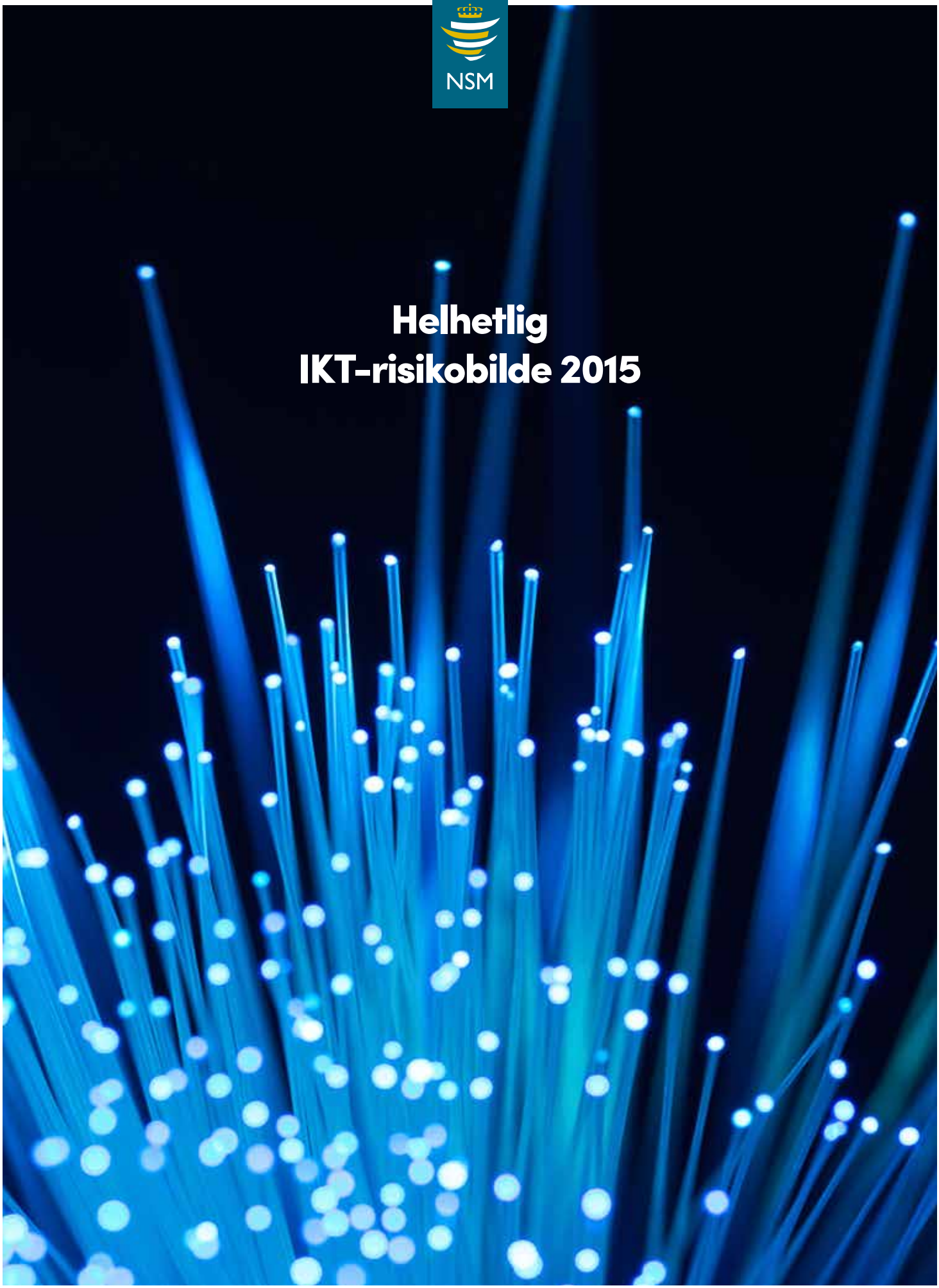
NSM

Helhetlig IKT-risikobilde 2015



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

Innhold

07 Forord
09 1 Sammendrag
013 2 Innledning

017 **3 Teknologiske og samfunnsmessige utviklingstrekk**
017 3.1 Innledning
017 3.2 Stordata
018 3.3 Skytjenester
018 3.4 Bruk ditt eget utstyr
018 3.5 Tingenes internett
019 3.6 På nett hele tiden, enten vi vil eller ikke
019 3.7 Det mørke nettet
019 3.8 IKT i Norge
020 3.9 Perspektiver om fremtiden

023 **4 Verdier og interesser**
023 4.1 Nasjonale og offentlige verdier
025 4.2 Store virksomheter
025 4.3 Små virksomheter / individer

027 **5 Farer og trusler**
027 5.1 Farer
027 5.2 Trusler
028 5.3 Trusselaktører
028 5.3.1 Innsidere, innsideaktører
028 5.3.2 Asosiale individer
028 5.3.3 Hacktivister
028 5.3.4 Kriminelle
029 5.3.5 Etterretningstjenester og andre informasjonssamlere
030 5.3.6 Cyberkrigere og terrorister
030 5.4 Metoder
031 5.4.1 Angrep mot Domenenavnsystemet (DNS)
031 5.4.2 Avanserte vedvarende trusler
031 5.4.3 Defacing
031 5.4.4 Radiokilder
031 5.4.5 Fysisk tyveri og innbrudd, misting og tap
032 5.4.6 Hetsing og utpressing
032 5.4.7 Identitetstyveri
032 5.4.8 Kortsvindel
032 5.4.9 Kriminelle tjenester
033 5.4.10 Løsepengevirus
033 5.4.11 Phishing og Spearphishing
033 5.4.12 Sosial manipulering
033 5.4.13 Tjenestenektangrep
034 5.4.14 Vannhullsangrep
034 5.5 Nasjonalt
035 5.6 Store virksomheter
036 5.7 Små virksomheter / individer

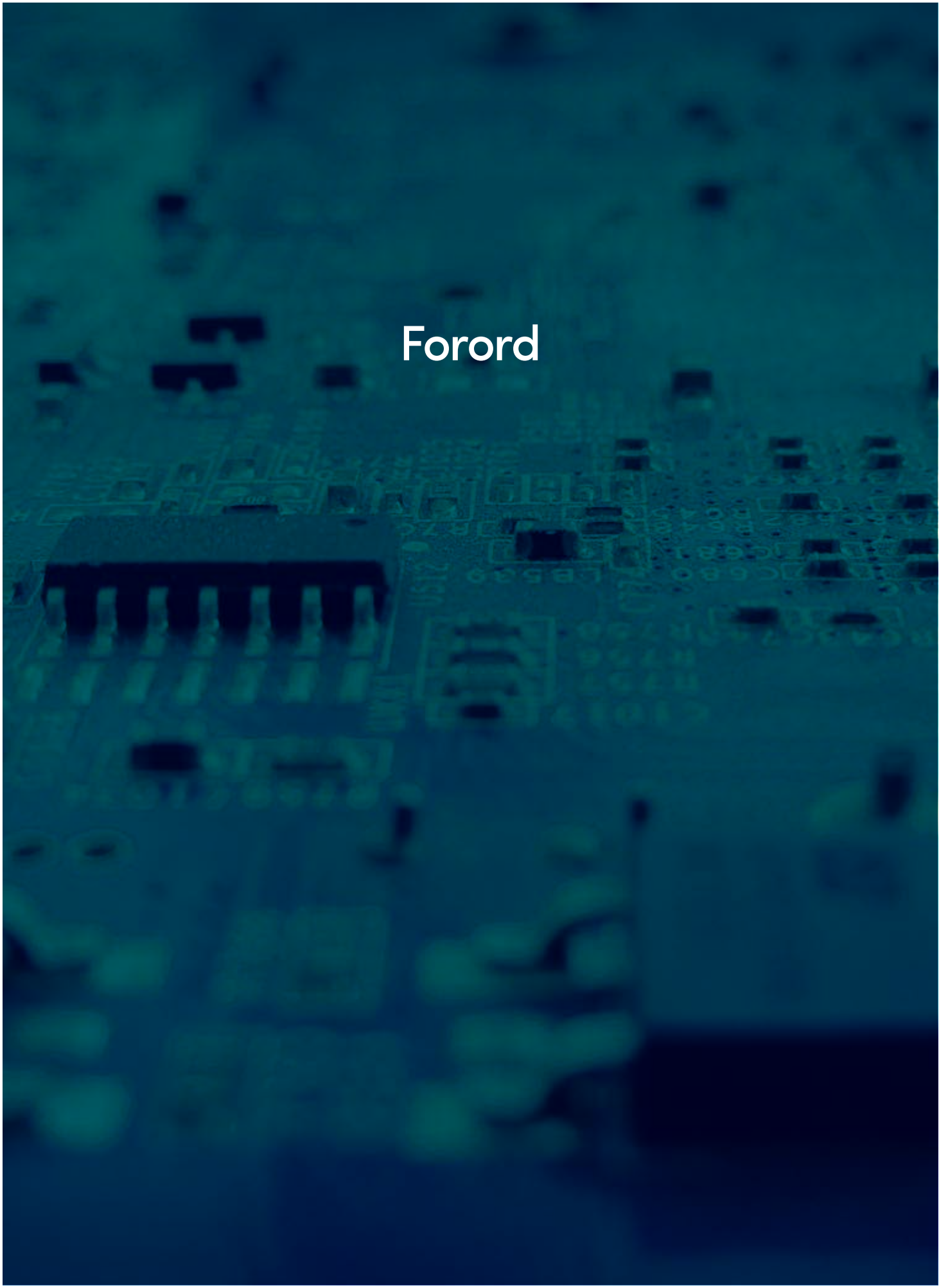
039 **6 Sårbarhetsutfordringer og tiltaksstatus**
039 6.1 Sårbarhetsutfordringer
039 6.1.1 Tekniske sårbarheter
039 6.1.2 Menneskelige sårbarheter
040 6.1.3 Organisatoriske sårbarheter
040 6.2 Nasjonale sårbarhetsutfordringer
040 6.2.1 Kompetanse
040 6.2.2 Organisering, ledelse og koordinering
041 6.2.3 IKT-sikkerhet
043 6.2.4 Behov for akkreditering av privat rådgivning
043 6.2.5 Kunnskap om teknologisk utvikling
043 6.2.6 Særskilt om sårbarheter i utvalgte kritiske infrastrukturer
044 6.3 Store virksomheter
044 6.4 Små virksomheter / individer
045 6.5 Konsekvenser
046 6.6 Tiltaksstatus
046 6.6.1 Roller og ansvar
046 6.6.2 Nasjonale beredskapssystemer
046 6.6.3 Felles europeiske standarder
046 6.6.4 Om ulovlig utstyr i ekomnett
046 6.6.5 Sikring av domenenavn
046 6.6.6 Allvis NOR
047 6.6.7 Håndtering av cyberangrep
047 6.6.8 SON
047 6.6.9 Internasjonalt samarbeid

049 **7 Risikovurdering**
049 7.1 Metodisk grunnlag
049 7.2 Verdier og interesser
049 7.3 Farer, trusler og metoder
049 7.4 Sårbarheter
050 7.5 NSMs vurdering av risikobildet
050 7.5.1 Risikobildet på nasjonalt nivå
051 7.5.2 Risiko for virksomheter og individer
052 7.6 Overordnet vurdering av IKT-risiko

055 **8 Forslag til tiltak og råd**
055 8.1 Nasjonale tiltak, forslag
056 8.2 Råd til store og små virksomheter
056 8.2.1 Den grunnleggende styringen
057 8.2.2 De grunnleggende tiltakene
057 8.2.3 Om nettskyen
058 8.2.4 Om Bruk ditt eget utstyr (BYOD)
058 8.2.5 Om uhell og ulykker
058 8.2.6 Om ansatte som er spesielt utsatt

061 Vedlegg 1 Ordliste
067 Vedlegg 2 Litteratur

Foreord



Norge er et trygt samfunn, men samfunnet er ikke uten sårbarheter. Utviklingen i Norge og verden for øvrig skjer hurtig og er stadig mer uforutsigbar. Dette gjør at vi må ha sterkere fokus på de sikkerhetsmessige sårbarhetene i samfunnet slik at vesentlige utfordringer kan møtes. Samtidig må det erkjennes at all risiko ikke kan elimineres, og at samfunnet må leve med en viss restrisiko.

Fremdyrking av kunnskap og kontinuerlig optimalisering av IKT-bruken vil være strategisk avgjørende for Norge som samfunn i tiden som kommer. Dette krever ressurser og omstilling på mange områder.

Sikkerhetsarbeidet har i for stor grad vært preget av usammenhengende og suboptimale organisatoriske og tekniske løsninger. Dette blir mer utfordrende desto mer nettverksorientert samfunnet blir. Sikkerhet som en grunnleggende forutsetning vil legge til rette for det motsatte, nemlig årvåkenhet, helhetsblikk, sammenheng, klarhet, gjenbruk og langsiktig besparelse.

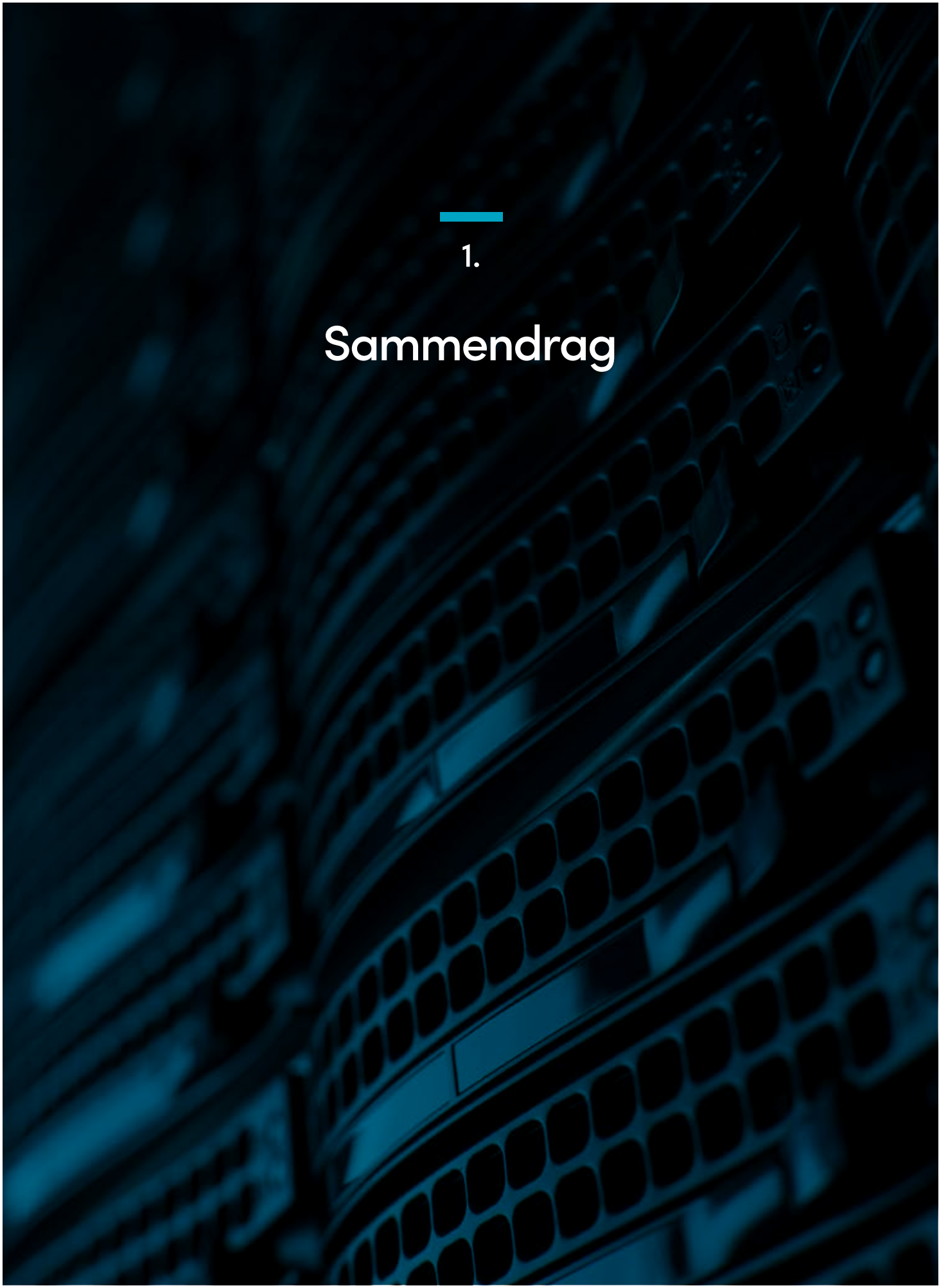
I arbeidet med denne rapporten har Nasjonal sikkerhetsmyndighet (NSM) mottatt innspill fra Cyberforsvaret, Datatilsynet, Direktoratet for forvaltning og IKT, Direktoratet for samfunnssikkerhet og beredskap, Finanstilsynet, Helse- og omsorgsdepartementet, KRIPOS, Nasjonal kommunikasjonsmyndighet, NorSIS, Norges vassdrags og energidirektorat, Olje- og energidepartementet, Politiets sikkerhetstjeneste, UNINETT CERT og UNINETT Norid AS. Alle takkes for innspill.

Det er dessuten avholdt møte med sekretariatet til Lysne-utvalget for gjensidig informasjon. De to rapportene koordineres ikke. Lysne-utvalget leverer sin rapport senere i år. Imidlertid er Helhetlig IKT-risikobilde 2015 koordinert med NSMs sikkerhetsfaglige råd til forsvarsministeren og justis- og beredskapsministeren som ble overlevert 10. september.

Rapporten Helhetlig IKT-risikobilde vil bli fornyet med jevne mellomrom. En ambisjon for kommende utgaver blir å involvere ulike virksomheter og fagpersoner i enda større grad enn det som har vært mulig i år. NSM ønsker å utvikle arbeidsprosessen og utvide tverrfaglig samarbeid. Flere innspill til denne rapporten peker mot en ambisjon om å utvikle et helhetlig tverrsektorielt produkt om IKT-risiko som grunnlag for felles politikkutforming. Dette vil kreve omfattende analysesamarbeid mellom en rekke virksomheter.

NSM er gjort kjent med et arbeid som konsulentselskapet BDO nylig har gjennomført for Justis- og beredskapsdepartementet med hensyn til målemetrikk for IKT-sikkerhet[1]. Ettersom dette er samtidige prosesser, har tidsfaktoren ikke gjort det mulig å inkludere resultater fra disse i dette dokumentet. BDO påpeker at de metodiske utfordringene med å produsere et nasjonalt IKT-risikobilde ut fra måleindikatorer er betydelige. Det er NSMs vurdering at dette vil kreve et betydelig utviklingsarbeid og kan ha organisatoriske og samvirkemessige konsekvenser som er tid- og ressurskrevende. Imidlertid kan potensialet for tallmessig å dokumentere trendutviklinger over tid rettferdiggjøre slike kostnader.

[1] BDO; Nasjonale indikatorer for IKT-sikkerhet, 2015.



1.

Sammendrag

Rapporten omfatter utviklingstrekk, utfordringer og mulige tiltak av betydning for statssikkerhet, samfunnssikkerhet og individsikkerhet. Rapporten har et vidt nedslagsfelt ved å omhandle utfordringer både for tilsiktede og utilsiktede uønskede hendelser knyttet til IKT-utstyr og internett.

