NSM

SIKKERHETSTILSTANDEN 2014

NASJONAL SIKKERHETSMYNDIGHET

NASJONAL SIKKERHETSMYNDIGHET

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

OPPSUMMERING

I 2013 ble ble det satt i gang flere tiltak for å bedre sikkerheten i Norge. NSM ser at sikkerhet er blitt satt tydeligere på dagsordenen i enkelte virksomheter og erfarer at interessen for sikkerhet er økende i samfunnet. Tiltakene har trolig økt mange virksomheters evne til å forebygge og forhindre sikkerhetstruende virksomhet.

Likevel finnes det fremdeles mange og omfattende sårbarheter, og nasjonale verdier er fortsatt utsatt for en betydelig risiko for spionasje, sabotasje og terror. Dette gjør at det er nødvendig å opprettholde trykket på arbeidet med å styrke sikkerheten i norske virksomheter. Særlig er det viktig at ledere engasjerer seg og bidrar til at sikkerhetsarbeidet gis nødvendig prioritet.

2013 var et år med fortsatt økning i de digitale truslene mot Norge. NSM håndterte 50 alvorlige digitale infiltrasjonsforsøk. Blant annet avdekket vi at sentrale norske virksomheter har vært utsatt for gjentatte, målrettede nettverksoperasjoner. Sårbarhetene i IKT-systemer eller i virksomhetene som forvalter disse, er fremdeles store. Dette til tross for at flere tiltak er iverksatt, som for eksempel etableringen av lokale responsmiljøer for håndtering av IKT-hendelser i egen sektor.

Det forventes økende antall spionasjeforsøk mot norske virksomheter tilknyttet forskning og utvikling av høyteknologi. Flere av de høyteknologiske virksomhetene har kompetanseutfordringer og sårbarheter knyttet til eget arbeid med forebyggende sikkerhet.

Terrorangrepet mot petroleumsanlegget i In Amenas i januar 2013 viste at også internasjonal olje- og gassindustri, og dermed også norske interesser, er blitt et attraktivt mål for terrorister.

Foto omslag: SCANPIX

Design: REDINK

Foto: NSM, THINKSTOCK

Illustrasjon: MARIUS HOLE

Trykk og distribusjon: RK GRAFISK

SITUASJONSBILDE

LEDELSE OG STYRING

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

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

Mangelfulle rutiner for styring av sikkerhetsarbeidet. NSM ser at toppledere i de ulike virksomhetene i svært liten grad blir målt på sikkerhet, og at bevisstheten rundt sikkerhet er tilsvarende liten. Handlekraft og gjennomføringsevne er essensielt for at sikkerhetsarbeidet skal bli gjort, og dette er et lederansvar. Vi ser at det tar for lang tid før sikkerhetsarbeid får prioritet og tiltakene blir implementert.

Sikkerhetsarbeid foregår ofte i små miljøer som har utfordringer med å etablere og beholde sikkerhetsfaglig kompetanse. Dette medfører ofte at virksomhetene har mangelfulle rutiner.

I noen tilfeller er sikkerhetsarbeid så lavt prioritert at evnen til å forebygge mot eller håndtere sikkerhetstruende hendelser vil være svært begrenset.

INFORMASJONSSIKKERHET

Truslene mot norske datasystemer øker. I fjor registrerte Nasjonal sikkerhetsmyndighet totalt 15 815 sikkerhetshendelser på nett. Svært mange av disse sakene krever liten til ingen manuell håndtering som for eksempel ved at det automatisk sendes ut en varsel-epost. Av disse nær 16 000 sakene ble 3901 saker håndtert manuelt ved varsling, dialog og analyse, og 50 av disse igjen ble karakterisert som alvorlige. Dette kan være hendelser relatert til industrispionasje mot norske interesser, hendelser som kan få store konsekvenser for mange brukere eller påvirke kritiske IKT-systemer

Økningen i antall saker som håndteres delvis automatisert skyldes i stor grad at nye kilder har medført økt innrapportering. NSM observerer at den oppadgående trenden i antall alvorlige saker fortsetter og vi regner med at det fortsatt er store mørketall på området.

