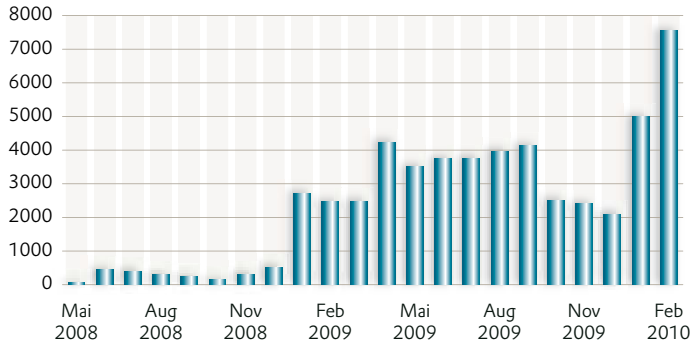
Cybertryggleik er eit tema internasjonalt. NATO ser på truslane mot IKT-system med aukande uro. NATO si parlamentarikarforsamling hevdar at cyberangrep saman med terrorisme og spreiing av kjernevåpen er ein av dei mest alvorlege asymmetriske truslane alliansen og medlemsstatane står overfor. Ein rapport frå Det kvite hus om cybertryggleik slår fast at risiko rundt cybertryggleik utgjer ein av dei mest alvorlege økonomiske og nasjonale tryggleiksutfordringane i det 21. hundreår

Kva gjer andre land?

Fleire andre land har det siste året sett i gong arbeidet med å styrkje informasjonstryggleiken. Britiske styresmakter gjekk i fjor inn for å styrkje tryggleiken gjennom ein eigen cybertryggleiksstrategi. I USA blei det i fjor foreslått ei rekkje tiltak, og utnemnt ein eigen koordinator for cybertryggleik i Det kvite hus. Den svenske regjeringa har bestilt ei utgreiing for å skape betre føresetnader for å førebyggje og handtere IT-hendingar. Og Australia har oppretta to nye organisasjonar for å styrkje datatryggleiken.

IKT OG RISIKO

Antall registrerte IP-adresser som skjuler infiserte PC-er



Økende: Oversikten viser antall rapporter til NorCERT om norske offentlige IP-adresser som skjuler infiserte systemer som er eller som har vært kompromittert. Flere tusen datamaskiner kan i enkelte tilfeller skjule seg bak en registrering. Databasen med mulighet for statistikkjøring ble først opprettet i april 2008. Økningen i januar og februar 2010 skyldes at kildene vi nå får informasjon fra er mer omfattende.

Programvare skreddersydd for etterretning:

Mye informasjon trolig på avveie

Det er ikke usannsynlig at store mengder informasjon er på avveie etter datainnbrudd. Det finnes store mangler i forhold til vedlikehold og oppdatering av sårbare datasystemer.

NSM har i løpet av 2009 mottatt informasjon om og bidratt til å avdekke og håndtere et stadig økende antall saker som involverer informasjonsinnsamling med målrettede trojanere. Dette er programvare som er særskilt egnet til etterretningsvirksomhet.

Målrettet dataspionasje

Det er ikke usannsynlig at store mengder informasjon er på avveie som følge av disse datainnbruddene. I de fleste av disse sakene har det blitt avdekket at berørte systemer har vært kompromittert over lengre tid. Målrettede trojanere retter seg typisk mot målgrupper som besitter informasjon av stor verdi, kommersiell eller strategisk. Typiske målgrupper vil være ledere på ulike nivåer, forsvarssektoren med underleverandører, høyteknologiske selskap og menneskerettighetsorganisasjoner og advokater.

Spredning av uønsket kode

Det er lenge advart mot spredning av uønsket kode via e-post og kompromitterte nettsteder. I begynnelsen av 2009 opplevde man også en betydelig spredning av programkode via USB-tilkoblede enheter som minnepinner. NSM antar at spredning av uønsket kode via mobiltelefon vil komme til å bli en betydelig utfordring (se mer informasjon i faktaboks til høyre).

Confickerormen som begynte å spre seg i 2008 og som fikk mye omtale i løpet av 2009, fikk betydelige konsekvenser for enkelte organisasjoner i Norge. Sikkerhetsoppdateringen for denne sårbarheten ble publisert av Microsoft 23. oktober 2008. Likevel fikk ormen stor utbredelse, fordi sikkerhetsoppdateringen ikke hadde blitt installert på samtlige maskiner. Conficker spredte seg også via minnepinner og nettverkskataloger, noe som gjorde at den kunne spre seg også på oppdaterte systemer. Skadevare som har kapasitet til å distribuere seg ved hjelp av flere ulike spredningsmekanismer vil oppnå videre utbredelse og inneha større motstandsdyktighet mot å bli fjernet.

Manglende oppdatering

De aller fleste cyberangrep går mot sårbarheter hvor det finnes sikkerhetsoppdateringer og andre sikkerhetstiltak. Likevel observeres det at mange enklere angrep er vellykkede. Det er urovekkende. Sikkerhetsbarrierene er ofte unødvendig lave. Det finnes store mangler i forhold til vedlikehold og oppdatering av sårbare systemer.

Ondsinnede aktører viser fortsatt stor interesse for å knytte infiserte PC-er sammen i nettverk for å utnytte datakraft. Slik datakraft kan utnyttes for målrettede angrep mot samfunnskritiske IKT-systemer. PC-er med svak sikkerhet er særlig utsatt for å bli utnyttet. På denne måten kan sikkerhetsnivået til den enkeltes private hjemme-PC være av betydning for samfunnssikkerheten.

SMS kan bli en sikkerhetsrisiko

Spredning av skadelig programvare via mobiltelefon kan bli en betydelig utfordring fremover.

Nasjonal sikkerhetsmyndighet er kjent med at skadelig programvare kan spres via SMS. Aktiviteten ansees fortsatt å være på et tidlig stadium, selv om den har økt betydelig.

Alle mobiltelefoner kan motta og behandle SMS. Tjenesten kan ikke skrus av, eller blokkeres med brannmur eller lignende. SMS mottas og behandles uten noen form for brukerinteraksjon.

I dag gir nye funksjoner i MMS-formatet støtte til ny funksjonalitet som multimedia, ringetoner, og andre større og komplekse filer og meldinger. Slike komplekse formater med mye innebygd funksjonalitet er sårbare for manipulasjon og infisering av skadevare.

