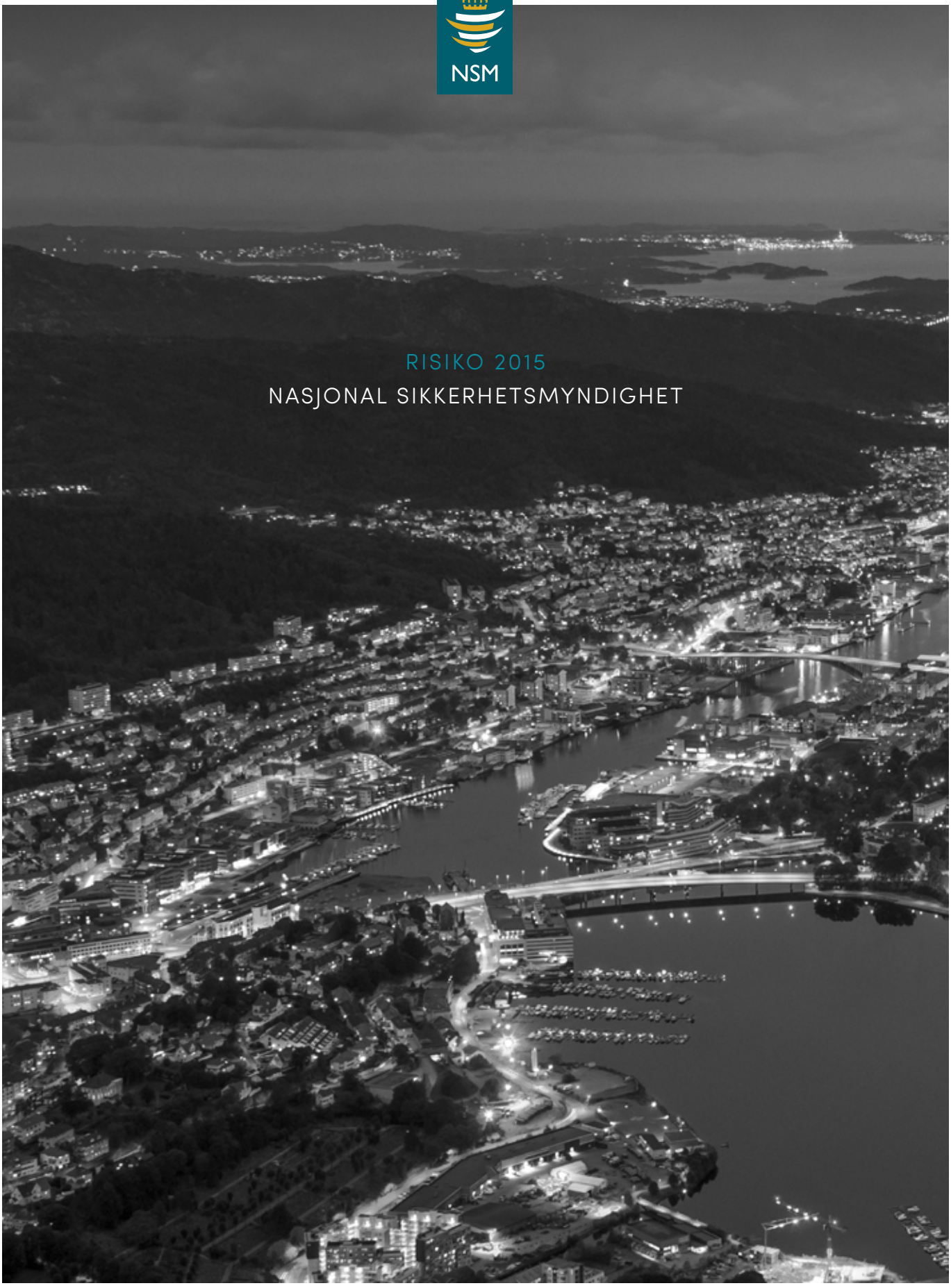
NSM



RISIKO 2015

NASJONAL SIKKERHETSMYNDIGHET

Nasjonal sikkerhetsmyndighet

Risiko 2015 gir en vurdering av sårbarheter i samfunnet, verdier som er verdt å beskytte og risiko for spionasje, sabotasje, terror og andre alvorlige handlinger. Målet med rapporten er at beslutningstakere både i offentlig og privat sektor skal få et bedre grunnlag for å redusere risiko for egen virksomhet og for samfunnet. Denne rapporten er basert på den sikkerhetsgraderte utgaven av Risiko 2015, og inneholder et utvalg temaer som er særlig relevante for norske virksomheter.

