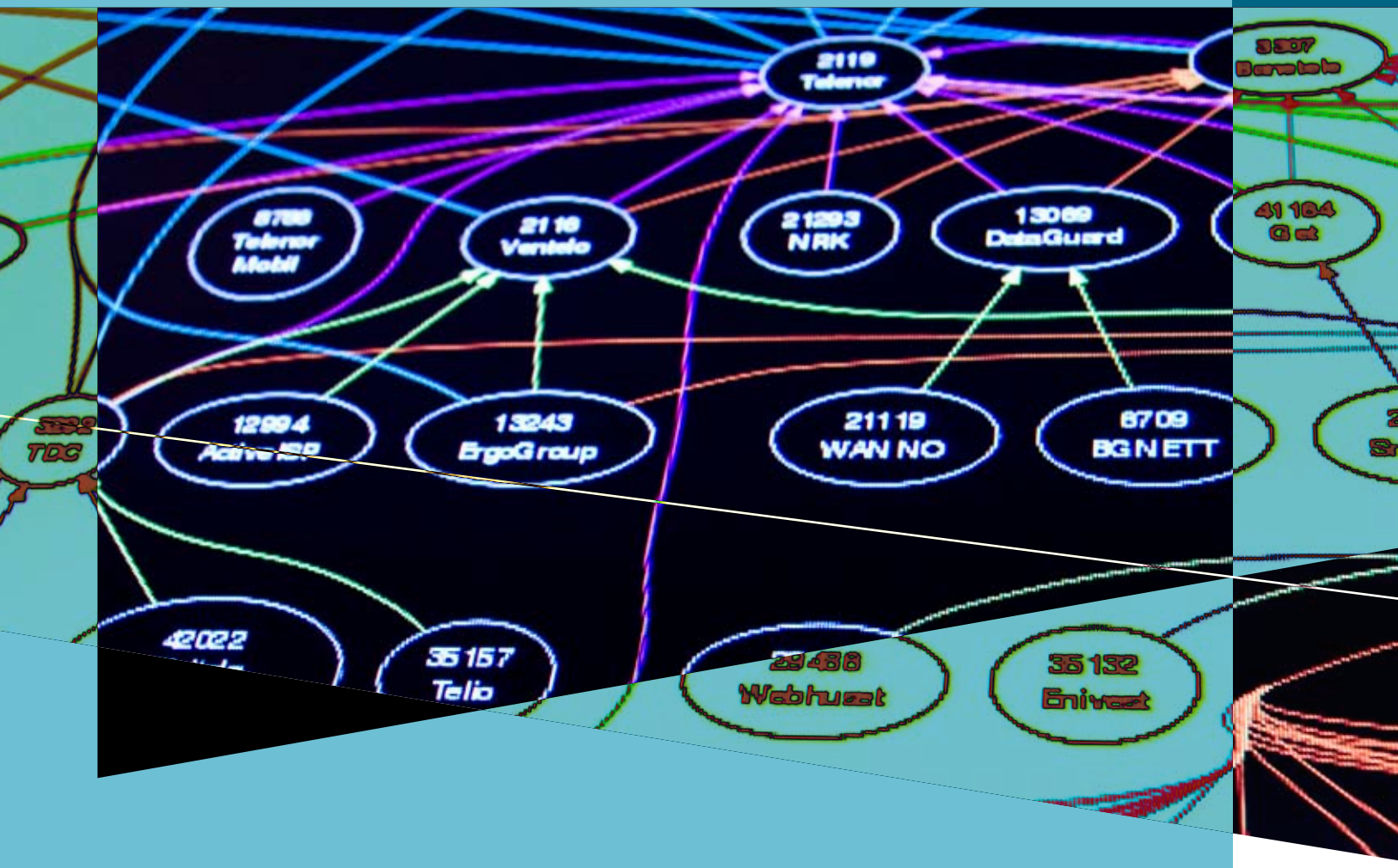
Årsmelding

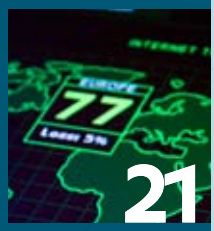
NSM



2008

Årsmelding for Nasjonal sikkerhetsmyndighet

Innhold



«Systematisk rapportering er en forutsetning for oversikt og valg av tiltak på alle nivåer.»
Direktør Kjetil Nilsen

Direktørens forord:

Sikkerhet er et lederansvar

Det er lederne i virksomhetene som er underlagt sikkerhetsloven, i alt opp mot 600, som har det primære ansvaret for at den forebyggende og defensive sikkerheten mot terror, sabotasje og spionasje er godt nok ivaretatt. I fjorårets Rapport om sikkerhetstilstanden fra Nasjonal sikkerhetsmyndighet slo vi fast at lederes opplæring og kompetanse innen forebyggende sikkerhetstjeneste var mangelfull. I år skriver vi at det er et økende gap mellom trusselbildet og sikkerhetstilstanden.

Lederforankring bør være en rød tråd i alt sikkerhetsarbeid. I rapporten for 2008 påpekes det mangelfull rapportering. Her har lederen en viktig rolle å spille med å legge forholdene til rette for god sikkerhetskultur. Systematisk rapportering er en forutsetning for oversikt og valg av tiltak på alle nivåer. Det er også et viktig supplement til NSMs tilsynsvirksomhet. Vi forventer at lederne tar denne oppgaven på alvor.

Effektivisering og forenkling er noe av det vi i Nasjonal sikkerhetsmyndighet har prøvd å legge til grunn for arbeidet som er gjort i 2008. Det er fordi vi ønsker å gjøre sikkerhetsarbeidet mer tilgjengelig for brukerne. NSM skal oppfattes som relevant, og våre råd og øvrige produkter skal være etterspurte.

I løpet av fjoråret så vi tydelige tegn til at våre brukere oppsøkte våre møteplasser og tjenester. NSMs årlige sikkerhetskonferanse satte deltakerrekord. Antall håndterte hendelser hos avdelingen NorCERT mer enn fordoblet seg fra 2007 til 2008. Antall medietreff tredoblet seg. Vi opplever fremdeles stor etterspørsel etter foredrag rundt nettsamfunn. Vi er internasjonalt etterspurt. Dette forplikter til å fortsette å levere det vi skal. Det er et arbeid vi tar på alvor.

Nasjonal sikkerhetsmyndighet er avhengig av å skjerme enkelte områder av virksomheten. Både personkontroll og sikkerhetsklareringer, kryptoteknologi og andre spesialiserte teknologiske områder inneholder skjermingsverdig informasjon. NSM gir i år for første gang ut en årsmelding beregnet for offentligheten. Gjennom denne sier vi mer om oss selv enn det vi tradisjonelt har valgt å gjøre. Dette er en årsmelding som vil ha en annen og bredere målgruppe enn den tradisjonelle årsrapporteringen til våre to overordnete departementer. Vi har forsøkt å popularisere viktige fagområder som NSM jobber med. Det er fordi vi finner disse områdene så viktige at flere bør vite om dem enn fagfolkene selv. I tillegg har vi, som et bakteppe, valgt å ta inn den årlige ugraderte rapporten om sikkerhetstilstanden i sektorer og virksomheter.

Med dette ønsker jeg god lesning.

Kjetil Nilsen

Dette er NSM

Nasjonal sikkerhetsmyndighet er et direktorat som rapporterer til Forsvarsdepartementet og Justisdepartementet. Det forebyggende defensive sikkerhetsarbeidet mot spionasje, sabotasje og terror er et linjeansvar og utøves først og fremst i hver enkelt sektor og virksomhet. NSM skal som fagmyndighet, tilsynsmyndighet og varslingsinstans legge forholdene best mulig til rette for dette arbeidet. Direktoratet skal ha oversikt over og rapportere om sikkerhetstilstanden, gi klargjørende og motiverende informasjon og veiledning, varsle om alvorlige hendelser som kan påvirke sikkerheten, og foreslå tiltak – herunder tekniske – som på kort og lang sikt kan forbedre og effektivisere sikkerhetsarbeidet. NSM er også nasjonalt kontaktpunkt i forhold til andre land og internasjonale organisasjoner.

NSM utøver i dag oppgaver i henhold til følgende lover, ordninger og beslutninger:

- Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)
- Lov om oppfinnelser av betydning for rikets forsvar og lov om forsvarshemmeligheter
- Sertifiseringsordningen for IT-sikkerhet i produkter og systemer (SERTIT)
- Beslutning om etablering av en nasjonal operativ varslings- og håndteringskapasitet for alvorlige angrep mot samfunnsviktig IKT-infrastruktur (NorCERT), herunder drift av Varslingssystem for digital infrastruktur (VDI)
- Beslutning om etablering av Koordineringsutvalget for forebyggende informasjonssikkerhet (KIS) der NSM har sekretariatet.
- Beslutning om av beredskapsmessige grunner å støtte norsk kryptoindustri
- Det nasjonale beredskapssystemet (NBS)

«Security is, after all, the art of making sure certain things don't happen: a thankless task, because when they don't happen, there will always be someone to say the security was excessive and unnecessary.»

Salman Rushdie i "Terror Versus Security", 2000.

HISTORIKK

1953 Det gis en felles sikkerhetsinstruks for de mest sentrale departementer og Forsvaret.

Det opprettes en stilling som sikkerhetsinspektør. Stillingen plasseres i Forsvarets etterretningsstab og inspektøren rapporterer til Regjeringen.

1955 Regjeringen gir en instruks for samarbeidet mellom politiet og Forsvaret til trygging av rikets sikkerhet.

NATO utformer et regelverk på sikkerhetssiden, som får stor betydning for de enkelte lands nasjonale bestemmelser.

1956 Iverksettelse av lov om oppfinnelser av betydning for rikets forsvar.

1960 NATO-landene inngår en gjensidig avtale om hemmelighold og gjensidig beskyttelse av oppfinnelser og patenter som er av betydning for landenes forsvar.

Strategien

NSM skal:

- Ha kunnskap og oversikt for å bedre sikkerhetstilstanden
- Utvikle balanserte forebyggende sikkerhetstiltak
- Gi god og tilgjengelig informasjon og rådgivning
- Styrke samfunnets evne til å oppdage og reagere på sårbarheter og sikkerhetstruende hendelser
- Forenkle og effektivisere sikkerhetsarbeidet
- Være en etterspurt samarbeidspartner innenfor sikkerhetsarbeidet nasjonalt og internasjonalt
- Være en attraktiv arbeidsplass med riktig kompetanse og en organisasjonskultur preget av stolthet, helhetstenkning og innovasjon
- Sikre det økonomiske grunnlaget for virksomheten

NSM skal være en tydelig pådriver, etterspurt bidragsyter og tilgjengelig samarbeidspartner for god sikkerhet i samfunnet. Vi skal være forutseende i forhold til endringer i risikobildet og ta ansvar for nye sikkerhetsoppgaver som følge av dette.