SIKKERHETSTILSTANDEN

Sikkerhetsarbeidet blir ikke prioritert:

Bekymret for sikkerhetstilstanden

Sikkerhetstilstanden i Norge er bekymringsfull, gitt dagens trusselbilde som viser at etterretningstrusselen er vedvarende høy mot Norge og norske interesser. Mye av etterretningsvirksomheten foregår via IKT-systemer.

Særlig de to siste årene har IKT-trusselen økt betraktelig. Denne trusselen er dynamisk og utvikler seg raskt. Risikoen for at virksomheter underlagt sikkerhetsloven kan bli utsatt for forsøk på etterretning via Internett er derfor økende.

Flere mangler

På bakgrunn av tilgjengelig empiri i 2009 samt utviklingen tidligere år ser NSM følgende hovedtendenser:

- Manglende ledelsesengasjement
- Mangelfull organisering og daglig styring

Dette understøttes av mangelfull kompetanse og bevissthet, og mangler i en rekke ulike områder som deteksjon, rapportering og håndtering av hendelser, sikkerhetsklarering og autorisasjon, mangelfull håndtering og oppbevaring av graderte dokumenter, og mangler innen håndteringen av graderte IKT-systemer

Omfanget av avvik tyder i stor grad på et fravær av lederengasjement innen forebyggende sikkerhet.

Virksomhetsleder bør iverksette den type tiltak som ellers er vanlig i virksomhetsstyringen, slik at disse også gjelder for den forebyggende sikkerheten.

Utilstrekkelig organisering

Avvikene tyder også på at det forebyggende sikkerhetsarbeidet er utilstrekkelig organisert og styrt. Forebyggende sikkerhet bør være en integrert del av virksomhetenes ordinære styringssystem. Dette er som regel godt utviklet og har gode rutiner for å oppdage og korrigere avvik innen styringsområder som HMS eller økonomi.

> «Omfanget av avvik tyder i stor grad på et fravær av lederengasjement innen forebyggende sikkerhet».

Økt fokus på lederne

NSM har i tidligere rapportering uttrykt bekymring for et økende gap mellom et dynamisk risikobilde og et stillestående sikkerhetsarbeid. Det er grunn til å gjenta denne bekymringen. Det er et behov for å angripe årsaker til at sikkerhetsarbeidet ikke prioriteres godt nok. Det er lederen i den enkelte virksomhet som sitter med nøkkelen til en god sikkerhetstilstand.

Nasjonal sikkerhetsmyndighet kommer i 2010 til å øke fokuset på ledernes rolle gjennom brosjyre, veiledning og NSMs årlige sikkerhetskonferanse.

Tilsyn i 2009

Tilsyn er en av NSMs hovedoppgaver. I 2009 har NSM gjennomført totalt 19 ordinære tilsyn med virksomheter som er underlagt sikkerhetsloven. Loven skaal forebygge mot spionasje, sabotasje og terrorhandlinger. Det er gjennomført sju tilsyn med leverandører av sikkerhetsgraderte anskaffelser, og to tilsyn med klareringsmyndigheter i 2009.

Tilsynene er et viktig virkemiddel for å få bedre kunnskap og oversikt over sikkerhetstilstanden.

Ny metodikk retter fokuset mot virksomhetenes styringssystem for sikkerhet og virksomhetsledelsen. Samtidig er NSM opptatt av at tilsynene skal oppfattes som et nyttig verktøy for sikkerhetsarbeidet i virksomhetene.

Nærmere 600 virksomheter er underlagt sikkerhetsloven, som omfatter Forsvaret, offentlig forvaltning samt enkelte private virksomheter.

ANALYSERER SKADEVARE

En krevende jobb

Gjennom avdelingen NorCERT analyserer NSM programvare som blir brukt i dataangrep. Analysen krever høy kompetanse og krever ofte samarbeid mellom NSM, og PST- og E-tjenesten, og tilsvarende organisasjoner i andre land og virksomheter.

Kodejegerne

De jakter på skadelig kode som blir brukt til spionasje eller dataangrep. – En stor del av jobben er å forstå hvordan koden fungerer. Da er det snakk om å se på alle mulige tegn på skjerm, og finne mønstre. Du skal være glad i puslespill, sier Markus på NorCERT.

I malware-laben på NorCERT står Markus med hendene ned i en boks med ledninger og kontakter hengende ut, med en liten harddisk plassert i midten. Blinkende skjermer står rundt, og kofferter med utstyr er plassert utover gulvet.

– Det er litt Petter Smart-virksomhet, dette. Laben er en hjemmesnekret verktøykasse satt sammen av teknikker og metoder som har fungert for oss de siste årene, sier Markus.

Den besværlige koden

For at PC-en din skal fungere og gjøre det du ønsker, har den en rekke programmer. Hvert program kan bestå av millioner av linjer med kode. Koden er instruksjonene datamaskinen trenger for å gjøre det den skal gjøre. Men ikke all kode er laget slik at maskinen gjør det du ønsker. Skadelig kode er bittesmå programmer som kan lures inn i maskinen skjult i et vedlegg til en e-post, på en minnepinne, eller fra nettsider. Den kan tappe maskinen din for sensitiv informasjon, bruke datakraften i angrep mot andre, eller gjøre alt det personene bak måtte ønske. NSM, som gjennom NorCERT varsler og håndterer alvorlige IKT-hendelser, er en av få virksomheter i Norge som har kompetanse til å analysere kode som blir brukt i slike hendelser.

– Vi leter som regel etter typisk informasjonsstjelende trojanere , altså små programmer som er laget for å stjele informasjon. I dette konkrete tilfellet vi sitter med nå er det en bruker som har reagert på at maskinen oppførte seg rart. Trojaneren vi leter etter har ligget der i flere år, sier Markus.

Studerer algoritmer

Det er ikke noen selvfølge å oppdage at maskinen din er i hendene på kriminelle eller andre trusselaktører. En godt laget trojaner lager ikke problemer for maskinen. Den blir ikke oppdaget av antivirus, og stoppes ikke av brannmurer. Maskinen oppfører seg som normalt.

Noen av de mest alvorlige sakene NorCERT håndterer er målrettede operasjoner mot norske bedrifter eller offentlige institusjoner. Dette er typisk forsøk på spionasje.

– Det er viktig å finne programkoden som blir brukt for å forstå hva den gjør på systemet og hva slags kapasiteter den har. Hva slags informasjon er de som står bak ute etter? Hvilke endringer gjør trojaneren på systemet? Hvordan ble datasystemet kompromittert? Hvordan sprer koden seg? Hvordan kjenner man koden igjen? sier Idar.