NSM har sett flere eksempler på vellykkede datainnbrudd der angriperne har fått tilgang til virksomhetskritisk informasjon, og at forretningshemmeligheter, kursdrivende eller annen sensitiv informasjon har kommet på avveier. Skadevirkningene kan variere fra sak til sak, men de alvorligste konsekvensene skjer i et langsiktig perspektiv hvor virksomhetene etter tap av immaterielle verdier mister sin konkurranseevne og eksistensgrunnlag.

For offentlige virksomheter kan skadevirkningene være tap av tillit til det offentliges digitale løsninger på en slik måte at det påvirker samfunnets evne til å ta ut ytterligere gevinster ved modernisering og digitalisering.

Konsekvensene av vellykkede datainnbrudd kan også medføre tap av personopplysninger og annen sensitiv informasjon. Risikoen for mulig tap av virksomhetens omdømme er også til stede. Nedetid på nettsider eller IKT-tjenester er også en konsekvens for mange virksomheter, slik for eksempel flere norske banker opplevde i 2014.

Nedetid i kritiske samfunnsfunksjoner som f.eks. helsevesen, energi- og vannforsyning kan ha alvorlige konsekvenser og medføre skade på innbyggernes liv og helse.

Gitt de verdier som står på spill, en økende og mer sofistikert trussel, og gitt betydelige sårbarheter i det norske samfunnet, konkluderer NSM slik om det helhetlige IKT-risikobildet:

NSMs overordnede vurdering av IKT-risikobildet er at det er stor risiko forbundet med bruk av IKT. Dette gjelder på alle nivåer i samfunnet. Alle er mål for IKT-angrep.

Det er stor risiko forbundet med at store og små virksomheter ikke tar i bruk grunnleggende tiltak for å sikre sine IKT-systemer. Sårbarhetene er den dimensjonen i risikobildet vi alle kan gjøre noe med. De samme sårbarhetene observeres gjentatte ganger og avslører at IKT-sikkerhetsarbeidet er mangelfullt styrt.

Norske statlige og private virksomheter har betydelige verdier som er ettertraktet for trusselaktørene. Trusselaktørene gjør gode vurderinger av hva som er informasjon av høy verdi. Konsekvensen av mangelfull IKT-sikkerhet er at det kan tapes store verdier.

Uønskede handlinger via IKT og internett fortsetter å øke i antall og kompleksitet. Imidlertid er det registrert færre alvorlige hendelser enn før. Vi har indikasjoner som tyder på at dette skyldes at dataangrepene har blitt mer avanserte og at det er betydelig læringsevne hos trusselaktørene.

Kunnskapsnivået og tilgang på fagkompetanse er for lavt, i et spenn fra den vanlige IKT-bruker til spesialister i hendelseshåndtering. Dette hemmer evnen til å gjennomføre gode IKT-sikkerhetstiltak. Dette vil sannsynligvis også føre til at det nasjonalt ikke vil finnes tilstrekkelig fagkompetanse til å håndtere større IKT-angrep. I tillegg er det en utfordring å følge med på konsekvensene av den teknologiske utviklingen for IKT-sikkerhetsområdet. Mangelfull rapportering av alvorlige IKT-hendelser vil svekke evne til forbedring og læring innen forebyggende IKT-sikkerhet.

Det er behov for å få etablerte strukturer til å virke bedre gjennom å videreutvikle samarbeidsarenaer og gode samarbeidsmekanismer, slik at prosesser rundt politikkutforming, forebyggende IKT-sikkerhet og hendelseshåndtering forbedres. Samarbeid mellom ulike offentlige og private aktører kan med fordel utvikles videre. Utvikling, forvaltning, og drift av offentlige IKT-løsninger kan samordnes bedre.

Manglende fellesløsninger for IKT-systemer for sensitiv, lavgradert og høygradert informasjon kan

føre til dårlig informasjonssikkerhet og kan være kritisk i en krisesituasjon.

Ugradert elektronisk kommunikasjon blir i liten grad blir kryptert. Dette senker terskelen for vellykket avlytting og sensitiv informasjon kan kompromitteres.

Tilbud om gode tjenester, som for eksempel inntrengningstesting av datasystemer, sertifiseringsordninger eller akkrediteringsordninger, blir ikke tilstrekkelig utviklet. Dette kan føre til utilstrekkelig koordinering av politikkutforming, forebyggende tiltak og krisehåndtering.

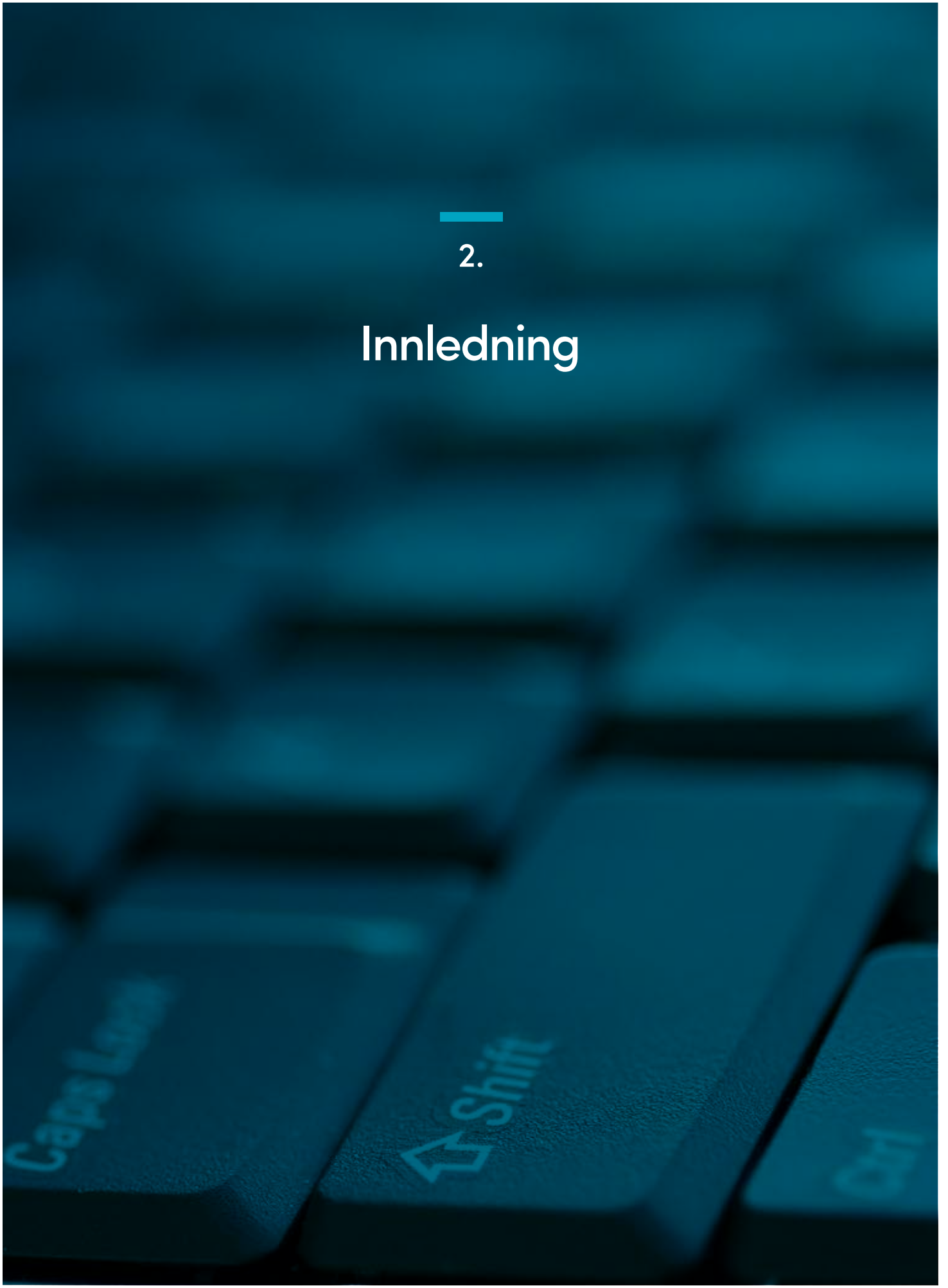
Sensorkapasiteten i varslingssystemet VDI er ikke tilstrekkelig utviklet. Utviklingen av truslene setter den nasjonale evnen til å håndtere IKT-hendelser under betydelig press og reduserer evnen til både å oppdage og håndtere disse. Det er risiko for at alvorlige IKT-angrep blir oppdaget for sent og ikke blir håndtert på en tilfredsstillende måte.

For å redusere risikoen er det behov for en omfattende nasjonal satsning på IKT-sikkerhet i årene som kommer.

NSM har i sikkerhetsfaglig råd foreslått 72 tiltak for å forbedre sikkerhetsarbeidet. En rekke av disse er relevante for IKT-sikkerhet og er gjentatt i Helhetlig IKT-sikkerhetsbilde. Det foreslås tiltak for å forbedre kunnskapssituasjonen, forbedre nasjonal styring og samarbeid, forbedre forebyggende sikkerhet og forbedre evnen til hendelseshåndtering.

NSM gjentar også sitt råd om å gjennomføre 10 (4+6) grunnleggende sikkerhetstiltak, som vil forhindre 90 % av alle dataangrep. 100 % av de alvorlige dataangrepene NSM har sett de siste 24 månedene hadde blitt stoppet dersom den rammede virksomheten hadde gjennomført 4 av de enkle tiltakene som NSM anbefaler.

Bakerst i rapporten finnes vedlegg med ordliste og litteratur.



2.

Innledning

Helhetlig IKT-risikobilde 2015 er utarbeidet av NSM etter oppdrag fra Justis - og beredskapsdepartementet (JD) og Forsvarsdepartementet (FD). Formålet med rapporten er å tilføre mer kunnskap som øker bevisstheten rundt behovet for IKT-sikkerhet og behovet for å vurdere informasjonens verdi.

NSM skriver denne rapporten for første gang, og har derfor et behov for å bruke rapporten til å produsere en basis som fremtidige tilsvarende rapporter kan utvikles videre fra. Formatet for fremtidige vurderinger av helhetlig IKT-risikobilde vil bli drøftet med oppdragsgiverne, men vil bygge videre på årets rapport.

Målgruppen for rapporten er bred, og den skal være tilgjengelig for alle. Begrepet helhetlig er i samråd med oppdragsgiver tolket slik at rapporten skal ha relevans i et spenn fra individ til samfunn og skal omhandle både uhellshendelser og bevisste uønskede handlinger. Rapporten omfatter IKT-risiko som kan ramme verdier på forskjellige samfunnsmessige nivåer; internasjonalt, nasjonalt, store virksomheter, små og mellomstore virksomheter og i visse fall på individnivå.

Rapporten er samordnet med NSMs sikkerhetsfaglige råd til justis- og beredskapsministeren og forsvarsministeren. Sikkerhetsfaglig råd omhandler blant annet personellsikkerhet, informasjonssikkerhet og objektsikkerhet, som er tre søyler i NSMs virksomhet. Innen informasjonssikkerhet er NSM bedt om å ha et særlig fokus på IKT-sikkerhet. Helhetlig IKT-risikobilde tar for seg den ene søylen – informasjonssikkerhet – og går mer i dybden på IKT-sikkerhet enn det NSMs sikkerhetsfaglige råd gjør.

Betegnelser som IT-sikkerhet, datasikkerhet, digital sikkerhet og cybersikkerhet er i vanlig bruk. Ulike betegnelser brukes i forskjellige bransjer og profesjoner. Begrepene er, med nyanseforskjeller, å betrakte som synonymer. I denne rapporten brukes IKT-sikkerhet spesifikt om informasjonstekno-logiske og administrative sikringstiltak. Når det gjelder begreper som digitale angrep, cyberangrep, IKT-angrep, IT-angrep, informasjonsoperasjoner med videre, brukes dataangrep og cyberangrep som synonymer. Ulike fagretninger legger ulike betydninger i betegnelsen dataangrep og cyberangrep. Når det gjelder betegnelser som digitale trusler, cybertrusler, IKT-trusler, IT-trusler, informasjonstrusler med videre, brukes cybertrusler.

NSMs sikkerhetsfaglige råd foreslår å erstatte IKT-sikkerhet som begrep med cybersikkerhet. Dette er på grunn av den stadig økende bruken av begrepet cybersikkerhet både internasjonalt og nasjonalt, og for å sikre at Norge har en terminologi som vil være sammenlignbar også i internasjonale sammenhenger.

Tilsvarende type teknologi og IKT-systemer brukes i de fleste land, og sårbarheter som er avdekket og utnyttet i andre land kan lett utnyttes også i Norge. En trusselaktør som ønsker å utføre digitale angrep kan virtuelt krysse tradisjonelle grenser, og internett er i så måte grenseløst.

Gjengse begreper innen informasjonssikkerhet gjelder også for IKT-sikkerhet, slik som:

- **Konfidensialitet**, at informasjon kun er tilgjengelig for autoriserte brukere
- **Integritet**, at informasjonen er fullstendig, nøyaktig og gyldig, det vil si ikke er endret på utilsiktet eller ondsinnet vis
- **Tilgjengelighet**, at autorisert bruker har tilgang til informasjonen til rett tid

Men også:

- **Autentisering**, at bruker av et IKT-system har rett identitet
- **Autorisasjon**, at bruker av IKT-system er gitt rett tilgang
- **Ikke-benekting**, at handlinger i IKT-systemer er logget og ikke kan tilbakevises

Ingen enkeltvirksomhet eller sektor sitter med noen form for totaloversikt over IKT-risikobildet. Bare i fellesskap kan kunnskap om den teknologiske utviklingen, sårbarheter, trusler og tiltak samles i et hele. Denne rapporten er derfor basert på innspill fra flere statlige og private virksomheter.

Bruken av IKT-utstyr og internett vokser i et høyt tempo. Stadig flere kategorier av IKT-utstyr utnytter mulighetene internett gir og antall sammenkoplinger stiger. Ett resultat av internetts økende strategiske betydning er at samfunnet både effektiviseres og endres. Et annet resultat er at informasjon og data som sirkulerer med større tydelighet fremstår som en kritisk ressurs, ikke bare med tanke på konfidensialitet, men også med tanke på tilgjengelighet og integritet. En nødvendighet for alle brukere av IKT-utstyr og internett er å vurdere hva som bør beskyttes og hva slags risikonivå som kan aksepteres.

Hendelser kan inntreffe raskt og uten forvarsel. I den digitale verden går utviklingen spesielt raskt. Trusselaktørene benytter mer avanserte metoder enn tidligere, og risiko- og sårbarhetsbildet er blitt mer komplekst. Dette utfordrer samfunnets evne til å reagere med kraft og hurtighet når et angrep skjer. En mer bevisst holdning til hvor stor risiko samfunnet er villig til å akseptere er nødvendig for å kunne prioritere ressurser hensiktsmessig. De tverrsektorielle avhengighetene øker, blant annet som følge av digitaliseringen i samfunnet. Datanettverk binder de fleste sektorene sammen. Dette innebærer økte muligheter og behov for samvirke i både offentlig og privat sektor, men også nye sikkerhetsutfordringer.

3.

Teknologiske og samfunnsmessige utviklingstrekk

3.1 INNLEDNING

Informasjonssamfunnet er i rask fremvekst og nye typer sikkerhetsutfordringer oppstår. Det kan forventes at informasjonssamfunnet vil utvikle nye strukturer for fordeling av makt og rikdom, og vil gi nye forutsetninger for sosial samhandling. Produksjon og fordeling av kunnskap, samt kontroll over informasjon vil utgjøre en ny konfliktarena. Informasjonssamfunnets fremvekst preges av en rekke såkalte megatrender som samvirker med den, for eksempel:

- **Globalisering** og utvikling av globale standarder, for eksempel design av operativsystemer på datamaskiner og økende gjensidige avhengigheter på teknologiske, økonomiske og sosiale områder.
- **Svekkelse av nasjonalstatens posisjon** gjør at mennesker, kapital og kunnskap har lettere for å flytte seg. Dette vil forskyve global fordeling av makt og rikdom. Nasjonalstaten strever tradisjonelt mot å maksimere sin uavhengighet, men svekkes av globaliseringen.
- **Befolkningsvekst og demografisk endring**, herunder urbanisering, flytting mellom land og endringer i aldersfordeling i befolkningen. Ungdom konsentrerer seg til geografiske områder med tilbud om utdanning, spennende jobber og muligheter for kommersialisering av forsknings- og utviklingsresultater.
- **Teknologivekst og innovasjon** er satt i system, som følge av utviklingen av utdannings- og forskningsinstitusjoner, særlig i løpet av de siste tiårene. Dette driver frem raske og omfattende teknologiske endringer, som ofte kan medføre uforutsette sosiale endringer.
- Endring i globalt miljø som følge av **klimaendring** kan bli en kraftig driver bak trendene nevnt ovenfor og en motivator for teknologiutvikling.

Større endringer av samfunnet er ofte basert i grunnleggende teknologigjennombrudd og går gjerne svært raskt. Nye teknologier brukes til et utall av samfunnsnyttige oppgaver, blant annet i form av konkurransedyktig, høyproduktiv industri og nye markedsplasser, men også i form av nye sosiale samhandlingsmønstre. Eksempelvis har mer effektiv kommunikasjon mellom samfunnsaktører bidratt til å øke tempo og volum i samfunnets produksjon.

Ofte klarer ikke etablerte strukturer og regelverk å henge med i utviklingen, slik at det skapes fundamentale sikkerhetsmessige utfordringer innenfor alle dimensjoner av begrepet sikkerhet, innen både «safety» og «security». Parallelt med samfunnets økte avhengighet av internett og mer komplekse IKT-systemer, skapes det også nye muligheter for potensielle trusselaktører til å utvikle angrepsmåter mot verdiskapningen, også gjennom IKT-angrep. Trusselaktørene tilpasser angrepsmetoder og er mer avanserte enn tidligere, og risikobildet er blitt mer komplekst. Erfaring tilsier at nye teknologier modifiseres for ondsinnede formål[2]. Det finnes allerede bekymringer rundt såkalte autonome våpen[3] og at våpen kan hackes.

Det regnes med at de utviklingstrekk og trender som dominerer handlingsmiljøet for IKT-sikkerhet i dag, vil fortsette å gjøre det i de nærmeste årene.

3.2 STORDATA

Stordata (Big Data) vil si utvikling av datakraft som muliggjør datainnsamling i et omfang som gjør det mulig å sammenstille og analysere et stort informasjonsvolum raskt eller i sanntid. Digital datalagring erstatter analog lagring på papir og muliggjør vesentlig større datasett. Kostnaden for å lagre og bearbeide store informasjonsmengder blir lavere. Fordelene med dette i forhold til produktivitetsvekst og evne til å klare nye oppgaver er åpenbare. Mange formål knyttet til denne kapasiteten er legitime. Teknologien kan brukes til å gjennomføre omfattende kartlegging av gitte personer, grupper av personer, virksomheter eller hele befolkninger. Stordata har sin styrke innen prediktive analyser, det vil si å forutse hendelser eller menneskelige handlinger, for eksempel hva du kommer til å kjøpe eller hvem som kommer til å utføre en kriminell handling. Imidlertid kan dette lett misbrukes. Ved analyse av store datamengder, vil enkeltopplysninger som hver for seg ikke er sensitive eller skjermingsverdige kunne systematiseres og sammenstilles til sensitiv informasjon. Mye informasjon er allerede lett tilgjengelig, og massiv registrering og sammenstilling av informa-

[2] Typisk innen 50 år etter de grunnleggende oppfinnelsene eller oppdagelsene, særlig med hensyn til å gjøre nye teknologier om til våpen. Jf. at kjernefysisk, biologisk og kjemisk kunnskap relativt raskt ble grunnlag for våpen.