NSM i utvikling

Noen særlig viktige utviklingsaktiviteter i 2008 har vært:

- Videreutvikling av NSMs tilsynsmetodikk i tråd med allmenne prinsipper for statlig tilsyn
- Arbeid med å forenkle og effektivisere prosessen for sikkerhetsgodkjenning av informasjonssystemer
- Etablering av en sentral kapasitet for inntrengningstesting (pentest) knyttet til graderte systemer
- Gjennomføring av Norges første nasjonale cyberøvelse IKT 08 i desember 2008 i et samarbeid med DSB
- Arbeid med å utvikle et tverrfaglig IKT-trusselbilde, herunder etablering av en ekstern koordineringsgruppe med deltakelse fra PST og E-tjenesten og sektorvise trussel- og sårbarhetsråd
- Videreutvikling av tekniske kapasiteter i NorCERT (VDI-systemet og malwarelab)
- Bistand til regelverksutvikling knyttet til informasjonssikkerhet og objektsikkerhet iht. sikkerhetsloven
- Internasjonalt utviklingsarbeid på sikkerhetssiden bilateralt og i en rekke fora
- Utarbeidelse av forslag til hvordan kontrollen med luftfotografering og kartproduksjon i fremtiden bør håndteres. Gjennomgang av register over skjermingsverdige objekter i samarbeid med Forsvaret
- Gjennomføring av lederutviklingsprogram
- Utgivelse av temahefte for sikkerhet knyttet til nettsamfunn
- Utviklingen av en daglig mediebrief som er gjort tilgjengelig for eksterne

1965 De strategiske sikkerhetsoppgaver, som har vært tillagt Etterretningsstaben, skilles ut i en egen sikkerhetsstab (FST/S). Den første sjefen var oberst Carl C. C. Ruge (foto).

Regjeringen fastsetter ved kgl. res. en ordning for det alminnelige sikkerhetsarbeidet i hele statsforvaltningen. Det utøvende ansvaret delegeres til FST/S.

1970 FST/S innlemmes i det nye Forsvarets overkommando som FO/S og får tildelt ressurser fra stabene til våpengrenene. De nye generalinspektørene for forsvarsgrenene skal ikke lenger ha egne stabsledd for sikkerhet.

1972 Regjeringen oppretter et utvalg for å føre kontroll med FO/S og Politiets overvåkingstjeneste. Dette som en oppfølging av Mellbye-utvalgets innstilling.

1980 Et datasikkerhetsdirektiv som utfyller sikkerhetsinstruksen og beskyttelsesinstruksen utgis av FO/S.

SIKKERHETSTILSTANDEN

HISTORIKK

1984 Direktivet for personellsikkerhetstjenesten i den sivile forvaltning gir FO/S en tydeligere rolle overfor departementer og etater.

1987 FO/S flytter til forsvarsbygget på Huseby. Funksjoner for produksjon og distribusjon av kryptomateriell forblir på Akershus festning.

1994 Stortinget oppretter en granskingskommisjon (Lund-kommisjonen) for å "granske alle forhold i forbindelse med påstander om at politiets overvåkingstjeneste, Forsvarets sikkerhetstjeneste og Forsvarets etterretningstjeneste, eller personer knyttet til disse tjenester, har vært engasjert i ulovlig eller irregulær overvåking av norske borgere".

Samme år avgir "Skauge-kommisjonen" sin innstilling om behov for lovregulering av kontrollen med de "hemmelige tjenester". Skauge foreslår i tillegg at tjenestene selv lovreguleres.

1996 Et parlamentarisk utvalg for kontroll med etterretnings- overvåkings- og sikkerhetstjeneste (EOS-utvalget) etableres ved lov (1995). Det tidligere regjeringsoppnevnte kontrollutvalget nedlegges.

En urovekkende utvikling

NSM er bekymret for et økende gap mellom trusselbildet og sikkerhetstilstanden. Aktiviteten til utenlandske staters etterretningstjenester mot Norge og norske interesser er høy, i følge PSTs åpne trusselvurdering for 2008. Dette gjentas i 2009. Det forebyggende defensive sikkerhetsarbeidet holder ikke følge med dette.

Tilstanden i virksomhetene 2008

NSM sammenfatter årlig erfaringer fra tilsyn med virksomheter underlagt sikkerhetsloven. I tillegg analyseres innrapporterte hendelser og annen innhentet informasjon. Det hele samles i en rapport om sikkerhetstilstanden. Denne formidles primært til Forsvarsdepartementet og Justisdepartementet, til nasjonale samarbeidspartnere, og virksomheter underlagt sikkerhetsloven. Det følgende er et ugradert sammendrag av rapporten for 2008.

En god sikkerhetstilstand handler om å sikre rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhets-interesser, slik det er omtalt i sikkerhetslovens § 1. Våre sikkerhetsinteresser skal i henhold til loven sikres mot spionasje, sabotasje og terror.

Sikkerhetstilstanden må ses i forhold til helt grunnleggende samfunnsverdier. Vi må blant annet ha tilstrekkelig sikkerhet rundt områdene konstitusjonell selvråderett, handlefrihet i utenriks- og sikkerhetspolitikken, og territoriell integritet. Den nasjonale handlefriheten på slike områder skal i best mulig grad sikres i forhold til potensielle trusselaktører. Vårt nettverksbaserte samfunn medfører at det også vil kunne være viktig å sikre skjermingsverdige objekter og informasjon innen energiforsyning, samferdsel, telekommunikasjon, helsetjenesten og bank- og finansnæringen.

Unnlatelse av å gradere

NSM har grunn til å tro at informasjon som burde vært gradert ikke blir det, bevisst eller ubevisst, og at dette skjer ofte. Man må derfor anta at informasjon som burde vært beskyttet av hensyn til rikets sikkerhet og vitale nasjonale sikkerhetsinteresser kompromitteres.

For lite kompetanse om sikkerhet

I mange virksomheter er kunnskapen innen forebyggende sikkerhet for dårlig, både på et generelt nivå og på spesialiserte områder. Dette gjelder både for ledere, saksbehandlere, sikkerhetsansvarlige og IKT-sikkerhetsansvarlige.

Det kreves høy kompetanse for å være i stand til å etterkomme sikkerhetskrav når teknologien er i stadig endring. Det finnes få utdanningstilbud spesielt rettet mot virksomhetsledere. NSM har satt i gang et arbeid med å vurdere sikkerhetsutdanningen. Dette kan på sikt bidra til å heve kvaliteten og statusen på sikkerhetsarbeidet.

«NSM har grunn til å tro at informasjon som burde vært gradert ikke blir det, bevisst eller ubevisst, og at dette skjer ofte».

1997 FO/S samlokaliseres i Kolsås leir i Bærum.

FD fastsetter ny instruks for fotografering mv. fra luften og kontroll av luftfotografier og opptaksmateriale fra luftbårne sensorsystemer. Denne typen kontroll ble første gang iverksatt i 1946.

1998 Sikkerhetsloven vedtas av Stortinget, men iverksettelsen avventer utfyllende forskrifter.

1999 FO/S får ansvaret for å utøve oppgaven som offentlig sertifiseringsmyndighet for IT-sikkerhet i produkter og systemer (SERTIT).

2000 Varslingssystemet for digital infrastruktur (VDI) opprettes som et prøveprosjekt i regi av EOS-tjenestene.

Ny forskrift om behandling av saker etter lov om oppfinnelser av betydning for rikets forsvar iverksettes som følge av lovendring i 1999.

NSMs tilsyn iht. sikkerhetsloven

Nasjonal sikkerhetsmyndighet skal føre tilsyn med sikkerhetstilstanden i virksomheter, herunder kontrollere at den enkeltes plikter i eller i medhold av loven overholdes, og eventuelt gi pålegg om forbedringer.

Tilsynsmetodikken i NSM er under revisjon. Tilsynene legges om, slik at de blir i samsvar med den internasjonale standarden NS-EN ISO 19011. Dette innebærer større vekt på styringssystemer for sikkerhet.

Også innrapporterte og analyserte sikkerhetstruende hendelser vil bli strukturert på en måte som tillater generelle og overordnede konklusjoner.

Se nærmere omtale av tilsyn på side 25.

Mangler i kommunikasjonssikkerheten
Mangler i kommunikasjonssikkerheten skyldes ofte rutinesvikt, for eksempel utilstrekkelig kontroll av den lokale kryptosikkerhetstjenesten, eller manglende oppdatering av kryptoregnskap og lokale tilpasninger til egen virksomhet. Krav til installasjon av utstyr som behandler sikkerhetsgradert informasjon tas imidlertid i stor grad til følge.

«NSMs tilsyn viser at det er grunnleggende mangler i virksomhetenes forebyggende sikkerhetsarbeid».

Manglende samsvar mellom sikkerhetsdokumentasjon og virkeligheten
NSM avdekker stadig at systemsikkerhetstiltakene som er påkrevd for å følge sikkerhetsloven ikke er på plass. Dette skjer til tross for at virksomhetene selv beskriver slike tiltak i sin sikkerhetsdokumentasjon. NSM jobber nå med å legge om godkjenningsprosessen med hensyn til graderte IKT-systemer, slik at hvilke krav som gjelder blir tydeliggjort. Virksomhetsledere og systemeiere vil bli ansvarliggjort i større grad enn i dag.

Et krevende regelverk
Funn fra våre tilsyn viser at sikkerhetsregelverket ikke etterleves godt nok. Sikkerhetsloven med forskrifter inneholder over tusen individuelle pålegg og krav. Forskrift om informasjonssikkerhet er den mest omfattende regelsamlingen. Den består av 12 kapitler med i alt 92 paragrafer. Flere virksomheter har vansker med å forholde seg til denne regelmengden. Det kan stilles spørsmål ved om regelverket er unødig komplisert, og for lite dynamisk i forhold til den teknologiske utviklingen.

Svak ledelse av sikkerhetsarbeidet
NSMs tilsyn viser at det er grunnleggende mangler i virksomhetenes forebyggende sikkerhetssarbeid. Dette gjelder både kunnskaper, prioritering, forankring og styring.

2001 Sikkerhetsloven med tilhørende forskrifter iverksettes.
FO/S får oppgaven som nasjonal sikkerhetsmyndighet iht. sikkerhetsloven.

2002 En tverrsektoriell arbeidsgruppe fremmer forslag til en utvidet regulering av objektsikkerhet iht. sikkerhetsloven.

2003 FO/S nedlegges. De tverrsektorielle strategiske oppgavene overføres til de nyopprettede direktoratet Nasjonal sikkerhetsmyndighet (NSM) og oppgaven som rådgiver for Forsvarssjefen knyttet til hans ansvar for sikkerheten i Forsvaret tillegges en nyopprettet Forsvarets sikkerhetsavdeling (FSA). Direktoratet underlegges FD administrativt, men rapporterer med faglig ansvarslinje i saker i de sivile sektorer til JD.
VDI sentralen legges permanent til NSM, men plasseres i midlertidige lokaler på Akershus festning.

For lite rapportering

Sikkerhetstruende hendelser skal iht. regelverket rapporteres til NSM. Svært få sikkerhetstruende hendelser eller vurderinger av slike er meldt inn i 2008. Det er grunn til å tro at det er en betydelig underrapportering. NSM understreker at det er av stor betydning for sikkerhetsarbeidet at sikkerhetstruende hendelser innrapporteres til intern sikkerhetsorganisasjon og til NSM. Etter NSMs mening bør virksomhetenes sikkerhetsorganisasjon sørge for at NSM mottar informasjon om alle innrapporterte grove sikkerhetstruende hendelser enkeltvis og gjerne også sammenfattet. Mangelfull rapportering av hendelser gir svekket grunnlag for å analysere og rapportere om sikkerhetstilstanden.