– Hvis koden er kryptert må vi begynne å studere algoritmene for å forstå hvordan den fungerer, og hvordan den krypterer data.

«Laben er en hjemmesnekret verktøykasse satt sammen av teknikker og metoder som har fungert for oss de siste årene.»

Et spisset felt

Når Markus og Idar vet mer, kan de kjøre søk på unike kjennetegn ved koden i NorCERTs systemer for å se hvilke virksomheter som kan være rammet, gi informasjon til andre som kan være i faresonen, og hjelpe de som har blitt rammet til å finne ut hva som faktisk har skjedd, og hva som kan være stjålet.

– Dette er et veldig spisset felt. Du skal være glad i puslespill. Det er hjernekirurgi. Det går tid og atter tid, det er komplekst. Du skal være nysgjerrig, tålmodig og samtidig resultatorientert. Jeg har alltid vært glad i Lego, og å plukke fra hverandre sykler og gressklippere. Reversingeniører er flinkere til å plukke ting fra hverandre og forstå hvordan det er bygd opp, enn å bygge det opp igjen, sier Markus.

Mistenkelig trafikk

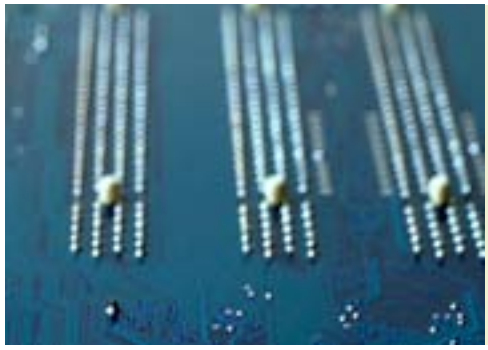
– Hva er det mest spennende dere gjør?

– Det mest spennende er å analysere mistenkelig kode. Når koden er sofistikert og gjør ting som overrasker, og personene bak åpenbart er veldig dyktige, da blir jeg fornøyd, sier Markus. Du har kompetansen til å være den første i verden til å finne ut hva som faktisk skjer. Det er veldig spennende.

– Hvordan får dere kred, hvis dere er de første i verden til å finne ut noe, men alt er veldig hemmelig?

– Det får vi ikke. Vi får følelsen av å være førstemann, og gjør det for konge og fedreland! sier Markus.

LETER ETTER SIKKERHETSHULL



Inntrengerne

I 2009 ble NSM for første gang operative med en egen enhet som tester datassikkerheten gjennom såkalt inntrengingstesting. NSM er de eneste som har lov til å teste sikkerheten i graderte datasystemer gjennom inntrengingstesting. Hensynet til personvernet og rettssikkerheten for de ansatte i virksomhetene hvor testene foregår står i høysetet.

Sikkert, eller ikke sikkert?

Fingertuppene blir svette når dataingeniør Øystein Thorvaldsen simulerer dataangrep for å teste sikkerheten i informasjonssystemer. – Det er en form for kontrollert angrep. Det du må være god til er å gjøre det i dokumenterte former, sier han.

Skjermen er svart med hvite bokstaver. Øystein Thorvaldsen skriver raskt inn noen kommandoer og trykker enter.

– Her kan jeg scanne hvilke porter som er åpne, hva slags oppsett og programmer PC-en jeg ønsker å komme inn på bruker. Operativsystemet virker sikkert, men jeg har funnet en FTP-server som har en sårbarhet jeg kan utnytte. Da kan jeg se om det finnes programvare som kan utnytte denne sårbarheten til å komme inn på maskinen, sier han.

Kan logge alt

PC-en i dette tilfellet er en demonstrasjons-PC som gutta i nettverkssikkerhetseksjonen i NSM bruker. Etter et par kjappe tastetrykk er han inne på PC-en som "angripes".

– Nå kan jeg i prinsippet gjøre det jeg vil med maskinen. Jeg har tilgang til alt som skjer på den, jeg kan hente ut dokumenter, og logge alle tastetrykkene, sier Thorvaldsen.

Alle datasystemer har sikkerhetshull og sårbarheter. Det gjør det enkelt for hackere å bryte seg inn, stjele informasjon, eller ødelegge. Øystein Thorvaldsens jobb er å finne hullene før kriminelle, etterretningsorganisasjoner eller andre gjør det.

NSM driver i dag med godkjenning, tilsyn, råd og veiledning og kravsetting til datasystemer som skal behandle gradert informasjon. Men det er vanskelig å gjøre komplekse systemer sikre mot alle typer innbrudd, sabotasje eller andre trusler. Derfor etablerte NSM i fjor en enhet for inntrengingstesting. Den tester sikkerheten i datasystemer ved å gjøre målrettede søk og analyser, og identifisere sårbarheter, feil og mangler. Testingen retter seg utelukkende mot selve datasystemene og sikkerhetsmekanismene, og innebærer ikke å lese innhold i kommunikasjon eller dokumenter, såkalt monitoring. Testene er strengt regulert i lov, forskrift og interne retningslinjer for aktiviteten i NSM.

> «Det blir som en kontrollert versjon av å angripe systemet på samme måte som en fiende eller en annen trusselaktør.»

En lang prosess

– Prosessen begynner lenge før vi setter oss ned med maskiner og programvare, sier Øystein Thorvaldsen. Han beskriver en omfattende prosess med oppstartsmøter, avklaring av forventninger, tidsplaner, samtykkeerklæringer, avgrensinger, ansvarsfordeling og så videre.

– Systemeier får også tilsendt et informasjonsskriv om hva vi driver med, og en mal for varsling av alle berørte som bruker systemet, sier Thorvaldsen.

Testplaner skal lages, og alt som blir gjort skal logges. Så skal utstyret settes opp.

Kartlegger sårbarheter

– Det første vi gjør er å sette opp utstyret, og sjekke at loggfunksjonalitet er i orden. Så varsler vi virksomheten om at vi begynner. Deretter rekognoserer vi trafikken som går på nettet, og prøver å danne oss et bilde av hva slags maskiner som kjører og hvordan systemet er bygd opp. Hva ser vi, og hva kan vi bruke?

Så kartlegges sårbarheter og svakheter og mulighetene for innbrudd. I ettertid lages det en rapport til virksomheten med testens resultater, og anbefalinger til hva som bør gjøres.