Sammendrag_

RISIKOEN ØKER: Risikoen for at sentrale kritiske funksjoner, samfunnsviktig infrastruktur, skjermingsverdig informasjon og mennesker blir rammet av spionasje, sabotasje, terror og andre alvorlige handlinger er økende. Utviklingen skyldes en rekke faktorer, fra mangelfull sikring og teknologisk utvikling, til sikkerhetspolitiske endringer og nye trusler. Samtidig er sårbarhetene store. NSM avdekket i 2014 alvorlige sårbarheter i norsk kritisk infrastruktur.

FLERE DATAANGREP: NSM vurderer at risikoen for spionasje mot norske verdier er høy. NSM håndterte i fjor 88 alvorlige dataangrep, mot 51 i 2013. De fleste av disse handlet om forsøk på spionasje mot norsk næringsliv og offentlige interesser. Norge opplevde sommeren 2014 det største dataangrepet vi har sett så langt, målrettet mot olje- og energisektoren. Vi forventer flere dataangrep av denne typen fremover.

STORT SKADEPOTENSIALE: Skadepotensialet er stort, blant annet fordi IKT-systemer i økende grad kobles sammen på tvers av sektorer. Små hendelser kan føre til stor skade. Strømbrudd kan for eksempel i løpet av få timer sette viktig infrastruktur ut av spill.

SYSTEMATISK ARBEID NYTTER: Mange gjør mye godt arbeid for å redusere risiko. Flere av sårbarhetene NSM har beskrevet i tidligere rapporter har blitt redusert eller fjernet. Det viser at systematisk arbeid med sikkerhet gir effekt. Vi ser likevel at tiltakene ikke utvikles i samme takt som truslene. Dette er et kontinuerlig løp, og det er derfor viktig fortsatt å styrke arbeidet med å redusere gapet mellom trusler og sikkerhetstiltak. Denne rapporten vil med dette utgangspunktet legge vekt på områder hvor det fortsatt er behov for å redusere risiko.

RISIKO 2015

SEKSJONER

Foto omslag:
ISTOCK

Design:
REDINK

Foto:
ISTOCK

Illustrasjon:
MARIUS HOLE

Trykk og distribusjon:
RK GRAFISK

Situasjon og trender_

Norge står overfor et endret risikobilde i 2015. Den sikkerhetspolitiske situasjonen endret seg vesentlig i 2014, med krisen i Ukraina, utviklingen i Midtøsten og Nord-Afrika, og en forhøyet terrortrussel mot Norge. Etterretningstrusselen fra andre stater er på et vedvarende høyt nivå. Samtidig øker samfunnets avhengighet av informasjons- og kommunikasjonsteknologi. Nye digitale tjenester og muligheter forandrer næringslivet, det offentlige og vanlige folks liv. Smarttelefoner og internett er uunnværlig. Virksomheter og infrastruktur blir tett knyttet sammen gjennom tele- og datatrafikk. Samfunnet blir dermed mer sårbart.

Endringene i den sikkerhetspolitiske situasjonen påvirker risikobildet i Norge. For eksempel vil den sikkerhetspolitiske verdien av norsk gass øke når konflikten mellom Russland og Ukraina har skapt usikkerhet rundt gassleveransene til Europa. Informasjon om norsk forsvar, norsk sikkerhets- og beredskapspolitikk, teknologi, romindustri og Norges strategiske posisjon i nord er av stor interesse for andre land.

Svak informasjonssikkerhet er i følge EU-rapporten ENISA Threat Landscape 2014 den viktigste årsaken til datainnbrudd. Det gjelder blant annet svake passord, sårbare nettverk og applikasjoner, virus, feil brukerautentisering, innsidetrussel og databasefeil. I følge rapporten blir dataangrepene mer avanserte og målrettede. Trusselaktørene utnytter sikkerhetssvakheter effektivt når de blir kjent. Flere av funnene i rapporten fra ENISA samsvarer godt med NSMs egne funn. NSM erfarer at trusselaktørene gjør gode vurderinger av hva som er informasjon av høy verdi. Trusselaktørene jobber stadig mer målrettet, og stadig mer profesjonelt.

Varslingstiden ved større kriser eller konflikter blir kortere. Konflikten i Ukraina og en rekke IKT-hendelser viser at man i mange tilfeller ikke har forvarsel før alvorlige hendelser inntreffer. Det påvirker evnen til å håndtere hendelsene. Svaret på et uforutsigbart risikobilde er god grunnsikring, god beredskap og godt sikkerhetsarbeid.