Typiske funn

Typiske funn fra tilsyn er:

- Virksomheten har liten oversikt eller mangler system for oversikt over sikkerhetstruende hendelser. Sikkerhetstilstanden er da ukjent for virksomheten.
- Nøkkelpersoner i virksomheten er ikke sikkerhetsklarert eller autorisert.
- Mangelfull adgangskontroll og fysisk sikring.
- Safer og sikkerhetsskap med feil og mangler.
- Safekombinasjoner oppbevares ikke i samsvar med regelverket.
- Manglende kontroll med graderte dokumenter og lagringsmedier.
- Anti-virusprogrammer oppdateres ikke.
- Passord finnes på «gule lapper» som er lett synlige.
- Rutiner innen kryptoforvaltning følges ikke.
- Gradert informasjon kommuniseres over åpne medier.
- Mangelfull dokumentasjon av sikkerhetsarbeidet i den enkelte virksomhet.
- Generelt manglende kompetanse, bevissthet og hos enkelte manglende interesse for forebyggende sikkerhetsarbeid.
- Sikkerhetsarbeidet gis for liten prioritet og ressurser, og er ikke godt nok forankret i ledelsen.

Private virksomheter som er underlagt sikkerhetsloven, synes å ha en tilfredsstillende sikkerhetstilstand. Det antas at dette er økonomisk motivert. En viktig utfordring er likevel å sikre kontinuitet i lovlig behandling av gradert informasjon ved at nøkkelpersoner alltid er klarert og autorisert, også ved organisatoriske endringer.

Etterretningstrykket mot Forsvaret er betydelig. I tillegg finnes det eksempler på kriminelle handlinger som blir utført av militært personell, og at sikkerhetsloven blir brutt. Dette tyder på mangler i grunnsikringen og administrasjonen av sikkerhet på det enkelte tjenestested. NSM har tillit til at Forsvarssjefen gjennom Forsvarets sikkerhetstjeneste (FOST) (tidligere Forsvarets sikkerhetsavdeling, FSA) tar tak i denne utfordringen.

NSM har tidligere hatt merknader til sikkerhetsarbeidet i utenrikstjenesten. NSM konstaterer at sikkerhetsarbeidet i departementet allerede er forbedret i vesentlig grad. NSM ser frem til en ytterligere forbedret sikkerhetstilstand i departementet og på utenriksstasjonene.

2004 NSM oppretter prøveprosjektet Norwegian Computer Emergency Response Team (NorCERT) som skal være et kontaktpunkt nasjonalt og internasjonalt ved alvorlige hendelser knyttet til samfunnsviktig IKT-infrastruktur. NorCERT får egne verifiserbare data gjennom VDI.

FAD oppretter Koordineringsutvalget for forebyggende informasjonssikkerhet (KIS). NSM får i oppdrag å bemanne sekretariatet for utvalget.

2006 Funksjonen NorCERT besluttes opprettet av regjeringen og legges til NSM. Dette som en helhetlig satsning hvor også NorSIS på Gjøvik inngår.

2007 Det opprettes et fagråd for sertifiseringsordningen SERTIT. Dette erstatter den tidligere styringskomiteen. Fagrådet skal gi råd til NSM om videreutvikling av SERTIT og sertifiseringsordningen.

Målrettede trojanere

Trenden med dataspionasje gjennom målrettede trojanere fortsetter. Målrettede trojanere er svært velegnet for etterretningsformål. Det antas at det i overskuelig fremtid ikke vil være mulig å utvikle effektive teknologiske mottiltak. En trojaner gjør det mulig for angripere å ta full kontroll over datamaskinen og hente ut opplysninger. Målgrupper for slike angrep er typisk:

- Ledere på ulike nivåer
- Forsvarssektoren
- Høyteknologiske selskap innen elektronikk-, forsvars-, fly-, farmasøytisk og petrokjemisk industri
- Menneskerettighetsorganisasjoner som besitter personsensitiv informasjon

NSM advarte mot målrettede trojanere mot toppledere i norske virksomheter i et sikkerhetsvarsel i april 2008.

IKT-trusselbildet

NSM har i oppdrag, i nær koordinering med PST og E-tjenesten, å formidle et bilde av trusler mot IKT-systemer. Trusselbildet gis i form av situasjonsavhengige varsler og situasjonsrapporter, men også som trusselvurderinger. Det følgende er en ugradert fremstilling av viktige elementer i IKT-trusselbildet.

Med IKT-trusler menes alle uønskede handlinger, herunder reelle og potensielle, som kan rettes mot nettverk og elektroniske informasjonssystemer.

Med IKT-trusselbildet menes informasjon om:

- Trusselaktører og deres intensjoner og kapasiteter
- Metoder som trusselaktører benytter eller kan tenke seg å benytte, herunder informasjon om sårbarheter, dvs. svakheter og mangler i teknologi, organisasjon og hos mennesker
- Hvilke mål som kan være attraktive for trusselaktører å angripe eller utnytte
- Erfarte hendelser

Trusselaktører har brukt Internett som effektivt medium for blant annet propaganda, kommunikasjon, etterretning og planlegging av anslag over lengre tid. Samtidig gjennomføres ulike former for dataangrep stadig oftere. Håndtering av slike angrep er utfordrende, da tidsvinduet for mottiltak er ekstremt lite. Det er også en stor utfordring å knytte angrep til en bestemt aktør, som kan operere fra hvor som helst i verden.

Et nettverksbasert samfunn

Det moderne nettverksbaserte samfunnet løser oppgaver på en ny og bedre måte som utnytter ressurser mer effektivt. Samtidig har dette resultert i et nytt risikobilde, med en stor og økende avhengighet mellom ulike tjenester og infrastrukturer. I tillegg stilles det stadig større krav til mobilitet og tilgjengelighet. Når dette kombineres med økende grad av outsourcing og offshoring (prosessering i utlandet), bidrar dette til at komplekse datasystemer som er sårbare av natur blir stadig mer utfordrende å sikre.

«Det er også en stor utfordring å knytte angrep til en bestemt aktør, som kan operere fra hvor som helst i verden.»

Politisk motiverte angrep

Dataangrep er nå et virkemiddel i politiske og militære konflikter. Både i Gaza-konflikten og krigen i Georgia så man dataangrep parallellt med væpnede konflikter. Denne typen IKT-angrep

er kommet for å bli, og er noe man må regne med i kommende konfliktsituasjoner. IKT-trusselbildet påvirkes direkte av økt avhengighet og sårbarhet til nettverk og elektroniske informasjonssystemer.

Økonomisk kriminalitet
Kriminelle har bygget opp kompetanse og nettverk til å utføre avanserte operasjoner for å tjene penger på Internett. Kriminelle grupperinger tilbyr forskjellige tjenester, produksjon av ondsinnet programvare, salg av personopplysinger, utpressing, tyveri av kredittkortinformasjon, "ran" av nettbanker, hvitvasking av penger, produksjon og salg av falske identifikasjonspapirer, industrispionasje, infrastruktur for reklame (spam) osv.

Spionasje (nettverksoperasjoner)
Bruk av målrettede trojanere i operasjoner mot mål i Norge er sterkt økende. En målrettet trojaner er en trojaner som i større eller mindre grad er skreddersydd for en målrettet operasjon. Målet kan for eksempel være en enkeltperson, en organisasjon eller en spesiell gruppe mennesker. De er derfor vanskelig å detektere, både for brukere, antivirus og brannmurprodukter. Typiske angrepsmål for en målrettet trojaner er ledere og nøkkelpersoner i både offentlige og private virksomheter.

Aktuelle utfordringer
Særlig aktuelle utfordringer er:

- Utnyttelse av sårbarheter i programvare før de blir alminnelig kjent
- Kompromittering av mobiltelefoner og mobile enheter slik at de kan bli brukt som avlyttingsverktøy
- Manipulasjon av brukerne slik at de røper detaljer om seg selv eller arbeidsgiver
- Distribuerte tjenestenektangrep, hærverk, eller oppfordring til voldshandlinger
- Profesjonelt utviklet ondsinnet programvare, som ikke blir oppdaget av antivirusprogrammer
- Målrettede operasjoner, det vil si ondsinnet programvare som for eksempel smugles inn som e-postvedlegg, og som deretter installerer bakdører inn i datasystemene

Anbefalinger

- Virksomheter og bedrifter bør arbeide målrettet med å øke organisasjonens og sine ansattes sikkerhetsbevissthet, sikkerhetskompetanse og sikkerhetsmessige atferd
- Virksomheter bør stille krav til internettleverandører som sikrer definerte krav til sikkerhet i infrastrukturen som skal leies
- Flere sikkerhetsmekanismer bør implementeres for å sikre redundans
- IKT-utstyr må konfigureres til å passe virksomhetens eget behov, nettverk og systemer. Rutiner for oppdateringer og vedlikehold må være på plass
- IT-avdelinger må evne både å detektere og reagere på sikkerhetsbrudd
- Sensitiv informasjon som sendes over usikre datanettverk bør krypteres. Dette kreves for gradert informasjon
- Umiddelbar implementering av Domain Name System Security Extensions anbefales

Høy etterretningsaktivitet mot Norge

Aktiviteten til utenlandske staters etterretningstjenester mot Norge og norske interesser er høy. Etterretningsvirksomheten er i hovedsak rettet mot politiske beslutningstakere, embetsverk, sentraladministrasjon og ulike private aktører. Informasjonen søkes særlig innenfor olje og gass, forskning og utvikling, teknologi samt forhold knyttet til NATO (Kilde: PSTs åpne trusselvurdering for 2009).

KOMMUNIKASJONSSIKKERHET

– Et ekstremt detaljarbeid

– Det blir stadig viktigere å møte brukeren der han eller hun er, om det er på gata eller i ørkenen i et annet land. Det stiller krav til forskning og utvikling av nye sikkerhetsløsninger, sier avdelingssjef i NSM, oberst Hans Robert Bjørnaas. Nasjonal sikkerhetsmyndighet stiller krav til sikkerhetsmekanismene i utstyret som utvikles, og fagfolkene hos NSM må kjenne alle bestanddelene i og gå god for sikkerhetsløsningen på detaljnivå for at det skal kunne brukes. – Det er snakk om et ekstremt detaljarbeid, som vi heldigvis har folk som er svært gode på, sier Bjørnaas.

Landets viktigste nøkler

En hullete papirremse sikrer sambandet for de norske soldatene i Afghanistan. Nå jobber forskere ved NSM med å utvikle ny teknologi for sikker kommunikasjon.

– De papirbaserte kryptonøklene har vært i bruk siden 50-tallet. Det sier Ole Olsen, som er forsker hos NSM. Hans oppgave er blant annet å bidra til å utvikle en løsning som gjør det mulig å gå bort fra hullete papirremser, og tre inn i den digitale verden.

«Så lenge folk kan løfte av røret, få summetonen og snakke gradert har vi gjort jobben vår.»