– Er dette hacking?

– I motsetning til en hacker som prøver å finne ett svakt punkt for å trenge seg inn, sikter vi oss inn på å finne flest mulige svakheter. Hensikten er derfor grunnleggende ulik den hackere har, selv om vi bruker samme type metoder. Personvern er avgjørende. Vi som jobber med dette har aller høyeste sikkerhetsklarering, sier Thorvaldsen.

– Det blir som en kontrollert versjon av å angripe systemet på samme måte som en fiende eller en annen trusselaktør. Av og til er angrep det beste forsvar, avslutter han.

SIKRERE MOBILTELEFONER

Mobiler kan avlyttes

Mye sensitiv informasjon kan komme på avveie gjennom dårlig sikrede mobiler. Beslutningstakere og nøkkelpersonell er spesielt utsatt for å bli avlyttet. Sikre, men enkle mobilløsninger har ikke alltid vært tilgjengelige. NSM arbeider nå med å finne kosteffektive løsninger som kan brukes av målgruppen.

Fra teori til praksis

Den stråler i alle retninger, blir brukt til alt mulig, og er proppet med forskjellige typer teknologi. Olaf Garnaas og de andre spesialistene i NSM jobber med å finne ut hvordan beslutningstakere og nøkkelpersonell kan få mobiltelefoner som er sikrere mot avlytting.

Det er ikke få tekstmeldinger og samtaler som går gjennom mobiltelefonene til mange norske beslutningstakere og nøkkelpersonell daglig. Mange viktige beslutninger skal tas, og mye informasjon må videreformidles. Mye av dette er sensitivt. Men mobiltelefonen er i utgangspunktet ikke avlyttingssikker. Akademiske miljøer har knekt krypteringen i GSM-nettet. Dataprogrammer for mobilavlytting har vært til salgs på Internett i flere år. Virus på mobiltelefonen kan overvåke den som har den. Den kan hackes som en vanlig datamaskin. Den kan knytte seg opp mot trådløse nettverk som kan avlyttes.

Bygger opp egen lab

Til nå har ledere, nøkkelpersonell og andre brukt spesialmobiler med kryptering for å snakke hemmelig. I løpet av veldig få år har mobilmarkedet eksplodert med nye muligheter, og gjort oss mer fleksible og samtidig kravstore med hvor og når vi vil jobbe.

Nå arbeider NSM med å se etter tilgjengelige løsninger som kan gjøremobiltelefonene mer avlyttingssikre, samtidig som funksjonaliteten opprettholdes.

– Vi bygger for tiden opp en lab hvor vi skal vurdere sikkerhetsfunksjonalitet i operativsystemer, kryptoløsninger, talekvalitet og brukervennlighet. Brukerne etterspør en enkel og praktisk løsning.

Det sier Olaf Garnaas, som er informatiker med en master i elliptiske kurver fra Selmersentret i Bergen.

En dynamisk verden

Nå er det han og en håndfull andre fagpersoner i Nasjonal sikkerhetsmyndighet som skal finne ut hvordan norske ledere og nøkkelpersoner kan få avlyttingssikre og samtidig praktiske mobilløsninger. Det er en stor utfordring.

– Vi er bundet av eksisterende teknologi. Teknologien er markedsdrevet, og det er mye usikkerhet forbundet med hva operatørene og produsentene gjør, og hvilke operativsystemer som blir dominerende. Dette er en veldig dynamisk verden, sier han.

> «Brukerne etterspør en enkel og praktisk løsning.»

I tillegg må spesialistene i NSM finne gode løsninger for både sikre samtaler og tekstmeldinger. I dag finnes det få løsninger som kombinerer krypto både for sms og tale.

Utfordrer mange fagmiljøer

For å sikre mobilen mot avlytting, må den ha en god kryptoløsning. Den må også ha streng kontroll med hva brukeren kan laste ned av programmer, slik at han eller hun ikke uforvarende laster ned spionprogramvare. Og den må ha et operativsystem som er robust og sikkert nok.

– Dette er en oppgave som naturlig nok utfordrer ulike fagmiljø, en tilfredstillende kryptoløsning forutsetter at mobilen innehar full integritet over tid. Flere må jobbe sammen og se på alt fra kryptoløsninger til operativsystemer og tilhørende sikkerhetsadministrasjon, sier Olaf Garnaas.

– Målet er å identifisere kommersielle løsninger som har et fornuftig sikkerhetsdesign i alle lag, samtidig som brukervennligheten forblir akseptabel, sier Olaf Garnaas.

VURDERER LAND

Økt arbeidsinnvandring

Datasystemer utvikles, driftes og brukes av personer. I Norge i dag har stadig flere ansatte familiebakgrunn fra andre land, eller har vært i utlandet i lengre perioder av sitt liv. De skal også kunne sikkerhetsklareres. NSM utvikler landvurderinger som skal hjelpe landets 44 klareringsmyndigheter til å fatte best mulige beslutninger. I fjor ble 440 utenlandske borgere søkt sikkerhetsklarert. Fire utenlandske statsborgere fikk ikke klarering.

Tar globaliseringen på alvor

Teknologi alene er ikke nok for å oppnå god cybersikkerhet: Årlig sikkerhetsklareres rundt 30.000 personer i Norge. Økt internasjonalisering er en av de nye utfordringene som må håndteres.

– Vi ser etter alle forhold i land utenfor Norge som gjør at en person kan komme under press, bli truet, fristet eller forledet til å begå handlinger som kan føre til sikkerhetsbrudd.

I NSMs bygninger på Kolsås utenfor Oslo sitter en kvinnelig historiker og en mannlig statsviter i midten av 30-årene. De studerer med lupe hva slags forhold utenfor Norges grenser som kan påvirke arbeidstakere som skal sikkerhetsklareres i Norge. De såkalte landvurderingene er sikkerhetsgraderte, og er kun til bruk for dem som skal klarere personer, i alt 44 klareringsmyndigheter.

Verden et lite sted

Verden er blitt et lite sted. Folk reiser mer og jobber mer på tvers av landegrensene. Det kan gi tilknytninger til andre land som må vurderes under sikkerhetsklareringer. Fra 2006 førte endringer i sikkerhetsloven til at også utenlandske statsborgere i større grad skal kunne klareres, samtidig som forbindelser til andre land også ble relevant for klareringen av norske statsborgere. En forutsetning for endringen var at klareringsmyndighetene fikk målrettet veiledning i hvordan slike saker burde håndteres. NSM fikk i oppdrag å vurdere hva som kan påvirke sikkerhetsklareringen til personer med relasjoner til andre land. Direktoratet har etter det utviklet flere personellsikkerhetsmessige vurderinger av fremmede stater, som er den offisielle tittelen.