[3] Droner og andre våpen som ikke krever menneskelig styring.

sjon vil sette personvernet ytterligere under press og åpne for målrettet kriminalitet eller fremmed etterretning, ved at det blir enda lettere å utnytte informasjonen.

3.3 SKYTJENESTER

En av de viktigste trendene innen leveranse av IKT-tjenester er utviklingen av skytjenester (Cloud computing) med fleksibel tilgang. Det utvikles metoder og strukturer for å lagre, prosessere og behandle store mengder data på steder der det finnes eller etableres ledig kapasitet. Det finnes store effektiviseringsgevinster og kostnadsbesparelser i dette. Det etableres derfor et marked for datalagringssentraler og webhotell. Det vil i økende grad bli en utfordring å holde informasjon på nasjonale hender eller innenfor en virksomhet når dette er ønskelig. Tilgjengelighet, integritet og konfidensialitet er vanskelig å garantere idet data behandles og lagres utenfor virksomhetens lokaler. Ca. 30 % av norske næringslivsaktører, med overvekt av de store, benytter seg av skytjenester[4].

Det er en rekke sikkerhetsmessige utfordringer knyttet til bruk av skytjenester både nasjonalt og internasjonalt. Det er viktig at man har gjort de nødvendige sikkerhetsmessige vurderingene med tanke på konfidensialiteten, integriteten og tilgjengeligheten til tjenestene og informasjonen som man ønsker å sette ut. Ved bruk av internasjonale skytjenester (såkalt offshoring) er det spesielt viktig å være oppmerksom på de begrensningene som vil ligge i norske myndigheters mulighet for kontroll av leverandøren, da disse ikke nødvendigvis er underlagt norsk regelverk og krav til sikkerhet. I tillegg vil det kunne være usikkerhet knyttet til hvilken tilgang utenlandske myndigheter, eller andre aktører, vil kunne få til informasjon i skyen. Dette er forhold som kan være utfordrende å regulere i kontrakt med leverandøren.

3.4 BRUK DITT EGET UTSTYR [5]

Utviklingen av mobilt IKT-utstyr muliggjør en økende sammenblanding mellom arbeid og fritid. Dette skaper fleksibiliteter som kan være til fordel både for arbeidsgiver og arbeidstaker. Imidlertid fører dette i økende grad til at medarbeidere tar med seg privat, mobilt IKT-utstyr på jobb, og kobler dette til virksomhetens systemer med eller uten arbeidsgivers samtykke. Det vil si at utstyret havner på baksiden av brannmurer og andre sikkerhetstiltak. Da privat utstyr oftest ikke er underlagt virksomhetens sikkerhetsregime, finnes det lite som stopper import til virksomhetens systemer av eventuell skadelig programvare som har kommet inn på utstyret gjennom bruk utenfor virksomheten. Videre kan mobile IKT-enheter lett bli misbrukt, mistet eller stjålet. Da kan de enten brukes av uvedkommende som nøkkel til å komme inn på virksomhetens systemer, eller det kan være at virksomhetskritisk eller konfidensiell informasjon faktisk er lagret på dem, bevisst eller av vanvare. Mobilt IKT-utstyr har innebygget kamera og mikrofon som kan registrere og lagre alt som foregår rundt utstyret og kan misbrukes av uvedkommende.

3.5 TINGENES INTERNETT [6]

Volumet på kommunikasjon mellom gjenstander er sterkt økende og vil overskygge volumet av kommunikasjon mellom mennesker. Hensikten med dette er velment, for eksempel å forenkle vedlikehold eller raskt og automatisk registrere og varsle feil eller ulykker. I noen tilfeller er hensikten å gjøre det mulig å laste ned programvare for å fornye en tjeneste. Når gjenstandene knyttes til internett, åpner det også en mulighet for at de kan infiltreres og manipuleres av andre enn de rettmessige brukerne. En mulig bieffekt kan være at enhver gjenstand er en potensiell personovervåker. Det er en økende trend at stadig flere bruksgjenstander blir utstyrt med sensorer og mikroprosessorer og kan kommunisere aktivt over internett: hvitevarer, brunevarer, biler, trafikkskilt, overvåkningskameraer, reklameplakater og betalingsterminaler, for å nevne noen eksempler. Proteser, pacemakere og til og med klær og andre kroppsnære gjenstander kan bli utstyrt med slik teknologi. Dette skaper potensielle personvern- og sikkerhetsutfordringer. Det finnes eksempler på at hackere har klart å ta over kontrollen av biler i fart[7].

Ting som kobles til internett er ofte utviklet av produsenter som ikke har erfaring og bakgrunn innen IKT. Mange av enhetene er sårbare, enten

[4] OECD Digital Economy Outlook 2015.

[5] Bring your own device, BYOD.

[6] Internet of (all) things.

[7] Nettmagasinet Wired.com, 21. juli 2015, sitert i Digi.no, 22. juli 2015.

grunnet direkte svakheter i programvaren, men også grunnet feilkonfigurering som for eksempel bruk av standardpassord. Dette gjør disse tingene godt egnet som springbrett videre inn i annen teknisk infrastruktur.

3.6 PÅ NETT HELE TIDEN, ENTEN VI VIL ELLER IKKE

Utviklingen av bærbart IKT-utstyr har endret menneskelig samhandling. Fra disse enhetene kan man få tak i et verdensomspennende bibliotek av informasjon og kontakte eller bli kontaktet av hvem som helst når som helst. Dette er en arena for samarbeid og nettverksbygging uten tidligere sidestykke, med stort sosialt og økonomisk potensial. Dette utstyret blir med overalt, til og med inn på steder der man er mest opptatt av privatliv, som møterom, stue, soverom og baderom. Det er vanlig at de har mikrofon og minst ett kamera som kan ta stillbilder og HD video. De brukes som vekkerklokker og til å overvåke varighet og kvalitet på søvn. Det siste kan kreve at mikrofonen er aktivert. Man risikerer å kringkaste sitt eget liv med lyd og HD video uten å vite det, fra steder man i utgangspunktet ikke ønsker å gjøre dette.

Utvikling av teknologi som egner seg for overvåking av og datainnsamling om personer er i rask utvikling. Det finnes utstyr som er i stand til å skille fra hverandre og ta opp alle samtaler i et forsamlingslokale, slik at de kan analyseres enkeltvis i løpet av kort tid etterpå. Personer kan lokaliseres og følges fra sted til sted på overvåkingskameraer, ved hjelp av signaler fra mobiltelefoner, og ved bruk av bankkort, elektroniske billetter og elektroniske nøkkelsystemer. Trusselaktører behøver ikke nødvendigvis selv eie kameraene som brukes, men andres kamerasystemer kan kompromitteres og misbrukes, f.eks. via internett. Innsamlet informasjon kan lagres og brukes til å analysere handlingsmønstre. Overvåkingen skjer internasjonalt, og differensierer i liten grad mellom venner og fiender. Den er upersonlig, den har stort volum og er billig pr. «mål». Den lagrer alt slik at det kan hentes frem ved behov. Uønsket reklame på mobiltelefon blir utløst ved at man for eksempel beveger seg forbi en bestemt butikk eller reiser med et bestemt transportmiddel, ofte i sammenheng med at man har surfet på bestemte sider på internett. Personopplysninger er blitt salgsvare[8].

Droner er nå tilgjengelig på det åpne forbrukermarkedet. I nettbutikker får man disse for en relativt billig penge. Droner kan filme inn vinduer i områder og rom der det tidligere ikke var innsyn. Under brannen i Lærdal i 2014 var det så mange av dem at de kunne utgjøre en risiko for redningsarbeidet og det ble innført flyforbud i området.

3.7 DET MØRKE NETTET

Det mørke nettet (Dark net, Deep web) består av skjulte og anonymiserte nettverk på internett[9]. The Onion Router (TOR) er et eksempel på en tjeneste som tilbyr et anonymisert nett. Tjenesten er basert på lagvis kryptering, ikke bare av innhold, men av metadata som identiteten til sender og mottaker. Nettverkene er ikke ulovlige å bruke og kan benyttes til en rekke legitime formål, for eksempel fortrolig kommunikasjon, kryptert informasjonslagring eller anonyme informasjonssøk. Dette kan ivareta personvern og andre sikkerhetshensyn på nettet. Det er imidlertid en utfordring at det mørke nettet også er en nærmest perfekt arena for kriminalitet. Markedsplassen Silk Road, som ble stengt i fjor, men som er relansert, er den mest kjente plassen for omsetting av narkotika og andre ulovlige varer som våpen, og brukes også som base for dataangrep. Det er normalt liten sannsynlighet for at kriminell aktivitet i det mørke nettet blir avslørt, da det er ressurskrevende å etterforske bruken av anonymiserende nettverk.

Bruk av det mørke nettet er en trend som motvirker de muligheter for overvåking og analyse som bruken av stordata og andre sterke trender står for. Det finnes her, som ellers og i forenklede termer, en potensiell motsetning mellom samfunnsmessige behov for sikkerhet og individuelle behov for frihet.

3.8 IKT I NORGE

Norge er et av verdens mest digitaliserte land (nr. 5 av 143)[10]. Industrielle prosesser styres av datamaskiner. Offentlig og privat saksbehandling foregår på PCer. Samfunnets produksjon er i stor grad koblet opp mot internett, ofte på permanent basis.

93 % av norske foretak med minst 10 ansatte

[8] CYFOR innspill.

[9] NorSIS og KRIPOS innspill.

[10] World Economic Forum/ Cornell University/INSEAD (eds.): The Global Information Technology Report 2015.

hadde internettilknytning i 2014. For foretak med 10-19 ansatte er tallet 90 %, og 98 % for foretak med minst 100 ansatte[11]. I 2013 hadde 55 % av norske private foretak utført elektronisk handel[12]. I 2014 kjøpte 29 % av norske private foretak en eller flere nettskytjenester[13].

Samme år brukte 42,8 % av statlige virksomheter en eller flere nettskytjenester[14]. I 2015 var antallet økt til 53,3 %. Nettskytjenester omfatter her kontorstøtteverktøy, webanalyseverktøy, økonomisystemer, webplattformer, prosjektverktøy, databaser, lagringsverktøy, virtuelle servere, virtuelle møterom, applikasjonsserver, back-up, kommunikasjon internt og eksternt, utviklingsplattform, driftsplattform og annet.

Norge kommer godt ut sammenliknet med andre land når det gjelder å holde internett «rent». Vi kjøper nye datamaskiner med stadig bedre sikkerhetsløsninger og bruker oppdaterte operativsystemer. 6,8 % av datamaskinene i Norge var infisert av skadevare i fjerde kvartal 2014, mot 15,9 % som verdensgjennomsnitt[15].

3.9 PERSPEKTIVER OM FREMTIDEN

I dag er det en banal påstand å si at teknologien er «i rask vekst». Alle og enhver kan se dette i sin hverdag. Imidlertid kan det av og til være på sin plass å tallfeste dette, for å visualisere hvor fort det går. I 1965 fremsatte Gordon Moore, som er en av gründerne bak Intel[16], en påstand som siden er blitt kjent som Moores lov. Hans påstand var at antallet transistorer på integrerte kretser fordobles omtrent hvert andre år. Fra 1958, da integrerte kretser ble oppfunnet, frem til 2011, økte antallet fra null til 2,6 milliarder transistorer i én krets, og veksten fortsetter. Denne trenden er til en viss grad overførbar til annen teknologiutvikling, og kan knyttes til systematiseringen av kunnskapsutviklingen som er nevnt ovenfor.

Videre utvikling av silikonbaserte teknologier for integrerte kretser begynner å nå grensen for hva som er fysisk mulig. På relativt kort sikt vil disse kunne bli avløst av eksempelvis karbonbaserte teknologier som nanorør og grafén[17]. På kort sikt kan dette føre til en forsinkelse i Moores lov, mens teknologien modnes. På noe lengre sikt kan det føre til vesentlige økninger i datakraft og prosesseringshastighet. I EUs 7. rammeprogram for forskning og teknologisk utvikling[18] er utvikling av graféntеknologi ett av flaggskipsprosjektene. Grunnleggende teknologiske utfordringer er løst og det finnes fungerende prototyper.

På lengre sikt vil såkalt Quantum Computing, kvantedatamaskiner basert på kvantemekanikk, utvikles. Det kan bli praktisk gjennomførbart å lage en datamaskin med mye raskere prosessorhastighet enn mer konvensjonell teknologi på samme tidspunkt. Tidspunktet for dette kan være få tiår unna, eller enda nærmere. Dette kan for eksempel gjøre mye av dagens krypteringsteknologi avleggs, da dekryptering vil kunne foregå mye raskere. Når dette skjer, vil man også kunne dekryptere seg *bakover i tid*, slik at tidligere kryptert kommunikasjon, f.eks. for 20 år siden, kan avleses, med de følger det kan ha.

En annen retning innen teknologiutviklingen gjelder forholdet mellom IKT og biologi. Det finnes i dag eksempler på datamaskiner som er basert på DNA-lignende kjemi eller er bygd opp av reelle nerveceller. Slike maskiner kan for eksempel tenkes operert inn i mennesker som erstatning for skadet nervevev, til å styre proteser på en bedre måte enn i dag, eller til å utvide hjernekapasiteten med en enhet som har fotografisk hukommelse og kommunikasjonsfunksjoner. Som del av EUs 7. rammeprogram er det under utvikling en stoffskiftedrevet strømforsyning[19]. Både EU[20] og USA har satt i gang store prosjekter for å kartlegge den menneskelige hjernen i egenskap av å ligne en datamaskin. I relativt overskuelig fremtid kan det bli utviklet datamaskiner med høykapasitet kunstig intelligens. Dette tidspunktet kalles ofte for *teknologisk singularitet*[21], da det vanskelig kan forutsies hvilke konsekvenser det vil få.

[11] Statistisk sentralbyrå (SSB), Statistikkbanken: Bruk av IKT i næringslivet, Tabell 09874: Private foretak. internettilknytning etter beste teknologi, etter mengd sysselsette (prosent).

[12] SSB, Statistikkbanken: Bruk av IKT i næringslivet, Tabell 09881: Private føretak. Elektronisk handel, etter mengd sysselsette (prosent).

[13] SSB, Statistikkbanken: Bruk av IKT i næringslivet, Tabell 10641: Private føretak. Kjøper nettskytenester, etter teneste og mengd sysselsette (present).

[14] SSB, Statistikkbanken: Bruk av IKT i staten, Tabell 10609: Statlige virksomheter. Bruk av nettskytjenester, etter type og sysselsettingsgruppe (prosent).

[15] Microsoft Security Intelligence Report Volume 18, Regional Threat Assessment, 2014, s. 618.

[16] Pionerbedrift i utvikling av integrerte kretser.

[17] Karbonmolekyl (karbonfilm) med tykkelse på ett atom.

[18] European Union, Future & Emerging Technologies (FET) FP7 Projects Compendium 2007-2013, December 2013.

[19] European Union, Future & Emerging Technologies (FET) ibid.

[20] Flaggskipsprosjekt, European Union, Future & Emerging Technologies (FET) ibid.

[21] Sort hull, hendelseshorisont.

4.

Verdier og interesser

Staten og annen offentlig myndighet, norske statlige og private virksomheter, samt enkeltpersoner, har en rekke verdier[22] som er attraktive for ulike trusselaktører. Mange av disse verdiene har sårbarheter i seg som gjør at verdiene kan angripes ved hjelp av IKT. Den grunnleggende verdien er trygghet, som videre kan deles i:

- Liv og (folke)helse
- Økonomi, kapital, penger, produksjonsmidler, kunnskapskapital
- Økologi, livsmiljø
- Suverenitet, selvstendighet[23], det demokratiske styresettet
- Navn og rykte, tillit, sosial kapital, identitet

Av disse verdiene kan man videre avlede konkrete informasjoner, objekter og symbolske verdier som er viktige for å realisere disse verdiene. Noen viktige avledninger er:

- Privatliv og personlige opplysninger
- Forretningshemmeligheter og intellektuell eiendom og kapital
- Informasjon som er sikkerhetsgradert
- Objekter av historisk, kulturell og identitetsskapende verdi
- Produksjonsanlegg og -utstyr
- Kritiske og viktige enkeltobjekter
- Kritiske infrastrukturer
- Politiske og administrative styringsorganer
- Territoriell integritet

I større eller mindre grad kan disse verdiene (og deres konkrete avledninger av dem) nås av trusselaktører via internett og stjeles, skades, gjøres utilgjengelige eller i visse fall ødelegges.

4.1 NASJONALE OG OFFENTLIGE VERDIER

Både offentlige myndigheter og en del offentlige og private forretningsforetak forvalter verdier som er av nasjonal betydning, eksempelvis:

- Politiske beslutningsprosesser med betydning for Norges selvstendighet eller posisjon i en forhandlings- eller konfliktsituasjon.
- Statlig virksomhet innen utenriks-, forsvars-, justis- og beredskapssektorene som er sentrale for rikets sikkerhet, og innehar sentrale verdier, blant annet militære forhold.
- Etterretnings-, overvåknings- og sikkerhetstjenestenes kunnskaper og metoder.
- Forsvarsindustri og andre teknologibedrifter som har informasjon, kunnskap og teknologi som er attraktive. Informasjon om ny teknologi kan kopieres og selges videre. Tap av kontroll over slike verdier kan svekke forsvarsevnen og industriell konkurransekraft.
- Informasjon om sivil og militær infrastruktur er attraktiv informasjon for andre stater. Informasjon om evner og kapasiteter, kommunikasjonslinjer og -systemer kan eksponere sårbarheter som kan utnyttes.
- Gjennom deltakelse i ulike allianser og internasjonalt samarbeid besitter Norge informasjon om andre land og deres kapasiteter og sårbarheter. Dette er verdifull informasjon for andre stater.

Målgruppene for de siste 12 måneders angrep har vært sentrale departementer, høyteknologisk industri, Forsvaret og forsvarsindustri.

Vi ser ingen empirisk forskjell på noen av de ovennevnte målgruppene når det gjelder hvem som er mest utsatt, hvis man legger til grunn fokus fra trusselaktør og antallet sårbarheter som utnyttes i sektorene. Graden av vellykkede angrep er stort sett den samme i disse sektorene.

Infrastrukturutvalget[24] definerte kritisk infrastruktur som «de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse». Utvalget nevnte konkret elektrisk kraft, elektronisk kommunikasjon, vann og avløp, transport, olje og gass, samt satellittbasert infrastruktur. Kritisk infrastruktur understøtter leveranse av et stort antall kritiske og viktige samfunnsfunksjoner. Eksempler er forsvar, lov og orden, finansvesen, vareforsyning, samfunnsledelse, energiforsyning, telekommunikasjon, transport, bygg og anlegg. Alle disse sektorene er støttet av IKT-systemer og kan i varierende grad få nedsatt funksjonalitet uten fungerende infrastruktur.

[22] Se ordliste.

[23] I sikkerhetsloven: rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser.

[24] NOU 2006:6 Når sikkerheten er viktigst, s. 16.

Noen eksempler med hensyn til kritiske infrastrukturer og kritiske samfunnsfunksjoner:

Finansiell stabilitet er en verdi som forvaltes på virksomhetsnivå, men som har betydning for hele det norske samfunnet, og som derfor kan anses som en nasjonal verdi. Finanstilsynet ser effektive, robuste og stabile betalingssystemer som grunnleggende for finansiell stabilitet, og så vel statlige som private virksomheter og enkeltindivider er alle avhengige av at betalingsformidlingen fungerer[25].