Strenge rutiner

Kryptonøkler er det som gjør det mulig å kommunisere sikkert. Nettbanken er ett eksempel hvor kryptografi sikrer forbindelsen. En kryptonøkkel er en liten hemmelighet som brukt i avanserte algoritmer kan omdanne informasjon til uleselig data. Nøkkelen består av tilfeldige rekker med tall som skal gjøre det umulig å gjette seg til nøkkelen. Til det kreves strenge rutiner rundt produksjonen og distribusjonen av kryptonøkler.

Beskytter Forsvarets samband

Bak stengte og godt bevoktede dører blir det produsert og sendt ut tusenvis av nøkler i året. Kryptonøklene blir kodet inn i lange remser med papir, med huller i ulike mønstre. Disse blir så sendt ut med kurer til de som skal ha dem, og omgjøres til digitale signaler ved at de blir trukket gjennom en optisk leser, før de mates inn i telefoner, datamaskiner og annet utstyr. I sin ytterste konsekvens kan hullete papirremser skille mellom liv og død for de norske soldatene i Afghanistan. Hvis papirstrimlene ikke kommer frem tidsnok, mister soldatene muligheten til sikker kommunikasjon. Uten kodene fra NSM mister Forsvaret, Utenrikstjenesten og flere andre rett og slett det sikre sambandet.

– Så lenge folk kan løfte av røret, få summetonen og snakke gradert har vi gjort jobben vår, sier de inne på NDA (National Distributing Authority).

Utvikler ny kryptoboks

I dag er det krypto i svært mye teknologi, fra sikker kommunikasjon på internett til våpensystemer, GPS, bildeoverføringer, radarinformasjon. Bare det å «gå inn i» motorstyringen på en Joint Strike Fighter krever en kryptonøkkel. Behovet for krypto blir stadig større ettersom Forsvaret tar i bruk ny teknologi.

Men etter flere tiårs trofast tjeneste må papirstrimlene vekk for å styrke sikkerheten. Det krever utvikling av ny teknologi.

– Målet er at kryptonøklene skal sendes over nettverk. Man vil først sende nøkkelen over et nettverk nærmere brukeren. Dette er på plass i dag. Men for å få nøkkelen til kryptoenheten må vi utvikle det vi kaller en nøkkellaster, en enhet som kan mellomlagre nøklene fra distribusjonssystemene til sluttbrukerne. Vi må utvikle noe som er intuitivt og dermed lett å bruke i såvel feltsituasjoner som på kontoret, sier Ole Olsen.

Sikrere system

NSM jobber akkurat nå sammen med Forsvaret for å ta frem en slik løsning som blir viktig for å nå mål innen det nettverksbaserte forsvaret.

– Det er viktig at Nasjonal sikkerhetsmyndighet er med på dette, fordi dette er en enhet som skal passe på kryptonøklene våre. Kryptonøklene er "Den hellige gral" i sikker kommunikasjon. Hvis nøkkelen blir kompromittert, er hele systemet og alt som skal beskyttes å anse som kompromittert, sier Ole Olsen.

Enheten skal kunne brukes og fungere både i fjellhaller og ute i skogen, tåle vær og vind og være lett og enkel å bruke, samtidig som den er robust, sier forskeren.

– Typiske ting vi må passe på er at det ikke blir liggende sensitiv informasjon i boksen, at boksen ikke stråler for mye, og at du skal kunne miste boksen uten å behøve å frykte at nøkler blir kompromittert. Målet er å få til noe som er mer sikkert enn dagens papirdistribusjon, mer effektivt, og samtidig kostnads- og tidsbesparende, sier Olsen.

Utrullingen av det nye systemet skal etter planen starte om et par år.

Forsker Ole Olsen i Nasjonal sikkerhetsmyndiget jobber med å utvikle en ny løsning som kan erstatte dagens papirstrimler.

Norskutviklet krypto i NATO

Flere tusen enheter av IP-kryptoapparatet TCE 621 er solgt til NATO og NATO-land. Apparatet er utviklet av Thales Norge i samarbeid med Forsvaret og Nasjonal sikkerhetsmyndighet. TCE 621 brukes til å kryptere forbindelsen på datanettverk. Norge konkurrerte om anbudet fra NATO blant annet med USA. TCE 621 blir blant annet brukt i ISAF-sammenheng i Afghanistan. Det jobbes nå med utvikling av en mindre feltvariant. Nasjonal sikkerhetsmyndighet har også her ansvaret for at utstyret blir sikkert nok.

Avhengig av tillit

– Papirstrimler med hull som legges i bokser fremstår jo som utrolig gammeldags i 2009, hvorfor har man ikke modernisert dette før?

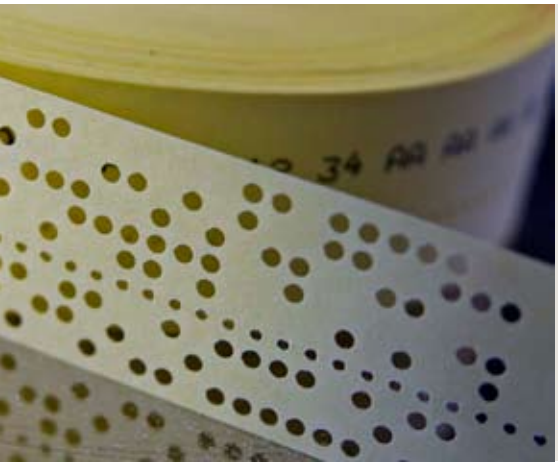
– Kryptoteknologi dreier seg om dyre og kompliserte systemer som er forventet å ha lang levetid. Teknologien kan ikke byttes ut uten videre. Utviklingen er så dyr at løsningene må leve i opp mot 30 år for å forsvare finansieringen.

I tillegg vil utviklingstiden være lang, og man har kanskje ikke vært sikker på at teknologien har vært moden nok for dette før nå, sier forsker Olsen til slutt.

Om fremtiden

- Bruk av krypto vil øke kraftig.
- Økende mobilitet gjør at det blir stadig større behov for å sikre kommunikasjon og data, fra mobile kontorløsninger i det sivile samfunn til behov for krypterte løsninger hos den enkelte soldat i felt.
- Løsninger for beskyttelse av data må være enkle, raske og robuste.

«Kryptonøklene er "Den hellige gral" i sikker kommunikasjon».



Distribusjon av kryptonøkler

NDA (National Distributing Authority) er den sentrale enhet for nøkkelproduksjon og – distribusjon i Norge. NDA produserer, distribuerer og fører sentral kontroll med krypto forvaltet under sikkerhetsloven. NSM ved NDA leverer disse tjenestene til alle virksomheter underlagt sikkerhetsloven, så som Utenrikstjenesten, Politiets sikkerhetstjeneste og Forsvaret.

Noen tall fra 2008:

- 22.000 kryptonøkler produsert på ulike media.
- 12 ukelange kureroppdrag til støtte for Forsvaret og norsk kryptoindustri
- 550 e-posthenvendelser til kryptosupport
- 3000 telefonhenvendelser

Norsk krypto sikret hotline mellom Det hvite hus og Kreml

Kryptografi har alltid vært et av hovedarbeidsfeltene til NSM (og tidligere FO/S). Et utslag av satsningen på kryptografi har vært at norsk industri i flere tiår har vært en ledende leverandør av kryptografisk utstyr til NATO. Under den kalde krigen sikret et norsk kryptoapparat en egen hotline mellom Washington og Kreml.

En forklaring på denne suksessen har vært et tett og målrettet samarbeid mellom industrien, sikkerhetsmyndighetene og Forsvaret.

Gjennombruddet for industrien kom på 50-tallet. Bedriften Standard Telefon og Kabelfabrikk (STK) startet i 1955 utviklingen av en kryptomaskin, som kom til å revolusjonere koding av sikkerhetsgradert informasjon. Maskinen ble kalt Electronic Teleprint Cryptografic Regenerative Repeater Machine (ETCRRM), og var andre systemer overlegen når det gjaldt både kapasitet og sikkerhet.

Norsk idémaker

Sjefen for Hærens Samband, oberst, sivilingeniør og krigsveteran Bjørn Rørholdt var idémakeren bak ETCRRM. Et samarbeid mellom Rørholdt og Kåre Meisingset ved STK resulterte i at det i 1952 ble tatt ut patent på den nye kryptografimaskinen.

NATO-landene ble raskt begeistret for den norsk nyvinningen. I løpet av få år oppnådde ETCRRM å bli standard kryptografimaskin i NATO.

ETCRRM kom også til å spille en rolle i rivaliseringen mellom øst og vest under den kalde krigen. I kjølvannet av Cuba-krisen ble ETCRRM brukt for å etablere en sikker telekslinje mellom Kreml og Det hvite hus.

Foto: Kryptomaskinen ETCRRM

Noen kryptosuksesser

- 50-tallet: Kryptomaskinen *ETCRRM* blir produsert av STK og solgt blant annet til USA og NATO.
- 70-tallet: Kryptoapparatet *Omnicoder* blir utviklet og produsert. Apparatet er basert på kryptografiske prinsipper utviklet av Cato Sedberg, ingeniør i Sjøforsvaret, og blir produsert av Lemkuhl. Omnicoder markerer starten på den elektroniske tidsalderen for norsk kryptoutstyr. Apparatet *RACE (Rapid Offline Crypto Equipment)* utvikles og produseres av STK. Apparatet blir brukt blant annet av NATOs handelsflåte til kryptering av meldinger.
- 80-tallet: *PACE (Pocket Automatic Crypto Equipment)* offline-kryptering av meldinger blir tatt i bruk, og blir det mest utbredte kryptoapparatet. PACE produseres av Lemkuhl i opp mot 20.000 eksemplarer, og er fremdeles i bruk.
- 90-tallet: *TCE 621*, også kjent som Cryptel IP, blir utviklet og produsert av Thales Communications.
- 2000-tallet: TCE 621 velges som standard NATO IP Crypto Equipment (NICE) i 2001, og er i dag NATO-standard for IP-krypto.

SIKKERHETSKULTUR

Noen råd om nettsamfunn

- Gi aldri bort tilgang til egne epostadresser, brukernavn og passord.
- Begrens den personlige informasjonen du legger ut om deg selv.
- Kontrollér vilkårene til nettsamfunnet du er med i, og bruk sikkerhetsinnstillingene de tilbyr.
- Vær skeptisk til fremmede du møter på nettet. En «venn» er ikke nødvendigvis din venn.
- Legg ikke ut informasjon om andre uten tillatelse.
- Legg ikke ut informasjon om din arbeidsgiver som ikke er allment tilgjengelig uten samtykke.
- Husk at internett er søkbart for alle, og at det som er lagt ut vil finnes der ute også i fremtiden!

Nettsamfunn fikk alarmen til å gå

Sikkerhetsgradert informasjon på internett fikk alarmen til å gå i Nasjonal sikkerhetsmyndighet våren 2007. To år senere er flere sårbare personellgrupper borte fra nettsamfunnet Facebook.

Det er vinter i 2007. Nettsamfunnet Facebook er i voldsom vekst i Norge. I Nasjonal sikkerhetsmyndighet oppdages det at egne ansatte bruker nettsamfunn som Facebook på en måte som kan være en sikkerhetsrisiko. Gjennom informasjonen de legger ut blir det avslørt at de har tilgang til store mengder informasjon av betydning for rikets sikkerhet.