Informasjonssikkerhet og IKT-sikkerhet

I fjor varslet og håndterte NSM totalt 88 alvorlige dataangrep, mot 51 i 2013. Flesteparten av angrepene har som formål å stjele informasjon fra datasystemene til store eller viktige norske bedrifter eller virksomheter.

Digital spionasje er en vedvarende og stor utfordring for Norge. Sommeren 2014 ble en rekke virksomheter i olje- og energisektoren rammet av et målrettet og koordinert dataangrep. Eposter til en rekke virksomheter prøvde å lure mottakerne til å klikke på lenker som ville infisert datasystemene med virus. Denne alvorlige hendelsen er trolig det største angrepsforsøket mot norsk IKT-infrastruktur frem til nå.

Flere større virksomheter har ikke kapasitet til å håndtere dataangrep på det nivået vi vet at flere trusselaktører behersker. Det innebærer at Norge til enhver tid kan bli frastjålet både sensitiv og sikkerhetsgradert informasjon. Evnen til å oppdage slike hendelser er varierende.

NSM avdekket også alvorlige sårbarheter i norsk vannforsyning i 2014. Sårbarhetene kunne i verste fall gitt uvedkommende mulighet til å lamme vannforsyningen. Risiko 2014 beskrev en rekke sårbarheter i kontrollsystemer for infrastruktur og industri. Stadig flere datasystemer kobles til internett, og kan styre alt fra lys og varme til oljeutvinning og

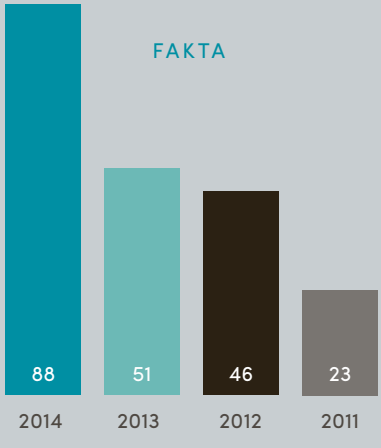
I fjor varslet og håndterte NSM totalt 88 alvorlige dataangrep, mot 51 i 2013.

vannkraftverk. Når systemene kobles til internett, blir de mer utsatt for digitale trusler. I følge en rapport fra tyske Bundesamt für Sicherheit in der Informationstechnik (BSI) førte et dataangrep mot et tysk stålverk til alvorlige skader i 2014. Dataangrepet førte blant annet til at en av ovnene ved stålverket ikke lenger lot seg kontrollere.

NSMs vurdering er at risikoen ved bruk av kontrollsystemer ikke er blitt mindre i 2015. En mulig utvikling er at dataangrep brukes til sabotasje slik hendelsen fra Tyskland viser. Dersom en trusselaktør har til hensikt å utføre sabotasje, kan et vellykket dataangrep mot kritiske IKT-systemer i kraft- eller ekom-sektoren få vesentlige konsekvenser for samfunnet. Statlige aktører har kompetanse og ressurser til å gjennomføre slike angrep. Aktører med mindre ressurser kan trolig gjennomføre vellykkede operasjoner ved hjelp av en innsider med nødvendige kunnskaper eller tilganger.

Sikring av sensitiv informasjon er en utfordring. Sikring av sensitiv men ugradert informasjon kan for eksempel være personellinformasjon i et selskap, børssensitiv informasjon, eller informasjon om

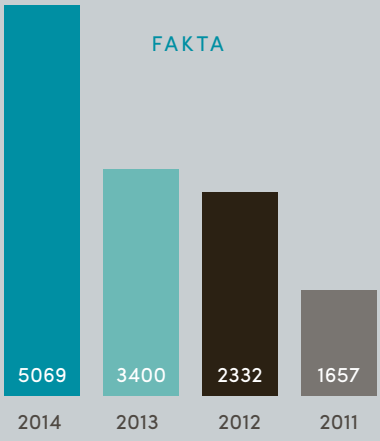
FAKTA



HÅNDTERTE FLERE DATAANGREP

I fjor varslet og håndterte NSM totalt 88 alvorlige dataangrep, mot 51 i hele 2013. Flesteparten av angrepene har som formål å stjele informasjon fra datasystemene til store eller viktige norske bedrifter.