Satellittbaserte tjenester for navigasjon, kommunikasjon og observasjon er viktige verdier for Norge. Romvirksomhet har blitt en forutsetning for effektiv og sikker samfunnsdrift, og for å følge opp prioriterte politiske målsetninger i nordområdene og i klima- og miljøpolitikken[26]. Rombasert infrastruktur har strategisk betydning og nasjonal kontroll og egenevne er viktig for å sikre nasjonale interesser.

I første kvartal 2015 var Norge den største **gassleverandøren** til Vest-Europa, trolig på grunn av EUs politikk for å gjøre seg mindre avhengige av russisk naturgass[27]. Fra en norsk finanspolitisk synsvinkel er dette en inntektskilde. For EU er dette sikkerhetspolitikk[28]. For virksomhetene som leverer gass, kan det ha alvorlige, men stort sett håndterbare økonomiske konsekvenser om leveransen svikter. For kunden, et alliert samfunn, kan flere samfunnsfunksjoner bli rammet ved bortfall av kritiske energileveranser. Norge kan muligens tåle virksomhetens økonomiske tap, men kan likevel bli berørt av de nedsatte samfunnsfunksjonene i det allierte samfunnet. Imidlertid kan Norges omdømme som leverandør og alliert bli svekket.

Industrielle styringssystemer (SCADA[29]) er viktige elementer i de fleste kritiske infrastrukturer. De tillater sentralisert styring med høyere kvalitet og med redusert bemanning. Dagens driftskontrollsystemer er svært komplekse, og det forventes i årene som kommer at kompleksiteten øker. For å utnytte driftskontrollsystemenes muligheter fullt ut, kobles gjerne driftskontrollsystemene sammen med andre IKT-systemer for å utnytte informasjonen fra driftskontrollsystemene til planlegging, analyse og reparasjonsberedskap i større grad enn før. Mange SCADA-systemer ble imidlertid designet for å stå og å jobbe lokalt. I ettertid fant man det hensiktsmessig å koble disse systemene til internett, og introduserte dermed en angrepsvektor disse systemene aldri var designet for å motstå. Det er derfor særlig koblinger mot internett som skaper sårbarheter. Også indirekte koblinger kan skape problemer. Eksempelvis var systemene som skadevaren Stuxnet[30] hadde som mål, ikke koblet til internett. Likevel kom skadevaren seg fra internett-koblede systemer og videre inn til SCADA-

[25] Finanstilsynet, Risiko- og sårbarhetsanalyse (ROS) 2014, april 2015.

[26] Meld. St. 32 (2012-2013), Mellom himmel og jord: Norsk romvirksomhet for næring og nytte.

[27] Dagens Næringsliv: Norge er igjen Vest-Europas største gassleverandør, publisert 2015-05-24. NTB, statistikk fra Gassco.

[28] EU European Energy Security Strategy, COM(2014) 330 final.

[29] Se ordliste.

[30] Se nedenfor.

systemene via minnepinner.

Innovasjon er et vesentlig element i samfunnsutviklingen etter oljealderen. Norge vil i vesentlig grad leve av den **intellektuelle kapital** som utvikles hos universiteter, forskningsinstitusjoner og fremtidsrettede bedrifter. Denne kapitalen vil være lagret på IKT-systemer. Den vil også kunne stjeles fra IKT-systemer dersom IKT-sikkerheten ikke er tilstrekkelig.

4.2 STORE VIRKSOMHETER

Informasjon om virksomheters produkter, produksjon, innsatsfaktorer, kundelister og ansatte er verdier som det er viktig å beskytte. Tap av slik forretningssensitiv informasjon kan gi økonomiske tap, men kan også ha betydning utover den enkelte virksomhet og kan få samfunnsmessig betydning. Eksempelvis vil tap av informasjon om teknologi eller strategier innen forsvarsindustri kunne ha betydning for rikets sikkerhet. Utilstrekkelig fokus på sikkerhet kan også føre til tap av kontrakter og eventuelt teknologisk forsprang, som kan få stor økonomisk betydning for næringslivet, samt føre til tap av anseelse og tillit overfor kunder og offentlighet.

Særlig høyteknologisk industri og energiprodusenter har informasjon som er attraktiv for trusselaktører[31]. Både produksjonsmåter og -kapasitet er interessant for andre å vite noe om. Også mindre produsenter, som underleverandører til større aktører, er interessante mål for ulike trusselaktører.

4.3 SMÅ VIRKSOMHETER / INDIVIDER

Blant de mest sentrale verdiene for små virksomheter og enkeltindivider er trygghet og tillit. Sikkerhetsmessig og følelsesmessig trygghet omfatter lov og orden, stabilitet og beskyttelse, ikke bare i den fysiske verden men også i den digitale. Som enkeltindivider ønsker vi at de verdiene vi har i digitale systemer skal være beskyttet. Dette gjelder eksempelvis elektronisk identitet, personlige opplysninger, privatliv, forhold til myndigheter og til andre virksomheter og personer, og ikke minst vår egen bankkonto.

Små virksomheter har gjerne få bein å stå på, og har verdiene konsentrert om disse. Rykte i markedet, markedsposisjon, kontantbeholdning, bankkontoer og kredittverdighet hører til blant verdier som kan påvirkes negativt via internett.

Digitaliseringen av offentlig sektor skal bidra til å forenkle samhandlingen mellom det offentlige og innbyggere og næringsliv[32]. Offentlige tjenester blir dermed mer tilgjengelige for brukerne, og det spares tid og ressurser for brukerne og forvaltningen. Informasjonssikkerhet blir imidlertid viktigere og det kan bli flere informasjonssikkerhetsutfordringer, blant annet at pålitelighet, troverdighet, tilgjengelighet og tillit sikres.

[31] Politiets sikkerhetstjeneste (PST): Åpen trusselvurdering 2015.

[32] Innspill fra DIFI.

5.

Farer og trusler

5.1 FARER

Her brukes begrepene fare og trussel. Begrepet fare beskriver en utilsiktet, uønsket hendelse, et ulykkestilfelle. Begrepet trussel beskriver en tilsiktet (alså en villet), uønsket handling, oftest ondsinnet.

EU-organet European Union Agency for Network and Information Security (ENISA)[33] har delt årsaker til fare- og trusselsituasjoner med IKT inn i følgende kategorier; naturlige hendelser (14 %), menneskelige feil (19 %), systemfeil (61 %) og ondsinnede handlinger (6 %).

Som alle andre kritiske infrastrukturer er IKT-systemer utsatt for naturkatastrofer og ulykker, som flom eller brann. I de fleste tilfellene vil effektene av dette være begrenset til lokale feil og avbrudd. Dette kan ha store konsekvenser for enkeltvirksomheter. Tendensen til opprettelse av store datasentre med mye konsentrert informasjon i forbindelse med stordatatrenden, kan imidlertid medføre store samfunnsmessige konsekvenser dersom datasentrene blir utsatt for fysiske ulykker.

De aller fleste sikkerhetsrelaterte hendelsene på IKT-systemer har elementer av menneskelige feil i seg. Menneskelig feil kan være involvert i opptil 95 % av alle hendelser[34]. Andre kilder[35] oppgir 57 % menneskelige feil. Slike feil kan variere fra en administrator som gjør feil ved installasjoner og oppdateringer til brukere som lar seg lure av sosial manipulering. Imidlertid finnes det også mange eksempler på IKT-løsninger som for så vidt er teknisk vellykkede, men hvor personvern eller andre sikkerhetshensyn ikke er ivaretatt. Eksempler på dette er velment opprettelse av personregistre for forskningsformål, men uten tillatelse eller sikring.

Der man ofte snakker om «systemsikkerhet», mener man vanligvis *produktsikkerhet*, altså IKT-teknisk sikkerhet ved produkter som implementeres i et system. Disse kan inneholde implementasjons- og designfeil, de kan konfigureres, installeres og brukes på måter som utgjør en sikkerhetsrisiko. Mulige sårbarheter kan finnes i maskinvare, operativsystemer og applikasjoner. Også lagrings- og nettverksteknologi er utsatt.

IKT-systemer er kompliserte, og alle opplever systemfeil i sin hverdag. Det oppstår fysiske feil i komponenter, og logiske feil florerer i programvare. Dette fyller mesteparten av IKT-administratorens hverdag. Verst blir dette når store offentlige IKT-satsinger mislykkes, kanskje fordi brukerens og systemutviklerens ambisjoner på den ene siden og de faktiske mulighetene på den andre siden ikke harmonerer. Det finnes nok av godt kjente eksempler på IKT-prosjekter som har vokst bruker og utvikler over hodet. NSMs erfaringer blant annet fra tilsyn og forskning[36] viser at tekniske systemer ikke løser sosiale, kulturelle eller organisatoriske utfordringer, men snarere at disse må være løst for at en teknisk løsning skal kunne fungere.

5.2 TRUSLER

Ondsinnede handlinger (trusler) er de scenariene som vies mest oppmerksomhet, også i denne rapporten. Det er forskjell på å bli utsatt for et uhell og å bli utsatt for et angrep.

Datanettverksoperasjoner er avdekket mot norsk forsvars-, sikkerhets- og beredskapssektor, politiske prosesser, norsk kritisk infrastruktur og enkeltvirksomheter eksempelvis innen petroleum, kraft, shipping og tele.

Alvorlige trusler retter seg mot flere sentrale samfunnsområder. Dette gjelder blant annet Forsvaret, departementene, utenrikstjenesten, EOS-tjenestene[37] og politiet. Det gjelder også viktige infrastruktur- og produksjonsområder som telekommunikasjon, kraftforsyning og petroleum. Trusler retter seg også mot nyhetsmedier og interesseorganisasjoner, næringslivet i sin alminnelighet og enkeltpersoner.

Målsettingen kan være å skaffe seg informasjon som stats- og forretningshemmeligheter, informasjon om forskningsresultater og teknologiske nyvinninger, og informasjon om strategier og planer. Den kan også være å skade en motpart ved å påvirke, redusere eller ødelegge funksjonalitet i produksjonssystemer, eller å stjele privat informasjon fra enkeltpersoner.

Nettverksoperasjoner blir stadig mer målrettede og teknisk avanserte. Det er statlige aktører som står bak den mest alvorlige trusselen. Russland og Kina er i følge Etterretningstjenesten de mest aktive aktørene bak nettverksbaserte etterretningsoperasjoner rettet mot Norge[38]. Listen over aktører som kan

[33] ENISA, Annual Incident reports 2013.

[34] IBM Security Services 2014, Cyber Security Intelligence Index.

[35] Center for Media, Data and Society, Data Breaches in Europe: Reported breaches of Compromised Personal Records in Europe, 2005-2014 (2014), sitert i ENISA Threat landscape 2014.

[36] FFI-rapport 2014/00948 Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet. DSB viser dessuten til: Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quartely, 34(3), 523- 548. Og Dhillon, G.. & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal. 16(3), 293-314.

[37] EOS-tjenestene er en felles betegnelse for de statlige etterretnings-, overvåknings- og sikkerhetstjenestene Etterretningstjenesten, Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets sikkerhetsavdeling (FSA).

[38] Etterretningstjenestens vurdering, FOKUS 2015.

tenkes å ha målsettinger som nevnt ovenfor er lang og spenner fra overbeviste aktivister og terrorister til organiserte kriminelle, konkurrenter og stater.

5.3 TRUSSELAKTØRER

5.3.1 INNSIDERE, INNSIDEAKTØRER

Mennesker som prøver å gjøre skade fra innsiden av en virksomhet utgjør et stort trusselpotensial. Årsakene kan være mange, for eksempel sterk misnøye eller vinning. Dersom sikkerhetsrammeverk og sikkerhetssystemer ikke har tatt hensyn til innsideproblematikk, kan innsideren omgå alle sikkerhetssystemer. Erfaringer fra tilsyn tilsier at virksomheter generelt har en mindre gjennomtenkt tilnærming til bruk av privilegier og tilgangskontroll i IKT-systemer enn tilgangskontroll i form av fysiske sikringstiltak.

5.3.2 ASOSIALE INDIVIDER

Blant asosiale individer på nett finner man vandaler som gjør skadeverk eller annen ugagn for moro skyld eller for å oppnå status i spesielle miljøer. Blant disse er såkalte nett-troll, ofte anonyme, som er ute etter å mobbe individer, og da gjerne individer som har gjort seg bemerket i offentligheten. Målet er ofte profilerte virksomheter eller personer, men også andre.

5.3.3 HACKTIVISTER

Hacktivister er en betegnelse på politiske aktivister som gjennom forskjellige typer nettangrep søker oppmerksomhet om sitt eget budskap. Angrepene er oftest tjenestenektangrep eller defacingangrep[39], og forekommer relativt ofte. Hacktivisten er mest interessert i kortsiktig synlighet og anerkjennelse. Tjenestenektangrep[40] mot politiske motstandere, endring av nettsider og lekkasjer av sensitiv informasjon er eksempler på angrepstyper. Denne type aktivitet er i vekst og NSM vurderer at det kan forventes å øke ytterligere. Aktiviteten er oftest av forstyrrende karakter.

5.3.4 KRIMINELLE

KRIPOS, Næringslivets sikkerhetsråd og NorSIS[41] peker alle på digital kriminalitet som en vesentlig og tiltakende sikkerhetsutfordring for samfunnet. Det samme gjør et stort antall utenlandske/internasjonale rapporter[42].

Selv om internettkriminalitet utgjør en liten del av den totale økonomien, er de faktiske pengesummene involvert enorme og i vekst. På global basis kan samfunnskostnaden målt i penger tentativt være mellom 375 og 575 milliarder amerikanske dollar. I Norge kan kostnaden utgjøre 0,64 % av BNP, som er sammenlignbart med USA og Kina. Dette utgjør ca. 3,2 milliarder amerikanske dollar eller ca. 19 milliarder norske kroner (i 2014)[43]. Det er grunn til å ta forbehold om tapenes størrelse, men de kan være betydelige.

Internett forenkler og effektiviserer en rekke eksisterende kriminelle virksomheter og skaper rom for nye. Det er enklere å integrere kriminell virksomhet både vertikalt og horisontalt med dimensjoner som rekruttering, logistikk og kontroll. Aktiv bruk av internett gjør det enklere for trusselaktører å etablere og drive grenseoverskridende, eventuelt globale, kriminelle organisasjoner på tvers av landegrenser. Det skapes fysisk avstand mellom utøver og offer, slik at utøveren lettere kan skjule egen identitet og aktivitet, og slik at offeret ikke nødvendigvis oppfatter at han eller hun er offer. Potensielle ofre kan identifiseres systematisk og det er mulig å rette målrettede angrep mot dem. Det kan etableres nye og kamuflerte markeder for pengespill, nettsvindel, narkotika, prostitusjon, menneskehandel, pornografi og barneporno, utpressing, forfalskninger, heleri (blant annet gjennom internettauksjoner), fildeling, hvitvasking (blant annet gjennom virtuelle valutaer som Bitcoins), illegale pengeoverføringer og andre illegale transaksjoner, miljøkriminalitet (handel med truede arter) falske eller stjålne identiteter, våpen og intellektuell eiendom (kunnskap), med mer.

Cyberkriminelle nettverk er i vekst og mange

[39] Se nedenfor.

[40] Se nedenfor.

[41] KRIPOS, Den organiserte kriminaliteten i Norge, trender og utfordringer 2015, Næringslivets sikkerhetsråd, Mørketallsundersøkelsen 2014 og NorSIS, Trusler og trender 2015.

[42] F.eks. Verizon Data breach investigation report for 2014 og 2015; Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, juni 2014; Center for Strategic and International Studies, The Economic Impact of Cybercrime and Cyber Espionage, 2013.

[43] Også referert i NSRs Mørketallsundersøkelse 2014.

opererer som hvilke som helst andre forretningsnettverk. Denne typen kriminelle har klare «forretningsmål», de vet hva slags informasjon de leter etter og hvordan de skal få tak i denne. Mange sender rekognoseringsskadevare for å finne ut hva slags sikkerhetsteknologi som er benyttet, slik at de kan målrette angrepene sine og være sikre på at skadevaren vil fungere etter hensikten[44].

Lite av dette utgjør noen større allmenn utfordring for samfunnssikkerheten, så lenge omfanget er som det er. Virksomheter og personer kan imidlertid rammes hardt, og av og til stå overfor eksistensielle utfordringer som for eksempel konkurs. Det er svært sannsynlig at hacking mot bedrifter og enkeltpersoner blir vanligere ettersom skadelig programvare blir lettere tilgjengelig. Det er svært sannsynlig at norske banker vil utsettes for omfattende hackerforsøk, der profesjonelle aktører står bak. De siste 12 måneder har NSM sett at fokus har vært på banktrojanere, løsepengevirus og identitetstyveri.

Det synes å være en trend at det har blitt mindre organisert vinningskriminalitet de siste årene, samtidig som IKT-kriminalitet øker[45].

5.3.5 ETTERRETNINGSTJENESTER OG ANDRE INFORMASJONSSAMLERE

På verdensbasis utgjør hendelser relatert til cyberspionasje i underkant av 1 % av de registrerte hendelsene som har med cyberkriminalitet å gjøre, men 22 % av de hendelsene hvor angrepet er vellykket[46].

Det kan tenkes at den økonomiske kostnaden for cyberspionasje på verdensbasis svært tentativt utgjør i overkant av 100 milliarder amerikanske dollar årlig, jf. tall ovenfor med hensyn til kriminalitet. Her er det store forbehold, med tanke på metodiske utfordringer og at det trolig er store mørketall. Norges økonomiske og teknologiske nivå tilsier at den reelle kostnaden kan være betydelig. Indirekte kostnader, for eksempel reparasjon av skader forårsaket av spionasjen, kan mangedoble kostnadene.

NSMs egne erfaringer, dokumentert gjennom flere års rapporter om sikkerhetstilstanden, indikerer en økende trend med hensyn til cyberspionasje, særlig fra og med 2007 og i akselererende grad de to siste årene. De mest kraftfulle vedvarende trusler vi ser på nettet (Advanced Persistent Threats – APT) dreier seg hovedsakelig om spionasje. Det antas at betydelige mengder informasjon stjeles på denne måten.

Etterretningsvirksomhet kan forekomme både i offentlig og privat regi eller i kombinasjon av disse. Digital industrispionasje er et økende fenomen, og kan like gjerne utføres av konkurrerende virksomheter som fremmede stater. Enkelte aktører innenfor internasjonal industri og næringsliv har dedikerte offensive ressurser, og bruker avanserte teknikker for å skaffe seg fordeler i forbindelse med anbud og forhandlinger om store kontrakter. Flere stater bruker sine etterretningstjenester til å søke etter høyteknologi og kunnskap i Norge, samt ramme Norge og andre land gjennom cyberangrep. Slik aktivitet kan knyttes til disse statenes sikkerhetsmessige og økonomiske interesser. I flere land understøtter etterretningstjenester landenes industri og næringsliv. Statlige aktører har særlig sterk evne til å utføre aktivitet med høy grad av kompleksitet og med et langsiktig perspektiv. Deres aktivitet er meget vanskelig å beskytte seg mot, og effektive mottiltak vil kreve en koordinert nasjonal innsats. Statlige aktører er en gruppe med særlig sterk evne til å utføre trusselaktivitet på internett. I sin årlige trusselvurdering for 2015 trekker Politiets sikkerhetstjeneste (PST) frem Russland og Kina som aktører med stor kapasitet.

Selv om en stor og kanskje økende andel av cyberspionasjen kan være økonomisk motivert, må det regnes med at en betydelig andel er sikkerhetspolitisk eller maktpolitisk motivert, og derfor i begrenset grad kan regnes som en økonomisk samfunnskostnad. Dette bidrar også til usikkerhet med hensyn til tallfestingen ovenfor. Fremmede etterretningstjenester forsøker også å påvirke og undergrave norske politiske prosesser der Norge

[44] CISCO 2014 Annual Security Report.