Nærmere undersøkelser viser flere alvorlige tilfeller i andre deler av statsforvaltningen.

– Vi grep inn da vi så sikkerhetsgradert informasjon ble publisert via nettsamfunn. Informasjonen ble fjernet umiddelbart. Vi så et stort behov for å bedre sikkerhetskulturen, sier seniorrådgiver Roar Thon.

Sikkerhetsbrudd på nett

Han har hatt hendene fulle med foredragsvirksomhet etter at han sommeren 2007 skrev en kronikk til Aftenposten om sikkerhetsrisikoen ved nettsamfunn med tittelen «Facebook truer rikets sikkerhet». I Ronald Byes og Finn Sjues bok «Overvåket» ble den beskrevet nærmest som et gjennombrudd i offentligheten for NSM.

– NSM bestemte seg for å gå bredt ut og advare og bevisstgjøre om sikkerhetsrisikoen ved nettsamfunn. Vi valgte hele tiden å ha fokuset på mennesker som var sikkerhetsklarerte og som jobbet med informasjon av betydning for rikets sikkerhet.

Kampanje med effekt

– Har informasjonsvirksomheten hatt noen effekt?

– Mange av de store gruppene eller nettverkene som vi reagerte på er borte i dag. Flere organisasjoner har jobbet aktivt med dette, sier Roar Thon.

I Nasjonal sikkerhetsmyndighet ble det utformet interne retningslinjer. Våren 2008 lanserte direktoratet et temahefte om nettsamfunn og sikkerhet. En egen informasjonsbrosjyre ble vedlagt Forsvarets forum i 17.000 eksemplarer.

– Hvorfor er nettsamfunn farlige?

– Fordi man gjennom disse utleverer personlig og til dels intim informasjon som ikke lar seg fremskaffe gjennom andre kilder. Gjennom det kan aktører finne svakheter hos mennesker, eller i organisasjoner eller i tekniske systemer, sier Roar Thon.

Må tenke worst case

– Er det ikke lett å bli litt paranoid rundt dette med nettsamfunn?

– Jo, men det er det man får betalt for i denne jobben, sier Thon og ler, før han igjen blir alvorlig.

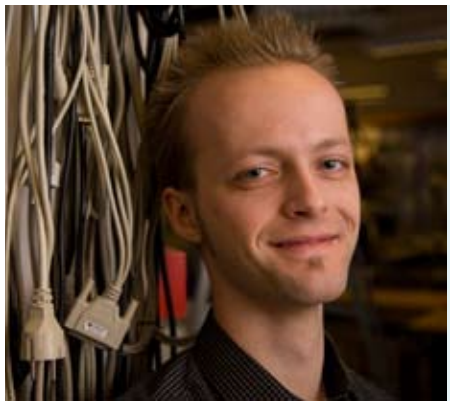
– Det er en oppgave for oss å tenke worst case. Vi har ikke noe imot verken Facebook eller andre nettsamfunn. Mange er gode sosiale verktøy for å holde kontakten med andre. Men jeg jobber med sikkerhetskultur, som er menneskelig adferd i et sikkerhetsmessig aspekt. Gjennom sine handlinger kan mennesker ødelegge for mange gode sikkerhetsmessige løsninger. I denne sammenhengen var det de store massene som tok i bruk et populært verktøy på nett uten å tenke på konsekvensene, avslutter Roar Thon.

Om fremtiden

- Menneskelige sårbarheter utfordres i et samfunn som blir mer og mer avhengig av teknologi.
- Ønske om fleksibilitet og mobilitet i form av minnepinner og bærbare data skaper store sikkerhetsmessige utfordringer.
- Økende antall ansatte med internasjonal ikke-kontrollerbar bakgrunn utfordrer arbeidet med personellsikkerhet.

«Vi grep inn da vi så sikkerhetsgradert informasjon ble publisert via nettsamfunn.»

SYSTEMSIKKERHET



Flere IKT-produkter bør sertifiseres

Sertifiseringsmyndigheten for IT-sikkerhet (SERTIT) utsteder internasjonalt anerkjente sertifikater for IT-produkter. Noen av målene med ordningen er blant annet å styrke IT-sikkerheten i offentlig og privat sektor, å skape tillit til e-handelsløsninger og annen kommunikasjon nasjonalt og internasjonalt, og å bidra til å gjøre norsk IT-industri mer konkurransedyktig i utlandet. Ved årsskiftet var fem prosjekter i gang innen områdene datafilter, svitjser, overvåkningsverktøy og meldingssystem. Flere nasjoner har satt krav til sertifisering for blant annet elektroniske pass, sikre signaturfremstillingssystemer og helsekort. NSM ved SERTIT oppfordrer både det offentlige og private til å benytte sertifiserte produkter for å bedre sikkerheten.

Forenkler godkjenningsarbeidet

Det skal bli raskere og enklere å få sikkerhetsgodkjent informasjonssystemer som behandler statshemmeligheter. Nasjonal sikkerhetsmyndighet legger nå om godkjenningsordningen.

Innerst i NSM-bygget på Kolsås, bak to solide ståldører med flere forskjellige kodelåser, er lab-en til blant andre overingeniør Per Øyvind Hodøl (foto over).

– Dette er utprøving av sikkerhetstiltak i praksis. Her er vårt rack, sier Hodøl, og peker mot en grå reol full av ledninger.

– Racket inneholder nå to switcher og fire servere. Akkurat nå holder vi på å montere opp mer nettverksutstyr.

Tester sikkerheten

Her kjøper sikkerhetsekspertene inn komponenter som skal brukes i datasystemer som for eksempel Forsvaret skal bruke. De monterer komponentene sammen, og lager kunstige nettverk for å teste sikkerheten.

– Vi anbefaler hvordan man kan herde produktene for eksempel i forhold til innstillinger. Vi gir råd om hvordan komponenter skal settes opp for på best mulig måte å ivareta sikkerheten. Det er som om du får levert et hus med åpne dører og vinduer. Vi anbefaler å lukke dørene og vinduene, deler ut nøkler, og gir anbefalinger om når og hvordan du bør låse dørene og lukke vinduene, sier Hodøl.

Tar grep om køene

Hans råd veier tungt når Nasjonal sikkerhetsmyndighet skal godkjenne datasystemer. Alle datasystemer skal være sikkerhetsgodkjente før de kan benyttes til håndtering av gradert informasjon. Det er for å ha et minimumskrav til at landets viktigste hemmeligheter er godt nok sikret.

Men i dag er det mange systemer som står i kø for å bli godkjent.

– Problemet har vært at datasystemer som skal godkjennes står i kø på grunn av begrenset kapasitet i NSM. Nå legger vi om godkjenningsordningen, sier fungerende avdelingsdirektør Lene Bogen Kaland.

> «Vår oppgave er å forhindre at sikkerhet blir nedprioritert.»

Ny teknologi utfordrer sikkerheten

Eieren av informasjonssystemet må nå selv ta et større ansvar for sikkerheten i sine egne systemer, inkludert å kunne dokumentere og verifisere at kravene til sikkerhet er oppfylt.

– En forutsetning for at dette skal lykkes er at NSM utarbeider gode veiledninger som gjør virksomhetene i stand til å oppfylle kravene som ligger til grunn for at systemet kan godkjennes, sier Kaland.

– I tillegg vil vi bruke mer ressurser på tilsyn for å følge opp at sikkerhetsarbeidet blir gjort godt nok også etter at systemet har fått en godkjenning, sier hun.

Antall teknologier som inngår i moderne IT-systemer har økt kraftig de siste ti årene. Eksisterende teknologier videreutvikles i et hurtig tempo. Dette gir NSM en stor utfordring i rollen som regelverksforvalter og pådriver for utvikling av nye IT-sikkerhetstiltak.

Stiller krav

En av de største eierne av datasystemer er Forsvaret.

– Klarer ikke Forsvaret å ta vare på sikkerheten selv?

– Det er vi som stiller kravene til sikkerhet i informasjonssystemer, også når det gjelder Forsvaret. Forsvaret har et veldig leveransepress på ulike prosjekter. I slike situasjoner kan sikkerhet bli en salderingspost. Vår oppgave er i samarbeid med sektormyndighetene å forhindre at sikkerhet nedprioriteres, og sørge for at kravene til konfidensialitet, integritet og tilgjengelighet alltid blir tilfredsstilt, sier Hodøl.

Om fremtiden

- Stadig flere virksomheter har behov for graderte datasystemer, både i sivil og militær sektor.
- Kompleksiteten i og avhengighetene av datasystemene øker.
- Flere systemer kobles sammen, og det kreves at informasjon på flere graderingsnivåer skal kunne behandles på ett og samme system.
- Omfanget av gradert informasjon tilsier at risikoen for kompromittering blir større.
- Kontrollvirksomhet fra sektormyndigheter og NSM som tilsynsmyndighet vil måtte intensiveres.

INTERNETTSIKKERHET

Øvet på IKT-krise

Flere hundre henvendelser gikk til og fra NorCERT under øvelsen IKT-08 i desember. Øvelsen var arrangert av Direktoratet for samfunnssikkerhet og beredskap (DSB) i samarbeid med NSM. Målet var å teste hvor godt forberedt Norge er på et større, koordinert IKT-angrep. Et trettitalls offentlige og private virksomheter deltok, blant annet innen olje- og gassektoren, bank- og finanssektoren, kraftforsyningen og telesektoren.

Varsler om dataangrep

Et eget sensornettverk varsler Nasjonal sikkerhetsmyndighet om alvorlige dataangrep mot Norge. Alarmen går flere tusen ganger i løpet av året ved avdelingen NorCERT. – Det å oppdage koordinerte dataangrep krever en god analysejobb, og ikke bare knapper som må trykkes på, sier senioringeniør Tor Inge Skaar.

Han og kollegaene er stadig på jakt etter trusler og sårbarheter som gjør livet vanskelig for mange databrukere, og som i verste fall kan true rikets sikkerhet eller kan føre til en nasjonal krisesituasjon.

Varsler om dataangrep

Det snakkes om malware, ondsinnet programkode, virus, målrettede trojanere, ormer, spyware. Dette er små dataprogrammer eller programkoder som er laget for å trenge seg inn i datasystemer, stjele informasjon, ødelegge eller manipulere datanettverk og tyvlåne IP-adresser. De kan også få PC-en din til å gjøre ting den ikke skal gjøre, som for eksempel å være med på å overbelaste nettsider med trafikk slik at de bryter sammen.

> «De siste par årene har vi sett at svakheter i datasystemer blir utnyttet samtidig med tradisjonelle angrepsmetoder.»

VDI, varslingssystem for digital infrastruktur, varsler om koordinerte dataangrep rettet mot kritisk infrastruktur i Norge. Det kan dreie seg om regjeringen, kraftforsyningen, finansinstitusjoner eller andre viktige samfunnsfunksjoner. Flere titalls offentlige og private virksomheter har installert sensorer som umiddelbart varsler operasjonssenteret på Akershus festning ved tilfeller som ser ut som koordinerte angrep. Systemet ble opprettet i 2000, og var et samarbeid mellom de tre EOS-tjenestene og virksomheter med kritisk infrastruktur i Norge.