– Vi vurderer alt fra familiesamhold, klantilhøringhet, kriminalitetstrender og korrupsjon til kultur og lojalitetsstrukturer. Vi beskriver også nettverk, det være seg kriminelle nettverk eller terrornettverk, som har fotfeste i ulike land og regioner. Et nettverk i et annet land som har fotfeste også i Norge kan være interessant for de som skal sikkerhetsklarere personer som kan ha tilknytning til nettverket, sier NSMs analytikere.

Gjør kildekritiske analyser

Analysene blir laget på grunnlag av et bredt spekter av kilder, som ulike organisasjoner, tenketanker, utdanningsinstitusjoner og åpent tilgjengelig forskning.

– Oversikten vi skaffer oss til å begynne med gir oss en pekepinn om hva slags områder som kan være av stor sikkerhetsmessig betydning. Det begynner vi å bli ganske gode på nå etter noen år.

Relevant informasjon fra samarbeidende tjenester blir hentet inn for å underbygge analysene. Personer med førstehåndskjennskap kan bli intervjuet. Deretter blir det gjort kildekritiske analyser for å sikre at informasjonen som kommer i landvurderingene ikke bare er relevant, men også objektiv og etterrettlig, sier analytikerne i NSM.

Utrolig hva man kan finne

– Det er utrolig hva man klarer å finne rundt omkring når man bruker et vidt spekter av kilder. Videoer på YouTube kan gi et innblikk i forhold du aldri ville fått mulighet til å lese deg til i dokumenter. Nyhetsreportasjer om korrupsjon i andre lands media kan gjøre at vi må revurdere analysene vi har gjort, sier analytikerne, som er fornøyd med jobben.

– Vi har en jobb som er helt topp. Det er noen frustrasjoner, blant annet skulle vi ofte gått både bredere og dypere. Mangelfullt kildetilfang er en annen frustrasjon, vi får aldri mange nok og gode nok kilder. Vi tror allikevel analysene er relevante og gode, sier de. Tilbakemeldingene fra klareringsmyndighetene tyder i hvert fall på det.

«Det er utrolig hva man klarer å finne rundt omkring når man bruker et vidt spekter av kilder.»

SKRIVER NSMS HISTORIE

NSM skriver historie

NSM har tatt initiativ til å skrive egen forhistorie. Prosjektet finansieres av NSM sammen med Forsvarsdepartementet og gjennomføres i regi av Institutt for forsvarsstudier (IFS). Arbeidet vil gi et nærmere bilde av sikkerhetstjenestens samfunnsrolle og supplere historieverkene om de øvrige EOS-tjenestene.

Teknologi alltid i høysetet

NSMs aktuelle rolle innen cybersikkerhet er en naturlig videreføring av en lang tradisjon, sier historiker Hans Morten Synstnes. Teknologi har hele tiden vært viktig for sikkerhetstjenesten, sier han.

Doktorgradsstipendiat ved IFS, Hans Morten Synstnes, har brukt mange timer i NSMs arkiv. Han skal skrive sikkerhetstjenestens historie i perioden fra andre verdenskrig og frem til Forsvarets overkommando/Sikkerhetsstaben ble lagt ned i 2003. Samme år ble NSM og Forsvarets sikkerhetsavdeling etablert for å følge opp henholdsvis fellesskapets og forsvarssjefens sikkerhetsbehov. Et historisk viktig skille inntraff i 1965 da sikkerhetstjenesten fra å bestå av to avdelinger i Etterretningsstaben, ble opprettet som en egen stab under forsvarssjefen, og på samme tid fikk ansvaret for sikkerheten i hele forvaltningen.

Store teknologiske ambisjoner

– NSM er kjent for sitt fokus på sikkerhet og teknologi. Når begynte det?

– Sikkerhetstjenesten har alltid hatt et sterkt fokus på det. Historisk er tjenesten mest kjent for sikkerhetsklareringer og dokumentsikkerhet. Arbeidet med teknisk sikkerhet derimot er mindre kjent. Lenge dominerte chiffertjenesten (i dag kryptotjenesten). Bruk av chifferutstyr skulle hindre at fiender så forsvar og regjering i kortene – dette var viktig under krigen, under den kalde krigen og er det selvsagt fortsatt.

Ettersom datateknologien fra 1960-tallet vant større plass har teknologifokuset styrket seg betydelig. Oppgavene som i dag er pålagt NSM i tilknytning til cybersikkerhet viser dette med all tydelighet. Aldri har ambisjonene for sikkerhetsmyndigheten vært større.

Teknologiinteresserte ildsjeler

– Hvordan har sikkerhetstjenesten greid å holde seg faglig på høyden?

– På flere måter vil jeg si. Et svar er at Forsvaret alltid har huset teknologiinteresserte ildsjeler som har ivret for sikkerheten. NATO-samarbeidet har gitt tidlig innsikt i teknologiske nyvinninger. Teknologisk innovasjon har ofte vært svar på militære behov, med Internett og kryptoløsninger som to eksempler. Enda en årsak til sikkerhetstjenestens teknologiforståelse har vært samarbeidet med universitetsmiljøer. Tjenesten har i tillegg lenge holdt seg med egne sivile forskere, som har studert kompliserte tekniske sikkerhetsspørsmål. Ser vi på utdanningsnivået i dagens NSM er det på teknisk side høyt – de fleste har bakgrunn fra universiteter og høyskoler. Nå som før er høy kompetanse nøkkelen for å lykkes innenfor teknologi og sikkerhet.

Samspill med akademia

– Tekniske sikkerhetstiltak er med andre ord et resultat av en bred kontaktflate?

– Ja, og det er interessant. En hemmelig tjeneste er gjerne forbundet med lukkethet, men i realiteten har sikkerhetstjenesten samarbeidet tett med ikke minst akademiske miljøer. Sikkerhetstjenesten regnet med at myndighetenes samband ble avlyttet og at kodete meldinger ble forsøkt brutt. Samarbeid med eksterne fagmiljøer ble derfor sett på som nødvendig for å komme i forkant av den teknologiske utviklingen. Spesielt tett har samarbeidet vært mot matematikk- og informatikkmiljøer ved universitetene. Sikkerhetstjenestens samarbeid med matematikere og militære sambandsmyndigheter, koplet sammen med industrien, viste seg å bli en kruttsterk kombinasjon. Denne alliansen har resultert i at lille Norge siden 1950-tallet har vært storleverandør av kryptoutstyr til NATO.