[45] KRIPOS Trendrapport 2015.

[46] Verizon 2014 ibid.

og den fremmede staten er uenige. Dette inkluderer forsøk på å påvirke norske sikkerhetspolitiske beslutninger i sin favør.

Reklamebransjen regnes ikke som en etterretningsaktør. Bransjen, i samarbeid med leverandører av IKT-tjenester, samler imidlertid inn så store mengder informasjon om individer og virksomheter via søkemotorer, sosiale nettverk, og annet at denne informasjonen frister etterretningstjenestene. Reklamebransjen kan være, eller kan bli, en bevisst eller ubevisst kilde til etterretning.

5.3.6 CYBERKRIGERE OG TERRORISTER

Utvikling av avanserte cybervåpen krever betydelig kompetanse og store økonomiske ressurser. Flere nasjonalstater har iverksatt programmer for å utvikle slike våpen. Cybervåpen er i rivende utvikling og utgjør en ny kapabilitet, og anvendes stadig mer målbevisst og effektivt av stater i internasjonale konflikter. Det har etter hvert utviklet seg betydelig innsikt med hensyn til ødeleggelsespotensialet forbundet med cybervåpen.

En særskilt kategori ekstreme aktivister er terrorister. Disse må antas å ha høyere villighet til å begå alvorlig skadeverk og ødeleggelse, men til nå har de vist liten evne eller vilje til å utføre terrorhandlinger på internett. Terrorister bruker imidlertid nettet til propaganda og planleggingsformål, herunder å innhente informasjon om mulige terrormål.

Det er ikke avdekket alvorlige angrep siste 12 måneder som har hatt til hensikt å ta ned konkrete tjenester. De alvorlige angrepene som er avdekket har hatt til hensikt å stjele informasjon og det har vært et mål i seg selv fra trusselaktør å ikke bli oppdaget.

5.4 METODER

Datanettverksbaserte operasjoner gjør informasjonsinnsamling enklere og kan ofte være mer kosteffektive og involvere mindre risiko sammenlignet med menneskebasert etterretning med bruk av kilder og kontakter. Noen ganger kan nettverksbaserte operasjoner være den eneste muligheten fordi trusselaktøren ikke har klart å etablere kilder eller andre støttespillere på innsiden av målet. Nettverksbasert informasjonsinnhenting kan gjøre det lettere å finne personellsikkerhetsmessige sårbarheter, som igjen kan utnyttes for å innhente ytterligere informasjon.

Det utvikles trusler som utnytter brukernes tillit til systemer, applikasjoner, menneskene og virksomhetene de kjenner. Det sendes eposter som tilsynelatende kommer fra velkjente selskaper, men som inneholder link til ondsinnede nettsider, og tredjeparts mobilapplikasjoner lanseres med skadevare og lastes ned fra populære online markedsplasser. I tillegg utnytter innsidere sine tilganger til informasjon til å stjele intellektuell eiendom fra arbeidsgivere. Cisco går så langt som å si at en ikke kan stole på noen ting i cyberverdenen. Det er en viktig påminnelse.

Det har i tillegg skjedd en stor teknologisk utvikling de siste ti årene. Mens det tidligere ble utført enkle angrep som forårsaket begrenset skade, gjennomføres det nå sofistikerte angrep som kan forårsake betydelig skade for virksomheten som blir angrepet[47].

Tidsfaktoren kan være kritisk ved dataangrep[48]. I 60 % av tilfellene er angriper i stand til å kompromittere en organisasjon i løpet av noen minutter. Skadevare brukt i dataangrep sprer seg fra et offer til et annet innen 24 timer. Over 40 % av sekundærangrepene skjer innen mindre enn en time.

Trusselaktørens fremgangsmåte ved alvorlige dataangrep kan deles inn i ulike faser. Dette kan illustreres av Cyber Kill Chain, som er en beskrivelse av syv faser som kan benyttes i avanserte dataangrep[49]. Det presiseres at ikke alle angrep trenger å benytte alle stegene. De syv fasene er:

1. Rekognosering: Angriper velger ut et offer og finner svakheter ved hjelp av personlige og profesjonelle websider samt sosiale medier. De ser spesifikt etter informasjon som kan hjelpe dem til å konstruere tillitsvekkende eposter med link

[47] Cisco 2014 ibid. Cisco er en ledende nettverksleverandør.

[48] Verizon 2015 ibid.

[49] Lockheed Martin.

til websider trusselaktør kontrollerer.
2. Våpenkonstruksjon: Bygging av ondsinnet kode i vedlegg, som sendes via epost, sosiale medier e.l.
3. Levering: Leverer ondsinnet kode ved hjelp av sosiale medier eller epost til en ansatt.
4. Utnyttelse: Den ansatte åpner filen og skadevaren blir eksponert.
5. Installering: Ondsinnet skadevare installeres på klienten.
6. Kommando og kontroll: Angriper tar kontroll over systemet.
7. Tiltak på målet: Angriper kan finne og få adgang til kritiske data.

5.4.1 ANGREP MOT DOMENENAVNSYSTEMET (DNS) [50]

Et mulig scenario er et massivt tjenestenektangrep mot navnetjenesten .no og/eller infrastrukturen til norske nettleverandører med den hensikt å gjøre norske domenenavn og tjenestene knyttet til dem utilgjengelige. Dette er sammenlignbart med å gjøre telefonkatalogen utilgjengelig for brukerne. Det er også mulig å gi falske svar til en bruker når denne søker et domenenavn. Dette er sammenlignbart med at det ligger et falskt navn på et telefonnummer. Hensikten kan være å sende brukeren til et nettsted som trusselaktøren kontrollerer, og få vedkommende til å legge igjen verdifull informasjon. Eventuelt kan noen endre data for enkeltdomener, enten for å gjøre tjenester utilgjengelige, eller for å lede oppslag videre til falske tjenester[51]. Angrep mot DNS forekommer.

5.4.2 AVANSERTE VEDVARENDE TRUSLER

Avanserte vedvarende trusler (Advanced Persistent Threats, APT) er vedvarende og målrettede angrep på systemer med formål å etablere bakdører, plante og spre skadevare og hente ut fortrolig informasjon. Angriperen er gjerne ressurssterk, bruker avansert skadevare og opererer langsiktig. Formålet kan være svindel, teknologityveri, etterretning eller sabotasje. Målet er ofte å etablere en permanent, skjult tilstedeværelse hos offeret. Metoden brukes av etterretningstjenester og kriminelle miljøer. APTer er brukt mot finansinstitusjoner, teknologisk industri og offentlige myndigheter, også i Norge. Det tar ofte lang tid før en APT oppdages. En APT kan inneholde programvare for å beskytte seg selv, eventuelt som er destruktiv dersom den oppdages.

5.4.3 DEFACING

Defacing er en type vandalisme mot websider der noen bytter ut et element, tekst og/eller bilder på en webside, ofte med angriperens eget budskap, for å påkalle brukerens oppmerksomhet. Man kan se på dette som en type graffiti på internett, som også kan være politisk eller ideologisk motivert. Dette er en kjent metode både for hacktivister og terrorister.

5.4.4 RADIOKILDER

Falske basestasjoner for mobiltelefoni er mye omtalt i medier i løpet av det siste året. Falske basestasjoner er kun en del av sikkerhetsutfordringene knyttet til radiosendere. Utfordringene omfatter også andre radiokilder som blåtannenheter (laptoper eller smartklokker) og trådløse nettverk (WiFi). Enheter med radiosendere kan utnyttes for å tappe informasjon også fra andre systemer. Ved å skape et elektronisk påtrykk fra for eksempel en mobilbasestasjon med forhøyet effekt eller fra en av de andre radiokildene som er nevnt over, kan det skapes en effekt som kalles flooding. Dette kan gjøre det mulig å hente ut informasjon uten at det er mulig å påvise dette på annen måte enn ved å måle det mens det skjer.

5.4.5 FYSISK TYVERI OG INNBRUDD, MISTING OG TAP

Angrep innenfor sikret område kan gjøres av innsidere eller ved innbrudd.

Direkte angrep på utstyr har flyttet seg også utenfor sikret område og har med utbredelsen av mobilt og bærbart utstyr og lagringsmedier å gjøre. Målrettede angrep kan gjøres i:

[50] Innspill fra UNINETT Norid AS. Se ordliste.

[51] ENISA ibid, Cisco ibid.

- private bosteder, på hoteller (spesielt i utland) og på reise
- møterom, f.eks. i pauser, lunsj, mellom møtedager der utstyret ligger ubevoktet
- transitt, gjennom toll, pakkepost, passkontroll, terminalbygg, oppbevaringsboks, reisegods
- café, spisested, park, pub, gjerne i forbindelse med reise.

Angrepsflater er tapping av informasjon fra utstyret, bytting eller planting av deler og enheter. Ondsinnet programkode kan injiseres i BIOS/UEFI og annen fastvare. Mikrofoner og kamera i IKT-utstyr er opptaksutstyr som kan fjernstyres. Avanserte angripere vil alltid kunne kompromittere utstyr de får fysisk tilgang til, og det vil være vanskelig eller umulig å oppdage for brukeren. Avanserte angrep er normalt svært vanskelige å oppdage.

Opportunistiske, ikke-målrettede angrep, som simpelt tyveri av verdigjenstand, f.eks. veske med laptop, mobiltelefon og minnepinner, utføres av aktører med lavere kapasitet. Gjenglemt utstyr i drosjer, på tog, i fly og på flyplasser[52], gjør det lett for tyven. Det samme gjør avhending av utstyr uten at innhold er ødelagt.

5.4.6 HETSING OG UTPRESSING

Det er en økende tendens til anonym mobbing og publisering av bilder uten tillatelse på nett. På sosiale nettverk er det etablert egne arenaer hvor formålet kun er å spre rykter og usanne påstander. Ofre blir truet med at intime bilder vil bli publisert på nett hvis de ikke betaler penger for å slippe. En trend er utpressing fra tidligere kjærester og venner hvor man har fått bildematerialet av offeret selv. En annen trend er kriminelle som bryter seg inn i databaser, for eksempel datingtjenester, og stjeler bilder, for så å presse offeret for penger.

5.4.7 IDENTITETSTYVERI

Identitetstyveri oppstår når noen anskaffer, overfører, besitter eller fremstår som rette innehaver av personlige opplysninger tilhørende en privatperson eller selskap på en uautorisert måte, med den hensikt å begå bedrageri eller annen kriminalitet. Identitetstyveri gjennomføres gjerne ved bruk av legitimasjonsdokumenter eller attraktive opplysninger om offeret, som navn, adresse, fødselsnummer og kontonumre. I følge KRIPOS[53] stemmer økningen av identitetstyverier i Norge overens med hva Europol ser i EUs medlemsland. Dette er med på å muliggjøre identitetssvindel, det vil si ervervelse av penger, varer, tjenester og andre fordeler eller unngåelse av økonomiske eller andre forpliktelser ved å utgi seg for å være en annen ved bruk av falsk identitet. Identitetstyveri er et stadig økende problem i Norge, og oppleves som svært belastende for de som utsettes for det[54].

5.4.8 KORTSVINDEL

Kortsvindel er organisert og omfatter mange metoder, alt fra skimming, kopiering/hacking av kredittkort, til salg av stjålet kortinformasjon på nettet. Dette gir muligheter til å svindle store beløp uten fysisk tilstedeværelse. Ifølge Finanstilsynet øker kortsvindel over nett i Norge, og det er en klar økning i tapene ved kortbruk i nettbutikk. Dette kan ha sammenheng med store datainnbrudd i internasjonale aktørers databaser som inneholder kortnummer. Det er grunn til å tro at det er store mørketall på dette området. Vellykkede angrep mot betalingstransaksjoner på nett utgjør også en betydelig andel.

5.4.9 KRIMINELLE TJENESTER

IKT-kriminalitet har blitt en storindustri. Det finnes et omfattende tilbud på internett der kriminelle kan kjøpe avansert skadelig programvare, infrastruktur eller verktøy, for eksempel hjelp til å utføre datasnoking på epostkonti, nettbanktrojanere eller leie av et botnet[55]. Dette er kjent som datakrimtjenester og gjør det mulig å utføre IKT-kriminalitet uten selv å være teknisk kompetent. Blant annet benyttes såkalte verktøysett som inneholder det aktørene trenger for å angripe, kunne

[52] I følge Digi.no ble det i 2011 gjenglemt nesten 3.000 mobiltelefoner på Gardermoen, samt ca. 70 nettbrett og 130 bærbare PCer.

[53] KRIPOS innspill.

[54] Nettsiden Rettighetsadvokater.

[55] Se ordliste.

beholde kontroll over og overvåke infiserte maskiner. Verktøyene er tilgjengelige for nedlasting, og koster lite eller ingenting. NSM erfarer at det skjer aktiv utvikling og forbedring av skadevare, og forskjellige type pakketeknikker blir flittig brukt for å vanskeliggjøre og unngå deteksjon.

5.4.10 LØSEPENGEVIRUS

Løsepengevirus låser alle eller noen filer på ofrenes PC med sterk kryptering. Ofrene får krav om å betale løsepenger for å låse opp innholdet eller forhindre at innholdet ødelegges. Løsepengevirus der kriminelle bruker blant annet Politiet, Europol eller Tono som avsendere er godt kjent i Norge. Datamaskinen blir låst og de kriminelle krever penger for å åpne maskinen igjen. Trojaneren Cryptolocker, som målrettet angriper Windows-maskiner, har hatt omfattende spredning i andre land, men man har foreløpig ikke sett noen spredning i stort omfang i Norge. Det er svært sannsynlig at stadig flere kriminelle vil prøve seg på slike angrep, ettersom de både blir enklere å gjennomføre og kan være økonomisk innbringende. Dette er en sterkt økende trend i 2015.

5.4.11 PHISHING OG SPEARPHISHING

Phishing, såkalt nettfisking, er en angrepsmetode der trusselaktøren prøver å lure til seg opplysninger som kan brukes i vinningsøyemed. Eksempler er henvendelser på epost der mottakeren bes om å oppsøke en webside eller klikke på et vedlegg. Formålet er å få mottaker til å gi fra seg personlig informasjon eller gi angriper tilgang til virksomhetens data.

Spearphishing er et phishingangrep som er skreddersydd og målrettet mot spesifikke personer og som ofte benytter seg av unik skadevare. Metoden er vanlig i forbindelse med spionasje og ble for eksempel brukt i forbindelse med spionasjeangrepet på Telenor i 2012. Ledere og andre nøkkelpersoner i viktige offentlige og private virksomheter er særlig utsatt.

I 100 % av målrettede angrep i 2014 og hittil i 2015, har epost vært brukt som hovedangrepsvektor. Alle angrep har startet med at noen utvalgte ansatte har mottatt en epost som inneholder skadevare.

5.4.12 SOSIAL MANIPULERING

Sosial manipulering utnytter tillit til personer eller virksomheter og falske identiteter til blant annet å lokke offeret til å åpne infiserte vedlegg til eposter. Angriper gir seg ut for å være noen offeret kjenner eller har tillit til, og lokker med informasjon offeret kan være interessert i, i forbindelse med arbeid eller fritid. Metoden er gjerne en inngang til spearphishing og krever ofte en god del kjennskap til offerets interesser eller vaner.

5.4.13 TJENESTENEKTANGREP

Et tjenestenektangrep ((Distributed) Denial of Service – (D)DoS) er et internettangrep som overbelaster en server ved at stor trafikk rettes mot serveren, gjerne ved bruk av et botnet. Hensikten er å hindre normal tilgang for ordinære brukere. Hendelsen medfører at man ikke kan betjene kunder og man får ikke tilgang til data. Tjenestenektangrep er bort i mot kostnadsfritt å utføre og det er lav risiko for å bli tatt. Angrepene kan få store konsekvenser for dem som blir rammet. Dette er en økende trend og det er derfor svært sannsynlig at det vil komme flere saker av denne typen. Slike angrep kan føre til at selskaper taper store summer på forventede reklameinntekter, transaksjoner, valutahandel og gjenoppretting av innhold på de aktuelle nettsidene. Det er spesielt bekymringsfullt at verktøyene for å gjennomføre tjenestenektangrep har blitt så kraftige og effektive at de truer kritisk infrastruktur. Man kan for eksempel se for seg mulig blokkering av teletjenester.

Tjenestenektangrep og endring av websider har som regel liten varig effekt, men kan være virkningsfulle inn i en sikkerhetspolitisk eller innenrikspolitisk krevende situasjon, og det kan også ha økonomiske konsekvenser både for tjenesteleverandør og eier av websiden.

5.4.14 VANNHULLSANGREP

Et vannhull er et nettsted som blir kompromittert i den hensikt å infisere utvalgte besøkende som regnes som attraktive mål. Internasjonale undersøkelser viser at angrep via webapplikasjoner (for eksempel nettsider) utgjør over en tredjedel av de vellykkede angrepene[56]. Denne angrepsformen har vært i sterk vekst de siste fire årene.

5.5 NASJONALT[57]

Antallet avanserte cyberangrep mot Norge går tilsynelatende betydelig ned i første halvår 2015. Så langt i år har det vært 13 saker som NSM NorCERT anser som alvorlige. Dette er et trendbrudd, da antallet cyberangrep økte kraftig de foregående årene. For første gang på flere år blir det registrert færre cyberangrep. Det gjenspeiler ikke en realitet, snarere at evnen til å oppdage angrep er under press, noe som understreker kompleksiteten i disse angrepene. NSM har holdepunkter for at det er stor aktivitet fra ondsinnede aktører. Samtidig har vi registrert 13.773 saker og håndtert 2.943 saker pr. 31. august 2015, mot henholdsvis totalt 17.662 registrerte og 5.066 håndterte saker i hele 2014. Det antas at angriperne i økende grad tilpasser seg den nasjonale evnen til å oppdage angrepene og klarer å gå under radaren. Det oppdages nå lite i bransjer som tidligere var under jevnlig angrep over internett. Det bedømmes at trusselaktører med stor sikkerhet er der, men at det ikke oppdages. Angriperne utvikler sine teknikker raskere enn utviklingen av mottiltak. Dette er i praksis et slags våpenkappløp. De angrepene som oppdages, har økt i størrelse, slik at flere virksomheter inkluderes i samme angrep. Angrepene blir mer avanserte og det gjøres forsøk på å få fotfeste innenfor IKT-strukturen i virksomheten som angripes.

Det blir vanskeligere å detektere angrep gjennom tradisjonell bruk av signaturer. Trusselaktørene bruker mer dynamiske vektorer og gjenkjennelige mønstre blir færre. Dette vil gjøre at behovet for kompetanse for å avdekke angrep vil bli sterkt økende og det vil være en stor risiko for at mange av de mindre aktørene i mye mindre grad vil evne å avdekke angrep.

De siste 12 månedene er det en økning i antallet kommando- og kontroll servere (CC-servere)[58] som står i norsk infrastruktur. Norske forsknings- og utdanningsinstitusjoner blir kompromittert og benyttet i angrep mot norske bedrifter og institusjoner. Angriperen bytter i større grad mellom mange servere i løpet av et angrep for å redusere sjansen for å bli oppdaget. Utfordringen er at en server som gjennom tradisjonell risikometodikk vil komme ut med lav risiko fordi innholdet på serveren ikke har et stort beskyttelsesbehov, benyttes som en vei inn til infrastruktur hvor verdiene er betydelig høyere.