Norge tidlig ute

– På den tiden var det ganske ukjent også internasjonalt å ha et nasjonalt sensorsystem med aktivt samarbeid mellom det private, offentlige og sikkerhetstjenestene. Fremdeles er Norge i en særstilling når det kommer til dette. Også andre ønsker å opprette lignende varslingssystemer innenfor kritisk infrastruktur. Vi er en ettertraktet samarbeidspartner for andre land med tanke på erfaringer som er blitt gjort, sier Tor Inge Skaar.

Gjennom nasjonalt og internasjonalt samarbeid håndterer og koordinerer Nasjonal sikkerhetsmyndighet dataangrep som er rettet inn mot kritiske samfunnsfunksjoner. VDI-systemet har vært en suksess, sier Skaar.

– Vi har varslet om og håndtert sikkerhetstruende hendelser. NSM har fått en mulighet til å verifisere sikkerhetstilstanden på internett basert på egne data. Og virksomhetene som har utplassert sensorer har økt sikkerhetsbevisstheten i egen organisasjon.

Analyse viktig

Håndteringen av det som kan være et større angrep betyr blant annet analyse av programkoden som blir brukt i angrepene. Malware-analyse blir sett på som en egen vitenskap blant dataeksperter. Det er en jobb som er langt fra enkel.

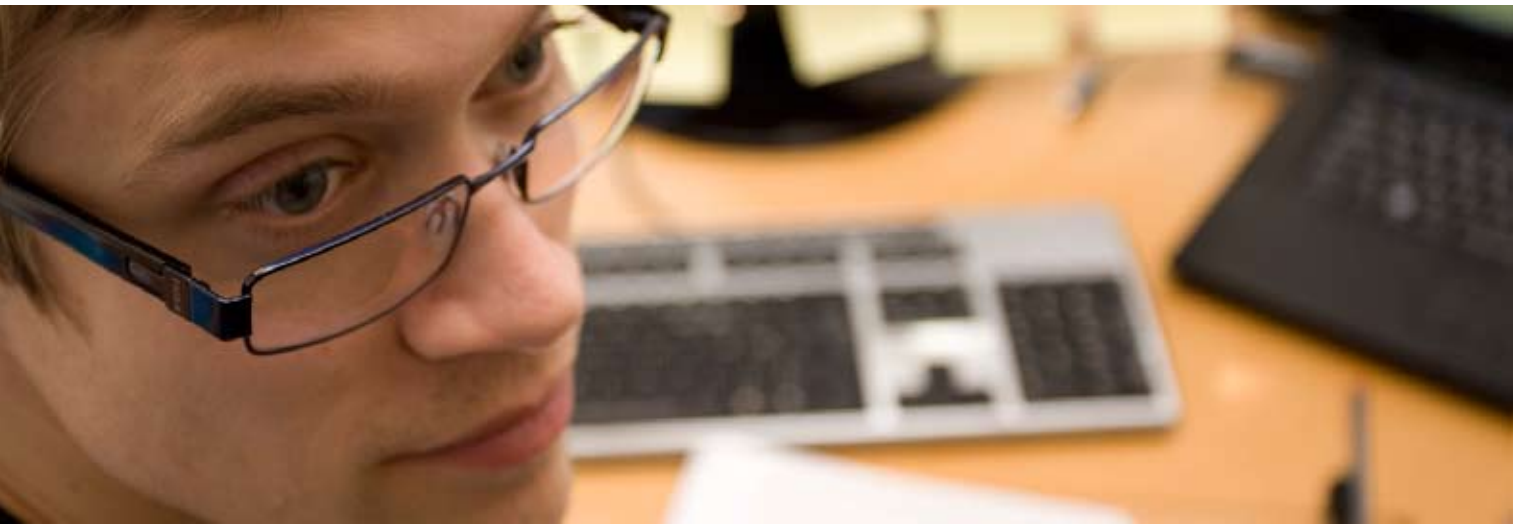
– De som utvikler malware er selvsagt klar over at det sitter noen som prøver å analysere programkodene deres. Kodene har som regel mekanismer i seg som ser etter hva slags system den blir kjørt i. Den prøver å finne ut om det er noen som analyserer den. Den kan for eksempel passivt "legge seg død", fordi den merker at den er satt inn i et kunstig miljø i en lab. Den kan endre adferd for å forvirre analytikerne, slik at den for eksempel later som den angriper noe annet enn det den er utviklet for å gjøre, sier Tor Inge Skaar.

– Er det et troverdig scenario at det sitter noen der ute som har tenkt å angripe datasystemene i Norge?

– De siste par årene har vi sett at svakheter i datasystemer blir utnyttet samtidig med tradisjonelle angrepsmetoder, enten det dreier seg om Estland og flytting av krigsmonumenter, Midtøsten og Muhammed-tegningene, eller konflikten mellom Israel og Gaza. Jeg vil si definitivt ja! sier senioringeniør Tor Inge Skaar.

Om fremtiden

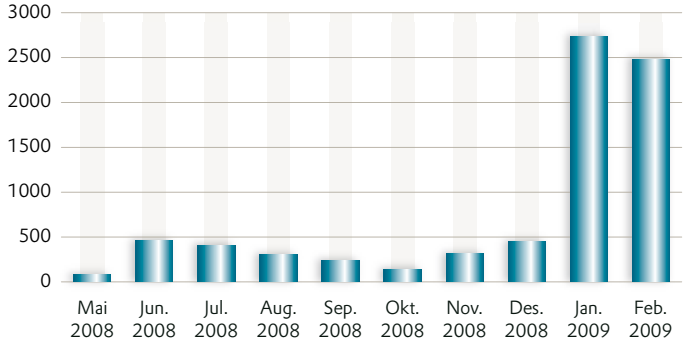
- Dataangrepene øker og blir stadig mer kreativt utført.
- Både nye teknikker og nye kombinasjoner av kjente teknikker benyttes i nye typer angrep, og det blir stadig mer ressurskrevende å ha en tilfredsstillende oversikt over situasjonen.
- Uønsket aktivitet på nett øker kraftig. Så lenge gevinsten fortsetter å være uforholdsmessig stor i forhold til risikoen, kommer bruken av denne type angrep bare til å øke videre.



Varslingssystem for digital infrastruktur (VDI)

- Opprettet av etterretnings-, overvåknings- og sikkerhetstjenestene i 2000.
- Opprinnelig fysisk plassert i daværende POTs lokaler (nåværende PST) frem til 2003
- Består av sensorer som et utvalg samfunnskritiske virksomheter har installert på sine internettforbindelser.
- Ansvaret for VDI lagt til Nasjonal sikkerhetsmyndighet i 2003.
- VDI er nå en del av NorCERT (Norwegian Computer Emergency Response Team), som er en avdeling i NSM.
- NorCERT ble formelt opprettet 1. januar 2006 etter to års prøvedrift.

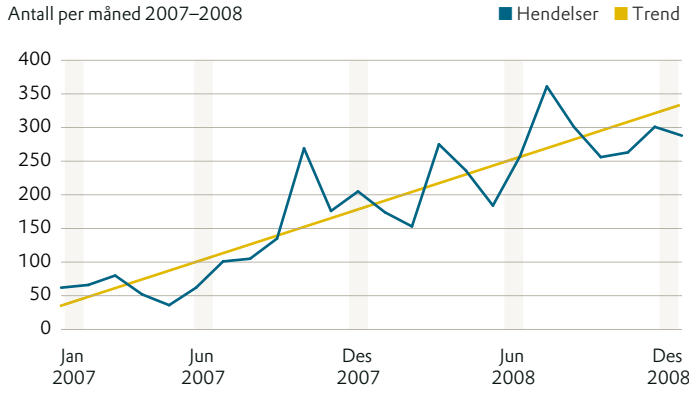
Registrerte IP-adresser som skjuler infiserte PC-er



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.

Hendelser

Antall per måned 2007–2008



Stadig mer å gjøre: Grafen viser antall håndterte hendelser i operasjonssenteret til NorCERT. Antall saker er mer enn fordoblet i perioden 2007 til 2008. I 2008 ble det håndtert over 3000 hendelser.

Et representativt utvalg

Et utvalg virksomheter med samfunnsviktige funksjoner er medlemmer i VDI-systemet, og har utplassert sensorer som varsler om datainnbrudd. Flere private virksomheter er med på å finansiere driften.

– Vi kan ikke ha en sensor hos alle som eier eller drifter kritisk infrastruktur i Norge. Det har vi ikke kapasitet til per i dag. I stedet søker vi å ha et mest mulig representativt utvalg som kan gi indikasjoner på om større angrep er under oppseiling, sier avdelingsdirektør i NorCERT, Christophe Birkeland.

NorCERT får tildelt midler over statsbudsjettet som en del av NSMs ramme. I tillegg er det forutsatt at det årlig hentes inn minimum 3 millioner kroner fra næringslivet. Både offentlige og private virksomheter er med i systemet. De private virksomhetene som blir med i VDI-systemet betaler en medlemsavgift, og får blant annet tilgang til unik informasjon, og hjelp til å håndtere større angrep.

– Samarbeidet er basert på gjensidig tillit. Vi deler mye data mellom oss, og vi må stole på hverandre, sier Birkeland.

Medlemmer og partnere
Finansieringsmodellen er basert på to hovedtyper samarbeidspartnere, medlemmer og partnere.

NorCERT-medlemmer får blant annet:

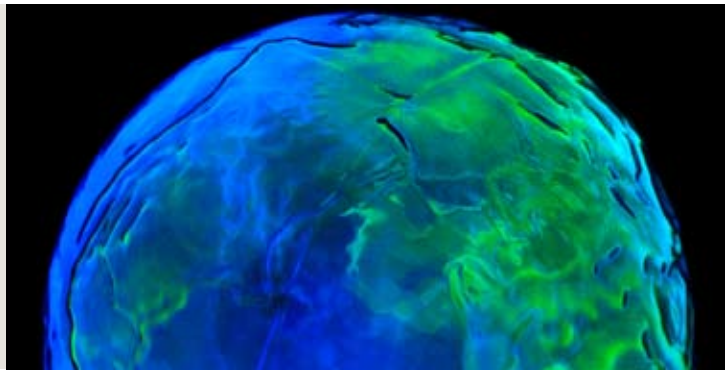
- Trekke på NorCERTs kompetanse og nettverk ved sikkerhetshendelser
- Tilgang til sensitiv informasjon om malware
- Bistand til analyse av malware
- Fortrinnsrett til utvalgte NorCERT-produkter. Herunder hendelseshåndtering, sensitive rapporter, tidlig varsling og øvelser
- Invitasjon til NorCERTs sikkerhetsforum
- Delta på kurs i regi av NorCERT

NorCERT-partnere får i tillegg:

- Tettere og bedre oppfølging i form av en-til-en-møter, skreddersydde rapporter samt skisser til operative prosedyrer.
- Deltakelse i NorCERT Ekspertråd hvor partnere kan gi råd om en ønsket videreutvikling av samarbeidet og få større innsyn i driften av NorCERT.
- Tilbud om hospitering hos NorCERT, deltagelse i pilotprosjekter om f.eks. uttesting av ny sikkerhetsteknologi.
- Innsikt i og enda større utbytte av det internasjonale nettverket som NorCERT opparbeider mot andre CERT-miljøer

Strategi for Cyber Defence

Nasjonal sikkerhetsmyndighet har fått i oppdrag for 2009 å fremme et forslag til en nasjonal strategi for Cyber Defence. Dette skal være i forlengelsen av regjeringens Nasjonale retningslinjer for informasjonssikkerhet, som ble utgitt i 2007.