FAKTA



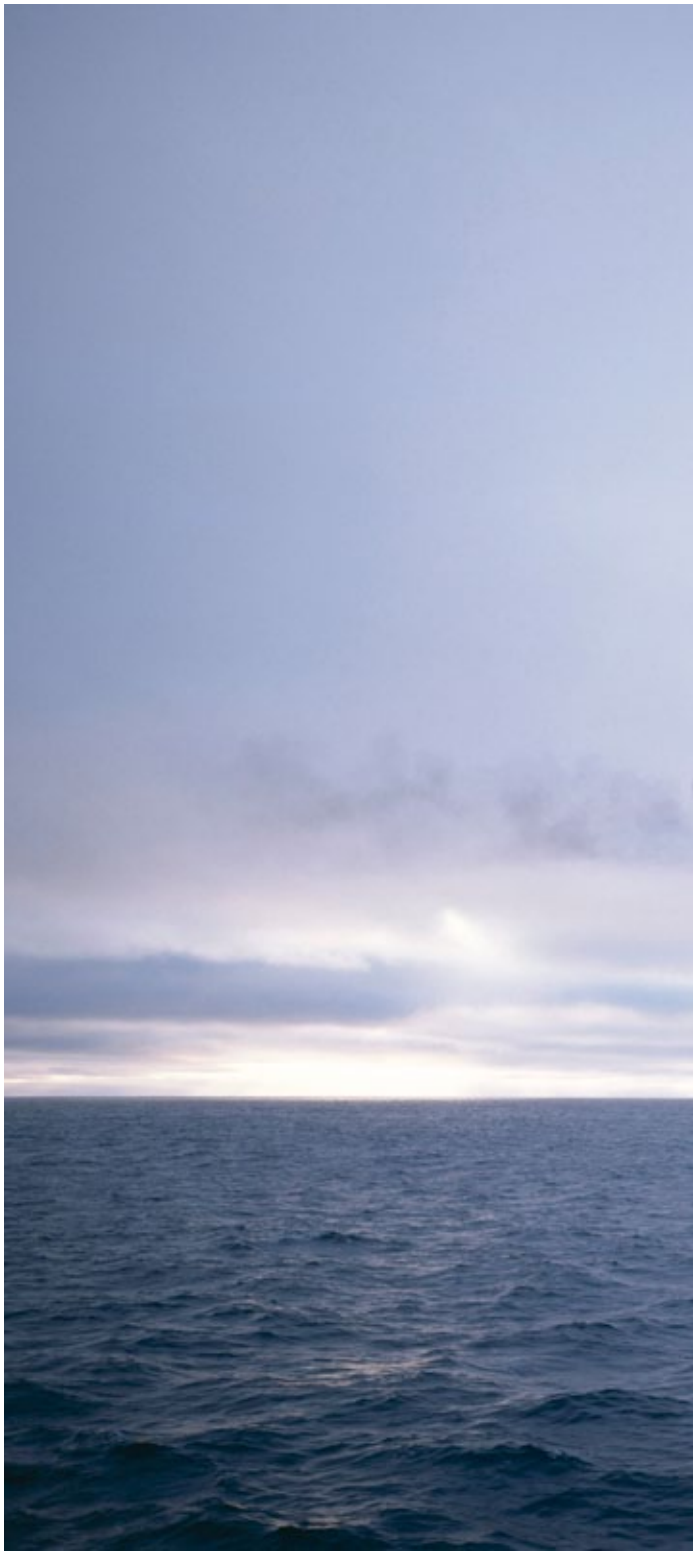
ANTALL MANUELT HÅNDTERTE SAKER

NSM håndterer en lang rekke andre IKT-sikkerhetshendelser på nett. I fjor håndterte vi totalt 5069 saker manuelt. Håndteringen blir ofte gjort ved å varsle nasjonalt eller internasjonalt, foreta manuell analyse av hendelser, be om bistand med mer. Forandringer i hvordan statistikken hentes ut har gjort at noen av tallene fra tidligere år har blitt revidert, men statistikken her er sammenlignbar fra år til år.

helsetilstanden til en pasient ved et sykehus. Dette er informasjon som av ulike grunner bør skjermes for utenforstående. For den enkelte virksomhet og saksbehandler er det trolig utfordrende å ha oversikt og behandle informasjonen riktig. I dag er det lagret store mengder av denne typen data i norske IKT-nettverk, ofte mer enn det virksomhetene selv er kjent med. Det finnes en rekke eksempler både fra Norge og utlandet på at ugradert men sensitiv informasjon har blitt stjålet eller på annen måte kommet på avveie.