For nasjonen og staten Norge er fremmede staters etterretning den største trusselen. En rekke land har i løpet av de siste ti årene utviklet en svært omfattende etterretningskapasitet i det digitale rom med vide juridiske og politiske fullmakter til å utnytte disse kapasitetene. Mange stater bruker store ressurser på etterretningstjenestene og tillegger informasjonen som disse produserer vesentlig rolle i beslutningskjeden.

Et eksempel på dette i 2015 er en nettverkskampanje som har gått målrettet mot offentlig sektor i Norge. Kampanjen bærer preg av nøye planlegging og kompetent fremgangsmåte, og den retter seg mot personer eller systemer som kan gi tilgang til sensitiv informasjon. Aktøren bak er kjent fra før, blant annet fra hendelser i 2014, og går mot mange mål med store ressurser. NSM vurderer dette som en avansert vedvarende trussel (APT). EOS-tjenestene vurderer at trusselaktøren er en fremmed sikkerhets- eller etterretningstjeneste.

De siste 12 månedene har det vært økt aktivitet fra de store statlige aktørene. En av hovedutfordringene er at skadevaren brukes en gang og deretter sendes ut på det kriminelle markedet. Den økte statlige aktiviteten gir andre kriminelle aktører en stor tilgang på skadevare.

[56] Verizon 2014 ibid.

[57] Basert delvis på PSTs og Kripos innspill.

[58] Server som er infiltrert av angriper og brukes til å styre angrep.

Tap av sikkerhetsgradert eller annen taushetsbelagt informasjon av operativ karakter kan både direkte og indirekte medføre tap av menneskeliv. Konsekvensen ved økt digital spionasje av militær karakter må sees i et langsiktig perspektiv. Skadevirkningene blir ikke nødvendigvis synlige før en militær konflikt begynner.

I løpet av 2015 er tidsvinduet mellom publisering av skadevare til en angrepsversjon er tilgjengelig, blitt mindre. Man har ofte ikke mer enn 7 dager fra en patch[59] blir sendt ut fra programvareleverandør, til det er skadevare på plass som utnytter sårbarheten. Utfordringen vil øke betydelig i tiden fremover når det gjelder omfang og tidsvinduet man har til å holde egen infrastruktur og klienter oppdatert.

Dette er tall fra siste år vedrørende statlige virksomheter[60]:

- 11,8 % hadde hatt sammenbrudd i forbindelsen til internett eller andre eksterne nettverk
- 8,3 % hadde hatt virusangrep, ormer eller lignende som resulterte i tap av data eller arbeidstid
- 15,4 % hadde hatt tjenestenektangrep
- 16,7 % hadde hatt uautorisert tilgang til systemer eller data
- 31,1 % hadde opplevd forsøk på identitetstyveri (phishing)
- 44,3 % hadde opplevd at virksomhetens IKT-utstyr hadde kommet på avveier

Det er svært sannsynlig at det i Norge har funnet sted flere alvorlige nettbaserte spionasjehendelser enn det som norske myndigheter har oversikt over. Det er svært sannsynlig at det vil bli flere slike angrep fremover.

Norge har så langt ikke vært utsatt for alvorlige forsøk på å slå ut kritiske infrastrukturer eller kritiske samfunnsfunksjoner. Erfaringer fra de siste årene, i forbindelse med kriser og hendelser i både det fysiske og det digitale rom, er at man ikke lenger kan forvente varslingstid som gir mulighet til å iverksette tiltak.

5.6 STORE VIRKSOMHETER

For store virksomheter kommer trusselen både fra statlig etterretning og fra ikke-statlige aktører. Skadelig programvare fra kriminelle miljøer utgjør også en risiko[61]. Blant de mange typene skadelig programvare, nevner Kripos spesielt skadevaren BlackShades som gjør det mulig for datakriminelle å ta kontroll over infiserte datamaskiner.

Hovedtyngden av angrepene skjer fortsatt via spearphishing[62]. Det ser ut til at angrepene blir stadig bedre forberedt, da det ofte er små grupper som mottar epostene og de ser ut til å ha blitt plukket ut utfra posisjon. NSM har også sett flere eksempler på at deltakerlister på konferanser har blitt brukt som utgangspunkt for spearphishing.

NSM har sett flere eksempler på vellykkede datainnbrudd der angriperne har fått tilgang til virksomhetskritisk informasjon, og at forretningshemmeligheter, kursdrivende eller annen sensitiv informasjon har kommet på avveier. Skadevirkningene kan variere fra sak til sak, men de alvorligste konsekvensene skjer i et langsiktig perspektiv hvor virksomhetene mister konkurranseevne og eksistensgrunnlag.

Noen nylige eksempler fra inn- og utland[63]:

- I 2014 ble flere norske virksomheter i olje- og energibransjen angrepet gjennom spearphishing. Angrepet skjedde ved at utvalgte ansatte mottok epost med infisert vedlegg. Det kan se ut til at dette var en rekognoseringskampanje. Et stort antall små og store norske virksomheter ble forsøkt angrepet. I samarbeid med Norges Vassdrags- og energidirektorat (NVE) og Petroleumstilsynet (Ptil) varslet NSM NorCERT 300 virksomheter.
- I april 2014 ble det oppdaget kompromittering i systemene til Ulstein-gruppen, som er en samling ulike selskaper innen marin industri. En skadevare ble plantet i selskapets systemer.
- I april 2015 opplevde det franske tv-selskapet TV5 Monde et større cyberangrep, hvor hackere tok

[59] Se ordliste.

[60] SSB, Statistikkbanken, Bruk av IKT i staten, Tabell 10859: Statlige virksomheter. IKT-sikkerhetsproblemer i løpet av det siste året (present). Tilsvarende tallmateriale var ikke tilgjengelig for private foretak. De nyeste SSB-tallene for IKT-sikkerhetsproblem i næringslivet var fra 2004, og derfor ikke sammenlignbare.

[61] Kripos Trendrapport 2015. Den organiserte kriminaliteten i Norge.

[62] Se ordliste.

[63] Se også Center for Strategic and International Studies, Significant Cyber Events.

11 tv-kanaler av lufta, samtidig som de forandret selskapets nettsider og sosiale medier. Hackerne hevdet i dette tilfellet at de var tilknyttet IS.

- Våren 2015 skrev tyske medier at datasystemene i Bundestag i Tyskland var blitt hacket, og data fra 20 000 kontoer stjålet.
- I juni 2015 måtte det polske flyselskapet LOT innstille ti og utsette 12 flyvninger som følge av dataangrep.
- I juni 2015 annonserte det amerikanske Office of Personnel Management (OPM) at de hadde vært utsatt for datainnbrudd[64]. Sensitiv informasjon om mer enn 22 millioner mennesker var stjålet, inkludert flere millioner offentlig ansatte med sikkerhetsklaring, deres familie og venner. Kinesiske hackere mistenkes for å stå bak[65]. Angrepet ble oppdaget i april 2015, men hadde startet i mars 2014 og kanskje enda tidligere, og omtales som historiens største digitale angrep i USA[66].

Angrepet mot OPM har satt i gang en stor diskusjon rundt hvor hensiktsmessig det er å lagre store mengder data i en fellesløsning. Bruk av fellesløsning stiller krav til separasjon av data og tilgangsstyring. De siste årene har det vært flere saker hvor angripere har vært ute etter både kontaktinformasjon, teknisk informasjon og forretningshemmeligheter. Tap av slik informasjon kan ha store konsekvenser for virksomheten det gjelder. I tillegg til rent økonomisk tap, kan tap av informasjon svekke tilliten til virksomheten.

En generell trend er at DDos-angrep mot bankers nettsider og nettbanker opptrer hyppigere enn før og med større tyngde. Finansnæringen erfarer at digitale angrep blir spesialsydd og rettet mot et bestemt foretak. Disse angrepene starter med phishing, infiserte minnepinner (USB) eller sosial manipulering, og angrepskoden er svært vanskelig å oppdage. «Angriperen tar seg god tid og går skrittvis frem. Et typisk angrep kan innlede med at angrepskoden kartlegger de ulike segmentene i nettverket. Deretter leter skadevaren etter høyrettighetsbrukere. Skadevaren bruker rettighetene og legger inn selvsignerte sertifikater i hvitelisten i operativsystemet og kopierer deretter innloggingssider for å få tak i brukerens påloggings-ID og passord»[67].

I 2014 varslet og håndterte NSM totalt 88 alvorlige dataangrep, mot 51 i 2013. Flesteparten av angrepene hadde som formål å stjele informasjon fra datasystemene til store eller viktige norske virksomheter. 4 % av norske virksomheter, og 5 % av de store, sier de har opplevd datainnbrudd. Realiteten er over 50 %[68]. Rapporteringen og anmeldelser på dataspionasje er ellers svært mangelfull i Norge.

5.7 SMÅ VIRKSOMHETER / INDIVIDER

For små virksomheter og individer er vinningsbasert cyberkriminalitet normalt den største trusselen, for eksempel basert på bredt anlagt phishing eller på botnet. Om den ansatte eller virksomheten har spesielle roller, eksempelvis knyttet til nasjonal sikkerhet, kan den ansatte eller virksomheten være i søkelyset til statlige etterretningstjenester. Små virksomheter og individer er oftest lett tilgjengelige mål. Nærmere 90 % av norske virksomheter tilhører denne kategorien og ligger utenfor den beskyttelse myndighetene har etablert for kritisk infrastruktur.

Dårlig sikrede hjemme-PCer kan kapres og brukes i botnet, som igjen kan benyttes i Ddos-angrep. Botnet-aktivitet utgjør 34 % av dataangrep. Det ser ut til nye botnet bygges opp rundt webservere, noe som gir større effekt enn hundrevis av PCer. Det er også observert botnet basert på Internet of Things-enheter[69].

[64] Wikipedia: Office of Personnel Management data breach.

[65] The Washington Post: Hacks of OPM databases compromised 22.1 million people, federal authorities says; ABC News: 22 Million Affected by OPH Hack, Officials Say; The Guardian.com: OPM hack: 21 million people's personal information stolen, federal agency says.

[66] U.S. News: Harsh Truths From OPM Hack: More Monitoring is Coming.

[67] Finanstilsynet ibid.

[68] NSR, Mørketallsundersøkelsen 2014.

[69] ENISA Threat Landscape 2014 (utgitt desember 2014).

6.

Sårbarhetsutfordringer og tiltaksstatus

Utfordringer er også beskrevet i NSMs sikkerhetsfaglige råd, og disse to rapportene bør leses i sammenheng.

6.1 SÅRBARHETSUTFORDRINGER

Sikkerhetsmessige sårbarheter kan ha tekniske, menneskelige og organisatoriske årsaker. NSMs egne erfaringer, bekreftet i en rapport fra Forsvarets forskningsinstitutt (FFI)[70], er at organisatoriske sårbarheter dominerer sårbarhetsbildet.

6.1.1 TEKNISKE SÅRBARHETER

Sikkerheten ved ulike komponenter i IKT-systemer er sterkt varierende. IKT-produkter kan inneholde implementasjons- og designfeil, som kan konfigureres, installeres og brukes på måter som utgjør en sikkerhetsrisiko. Mulige sårbarheter kan finnes i maskinvare, operativsystem og applikasjoner.

Økt kompleksitet i internett-arkitekturen forårsaker i økende grad informasjonslekkasjer[71]. Verdifull informasjon blir tilgjengelig for uvedkommende, uten at disse trenger å bryte seg inn i datasystemene. En av sårbarhetene som gjør dette mulig er Heartbleed, en alvorlig sårbarhet i krypteringssystemet OpenSSL[72].

OpenSSL

OpenSSL brukes både av epost-applikasjoner og websider og har åpen kildekode. Det har vært en utbredt oppfatning at åpen kildekode er tryggere enn kommersiell, siden kildekoden kan granskes av hvem som helst, og at feil derfor lettere vil bli funnet. Heartbleed-sårbarheten viser at dette ikke er tilfelle. I 2014 ble OpenSSL brukt av to tredeler av alle internettbrukere[73], og 17 % av brukerne av OpenSSL var mottakelig for Heartbleed-sårbarheten[74]. Sårbarheten eksisterte i cirka to år før den ble kjent i april 2014, og tillot hvem som helst på internett å lese av minnet til systemet den sårbare versjonen av OpenSSL skulle beskytte, og kompromitterte krypteringsnøkler, brukernavn og passord, samt eposter, kritiske dokumenter og kommunikasjon[75]. NSM anbefaler bruk av TLS[76] som en av metodene for sikring av kommunikasjon over internett.

Styringssystemer, SCADA-systemer, for eksempel driftskontrollsystemer i kraftselskapene[77], utgjør også en teknisk sårbarhet. Disse systemene er svært komplekse og det forventes at kompleksiteten øker. For å utnytte SCADA-systemenes muligheter fullt ut, kobles gjerne driftskontrollsystemene sammen med andre IKT-systemer for å utnytte informasjonen fra dem til planlegging, analyse og reparasjonsberedskap. Dette krever god kompetanse for å sikre høy tilgjengelighet og god beskyttelse av disse systemene. De største risikoene knyttet til dette er tekniske og menneskelige feil, som medfører bortfall av SCADA-systemene.[78] Den mest ødeleggende nettverksoperasjonen kjent hittil er Stuxnet, sannsynligvis rettet mot SCADA-systemer anvendt i iransk kjernekraftindustri. Ondsinnede aktører vil finne og utnytte enhver svakhet i den teknologiske næringskjeden. Bakdører i teknologiprodukter kan gi dem full tilgang til virksomheten.[79]

6.1.2 MENNESKELIGE SÅRBARHETER

Blant de menneskelige sårbarhetene er vår evne til å la oss lure. Denne sårbarheten utnyttes aktivt gjennom sosial manipulasjon. På denne måten lures ansatte til å gi fra seg passord, beskrive vedlikeholds- og sikkerhetsrutiner eller benytte minnepinner som er infisert. Erfaringsmessig er det alltid noen som lar seg lure av slike angrep. En annen menneskelig sårbarhet er lav motivasjon for å følge sikkerhetsbestemmelser, eksempelvis fordi dette vil gå ut over effektiviteten. Manglende kunnskap og evner er også en betydelig menneskelig svakhet.

Hendelser som cyberangrep, tap av kundedata og identitetstyveri, svekker tilliten til informasjonsteknologi. Det er en økning i bevisstheten omkring IKT-sikkerhet. Sikkerhetsaspektet glemmes imidlertid ofte når det dukker opp spennende tjenestetilbud eller muligheter for gevinst. Slike tilbud krever ofte at det avgis omfattende personlige opplysninger. Selv på virksomhetsnivå unnlater man å gjennomføre åpenbare og enkle sikkerhetstiltak. Dette blir ikke bedre – det blir verre. Bundesamt für Sicherheit in der Informationstechnik (BSI) kaller dette for *digital sorgløshet*[80].

Til tross for at organisatoriske sårbarheter ofte er årsaken til avvik, er det menneskelige årsaker som

[70] FFI-rapport 2014/00948, Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet.

[71] ENISA Threat Landscape 2014.

[72] Se ordliste.

[73] Wikipedia: OpenSSL.

[74] Trend Micro: OpenSSL: Are You Vulnerable.

[75] Codenomicon, april 2014, The Heartbleed Bug.

[76] Se ordliste.

[77] Se nedenfor.

[78] NVE innspill.

[79] Cisco 2014 ibid.

[80] Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2014.

oftest beskrives i mediebildet[81] og i forskjellige sikkerhetsrapporter[82]. Årsaken til dette er at svikt i organisatoriske tiltak skyver ansvaret for sikkerhet over på enkeltmennesket. Bruk gjerne ditt eget utstyr, men hvis noe går galt, har du ansvaret selv. Dessuten oppfattes det digitale rom ofte som noe abstrakt, hvor risiko erfares på en annen måte enn i det fysiske rom.

6.1.3 ORGANISATORISKE SÅRBARHETER

Organisatoriske rammer skal avverge sårbarheter som følge av forskjeller i individuell adferd. De samme sikkerhetsavvikene går ofte igjen i mange virksomheter og gjentas i en og samme virksomhet[83]. Dette understreker hvor viktig det er å ha det organisatoriske grunnlaget for det forebyggende sikkerhetsarbeidet på plass.

Typiske organisatoriske sårbarheter er:

- Manglende risikovurdering og manglende bevissthet i forhold til risiko
- Virksomhetsleder avsetter ikke nødvendige ressurser i form av personer og penger til å ivareta forebyggende sikkerhet[84]
- Ledere måles sjelden på hvor godt de ivaretar forebyggende sikkerhet[85]. Dersom ledelsen ikke etterspør status på sikkerhetstiltak og sikkerhetstilstanden i virksomheten, vil sikkerhet heller ikke bli prioritert
- Manglende situasjonsforståelse
- Dysfunksjoner i virksomhetskultur, for eksempel høyt konfliktnivå
- Manglende sikkerhetsstyring fører til svak sikkerhet i resten av virksomheten
- Manglende gjennomføringsevne for sikkerhetstiltak
- Manglende oppdatering av dataprogrammer
- Manglende logging av datatrafikk og manglende tiltak for å oppdage mulige illegitime brukere
- Sikkerhetsarbeidet er ikke dokumentert gjennom målsetninger, krav, instrukser og resultater
- Kritiske komponenter eller funksjoner gjøres avhengige av én ressurs med potensial for feil (single point of failure)
- Virksomheter er avhengige av leverandører, og angrep på en virksomhet kan forplante seg videre i leverandørkjeden
- Mangler i passordadministrasjon og annen tilgangskontroll
- Utilstrekkelig kompetanse til å bestille tekniske sikkerhetsløsninger.

Organisatoriske sårbarheter omfatter blant annet mangler i sikkerhetsrutiner, organisering, virksomhetskultur, ledelse og ledelsesforankring, ansvarsfordeling og sikkerhetsstyring. Sårbarheter kan oppstå ved at arbeidet er organisert på en måte som ikke ivaretar virksomhetens sikkerhetsbehov, eller når det ikke er en etablert bevissthet om at alle har ansvar for sikkerheten, ikke bare den som har «sikkerhet» i stillingstittelen sin.

6.2 NASJONALE SÅRBARHETSUTFORDRINGER

6.2.1 KOMPETANSE

Mangel på kompetanse om IKT-sikkerhet

På kort sikt er nasjonal mangel på IKT-sikkerhetskompetanse kritisk. Konkurransen om nyutdannede er hard, da det er få kvalifiserte kandidater med både sikkerhetsfaglig og høyere teknisk utdanning. NSM merker også dette selv, og fungerer til en viss grad som videreutdanningsinstitusjon til fordel for næringslivet. Mangel på kompetanse påvirker evnen til både å løse nasjonale sikkerhetsoppgaver, og sikre norske virksomheter. Opplæringen innen informasjonssikkerhet i Norge er individuell og tilfeldig[86]. Denne mangelen finnes også internasjonalt og bidrar i betydelig grad til digitale sårbarheter[87].

Årlig tas rundt 1.500 studenter opp i ulike IKT-utdanninger på universiteter og høgskoler i Norge og dette er for få. På flere universiteter er ikke IKT-sikkerhet et obligatorisk fag som ledd i IKT-utdannelsen. Studenter som skal bygge fremtidig infrastruktur og applikasjoner har ikke grunnleggende kompetanse i sikring av IKT-systemer.