Dataangrep. For fremmede etterretningstjenester, kriminelle og hackere er internett en arena for informasjonsinnhenting og spionasje. Aktørene som står bak truslene i det digitale rom spenner i følge rapporten Fokus 2014 fra Etterretningstjenesten, fra statlige etterretnings- og sikkerhetstjenester, via tradisjonelle militære motstandere, globale næringsbedrifter, terrorist- og ekstremistgrupper, til organiserte hackergrupper. Rapporten fremhever spesielt Russland og Kina som land som har etablert betydelig kapasitet til å utføre operasjoner innenfor cyberdomenet.
Til forskjell fra fysiske innbrudd og angrep, er det ofte svært liten åpenhet rundt et dataangrep. Norske virksomheter som utsettes for dataangrep velger nærmest uten unntak, å ikke la angrepet bli gjort offentlig kjent. Dette betyr igjen at det blir liten samfunnsmessig bevissthet rundt den faktiske situasjonen i Norge.
I lys av dette er Telenors åpenhet i etterkant av angrepet på egne systemer i begynnelsen av 2013, et meget godt eksempel på at åpenhet ikke nødvendigvis gir en negativ effekt for virksomheten.

Observerte sårbarheter. Dataprogrammer som ikke er oppdaterte og andre sårbarheter i datasystemene, er ofte veien inn for kriminelle og hackere. Andre typiske fremgangsmåter er å sende epost med vedlegg som er infisert med virus, eller infisere nettsider med virus, som igjen infiserer de besøkende.

Noen av NSMs observasjoner er:

- Virksomheter verdivurderer ikke informasjonen godt nok, og skjermingsverdig informasjon blir oppbevart og behandlet i ugraderte nettverk.
- Virksomheter kjøper inn kommersielle sikkerhetsprodukter, herunder brannmurer og antivirusløsninger, som ikke er egnet til å stoppe annet enn kjent skadevare.
- Enkelte virksomheter gjennomfører ikke nødvendige sikkerhetsoppdateringer og benytter ikke-godkjente IKT-systemer.
- Det er for enkelt å skaffe seg tilgang til kritiske datasystemer enten fysisk eller via nettet.
- Mange virksomheter mangler fortsatt dedikerte sikkerhetsmiljøer for å ivareta IKT-sikkerhet (responsmiljøer)
- Allerede etablerte miljøer har ikke nødvendig beredskaps- eller krisehåndteringskompetanse.
- Så mange som en tredjedel av tilsynsobjektene kunne ikke fremlegge dokumentasjon på at sikkerhetsgraderte informasjonssystemer hadde nødvendig sikkerhetsgodkjenning.