Interessant er det også at flere tidligere ansatte i sikkerhetstjenesten fikk sentrale posisjoner ved våre universiteter. Fremtredende navn som Ernst Sejersted Selmer, Arnljot Høiland, Erling Sverdrup og Tor Helleseth ble alle professorer og nybrottsmenn innen matematikk- og informatikkfag. Det er videre interessant at tjenesten har vært en pådriver for å utvikle fagområder som statistikk, matematikk og informatikk ved norske forsknings- og universitetsmiljøer. Et eksempel var samarbeidet med Forsvarets forskningsinstitutt (FFI) på 1950-tallet hvor trioen Jan Garwick, Kristen Nygaard og Ole-Johan Dahl holdt hus, og som var foregangsmenn for en hel generasjon norske dataforskere. Sikkerhetstjenestens egne forskere nedla flere årsverk sammen med FFI og støttet opp under utviklingen av informatikk som fag. Sentrale navn her var Alf Gulbrandsen, Svein Øvergaard og Torbjørn Gravseth.

Teknisk sikkerhet ikke bare teknologi

– Kan teknologene bli for dominerende?

– Det kan de selvsagt bli. De mest avstemte sikkerhetstiltakene har helst blitt til gjennom samarbeid mellom de ulike fagmiljøene. Hver for seg tenkes det gjerne for smalt. Sikkerhetsarbeidet begynner uansett alltid med å definere hva som skal beskyttes, avslutter Synstnes.

«Nå som før er høy kompetanse nøkkelen for å lykkes innenfor teknologi og sikkerhet.»

NØKKELINFORMASJON

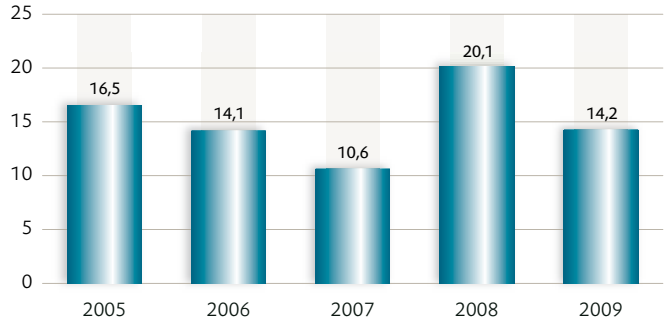
NSM i året som gikk:

Økonomi

Tall i millioner kroner	**Budsjett 2009**	**Regnskap 2009**	Regnskap 2008	Regnskap 2007	Regnskap 2006	Regnskap 2005
Lønnsutgifter	*78,5*	***77,9***	*71,5*	*66,0*	*62,0*	*59,7*
Utgifter til varer og tjenester	*33,0*	***41,5***	*44,5*	*49,6*	*51,5*	*41,7*
Sum driftsutgifter	111,4	**119,4**	116,0	115,6	113,5	101,3
Inntekter og refusjoner	2,8	**11,4**	9,9	10,6	14,4	6,6
Netto	**108,6**	**108,0**	106,1	104,9	99,1	94,7

Utgifter til FoU og materiellinvesteringer 2005-09, faste 2009-kroner

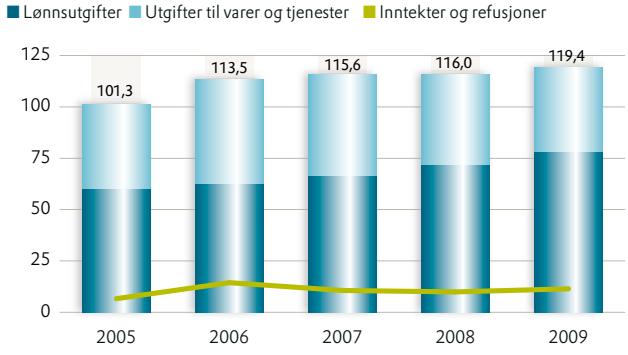
Tall i millioner kroner



Figuren viser utviklingen i NSMs utgifter til forskning og utvikling og materiellinvesteringer ført på kapittel 1760 i perioden 2005-09, korrigert for prisvekst.

Driftsregnskap 2005–2009

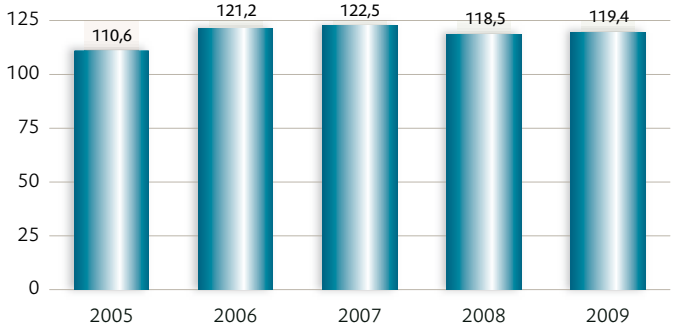
Tall i millioner kroner



Figuren viser utviklingen i NSMs driftsregnskap i perioden 2005-09. Økningen i sum driftsutgifter fra 2005 til 2006 skyldes opprettelsen av NorCERT som egen avdeling i NSM.

Sum driftsutgifter 2005-09, faste 2009-kroner

Tall i millioner kroner



God måloppnåelse

Budsjettet er gått i balanse, og de fleste målene er nådd. Allikevel er NSM en sårbar virksomhet, sier Kjetil Nilsen.

– Blant sårbarhetene er spisskompetansen NSM er avhengig av for å nå målene, sier han. NSMs høyt kvalifiserte medarbeidere er attraktive i arbeidsmarkedet.

I 2009 har NSM utviklet og styrket fagmiljøet for tilsyn, og gjennomført tilsyn etter en ny metodikk basert på den internasjonale revisjonsstandarden NS-EN ISO 19011.