6.2.2 ORGANISERING, LEDELSE OG KOORDINERING

Justis- og beredskapsdepartementets koordineringsrolle

Justis- og beredskapsdepartementets (JDs) koordinerende rolle innenfor forebyggende IKT-sikkerhet i sivil sektor er ikke tilstrekkelig tydelig til at departementet kan ta rollen med nødvendig kraft. Videre må denne rollen aksepteres av de som skal bidra i koordineringen. Dette kan være utfordrende innen rammene av konstitusjonelle ansvarsforhold, der den enkelte statsråd er ansvarlig innen sitt fagfelt. I mange tilfeller samarbeider ikke aktørene godt nok. Dette gir utilstrekkelig koordinering innenfor IKT-området. Flere av bidragsyterne til denne rapporten opplever uklarheter knyttet til dette.

[81] FFI-rapport 2014/00948 Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet.

[82] Blant annet i ENISA, Annual Incident reports 2013.

[83] FFI-rapport, ibid.

[84] FFI-rapport, ibid.

[85] FFI-rapport ibid.

[86] «Opplæring i informasjonssikkerhet», Nina Hoddø Bakås, Universitetet i Oslo, 2015.

[87] «Cybersecurity through Secure Software Development», artikkel av Audun Jøsang, Marte Ødegaard og Erlend Oftedal 2015.

Evne til samvirke i beredskaps- og krisesituasjoner

Ukraina-krisen viste at samvirkemekanismene i den norske beredskapskjeden hadde mangler. Dette var særlig tydelig innenfor IKT-sikkerhet og oppgaver i tilknytning til hendelseshåndtering. Beredskapsplanverk var ikke oppdatert og tydeliggjort når det gjaldt tiltak innenfor IKT-sikkerhet, men er revidert i ettertid. Operasjonalisering gjenstår. Det finnes ikke enhetlig og sikker kommunikasjonsinfrastruktur for rask og effektiv informasjonsdeling og koordinerte beslutningsprosesser. Mange private aktører har en rolle i kriser og beredskap og må få tilgang til sikkerhetsgradert informasjon, men fordi de ikke er underlagt sikkerhetsloven kan ikke slik tilgang gis.

Det er for få tverrsektorielle IKT-øvelser på jevnlig basis. Det er behov for å systematisere øvelsesplanleggingen og tydeliggjøre et hovedansvar innen dette feltet.

6.2.3 IKT-SIKKERHET

Mangler i grunnleggende IKT-sikkerhet

Noen få grunnleggende tiltak innen IKT-sikkerhet ville ha stanset inntil 90 % av alle IKT-angrep. Selv store virksomheter med mye bruk av IKT feiler ofte på dette punktet. Andre tiltak har liten virkning dersom grunnleggende sikkerhetstiltak ikke er iverksatt. Relevante tiltak er gjentatt mot slutten av denne rapporten.

Manglende tydeliggjøring av den nasjonale myndigheten for IKT-sikkerhet

NSM er nasjonal myndighet for IKT-sikkerhet innen sikkerhetslovens område. I tillegg er NSM nasjonalt fagmiljø for IKT-sikkerhet som følge av JDs ansvar for sivil IKT-sikkerhet[88]. NSMs direktør er, av FD, gitt mandat til å være ansvarlig for å koordinere håndteringen av alvorlige IKT-angrep og å være forsvarsministerens og justis- og beredskapsministerens nærmeste rådgiver for forebyggende tiltak mot sikkerhetstruende virksomhet som kan ramme nasjonale og samfunnsmessige verdier. Instruksen er ikke bindende for etater utenfor forsvarssektoren, men fordrer utstrakt samhandling med sivile sektorer og mellom sivil og militær sektor. Dette er en svakhet og det er behov for tydeliggjøring av nasjonal myndighet for IKT-sikkerhet.

Ikke oppdatert nasjonal strategi for informasjonssikkerhet

Nasjonal strategi for informasjonssikkerhet ble vedtatt i 2012. Det har siden skjedd endringer som tilsier at strategien og tilhørende handlingsplan må gjennomgås og revideres. I 2013 ble ansvaret for forebyggende IKT-sikkerhet overført fra nåværende KMD til JD. Strategien tydeliggjør i for liten grad roller og ansvar og er ellers lite konkretisert. Dette svekker evnen til effektiv oppfølging av den.

Manglende oversikt over alvorlige IKT-hendelser

Alvorlige IKT-hendelser innenfor sikkerhetslovens område skal rapporteres til NSM. Det finnes også rapporteringsordninger til eksempelvis Finanstilsynet og Nasjonal kommunikasjonsmyndighet. Disse tilflyter ikke nødvendigvis NSM. Dette svekker NSMs evne til å kunne utarbeide et nasjonalt IKT-risikobilde og nasjonal evne til tverrsektoriell respons.

Utviklingsbehov i den nasjonale CERT-funksjonen (NSM NorCERT)

NSM har i løpet av 2015 gjennomført en større strategiprosess, som har resultert i økt fokus på sektorvise responsmiljøer og skaleringspotensial. Dette vil til en viss grad imøtekomme økningen i antall cyberangrep, men er ikke et robust nok tiltak. Full effekt forutsetter at det legges fysisk til rette for at sektorvise responsmiljøer, eiere av kritisk IKT-infrastruktur, EOS-tjenestene og andre viktige aktører er til stede i samme lokale for å sikre effektiv hendelseshåndtering. Det mangler også nasjonale møtearenaer og nettverk med deltakelse fra sentrale myndigheter, næringsliv og eiere av kritisk IKT-infrastruktur. Dette svekker evne til koordinering, samvirke og kunnskapsdeling.

Både NorCERT og de sektorvise håndteringsmiljøene har kapasitetsutfordringer, særlig med hensyn til å rekruttere og holde på tilstrekkelig antall personer med rett kompetanse. Selv med de siste årenes vekst, klarer NorCERT knapt å holde tritt med trusselutviklingen. De sektorvise håndteringsmiljøene er ofte små og kan ha utfordringer med kompetanse og usikker finansiering. De er relativt nylig opprettet og har utviklingspotensial.

Svakheter ved nasjonal deteksjonsevne

Varslingssystem for digital infrastruktur (VDI) gir

[88] Kgl. res. av 22. mars 2013.

et bilde av angrep som rammer samfunnsviktige virksomheter og er et sentralt element i den nasjonale deteksjonsevnen. Dette er basert på frivillig deltakelse og finansiering fra private aktører. Deteksjonsevnen er utilfredstillende som følge av få sensorer og manglende dekningsomfang. Videre er deltagelse i systemet basert på frivillighet og på at deltagende virksomheter, ofte private, deltar i finansieringen. Situasjonsbildet for viktig IKT-infrastruktur er avhengig av virksomheter som ønsker å være med i samarbeidet.

Fragmenterte IKT-løsninger i det offentlige
Utvikling, forvaltning og drift av IKT-løsninger for det offentlige er spredt på forskjellige aktører og er bygd opp på ulike måter med ulik grad av sikkerhet. For ugradert informasjon er det mange driftsorganisasjoner og betydelig fragmentering i staten. Antallet leverandører og ulike løsninger utfordrer effektivitet, samhandling og kommunikasjon. Misnøye med tidligere leveranser kan ha bidratt til at aktører har utviklet egne løsninger. Forsvarssektoren ikke er et unntak.

Manglende fellesløsninger for høygraderte IKT-løsninger
Flere aktører i Norge har behov for høygraderte IKT-løsninger med elektronisk samhandling. Utvikling av disse er ressurskrevende og krever spesiell kompetanse. Forsvaret, FD, Departementenes sikkerhets- og serviceorganisasjon (DSS) og NSM leverer alle forskjellige løsninger for sikkerhetsgradert informasjon. Dette kan utfordre samhandling mellom de ulike aktørene og være kostnadsdrivende.

Manglende fellesløsninger for ugradert sensitivt og lavgradert[89] nivå
Mange aktører har behov for ugraderte og lavgraderte IKT-systemer for sensitiv informasjon. Det mangler gjennomgående fellesløsninger på lavgradert nivå. Ulike løsninger anvendes for ulike sensitivitetsnivåer. Dette skaper utfordringer med utveksling av informasjon og ved håndtering av hendelser. Både Difi og CYFOR peker på det samme, og poengterer et økende behov for felles, sikker, behovsdimensjonert og brukervennlig informasjonsutveksling mellom departementene, Forsvaret og sivile offentlige og private virksomheter. Forsvaret, FD, DSS og NSM leverer slike løsninger. Enkelte etater har også egne løsninger.

Utilstrekkelig sikkerhet mot avlytting av elektronisk informasjon
Det er varierende bruk av kryptering på data som er sensitive, men ikke underlagt sikkerhetsloven. Det eksisterer kommersielt tilgjengelige løsninger, men de benyttes i for liten grad. Eksempler på sensitiv ugradert informasjon kan være helseopplysninger, privat epost og bedriftshemmeligheter. Manglende bruk av kryptering medfører at ugradert men sensitiv informasjon ofte er utsatt for avlytting[90].

Behov for tillit til digitale sertifikater
Et digitalt sertifikat kan sammenlignes med et elektronisk pass eller identitetskort som kan brukes som digital legitimasjon. Det finnes hendelser der sertifikatutsteder har hatt svakheter i sikkerheten. Kjøp av sertifikattjenester fra aktører som er underlagt kontroll av andre lands myndigheter kan være problematisk. Det må finnes tillit til sertifikatutsteder og dennes løsninger. NSM utsteder digitale sertifikater til bruk i forsvarssektoren. Det er ikke en enhetlig tilnærming til dette i offentlig forvaltning.

Utilstrekkelig bruk av inntrengningstesting
I mange tilfeller er det enkelt å gjøre digitale innbrudd i datasystemer, fysisk stjele informasjon eller ødelegge systemer. NSM har avdekket en rekke alvorlige sårbarheter innen en lang rekke samfunnssektorer gjennom inntrengningstesting. Slik testing bidrar til sikkerhet i samfunnet, men er lite utbredt i de fleste sektorer. NSM har mandat til å gjennomføre inntrengningstesting i graderte og ugraderte systemer i virksomhet omfattet av sikkerhetsloven og etter forhåndsavtale. Utover dette har ikke NSM hjemmelsgrunnlag for slik testing.

Manglende tilsynskompetanse på IKT
Tilsynsmeldingen (St.meld. nr. 17 (2002-2003)) peker på at man bør unngå at samme formål ivaretas av forskjellige tilsyn. Om flere organer fører tilsyn med IKT-sikkerhet i samme virksomhet, virker dette fragmentert og ukoordinert og oppleves unødvendig ressurskrevende for alle. Det finnes ikke tilstrekkelig IKT-sikkerhetskompetanse

[89] Med lavgradert nivå menes informasjon sikkerhetsgradert som BEGRENSET.

[90] Også påpekt i Datatilsynets innspill.

nasjonalt til at alle tilsynsmyndigheter kan bygge opp egne IKT-sikkerhetsmiljøer. Kompetansen til å gjennomføre tekniske IKT-sikkerhetstilsyn er varierende. NSM har høy kompetanse på IKT-sikkerhetsområdet, men begrenset kapasitet til å gjennomføre tekniske IKT-sikkerhetstilsyn. NSM vektlegger sikkerhetsstyring[91] i sine tilsyn.

6.2.4 BEHOV FOR AKKREDITERING AV PRIVAT RÅDGIVNING

Det er vanskelig å få oversikt over aktører og kvalitet på tjenester innen IKT-sikkerhetsrådgivning. Det finnes ikke en akkrediteringsordning som omfatter aktører som tilbyr rådgivning og andre tjenester innenfor IKT-sikkerhetsområdet. NSM har startet arbeidet med å etablere en akkrediteringsordning.

6.2.5 KUNNSKAP OM TEKNOLOGISK UTVIKLING

Den teknologiske utviklingen går raskt, og utfordrer både strategisk og teknisk nivå. Mesteparten av utviklingen av IKT-produkter og -tjenester foregår internasjonalt. Andre land utvikler fortløpende strategier og handlingsplaner for å møte utviklingen sikkerhetsmessig. I fremtiden vil flere sikkerhetsløsninger, selv for høygraderte systemer, basere seg på kommersielle produkter som utvikles raskere enn tradisjonelle offentlige produkter. Det er en utfordring å ligge i forkant for å utvikle sikkerhetsmessige løsninger på ny teknologi.

6.2.6 SÆRSKILT OM SÅRBARHETER I UTVALGTE KRITISKE INFRASTRUKTURER

Elektrisk kraft og elektronisk kommunikasjon (ekom) utgjør ryggraden som bærer det moderne samfunnet. Sårbarhetsbildet for disse kommenteres derfor spesielt[92].

Elektrisitetsforsyningen

I følge NVE vil tap av driftskontrollsystemene i kraftforsyningen i seg selv ikke medføre strømutfall, da man kun mister muligheten for fjernovervåking og -styring. Overvåking og styring kan foregå lokalt med mannskaper ute i anleggene. Kraftforsyningens beredskapsforskrift krever at kraftselskapene har evnen til å overvåke og styre anleggene uten driftskontrollsystem. En slik situasjon vil imidlertid redusere kvaliteten på kraftleveransen, med blant annet hyppigere lokale strømutfall, eventuelt strømutfall av en viss varighet. NSM finner denne vurderingen troverdig.

Bruken av informasjonsteknologi har økt betydelig i kraftforsyningen i takt med samfunnets økende avhengighet av elektrisitet, og i dag er informasjonsteknologien nødvendig for å sikre en stabil og sikker strømforsyning, og bidrar til raskere lokalisering av feil og gjenoppretting. Avhengigheten har ført til at sikringen av kritiske IKT-systemer og infrastruktur er blitt en integrert del av energiforsyningen og er således en integrert del av NVEs generelle forvaltning av sektoren.

Innføringen av strømmålere med toveiskommunikasjon (AMS) og Elhub, som blir den sentrale datanoden for måleverdier fra alle strømkunder i Norge og markedsprosesser i det norske kraftmarkedet, gjør at IKT-kompleksiteten blir meget stor. Risikoene her er etter NVEs mening todelt; at uvedkommende får tak i måleverdier inkludert personopplysninger fra Elhub, eller at kraftmarkedene blir manipulert i den grad at det er fare for ubalanse i kraftnettet. Hovedutfordringen er å innarbeide tilstrekkelige sikkerhets- og beredskapsmessige hensyn i kravspesifikasjoner, innkjøp, implementering og tilpasninger i ulike IKT-systemer og -løsninger.

Telekommunikasjon

I løpet av de neste 10 årene vil stort sett all datakommunikasjon som understøtter kritisk infrastruktur og andre funksjoner i Norge bruke internett som bærer av datatrafikk. Også Forsvaret får økt avhengighet av internett som bærer av informasjon og infrastruktur. Det vil ikke være vesensforskjell mellom telesystemer og store IKT-systemer og de vil ha de samme tekniske sårbarhetene.

Tjenester i ekomnettene er avhengige av sentraliserte funksjoner. Dette gir mulighet til å bygge mye robusthet inn i løsningene. Store hendelser som har relativt lav sannsynlighet, kan imidlertid få svært store konsekvenser. Eksempler på dette er programvarefeil i sentrale nettkomponenter. Slike feil, utilsiktede eller plantede, har potensial til å slå ut hele tjenester i hele landet. De ulike tilbyderne av ekomtjenester benytter i stor utstrekning Telenors sambandslinjer og IP-infrastruktur. Det betyr at de sårbarheter som denne infrastrukturen har, er felles for mange tilbydere.

[91] Se henvisning til veileder i litteraturliste.

[92] Innspill fra NVE og Nkom.

De større elektroniske kommunikasjonsnettene er sammensatt av en omfattende utstyrsportefølje fra ulike leverandører. Programvarene for styring av de enkelte komponenter og for samvirket mellom de ulike komponenter er svært kompleks. Det kan være tilnærmet umulig å verifisere at det ikke foreligger alvorlige intenderte eller ikke-intenderte logiske sårbarheter. Forholdet mellom leverandør og kunde av slikt utstyr og programvare, må derfor bygge på tillit. Tradisjonelle tilbydere setter ut oppgaver og blir prisgitt kompetansen og kapasiteten hos leverandør. Erfaring fra hendelser flyter ikke tilbake til tilbyder og evnen til å improvisere og håndtere situasjoner svekkes over tid.

Utsetting av tjenester fra de tradisjonelle operatørene, internasjonal konsolidering i bransjen og nye internett-baserte aktører bidrar til et nytt bilde hvor de nasjonale landegrensene mister relevans. Dette kan føre til at en ikke har nødvendige virkemidler overfor slike aktører, og ikke tidsnok kan gå i inngrep og håndtere uheldige forhold som kan svekke sikkerheten.

6.3 STORE VIRKSOMHETER

Norske virksomheter begår gjentatte brudd på sikkerhetsloven og lukker ikke alvorlige avvik etter tilsyn fra NSM. Sårbarheter blir ikke lukket. Interne årsaker til dette kan påvirkes og utbedres. Organisatoriske årsaker, som manglende organisatoriske sikringstiltak, forklarer oftest sikkerhetsbrudd i norske virksomheter[93].

Virksomheter prioriterer ofte ikke forebyggende sikkerhet. Resultatet er underdimensjonerte og ressurssvake sikkerhetsorganisasjoner[94]. Finanstilsynet melder at dokumenterte risikoanalyser jevnt over er fragmenterte og mangelfulle. Det vil si at virksomhetene kan være utsatt for større risiko enn de selv er klar over, og risiko kan videreføres til kunder og samarbeidspartnere. Mange virksomheter synes å ha mangelfull kompetanse til å risikovurdere egen virksomhet, samt se hvilke gjensidige avhengigheter de har i forhold til andre virksomheter.

Store virksomheter har som regel store og kostbare IKT-systemer. Komplekse IKT-systemer er sårbare. Slik kompleksitet oppstår når funksjoner som ikke lenger er i bruk erstattes av ny funksjonalitet uten å fjernes fra produksjonsmiljøet. IKT-systemer kan være så komplekse at de utgjør en risiko for stabil drift og bremser nyutvikling. Det finnes tilfeller av IKT-systemer som har utgjort et så stort løft for virksomheten at reinvesteringer i IKT blir vanskelige. Dette er ikke økonomisk eller teknologisk bærekraftig.

Utkontraktering av IKT-virksomhet kan innebære økt sikkerhet siden IKT-tjenesteleverandøren ofte er en stor virksomhet med profesjonelle ressurser. Samtidig gir dette potensielt økt sårbarhet, siden informasjonseier ikke har full styring med egen informasjon.

Avhengighet av internettilgang kan utgjøre en sårbarhet dersom løsningen ikke er robust nok, eksempelvis dersom virksomheten kun har én leverandør av all elektronisk kommunikasjon.

Avhengighet av stabil strømforsyning utgjør en vesentlig sårbarhet for mange virksomheter. Et eksempel på konsekvensen av dette er svikt i strømforsyningen i en datahall som i 2014 førte til nedetid og forsinkelser i kjøremønsteret for bankenes betalingssystemer i flere dager[95].

6.4 SMÅ VIRKSOMHETER / INDIVIDER

Næringslivet er dominert av små og mellomstore virksomheter. Av 547 232 virksomheter i Norge ved inngangen til 2015 hadde 99,4 % (544 148) færre enn 100 ansatte, og 98,45 % (538 776) av virksomhetene hadde færre enn 50 ansatte[96]. Virksomhetenes størrelse kan legge premisser for hva som er mulig å innføre av dedikert sikkerhetsadministrasjon, spesielt med tanke på IKT-kompetanse, som før nevnt, er et knapphetsgode.

20 % av private foretak sysselsatte IKT-spesialister i 2013[97]. Det vites ikke om disse også hadde IKT-sikkerhetskompetanse. 7 % av private foretak hadde rekruttert eller prøvd å rekruttere IKT-spesialister året før. 37 % av virksomhetene opplevde imidlertid vanskeligheter med å rekruttere IKT-spesialister året før.