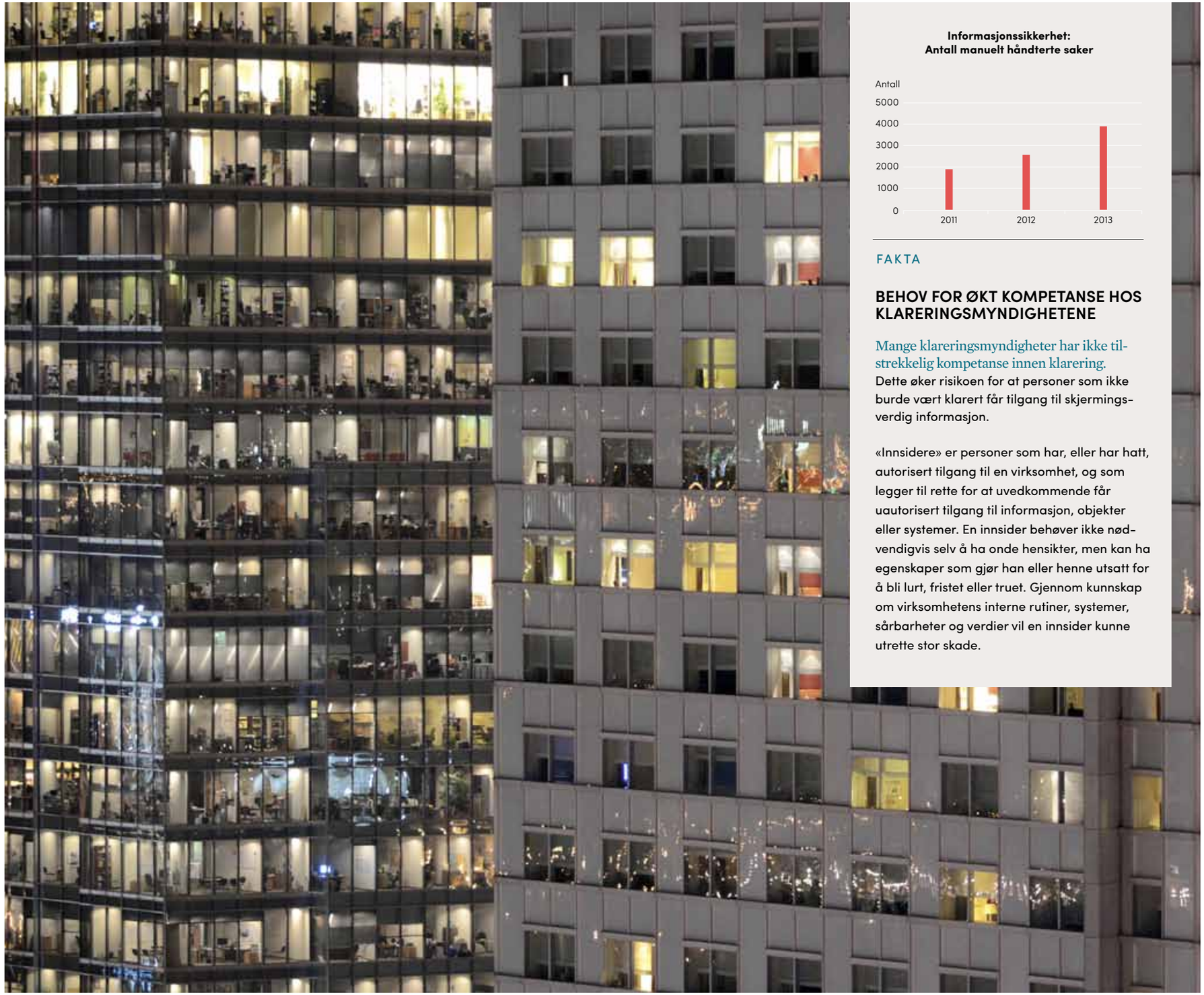
Sikkerheten i mange offentlige IKT-systemer er synes ikke god nok i forhold til risikobildet. Manglende responsmiljøer til å håndtere dataangrep, og manglende helhet i informasjonssikkerhets arbeidet er sannsynlige sårbarheter. Det eksisterer for eksempel mange forskjellige, statlige nett med egne aksesspunkter til internett. Det betyr i praksis at det er mange dører og vinduer inn til systemene for de som ønsker å bryte seg inn. Det krever betydelige ressurser både personellmessig og økonomisk å sikre systemene.

«

En mulig sikkerhets-utfordring er at virus verken blir oppdaget eller stoppet.

Kontrollsystemer utsatt. De siste årene har stadig flere kontrollsystemer for blant annet infrastruktur og industri blitt koblet til internett. Kontrollsystemene kan styre alt fra lys og varme til oljeutvinning og vannkraftverk. Kontrollsystemer har tradisjonelt vært utviklet for å fungere i lukkede datamiljøer, og er ikke designet for å styres og kontrolleres over internett. Det innebærer at de blir mer utsatt for digitale trusler. Virksomhetene som bruker teknologien mangler ofte kunnskaper om hva som ligger bak systemene, og har liten mulighet til å kontrollere hva de faktisk inneholder. En mulig sikkerhetsutfordring knyttet til slike systemer er at virus verken blir oppdaget eller stoppet. Dagbladet påviste en rekke sårbarheter innen denne typen systemer høsten 2013.

Flere stater har utviklet, eller er i ferd med å skaffe seg, avanserte virus for å kunne utnytte sårbarheter mot denne typen kontrollsystemer. Også terrorist- eller ekstremistgrupper, globale næringslivsbedrifter, hackergrupper og mulig også enkeltpersoner kan ha interesse av å bryte seg inn i denne typen systemer. Sabotasjeangrep mot kritisk infrastruktur og samfunnskritiske tjenester via denne typen systemer kan potensielt utrette stor skade.