Også menneskelige sårbarheter er en utfordring. NSM har ved flere tilfeller sett at sikkerhetsgradert informasjon er lagret eller kommunisert på usikre systemer og internett. Teknologi som setter oss i stand til å overføre enorme mengder informasjon ved hjelp av få klikk, innebærer også en risiko for at mye informasjon kan bli kompromittert som følge av én feil, i verste fall uten at feilen blir oppdaget.

NSM har i løpet av 2014 også sett flere eksempler på utilstrekkelig evne til å håndtere sikkerhetsgradert informasjon. Blant annet har vi sett flere eksempler på at viktige prosesser er blitt hindret av at riktig informasjon ikke er kommet frem til riktig tid.



FAKTA

DATAANGREP MOT OLJE- OG ENERGI-SEKTOREN

I slutten av august varslet Nasjonal sikkerhetsmyndighet en rekke virksomheter innen olje- og energisektoren om forsøk på dataangrep. Da varslingen gikk ut var det avdekket over 50 forsøk på dataangrep mot selskaper og virksomheter i sektoren, og angrepene kom i første rekke i form av eposter med infiserte vedlegg. Dersom vedlegget ble åpnet, kunne bedriftene få skadevare inn i systemene.

ULSTEIN UTSATT FOR DATA-ANGREP

Det norske industrikonsernet Ulstein Group ble i fjor utsatt for dataangrep. Dataangrepet ble oppdaget ved at det var unaturlig trafikk, og det viste seg at stjålne datafiler ble samlet inn, kryptert og deretter sendt ut. Derfor ble det vanskelig å finne ut hva slags informasjon som faktisk ble hentet ut.

NSM har sett flere tilfeller av bevisste lekkasjer av sikkerhetsgradert informasjon de siste årene.

Objektsikkerhet og fysisk sikring

Skjermingsverdige objekter er eiendom som må beskyttes mot spionasje, sabotasje eller terrorhandlinger av hensyn til rikets eller dets alliertes sikkerhet, eller andre vitale nasjonale sikkerhetsinteresser. NSM fører tilsyn med sikringen.

Mye infrastruktur som ikke er klassifisert som skjermingsverdige objekter er også verdt å beskytte av hensyn til sensitiv informasjon den behandler. Dette gjelder for eksempel datahaller og skytjenester. Bruk av skytjenester og datahaller kan være positivt dersom det erstatter dårlig sikrede lokale løsninger. Samtidig kan store datahaller gi økt sårbarhet hvis de ikke har tilstrekkelig redundans og separasjon. Likevel ser vi at datahaller ofte er dårligere sikret enn hva markedsføringen og verdiene tilsier. Det er en særskilt utfordring at myndighetene har liten oversikt over hvilke samfunnsviktige funksjoner som har drift av sine data hos ulike leverandører av datahaller.

Personellsikkerhet

Globalisering gjør det vanskeligere for nasjonale myndigheter å holde oversikt over leverandørkjeder, personell og strømmer av varer og tjenester på tvers av landegrenser. Outsourcing og kompliserte internasjonale selskapsstrukturer gjør det vanskelig å undersøke, godkjenne eller klarere både virksomheter, produkter og personell.

Stadig flere mennesker med utenlandsk tilknytning er ansatt i virksomheter som har befatning med nasjonale verdier, ved at de for eksempel eier eller driver vedlikehold av kritisk infrastruktur eller på annen måte har tilgang til informasjon eller systemer som er viktig for Norge. Det er ikke i seg selv en sårbarhet, men stiller nye krav til hvordan vi beskytter våre verdier. Samtidig har flere nordmenn enn før sitt virke i områder hvor norske myndigheter ikke har oversikt, og hvor risikoen for å bli utsatt for uønsket påvirkning er langt høyere enn i Norge.

Det blir stadig mer krevende å skaffe seg oversikt over bakgrunnen til mennesker som skal behandle sikkerhetsgradert informasjon. Endringer i befolkningens sammensetning, bo- og reisemønster gir flere tilfeller av usikker tilknytning og lojalitet. Det er nå også flere mennesker enn tidligere med tilknytning til stater med interesser i strid med de norske, som har tilgang til sensitiv og sikkerhetsgradert informasjon.

I sum innebærer dette en økt risiko for samfunnet.

BEVISSTE LEKKASJER. NSM har sett flere tilfeller av bevisste lekkasjer av sikkerhetsgradert informasjon de siste årene.