TILSYNSVIRKSOMHET

Tar tempen på rikets sikkerhet

Ni nyutdannede revisjonsledere skal måle temperaturen på sikkerhetstilstanden når de er ute på tilsyn for Nasjonal sikkerhetsmyndighet. Virksomhetene som er underlagt sikkerhetsloven vil få bedre hjelp til å styrke sikkerhetsarbeidet gjennom tilsyn.

– Vi har løftet fokuset fra detaljnivå til det overordnede nivået. Det betyr at vi ikke bare ser etter spesifikke feil og mangler når vi er ute på tilsyn. Vi ser etter årsakene til manglene, sier seniorrådgiver Jørn Arnesen i Nasjonal sikkerhetsmyndighet. Han har tilsynserfaring blant annet fra Statens jernbanetilsyn, Datatilsynet, og som internrevisor i Deloitte.

Omfattende opplæring

Det har vært hektisk aktivitet for de som jobber med tilsyn i NSM i 2008. Ni revisjonsledere har gjennomgått et omfattende opplæringsprogram blant annet med kurs fra Universitetet for miljø og biovitenskap, i tillegg til intern opplæring, praktisk gjennomføring og øvelser.

Nærmere 600 virksomheter er underlagt sikkerhetsloven. Det dreier seg om alt fra store organisasjoner som Forsvaret med rundt 23.000 ansatte inkludert vernepliktige, til departementer og kommuner samt private virksomheter som har betydning for rikets sikkerhet.

Styrker tilsynet

NSM har som oppgave å føre tilsyn og gi pålegg til virksomhetene som er underlagt sikkerhetsloven. Direktoratet tar nå grep for å styrke tilsynet med disse, blant annet gjennom å etablere en metodikk basert på en internasjonalt anerkjent standard for revisjon, NS-ISO EN 19011.

– Det er viktig for oss at tilsynsrapportene skal være et godt hjelpemiddel overfor tilsynsobjektene i deres arbeid med å styrke sikkerhetstilstanden. Tilsynsrapportene vil være som en temperaturmåling der og da. I dette arbeidet har vi sammenfallende interesser, både NSM og tilsynsobjektene. Gode tilsyn bidrar til å styrke sikkerhetstilstanden, sier Jørn Arnesen.

«Tilsynsrapportene skal være et godt hjelpemiddel overfor tilsynsobjektene i deres arbeid med å styrke sikkerhetstilstanden.»

Setter fokus på ledelsen

Når tilsynets mål ikke er å finne feil, men å finne årsakene til feil, blir ofte ledelsen fokus for undersøkelsene, og for oppfølgingsarbeidet etterpå.

Virksomhetens sikkerhetsnivå er lik summen av alt sikkerhetsarbeid i organisasjonen. Det er den enkelte medarbeider som må gjøre de riktige sikkerhetsvalgene. Men det er virksomhetsledelsen alene som har det overordnede ansvar for å legge plan og systematikk til grunn for arbeidet med sikkerhet.

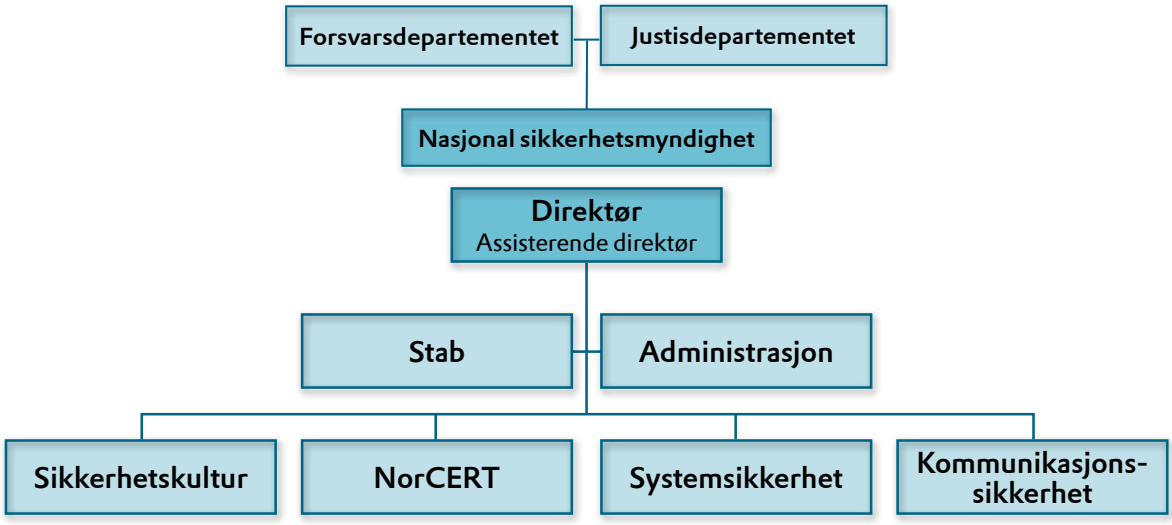
Virksomhetsledelsen utøver dette ansvaret gjennom å fastlegge de grunnleggende forutsetningene for den forebyggende sikkerhetstjenesten. Ansvaret utøves gjennom å utpeke sikkerhetsorganisasjonen, og samtidig gi denne mulighet til å oppfylle forventningene som stilles gjennom kompetanseutvikling og -vedlikehold.

Kjernespørsmålet, for tilsynsmyndigheten og for virksomheten selv er: Kan sikkerhetsbrudd tilbakeføres til mangler ved sikkerhetsledelsen? Svaret er alt for ofte et ubetinget ja, og det må det fokuseres på – under tilsyn og hos ledere.

NØKKELINFORMASJON

Bilde til venstre: NSMs ledergruppe.
Foran t.v.: Geir Samuelsen (Assisterende direktør), Lene Bogen Kaland (Systemsikkerhet) og Kjetil Nilsen (Direktør). Bak t.v. Tore Gustafsson (Sikkerhetskultur), Anders Bjønnes (Stab/Strategi & policy), Åshild D. Salmela (Administrasjon), Liv Nodeland (Stab/Kommunikasjon & samfunnskontakt), Christophe Birkeland (NorCERT) og Hans Robert Bjørnaas (Kommunikasjonssikkerhet).

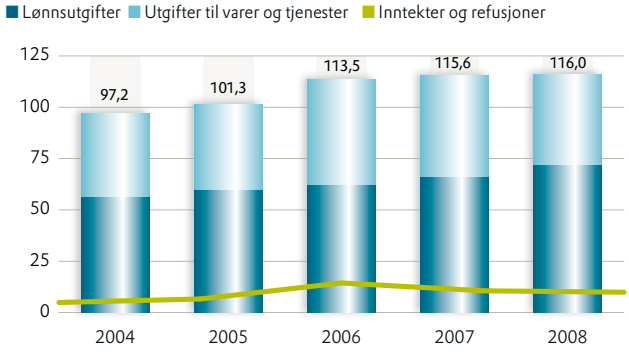
Organisasjon



Økonomi

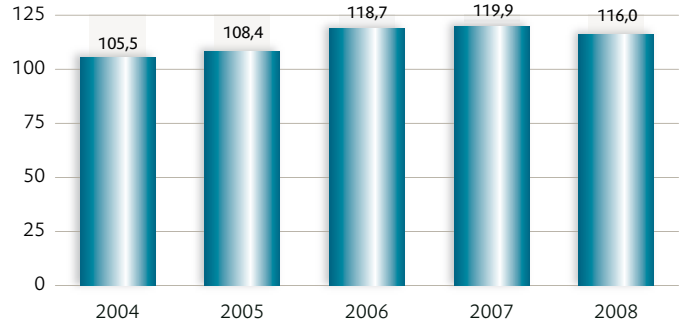
Tall i millioner kroner	**Budsjett 2008**	**Regnskap 2008**	Regnskap 2007	Regnskap 2006	Regnskap 2005	Regnskap 2004
Lønnsutgifter	*71,5*	***71,5***	*66,0*	*62,0*	*59,7*	*55,9*
Utgifter til varer og tjenester	*37,6*	***44,5***	*49,6*	*51,5*	*41,7*	*41,3*
Sum driftsutgifter	109,1	**116,0**	115,6	113,5	101,3	97,2
Inntekter og refusjoner	2,7	**9,9**	10,6	14,4	6,6	4,9
Netto	**106,4**	**106,1**	104,9	99,1	94,7	92,3

Driftsregnskap 2004–2008
Tall i millioner kroner



Diagrammet viser utviklingen i NSMs driftsregnskap i perioden 2004-08. Økningen i driftsutgifter fra 2005 til 2006 skyldes opprettelsen av NorCERT som egen avdeling i NSM. Inntekter og refusjoner består av brukerfinansiering til NorCERT, sykelønnsrefusjon samt andre utgiftsrefusjoner.

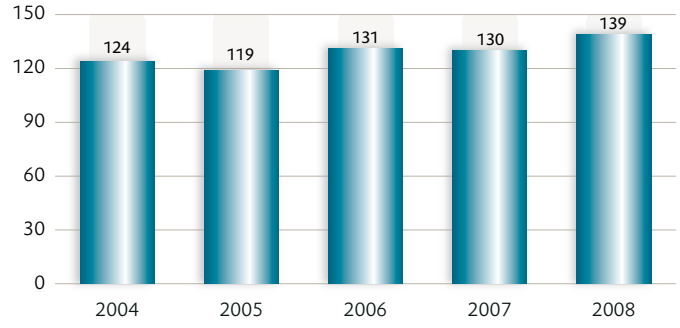
Sum driftsutgifter 2004-08, faste 2008-kroner
Tall i millioner kroner



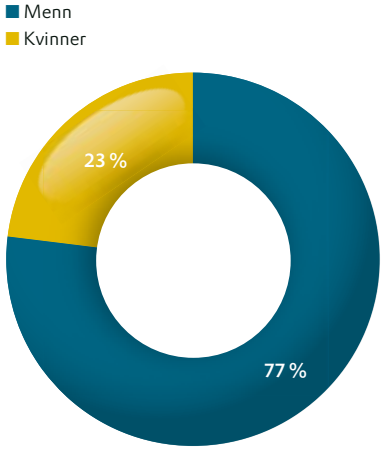
Diagrammet viser utviklingen i NSMs samlede bruttoutgifter i perioden 2004-08 korrigert for prisvekst.