Informasjonssikkerhet:
Antall manuelt håndterte saker

FAKTA

BEHOV FOR ØKT KOMPETANSE HOS KLARERINGSMYNDIGHETENE

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

«Innsidere» er personer som har, eller har hatt, autorisert tilgang til en virksomhet, og som legger til rette for at uvedkommende får uautorisert tilgang til informasjon, objekter eller systemer. En innsider behøver ikke nødvendigvis selv å ha onde hensikter, men kan ha egenskaper som gjør han eller henne utsatt for å bli lurt, fristet eller truet. Gjennom kunnskap om virksomhetens interne rutiner, systemer, sårbarheter og verdier vil en innsider kunne utrette stor skade.

NSM avdekket at en norsk teknologi - bedrift har vært utsatt for gjentatte målrettede nettverksoperasjoner over tid.

DIGITAL ETTERRETNING

I 2013 håndterte NSM 50 alvorlige digitale infiltrasjonsforsøk. Tilsvarende tall for 2012 var 46, og 23 for 2011. Ved flere tilfeller kan angriperne ha vært inne i datasystemene over flere år.
NSM har i 2013 avdekket at sentrale norske virksomheter som myndighetsorganer, forsvarsindustri og teknologibedrifter har vært utsatt for gjentatte, målrettede nettverksoperasjoner.

For eksempel avdekket NSM at det ved en alvorlig hendelse trolig gikk 15 - 18 måneder fra systemet ble kompromittert til hendelsen ble oppdaget.

Gjentatte nettverksoperasjoner

NSM avdekket at en norsk teknologibedrift har vært utsatt for gjentatte målrettede nettverksoperasjoner over tid. Nærmere undersøkelser avdekket tre alvorlige infiltrasjonsforsøk mot den samme bedriften. Angriperen kan ha vært inne i systemene over flere år. NSM avdekket også at en norsk annen teknologibedrift i praksis ikke hadde noe fungerende sikkerhetssystem. Bedriften ble samtidig utsatt for nettverksangrep, som mest sannsynlig var forsøk på industrispionasje. I 2013 oppdaget også NSM en hendelse mot IKT-systemene til en større, norsk industribedrift. Viruset som ble brukt hadde vært brukt ved tidligere hendelser mot samme aktør. Tidligere håndtering hadde ikke vært tilstrekkelig, og trusselaktøren hadde trolig hatt fotfeste i datasystemene over lengre tid.

OBJEKTSIKKERHET

Terrorangrepet mot petroleumsanlegget In Amenas i 2013 viste med all tydelighet at også internasjonal olje- og gassindustri, og norske interesser, er blitt et attraktivt mål for terrorister. NSM vurderer at sektorens verdier utsettes for stor risiko. Objektsikkerhet har i rapporteringsperioden vært et særskilt satsningsområde for NSM. Skjermingsverdig objekt er definert som «... eiendom som må beskyttes mot spionasje, sabotasje eller terrorhandlinger av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser». Dette dreier seg om objekter som anses helt essensielle for nasjonale sikkerhetsinteresser. Dette kan være områder, bygninger, anlegg, transportmidler eller annet materiell, eller deler av slik eiendom.
Ifølge sikkerhetsloven skal det enkelte departement utpeke og klassifisere objekter innenfor sitt myndighetsområde basert på en dokumentert skadevurdering fra objekteier.

Grunnsikring

Lovverket stiller krav om at skjermingsverdige objekter skal sikres med permanente grunnsikringstiltak bestående av en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon som til sammen tilfredsstiller sikkerhetslovens funksjonelle krav. Med tiltak menes her organisatoriske, fysiske og IKT tiltak.

Departementene har utpekt flere hundre objekter som skjermingsverdige i henhold til sikkerhetsloven. Disse varierer i type fra enkeltstående master for digital kommunikasjon og dataservere, til større bygg og anlegg. Forsvaret og justissektoren står til sammen for ca. 75 prosent av de innmeldte objektene. I tillegg er det meldt inn et betydelig antall objekter tilknyttet departementsfellesskapet og sivil infrastruktur.
Mange av de innmeldte objektene er tilknyttet kommando-, kontroll- og kommunikasjonsfunksjoner. Disse har i stor grad en IKT- basert funksjonalitet. Det blir derfor meget viktig å samordne fysisk og logisk sikring i objektsikkerhetsarbeidet.