Bevisst kompromittering av gradert informasjon er alvorlig. Slike lekkasjer trenger ikke være gjort med den hensikt å gi en trusselaktør tilgang til informasjonen. Likevel er det grunn til å frykte at informasjonen kan ende opp hos noen andre enn hva som var hensikten. Lekkasjer vil også kunne skade samarbeid med allierte, hvor tillit og fortrolighet er bygget over tid.

Den som velger å lekke gradert informasjon, skjønner ikke alltid alle konsekvensene av at informasjonen blir kjent for uvedkommende. Én bit med gradert informasjon kan være den siste som mangler i et større bilde hos noen som ønsker å ramme oss.

UFORSIKTIGHET OG UTRO TJENERE. Det er trolig store mørketall hva gjelder ubevisst kompromittering av gradert informasjon. I en hektisk hverdag kan det være fristende å improvisere kodespråk i mobiltelefon, men en god analytiker vil raskt resonnere seg frem til det reelle innholdet i samtalen. Tilsvarende gjelder bruk av ugradert epost. Det kan også være lett å forsnakke seg i sosiale situasjoner utenfor arbeidstid.

Sosiale medier har skapt nye arenaer hvor det kan være lett å gi fra seg for mye informasjon for sikkerhetsklarert personell. For eksempel er det mange forsvarsansatte som har delt informasjon om utenlandsoppdrag i sosiale medier uten å ha forvisset seg om at informasjonen trygt kan gjøres tilgjengelig for alle.

Vi vil aldri kunne sikre oss fullstendig mot at noen som er betrodd kritiske oppgaver eller sensitiv informasjon vil misbruke tilliten de er gitt. Dette er ekstra utfordrende når teknologien kan sette én enkelt utro tjener i stand til å volde mer skade enn før.

Sikkerhet i leverandørkjeden

NSM har i løpet av 2014 sett flere eksempler på dataangrep mot underleverandører til større selskaper. I ett tilfelle ble over tusen eposter fra datanettverket til underleverandøren stjålet og sendt ut av datasystemene. En trusselaktør vil som regel velge det svakeste leddet for å få tilgang til datasystemer og sensitiv informasjon. En liten leverandør med lav sikkerhetsbevissthet kan utgjøre en vesentlig sårbarhet for en stor kunde. Ingen av dem trenger noensinne merke at de har vært gjenstand for et angrep. Det er viktig med høyere bevissthet og gode krav til sikkerhet også i små og mellomstore bedrifter.

FAKTA

FLERE UNDERLEVERANDØRER UTSATT FOR DATAANGREP

NSM oppdaget i 2014 flere dataangrep rettet direkte mot underleverandører til store, norske selskaper. I ett tilfelle hadde trusselaktørene tilgang til VPN-innlogginger til flere titalls brukere, og tilgang til samtlige datamaskiner på virksomhetens interne nettverk.

Tiltak_

I løpet av 2014 ble det iverksatt en rekke tiltak for å styrke sikkerheten og redusere sårbarheter i det norske samfunnet. Likevel er det helt avgjørende for en forbedring av sikkerhetstilstanden at arbeidet videreføres på en målbevisst måte og i takt med den teknologiske utviklingen. Forsvarsministeren har bedt NSM om å levere et sikkerhetsfaglig råd i forbindelse med ny langtidsplan for forsvarssektoren. Rådet skal foreligge innen 1. juli 2015, og vil inneholde forslag til tiltak for å styrke arbeidet med sikkerhet på nasjonalt nivå. Uavhengig av dette bør ledere og ansatte i norske virksomheter etter NSMs vurdering særlig legge vekt på å:

- **FORSTÅ SITUASJONSBILDET:** Hva er risikoen for at spionasje, sabotasje, terror eller andre alvorlige hendelser kan ramme virksomheten din? Kan det dere jobber med ha betydning for samfunnsviktige funksjoner utenfor eget ansvarsområde?

- **ERKJENNE RISIKO:** Er virksomheten klar over risikoene, og gjør dere noe med dem? Gjennomføres risikovurderinger?

- **FORSTÅ SÅRBARHETENE:** Er virksomheten din klar over hvor sårbarhetene er, og har dere gjort nok for å redusere eller lukke dem?

- **SKAFFE KOMPETANSE:** Har dere kompetansen dere trenger for å ivareta sikkerheten på en god nok måte? Vet de ansatte hva de skal gjøre for å bidra til en god sikkerhetskultur?

- **GJØRE NOE MED SITUASJONEN:** Har dere iverksatt tiltakene som bør på plass for å redusere risikoen til et akseptabelt nivå?

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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