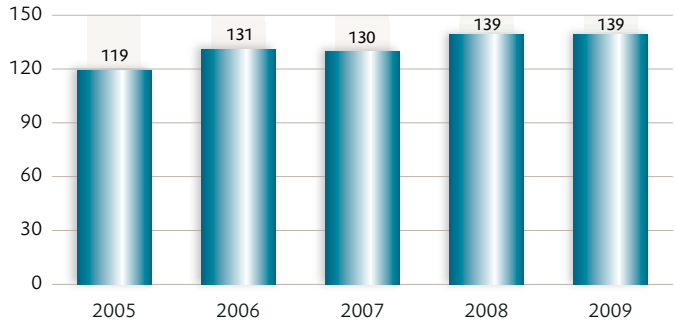
I 2009 ble det også satset mye på å redusere saksbehandlingstiden for klareringssaker og personkontroller. Den målrettede innsatsen har gitt resultater i form av kortere saksbehandlingstid. I fjor ble det også etablert en kapasitet for inntrengingstesting av IKT-systemer.

Blant målene som ikke er nådd er å få på plass en ny prosess for sikkerhetsgodkjenning av informasjonssystemer, og utrede behovet for revisjon av regelverk knyttet til krypto. Arbeidet vil bli prioritert i 2010.

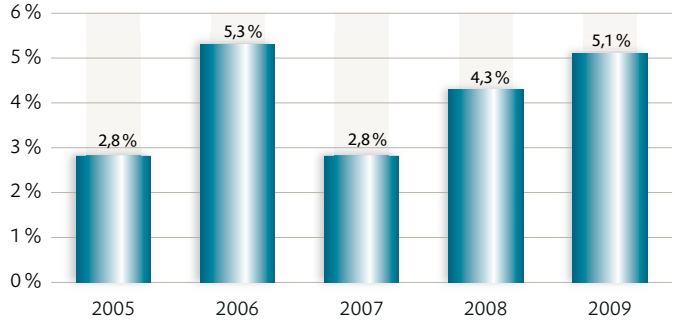
NSM fikk i 2009 ingen negative merknader fra Stortingets kontrollorgan, EOS-utvalget.

Ansatte i NSM

Antall årsverk
Totalt per 31. desember

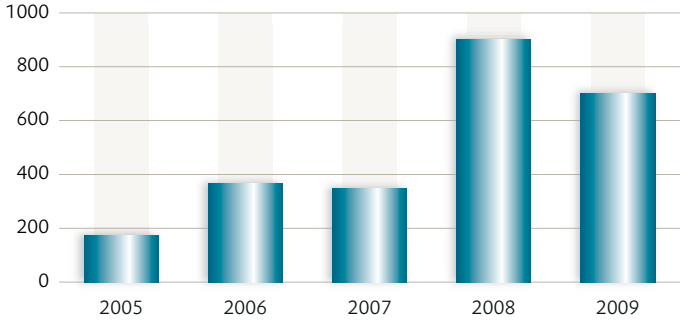


Sykefravær
Per år



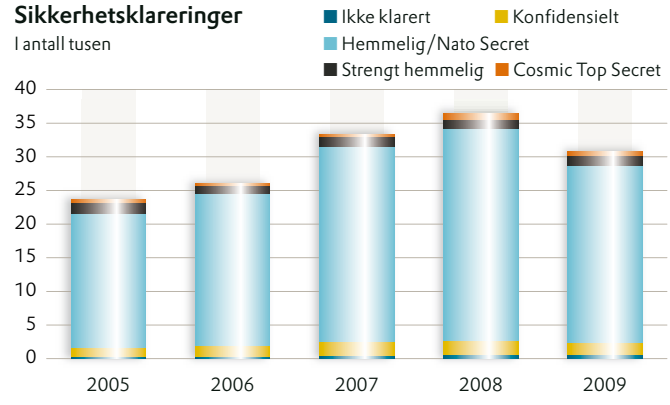
NSM i media

Antall medietreff
Per år

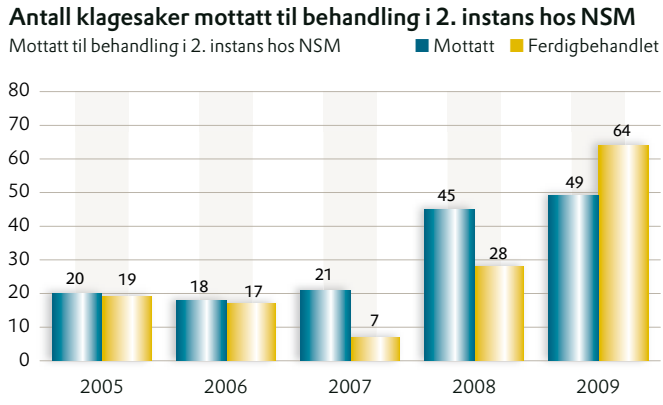


Antall medietreff gikk noe ned i 2009. Blant sakene som likevel har fått mye oppmerksomhet er nye tall som viser hvor utsatt Norge er for dataangrep fra NSM, interessen rundt sikkerhetstjenesten i Forsvaret, en ny brosjyre for sikkerhet rundt minnepinner fra NSM, og saker rundt dataspionasje.

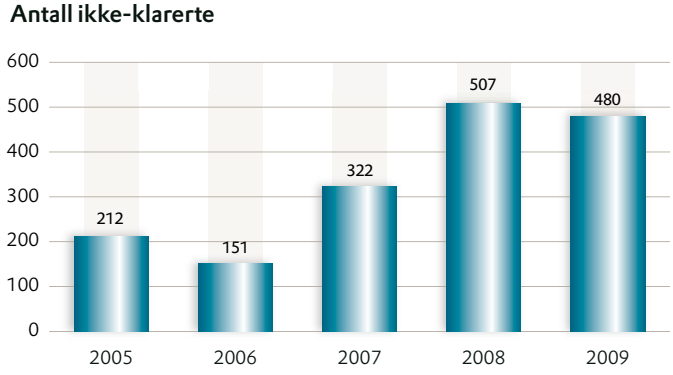
Sikkerhetsklareringer



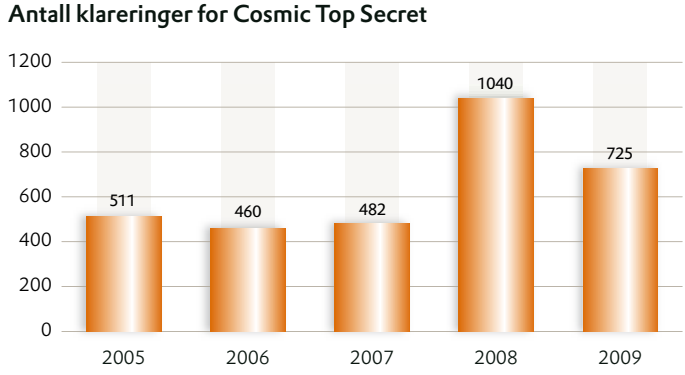
Antall personkontroller har gått ned fra over 35.000 til i overkant av 30.000 i 2009. NSM er sentral personkontrollinstans.