Utsatt frist

På bakgrunn av de innmeldte objektene ser NSM at enkelte virksomheter og departementer ikke har fulgt sikkerhetslovens skadevurderingssystematikk for utpeking og klassifisering av skjermingsverdige objekter. Totalt har den enkelte sektor hatt tre år på seg til å identifisere og sikre skjermingsverdige objekter. Flere virksomheter og departementer har også signalisert at de vil søke om utsettelse på tidsfristen for sikring av objekter. Fristen for sikring av objekter var 1. januar 2014.

FAKTA

SIKKERHETS-HULL BLIR IKKE LUKKET

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

NSMS VURDERING

Flere tiltak ble satt i verk i 2013 for å styrke sikkerhetstilstanden. Basert på forholdet mellom det samlede risikobildet og foreslåtte og iverksatte tiltak vurderer NSM at sikkerhetstilstanden er bedret på enkelte områder. Men evnen til å forebygge mot og håndtere spionasje, sabotasje og terror er mangelfull hos flere, og det finnes fremdeles mange og omfattende sårbarheter. Nasjonale verdier er fortsatt utsatt for betydelig risiko. Situasjonsbeskrivelsen underbygger dette.

I tråd med gjeldende langtidsplan for forsvarssektoren styrket regjeringen det forebyggende sikkerhetsarbeidet også i 2014. I tillegg ble samordningsansvaret for forebyggende IKT-sikkerhet i sivil sektor fra 1. april 2013 samlet i Justis- og beredskapsdepartementet. Denne typen strukturelle og organisatoriske tiltak er viktige skritt i riktig retning og bidrar etter NSMs vurdering til en mer helhetlig tilnærming til sikkerhetsarbeidet.

NSM vurderer også at satsingen på tilsynsvirksomheten i NSM har bidratt til å styrke sikkerhetstilstanden i flere virksomheter. Holdningskampanjer som Nasjonal sikkerhetsmåned, kurs og foredrag bidrar til økt oppmerksomhet og kompetanse som er verdifullt for arbeidet i virksomhetene. NSM vurderer at dette er relevante tiltak, og registrerer betydelig økt deltakelse på slike arrangementer enn tidligere.

Arbeidet med å identifisere skjermingsverdige objekter som må sikres spesielt mot sabotasje og terror har også trolig bidratt til å styrke sikkerheten i flere virksomheter.

Men fremdeles er sårbarheten og risikoen etter NSMs syn for store. En hovedutfordring er fremdeles manglende lederforankring og risikoforståelse, og helt grunnleggende sikkerhetsarbeid. Manglende risikoforståelse bidrar til å øke sikkerhetsmessig risiko. Virksomheter uten oppdatert, helhetlig og realistisk risikoforståelse vil ikke være i stand til å etablere relevante sikkerhetstiltak. Spesielt har NSM observert at virksomheter undervurderer verdien av informasjon. Dette øker risikoen for at sensitiv eller skjermingsverdig informasjon kompromitteres. Det er NSMs vurdering at manglende risikovurdering vil kunne medføre feil prioritering av hva som må beskyttes og feil nivå på sikkerhetstiltakene. Dette kan igjen føre til reduksjon i, eller ødeleggelse av, kritiske samfunnsfunksjoner og infrastrukturer.

Kraftproduksjonen er av vesentlig betydning for alle funksjoner og sektorer i samfunnet. Forstyrrelser i leveranse av elektrisk kraft kan få lammende effekter på samfunnets evne til å levere varer og tjenester til befolkningen. Effekten på evnen til styring på alle nivåer i samfunnet vil etter NSMs vurdering også trolig være svært omfattende. Omfattende eller langvarig stans i energiforsyning reduserer også mest sannsynlig statssikkerheten og den nasjonale handleevnen.
Det at enkelte virksomheter og departementer ikke har fulgt sikkerhetslovens skadevurderingssystematikk for utpeking og klassifisering av skjermingsverdige objekter medfører en risiko for at objekter er klassifisert feil. Etter NSMs vurdering kan dette medføre at det ikke er iverksatt nødvendige sikringstiltak, og det kan medføre at det er iverksatt unødvendig ressurskrevende sikringstiltak.