Personell

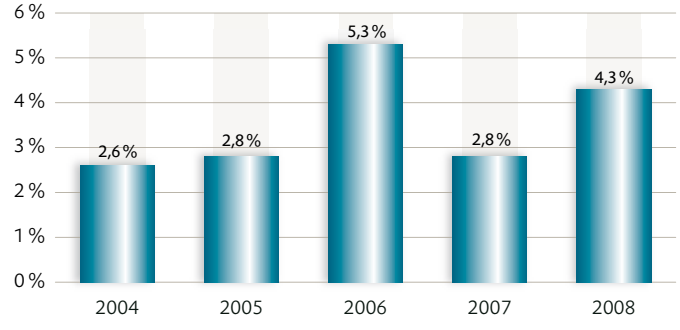
Antall årsverk
Totalt per 31. desember



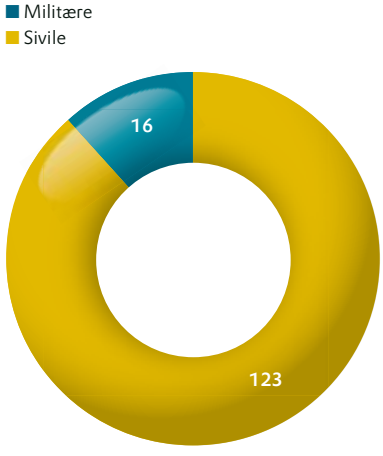
Kjønnsfordeling
Ansatte per 31. desember 2008



Sykefravær
Per år



Antall ansatte
per 31. desember 2008

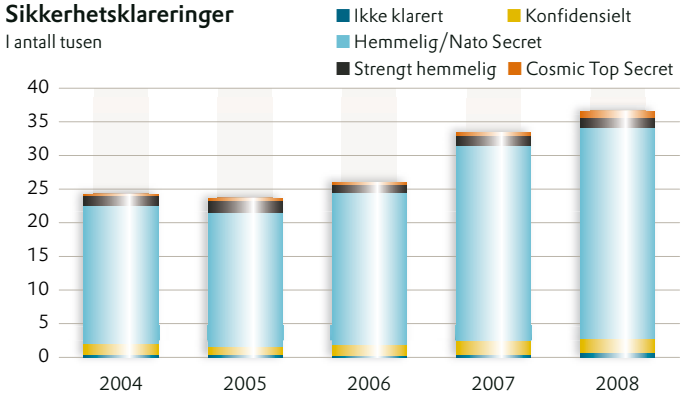


Produksjon

Oversikten viser noen utvalgte eksempler på myndighetsutøvelse og annen utførende aktivitet i Nasjonal sikkerhetsmyndighet.

Sikkerhetsklareringer

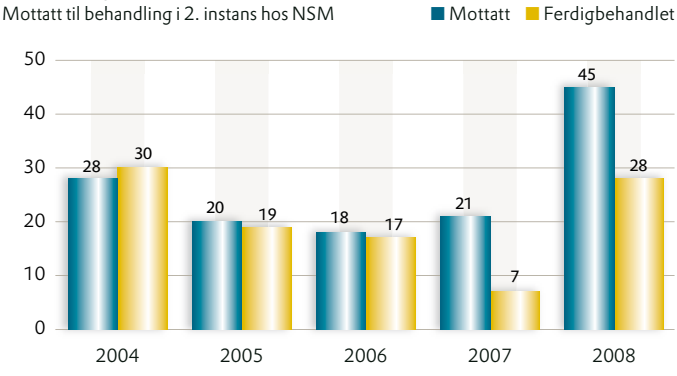
I antall tusen



Antall personkontroller har økt fra rundt 25.000 pr år i 2004-06 til over 36.000 i 2008. NSM er sentral personkontrollinstans.

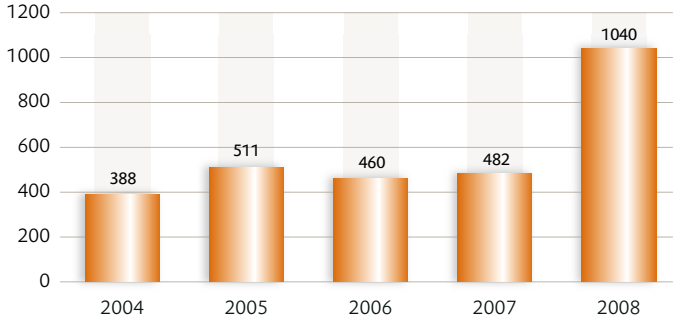
Antall klagesaker

Mottatt til behandling i 2. instans hos NSM



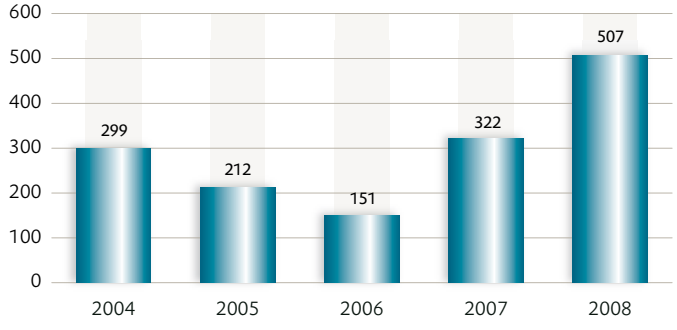
Antall klagesaker har økt betydelig i 2008 sammenlignet med tidligere år. Dette henger til dels sammen med økningen i antall klareringssaker.

Antall CTS-klareringer



Antall personer klarert for det høyeste sikkerhetsnivået i NATO, Cosmic Top Secret, er doblet i 2008 i forhold til tidligere år. Mye av økningen skyldes en endring i NATOs regelverk. NSM er klareringsmyndighet.

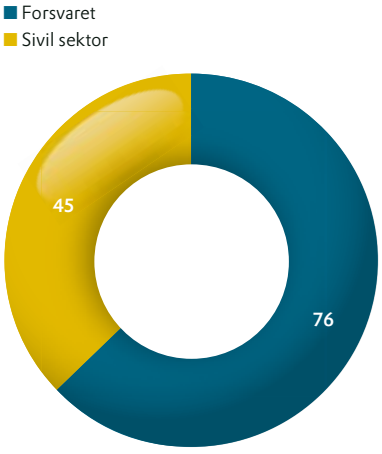
Antall ikke-klarerte



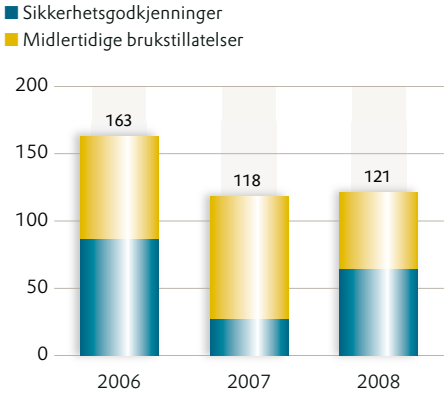
Antall ikke-klarerte har økt betydelig i 2008. Antall klareringer i Forsvaret har økt. Dette har igjen ført til flere negative klareringsavgjørelser.

Antall godkjente systemer

Per sektor i 2008



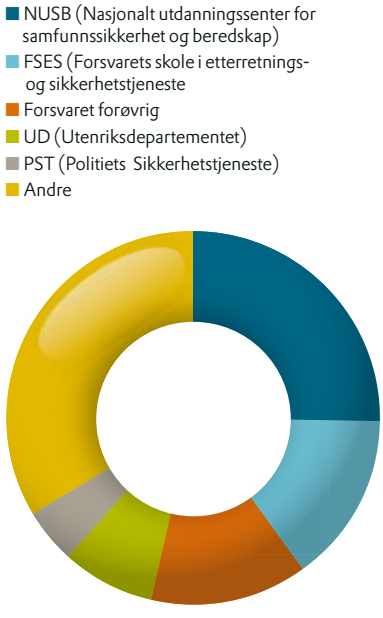
Antall sikkerhetsgodkjenninger og midlertidige brukstillatelser for graderte informasjonssystemer hvor NSM er godkjenningsansvarlig



Diagrammer t.v.: *Oversikten skiller ikke mellom omfang og kompleksitet i de ulike sakene, men det er stor variasjon i dette mellom de ulike systemene. Tallene er således ikke direkte sammenlignbare fra år til år, men gir likevel et bilde av aktivitetsnivået.*

Antall foredrag

Per oppdragsgiver i 2008

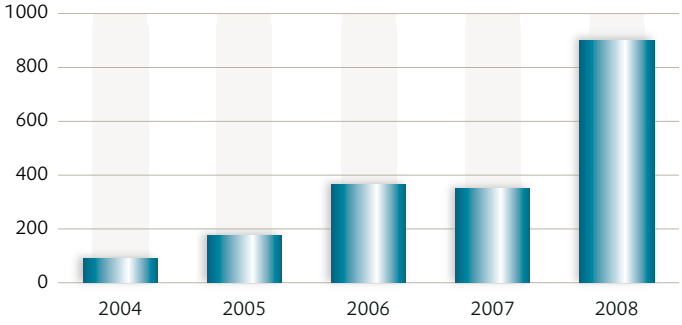


T.v.: *Diagrammet omfatter foredragsvirksomhet, og er basert på andel timer pr oppdragsgiver.*

Gruppen "Andre" representerer flere forskjellige oppdragsgivere innen både offentlig og privat sektor, inkludert forum og konferanser som omfatter begge sektorene. Foredragsvirksomheten utgjør totalt over 150 timer.

Antall medietreff

Per år



T.v.: *Antall saker i media har økt kraftig i løpet av 2008. Spesielt stor oppmerksomhet har det vært rundt nettsamfunn, offentlige nettsteder som ble infisert av virus samt den nå spiondømte Herman Simm.*

Styring og kontroll

Styringsmodellen

Forsvarsdepartementet og Justisdepartementet har det overordnede sektorovergripende ansvar for forebyggende sikkerhet i henholdsvis militær og sivil sektor. Nasjonal sikkerhetsmyndighet er utøvende organ for de to departementene innen forebyggende sikkerhet. NSM er administrativt underlagt Forsvarsdepartementet.

Parlamentarisk kontroll

EOS-utvalget er et kontrollorgan oppnevnt av Stortinget for å føre kontroll med etterretnings- og sikkerhetstjenestene. Kontrollen er innrettet mot individuell rettssikkerhet, men omfatter også en generell kontroll med at tjenestene holder sin virksomhet innenfor de rammer som er fastsatt av lover og annet regelverk. NSM kontrolleres også av Riksrevisjonen.

Regjeringens kontroll

Forsvarsdepartementet kontrollerer NSMs oppgaveløsning på Regjeringens vegne.

Etterretnings- og sikkerhetstjenestene (EOS)

Nasjonal sikkerhetsmyndighet er en av de tre sektorovergripende EOS-tjenestene. De to andre er Etterretningstjenesten (E-tjenesten) og Politiets sikkerhetstjeneste (PST).

Årsmelding for NSM 2008
Utgitt av Nasjonal sikkerhetsmyndighet, mai 2009.
Ansvarlig redaktør: Kjetil Nilsen.
Redaktør: Anders Bjønnes.
Redaksjonen: Kjetil Berg Veire (redaksjonssekretær), Stein Henriksen, Øivind Mandt og Liv Nodeland.
Grafisk design: Håvar Haug. Layout/produksjon: NSM.
Foto: Pål Rødahl/tinagent, Statnett, Stortinget, Forsvarets mediearkiv, Håvar Haug og NSM.
Opplag: 1200 - mai 2009.
Trykk: Allkopi.

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