Grunnen til at det er behandlet flere klager enn mottatt i 2009 skyldes etterslep fra tidligere år.



Antall ikke-klarerte økte betydelig i 2008, blant annet som følge av at antall klareringer i Forsvaret økte. Antall ikke-klarerte i fjor holdt seg på et høyere nivå enn tidligere.



Antall personer klarert for det høyeste sikkerhetsnivået i NATO, Cosmic Top Secret, ble doblet i 2008, blant annet på grunn av en endring i NATOs regelverk. NSM er klareringsmyndighet for Cosmic Top Secret-klareringer i Norge.

Besøkte NSM

Torkjell Berulfsen besøkte i september NSM for opptak til serien "Berulfsens konspirasjoner". Seniorrådgiver Roar Thon uttalte seg om trusler på Internett.

– Man skal ikke ha fulgt med mye før man skjønner at det foregår en del ting man skulle vært foruten. Og det er det dere som skal forhindre. Jeg trodde jeg var trygg med Mac, men nå skjønner jeg at jeg ikke kan være sikker på den lenger heller, sier Berulfsen.

NSM i året som gikk:

Smått og stort

Mange store og små oppgaver blir utført i løpet av året i NSM. Her er et lite utvalg av hva som har skjedd av små og store ting i 2009.

6. jan. Full nettkrig i Gaza: Bare dager etter at israelske tropper starter militære operasjoner på Gaza-stripen, rammer en serie hackerangrep israelske nettsider. – Dette er et nytt verktøy i kassen, og vi må bare innse at nettet er en ny dimensjon i konflikter. Det henger sammen med samfunnsutviklingen, sier avdelingsdirektør Christophe Birkeland til VG Nett.

25. feb. Den estiske spionen Herman Simm blir dømt til tolv år og seks måneder i fengsel for å ha overlevert hemmelige opplysninger om Estland og NATO til fremmed makt. Simm er tidligere leder av Estlands nasjonale sikkerhetsmyndighet, og har tidligere besøkt NSM.

4. mar. NSM bruker ny tilsynsmetodikk under tilsyn ved Landsdelskommando Nord-Norge. – Vi oppfattet tilsynet som positivt og lærerikt i forhold til det sikkerhetsansvaret som personellet og organisasjonen har, sier daværende stabssjef ved LDKN, Tor Eystein Sæther til Forsvarets intranett.

9. mar. Kjetil Nilsen starter som ny direktør i Nasjonal sikkerhetsmyndighet. Ferden går umiddelbart til Brussel der han og ledergruppen blir orientert om NATOs arbeid og planer for cybersikkerhet. – Et skikkelig "crash course", sier sjef NSM.

13. mar. Conficker-ormen slår ut politiets datamaskiner. Ormen har tidligere rammet sykehus og fylkeskommuner. – Dette viser at vi har et komplekst IKT-trusselbilde, og at dataangrep kan ramme alle, sier avdelingsdirektør Christophe Birkeland til Aftenposten.

Diskuterte sertifisering i Tromsø

Nasjonal sikkerhetsmyndighet arrangerte sertifiseringskonferansen Common Criteria i Tromsø 22. – 24. september i 2009. 258 deltakere fra 28 nasjoner deltok. Mary Ann Davidson fra Oracle og Steven B. Lipner fra Microsoft var blant deltakerne.

Fikk kunstgave

NSM har et godt forhold til virksomheter i nærområdet. Fire barn fra barnehagen i Kolsås leir, Kolsåstrollet barnehage, overrakte i april en gave til NSM. Gaven var et maleri som var malt av barna selv. Assisterende direktør Geir Samuelsen tok i mot på vegne av Nasjonal sikkerhetsmyndighet.

3. apr. Regjeringen går inn for at Norge skal delta i utbyggingen av det felleseuropeiske satellittnavigasjonsprogrammet Galileo. NSM har ansvaret for sikkerheten i den norske delen av prosjektet. NSM skal sørge for sikkerhetsgodkjenning av installasjoner på norsk jord, blant annet på Svalsat bakkestasjon utenfor Longyearbyen på Svalbard.

8. sep. NorCERT-pulsen heves til nivå 3 på grunn av sårbarheter i TCP/IP-protokollen. TCP er protokollen som benyttes når man besøker nettsider eller leser e-post. Nivå 3 betyr at det er fare for vellykkede angrep rettet mot kritisk digital infrastruktur.

Uke 31 Fregatten Fridtjof Nansen drar til Adenbukta for å bistå EU-styrken i kampen mot sjørøvervirksomheten. Nasjonal sikkerhetsmyndighet er ansvarlig for å godkjenne informasjonssystemene ombord.

22.–24. sep. Nasjonal sikkerhetsmyndighet arrangerer sertifiseringskonferansen Common Criteria i Tromsø. 258 deltakere fra 28 nasjoner deltar. – For folk som jobber med smartkort-sikkerhet er dette årets store begivenhet, sier Albert Dorofeev fra Sony i Belgia.

17.–18. nov. NSMs årlige sikkerhets-konferanse blir arrangert i Oslo. 330 deltakere følger foredrag om IKT, forebyggende sikkerhetstiltak, trusselbildet i Norge med mer.

22. des. NSMs utkast til en nasjonal strategi for cybersikkerhet overleveres Forsvarsdepartementet.

Årsmelding for NSM 2009

Utgitt av Nasjonal sikkerhetsmyndighet, juni 2010.
Ansvarlig redaktør: Kjetil Nilsen.
Redaktør: Anders Bjønnes.
Redaksjonen: Kjetil Berg Veire (redaksjonssekretær), Stein Henriksen, Øivind Mandt og Liv Nodeland.
Grafisk design: Håvar Haug/Marit Sylstad (NSM). Layout/produksjon: NSM.
Foto: Pål Rødahl/tinagent, Colurbox (s.10, 11, 12, 14, 17, 19, 21, 22, 23), Asgeir Spange Brekke/FD (s.6) og NSM.
Opplag: 1200 – juni 2010.
Trykk: 07-Gruppen.

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