TILTAK

I løpet av 2013 har det blitt iverksatt flere tiltak for å redusere organisatoriske sårbarheter. Likevel er det helt avgjørende for en forbedring av sikkerhetstilstanden at opplæring og informasjon skjer på et tidlig stadium.

På et samfunnsnivå må bevissthet om sårbarheter bygges parallelt med adopsjon av tekniske verktøy. Denne bevisstheten kan oppnås gjennom sikkerhetsveiledning i skole- og utdanningssystemet, samt egne utdanningsprogrammer ved universitet og høyskoler. Det har blant annet blitt etablert et senter for cyber- og informasjonssikkerhet (CCIS) på Høgskolen i Gjøvik som vil bidra til å øke den generelle forståelsen for forebyggende sikkerhet hos studenter.
Det er viktig at sikkerhetstiltak utvikles i takt med samfunns- og teknologiutviklingen. Det må fokuseres på kompetansehevende tiltak og forskning og utvikling innen fagfelt som omhandler sikkerhet innen digital kommunikasjon. Tiltak må være basert på en helhetlig sikkerhetsfaglig forståelse. Eksempelvis kan brannmurer og tilsvarende logisk skallsikring gi en falsk trygghet dersom det ikke suppleres med andre forebyggende sikkerhetstiltak.

Opplæring i risiko- og skadevurderinger

Både offentlige etater og privat næringsliv må forstå og erkjenne risiko, prioritere sikkerhetsarbeidet og generelt øke sin samlede sikkerhetsfaglige kompetanse. Dette innebærer blant annet at virksomheter må kunne utarbeide risiko- og skadevurderinger, evaluere, styre og rutinemessig rapportere om sikkerhetsarbeidet. Virksomheter både i offentlig og privat sektor må etablere gode rutiner for vedlikehold og oppdatering av informasjonssystemer og gjennomføre risikovurderinger.

Ledere må måles på sikkerhet. NSM anbefaler at det gis en felles føring om mål- og resultatkrav på forebyggende sikkerhet i tildelings- og iverksettingsbrev i statlig sektor slik at dette følges opp i etatsstyringen og underliggende etaters periodiske rapportering. Tilsvarende anbefaler NSM at det private næringsliv implementerer mål- og resultatkrav på sikkerhet i sine organisasjoner. Toppledelse og styre må etterspørre nødvendige rapporter som gir ledelsen en oversikt over risikobildet. Å ikke iverksette slike krav og tiltak kan være utslagsgivende på bunnlinjen.

NSM er i dialog med flere virksomheter for å bidra til å redusere sikkerhetsmessig risiko. Evne til deteksjon og håndtering av digitale infiltrasjonsforsøk hos virksomhetene må styrkes. Norske høyteknologivirksomheter er særlig utsatt for spionasje, noe som krever at forebyggende sikkerhetsarbeid er effektivt implementert i hele organisasjonen.

I tillegg anbefaler NSM at virksomhetene prioriterer utdanning og kurs som hever virksomhetenes risikoforståelse og sikkerhetsfaglige kompetanse.

Implementering av grunnleggende IKT-tiltak

NSM har i 2013 utarbeidet tiltak og veiledning for implementering av grunnleggende IKT-sikkerhetstiltak. Tiltakene skal bidra til å øke sikkerhetskompetanse og robusthet i den enkelte virksomhet og deres nett. Det anbefales at disse grunnsikringstiltakene implementeres i alle virksomheter.

Fortsatt forskning og utvikling av hensiktsmessige og sikre løsninger for å redusere sårbarheter innen digitale kommunikasjonsløsninger, vil ha betydning for risikoreduksjon. NSM foreslår å etablere mer robuste miljøer innen forskning og utvikling på sårbarheter og tiltak, åpne for at tredjeparter kan benyttes for å utvikle detaljerte teknologikrav, og styrke råd- og veiledningskapasiteten innen IKT-sikkerhet. I tillegg anbefaler NSM å iverksette tiltak for å harmonisere krav til graderte informasjonssystemer med andre beste praksiser og standarder.

FIRE TIPS TIL ALLE

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

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

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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