49,8 % av statlige virksomheter har forsøkt å rekruttere IKT-spesialister i løpet av det siste året, og 39,5 % hadde problemer med dette[98]. 22,2 % av statlige virksomheter med færre enn 100 ansatte har forsøkt å rekruttere IKT-spesialister det siste året, og 16,7 % av virksomhetene hadde problemer med dette.

Små virksomheter har ofte dårligere forutsetninger enn større virksomheter for å ivareta nødvendig sikkerhet og opprettholde god sikkerhetskultur. I en liten virksomhet er mye personavhengig, og det etableres gjerne færre rutiner. Dette vil

[93] FFI-rapport 2014/00948 Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet.

[94] FFI-rapport ibid.

[95] Finanstilsynet ibid.

[96] SSB, Statistikkbanken, Virksomheter.

[97] SSB, Statistikkbanken, Bruk av IKT i næringslivet, diverse tabeller.

[98] SSB, Statistikkbanken, Bruk av IKT i staten. Tabell 10860: Statlige virksomheter. Rekruttering av IKT-spesialister, etter sysselsettingsgruppe (prosent).

ha store konsekvenser dersom sentrale personer forsvinner. Tilgang til eksempelvis kunderegister og informasjon om virksomhetens tjenester eller produkter er helt nødvendig for at virksomheten skal kunne eksistere. Bortfall av tilgang til denne type informasjon kan bety konkurs, og kan ha store konsekvenser for virksomhetens kunder.

Når grensen mellom den private sfæren og arbeidsplassen viskes ut ved bruk av mobile IKT-systemer og hjemmekontorløsninger, medfører dette økt risiko for at virksomhetens informasjon flyter over på private IKT-enheter og til private brukerkontoer.

Bruk av sosiale medier og eksponering av personlig informasjon om ansatte i en virksomhet kan utnyttes av potensielle angripere. Sosiale medier benyttes i noen tilfeller også til å diskutere arbeidsrelaterte saker. Slik informasjonslekkasje kan være problematisk for mange virksomheter[99].

Mange bruker foreldet programvare som inneholder mange sårbarheter som lett kan utnyttes av en trusselaktør. Selv om den enkelte privatperson kanskje ikke er målet for slike ondsinnede angrep, kan private datamaskiner bli brukt til å muliggjøre angrep mot andre mål[100].

Små virksomheter og individer er som regel lite sikkerhetsbevisste, lar seg lett lure[101] og preges av digital sorgløshet. Dessuten er de i liten grad støttet av en profesjonell sikkerhetsorganisasjon.

6.5 KONSEKVENSER

Alle betydelige angrep de siste 12 måneder har dreid seg om tyveri av informasjon. Konsekvensene[102] av IKT-angrep vurderes å være betydelige. Mange mål kan rammes på en gang og store mengder informasjon kan stjeles. Vellykkede datainnbrudd kan medføre tap av personopplysninger og annen sensitiv informasjon. For offentlige virksomheter kan skadevirkningene være tap av tillit til det offentliges digitale løsninger på en slik måte at det påvirker samfunnets evne til å ta ut gevinster ved modernisering og digitalisering. Difi sier at digitaliseringen av offentlig sektor skal bidra til å forenkle samhandlingen mellom det offentlige, innbyggere og næringsliv. Offentlige tjenester blir mer tilgjengelige for brukerne, og det spares tid og ressurser for brukere og forvaltningen. IKT-sikkerhet blir imidlertid viktigere og det kan bli flere utfordringer, blant annet:

- Digitale offentlige tjenester i åpne nett må være pålitelige, troverdige og tilgjengelige, men være robuste overfor uønskede hendelser både i egne og brukernes nett.
- Automatisert saksbehandling og vedtak vil kreve høy grad av innbygd IKT-sikkerhet med sporbarhet og pålitelige digitale arkiv.
- Økende teknologiavhengighet krever at den digitale infrastrukturen er robust og at det på tvers av gjensidige avhengigheter og i hele leveransekjeden skapes felles risikoforståelse.
- Digitaliseringen av offentlig sektor stiller høye krav til risikostyring og sikkerhetskompetanse.
- Økt samhandling mellom spesialiserte forvaltningsledd skaper utfordringer med å få sikkerhetsmessig oversikt og felles risikoforståelse.[103]

Helse- og omsorgsdepartementet (HOD) viser i sitt innspill til konkrete utfordringer som kan knyttes direkte til momenter nevnt andre steder i denne rapporten. Dette gjelder blant annet potensialet for bortfall av infrastruktur som for eksempel vann og avløp til sykehus eller elektroniske kommunikasjoner, som vil føre til store vansker, eventuelt stengning av sykehus, med de følger for folkehelsen det vil få. Ved et ekom-bortfall i fem døgn anslås 50 ekstra døde som følge av manglende mulighet til å ringe etter ambulanse og varsle nødetatene ved akutte hendelser. Svikt i Helsenettet og annen IKT-infrastruktur vil gjøre journaler og resepter utilgjengelige. Det er en stor utfordring å sikre helsetjenestens 400.000 medarbeidere tilstrekkelig IKT-kompetanse, også i forhold til nødvendig tilgang til gradert materiale i forbindelse med helseberedskap. Utfordringer med Bruk ditt eget utstyr og Skytjenester finnes også i helsevesenet, særlig i forbindelse med å kunne sikre personvern ved behandling utenfor institusjon med støtte i medbragt IKT-utstyr. Det finnes også mye gammelt utstyr med IKT som det ikke lenger finnes oppdateringer for. HOD peker også på manglende risiko- og sårbarhetsanalyser i virksomhetene og uklare nasjonale ansvarsforhold med hensyn til IKT-sikkerhet[104].

Kritisk infrastruktur kan skades. Det kan planlegges for alvorlig sabotasje eller krigshandlinger i eventuelle fremtidige konflikter. Digitaliseringen av samfunnet har gitt fremmede etterretningstjenester enklere arbeidsvilkår, blant annet fordi sår-

[99] CYFORs innspill.

[100] Se kapittel 5 Trusler og aktører og ordliste.

[101] FFI-rapport.

[102] PSTs innspill.

[103] Innspill fra DIFI.

[104] HOD sitt innspill.

barhetene er store og fordi oppdagelse og identifisering av angriper er utfordrende. Trusselaktørene gjør gode vurderinger av hva som er informasjon av høy verdi. Trusselaktørene jobber stadig mer målrettet, og stadig mer profesjonelt.

Alle typer virksomheter risikerer betydelige økonomiske tap.

6.6 TILTAKSSTATUS

6.6.1 ROLLER OG ANSVAR

Samordningsansvaret for IKT-sikkerhet på sivil side ble i 2013 overført fra det daværende Fornyings-, administrasjons, og kirkedepartementet (FAD), nå Kommunal- og moderniseringsdepartementet (KMD), til Justis- og beredskapsdepartementet (JD). Alt samordningsansvar innen samfunnssikkerhet på sivil side ble samlet i JD. Tilsvarende ansvar på militær side tilligger Forsvarsdepartementet (FD). Ansvaret for koordinering av regjeringens helhetlige IKT-politikk, samt særskilt ansvar for å arbeide for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen ble imidlertid beholdt i KMD. Sentralt utviklingsmiljø for KMD er Direktoratet for forvaltning og IKT (Difi) og sentralt driftsmiljø for departementsfellesskapet er Departementenes sikkerhets- og servicesenter (DSS).

Innenfor sikkerhetslovens område er NSM den nasjonale myndigheten for IKT-sikkerhet. Ved inngangen til inneværende langtidsperiode ble NSMs rolle som ekspertorgan for informasjons- og objektsikkerhet, samt det nasjonale fagmiljøet for IKT-sikkerhet. Gjennom instruks til Sjef NSM av 5.12.2014 er NSM gitt omfattende oppgaver og ansvar for IKT-sikkerhet, herunder å koordinere håndteringen av alvorlige IKT-angrep.

6.6.2 NASJONALE BEREDSKAPSSYSTEMER

Våren 2015 er det gjort enkelte endringer i Nasjonalt beredskapssystem (NBS)[105]. Endringene er av betydning for hvordan IKT-sikkerhetsarbeidet og NSMs oppgaver skal utføres. En viktig endring er at NSMs direktør med utgangspunkt i ansvaret for Varslingssystem for digital infrastruktur (VDI) og den nasjonale responsfunksjonen har fått i oppdrag å iverksette, eller å gi anbefalinger om å iverksette tiltak, og ellers koordinere håndteringen.

6.6.3 FELLES EUROPEISKE STANDARDER

Internasjonal utvikling påvirker også hvordan vi besvarer behovene nasjonalt. IKT-sikkerheter er høyt på agendaen internasjonalt, blant annet i NATO og EU. Utviklingen og implementeringen av EUs program Digital Agenda for Europa vil ha stor betydning også for Norge gjennom vår EØS-tilknytning. IKT-sikkerhet er viet en egen pilar i Digital Agenda, pilar III «Trust & Security». Som en del av oppfølgingen av pilar III er det utarbeidet et forslag til direktiv for forsterket nettverks- og informasjonssikkerhet (NIS-direktivet)[106]. Direktivet vil omfatte offentlig forvaltning, tilbydere av informasjonstjenester for samfunnet, samt eiere og driftere av samfunnskritisk IKT-infrastruktur. Hensikten er å etablere felleseuropeiske sektorovergripende minimumsstandarder for IKT-sikkerhet.

6.6.4 OM ULOVLIG UTSTYR I EKOMNETT[107]

Nkom har arbeidet med kartlegging av sårbarheter og identifisering av tiltak knyttet til de såkalte falske basestasjonene, og til SS7-protokollen[108], som fikk betydelig oppmerksomhet i desember 2014. Nkom har i revidert nasjonalbudsjett for 2015 fått økte ressurser til å etablere 24/7 vaktordning, beredskapsrom, og til utstyrsinvesteringer for å styrke monitoreringskapasiteten for å avdekke bruk av ulovlig utstyr i ekomnett, for eksempel falske basestasjoner.

6.6.5 SIKRING AV DOMENENAVN[109]

DNSSEC (DNS Security Extensions) er en sikkerhetsmekanisme som legges til domenenavnsystemet. Med DNSSEC sikres svaret på et domeneoppslag på en slik måte at det er mulig å kontrollere at det kommer fra riktig kilde, og ikke er endret underveis. UNINETT Norid[110] åpnet for signering med DNSSEC i desember 2014, og allerede nå er nesten halvparten av alle norske domenenavn sikret. Det norske toppdomenet ligger dermed helt på topp i Europa i andel sikrede domener. Videre jobb her vil ligge hos de som driver domenenavntjenester[111] i Norge.

6.6.6 ALLVIS NOR

NSM har etablert en tjeneste som kalles Allvis NOR, for å bedre sikkerheten hos statlige og kommunale aktører, samt øvrige virksomheter underlagt sikkerhetsloven. Tjenesten består i hovedsak av regelmes-

[105] NBS består av Sivilt beredskapssystem (SBS) og Beredskapssystem for forsvarssektoren (BFF). SBS og BFF er vedtatt med hjemmel i beredskapsloven § 18 og Kongens instruksjonsmyndighet.

[106] European Union, The Network and Information Security (NIS) Directive, COM(2013) 48 final, datert 7.2 2013.

[107] Nkom innspill.

[108] Vedrørende sårbarhet som tillater sporing av mobiltelefonbrukere.

[109] Norid innspill.

[110] UNINETT Norid, også omtalt som Norid, driver registeret for norske domenenavn som .no.

[111] Se DNS i ordliste.

sig kartlegging og sårbarhetsundersøkelse av utvalgte IP-adresser som er tilgjengelige på internett. Det foretas ikke sårbarhetsundersøkelser av utstyr eller tjenester som ikke er direkte tilkoblet internett. Alle undersøkelser foretatt av Allvis NOR vil være av ren systemteknisk art. Dette er imidlertid overfladiske undersøkelser som hverken kan eller er ment å erstatte helhetlige sikkerhetsundersøkelser eller inntrengingstester. Tjenesten vil gi NSM bedre muligheter til å gi mer relevant og målrettet rådgiving innen forebyggende IKT-sikkerhet.

6.6.7 HÅNDTERING AV CYBERANGREP

I 1999 etablerte EOS-tjenestene VDI. Hensikten var å gi myndighetene tidlig varsel om koordinerte og alvorlige dataangrep. VDI ble i 2003 lagt til NSM. I 2006 ble VDI utvidet til også å omfatte en nasjonal responsfunksjon ved slike angrep, Norwegian Computer Emergency Response Team (NorCERT). NSM NorCERT skal koordinere håndteringen av alvorlige IKT-hendelser mot samfunnskritisk infrastruktur og informasjon. NorCERT-funksjonen ble etablert som en integrert del av NSM fra 1. januar. NSM NorCERT samarbeider tett med Etterretningstjenesten og PST, blant annet gjennom Cyberkoordineringsgruppen (CKG). Formålet med gruppen er at EOS-tjenestene mest mulig effektivt skal kunne forebygge og håndtere alvorlige cyberangrep, samt gi overordnede beslutningstakere og utsatte virksomheter et best mulig virkemiddel for å iverksette tiltak. NSM støtter i tillegg politiet ved cyberkriminalitet som ikke omfattes av PSTs ansvar. Blant andre særlige nære samarbeidspartnere for NSM i rollen som nasjonal håndteringsinstans er Nkom. Nkom har et oppfølgingsansvar for ekominfrastrukturen, herunder internett i Norge.

Nasjonal strategi for informasjonssikkerhet har utkommet i tre versjoner siden 2003. Den siste versjonen kom i 2012. Strategien gir føringer for videreutvikling av det samlede informasjonssikkerhetsarbeidet i samfunnet. Et viktig grep i strategien er målsettingen om at de enkelte fagdepartementer skal etablere sektorvise responsmiljøer i egen sektor. Sektormiljøer er til nå etablert i Forsvaret (ved Cyberforsvaret/Avdeling for beskyttelse av kritisk infrastruktur – BKI), helsesektoren (HelseCSIRT), finanssektoren (FinansCERT), kraftsektoren (KraftCERT), og universitets- og høyskolesektoren (UNINETT CERT).

Forskningsnettet er et robust høykapasitetsnett for forskning og utdanning, men er i økende grad utsatt for spionasje[112]. Det er iverksatt et program fra 2008 for å få på plass en ledelsesforankret sikkerhetspolicy. UNINETT CERT har utplassert en egen sensorinfrastruktur i det nasjonale forskningsnettet og utvikler dette videre med teknologier som brukes av NorCERT (VDI). UNINETT CERT har etablert redundanser i sine nettverk og i sikkerhetsløsningene, dessuten er det etablert redundans i de norske samtrafikkpunktene (NIX) drevet av Universitetet i Oslo.

Det vil bli opprettet en CERT for justissektoren. Det er etablert et responsteam for et felles datautvekslingssystem og et informasjonsforum knyttet til sikkerhet og beredskap for olje- og gassbransjen. Nkom har nylig ansatt leder for Nkom-CSIRT, som nå skal bygges opp i løpet av en toårsperiode for å koordinere håndteringen av logiske hendelser i ekom-sektoren, i tråd med Nasjonal strategi for informasjonssikkerhet[113].

6.6.8 SON

Sikrere offentlig nett (SON) utredes som en mulighet for et sikrere «nett i nettet», med tilgang til en redundant høyhastighets internettforbindelse. SON gir mulighet til å koble fra internett og fremdeles kommunisere mellom aktørene. SON vil bidra til å sikre kritisk infrastruktur og gjøre det mulig å beskytte seg bedre mot blant annet tjenestenektangrep. SON kan også benyttes for å stoppe trafikk mot internettadresser som er skadelige eller leverer virus. NSM kan tilby deltagerne i nettet sikkerhetsgraderte sensorer, noe som i betydelig grad styrker den nasjonale deteksjonsevnen.

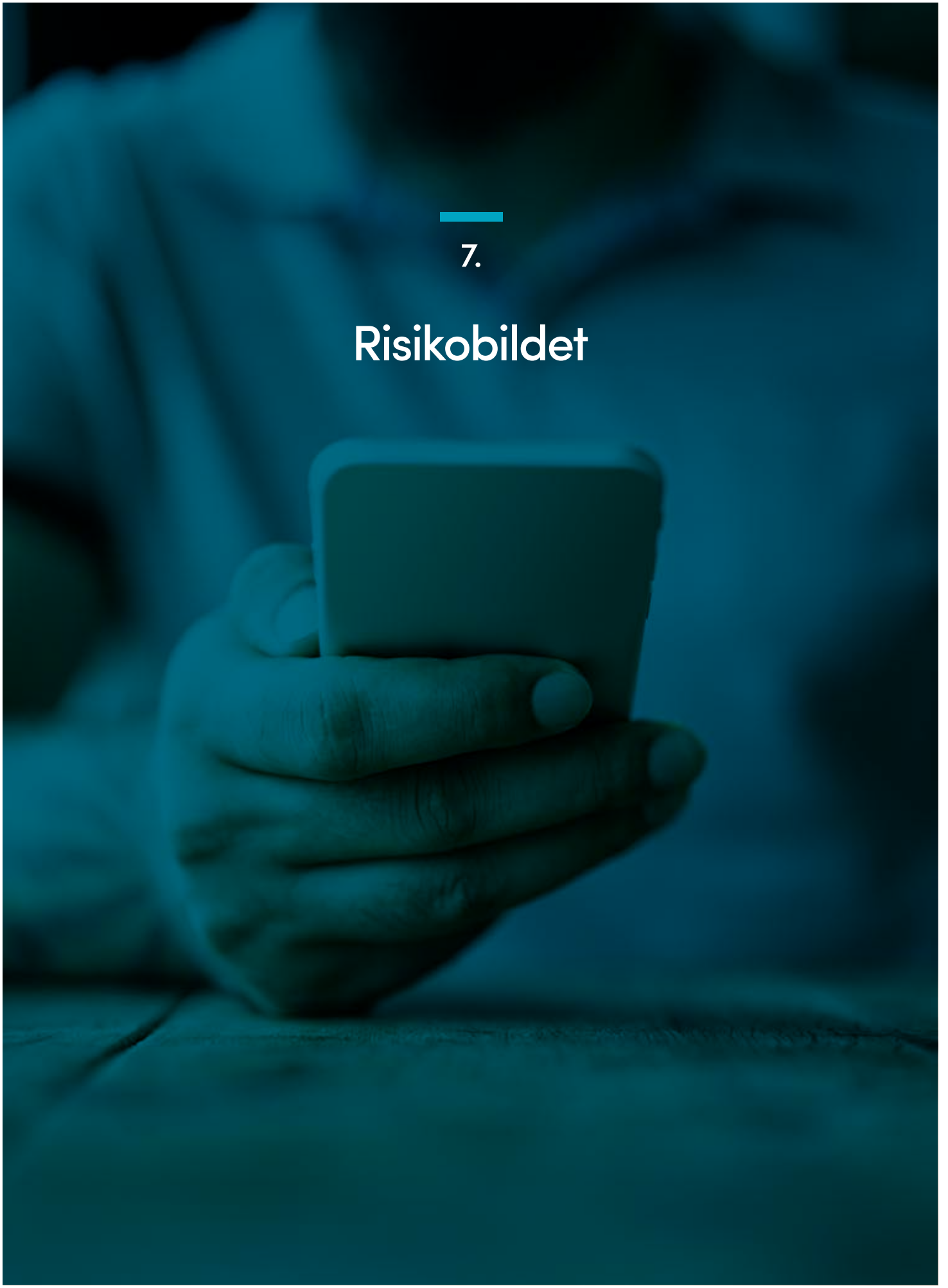
6.6.9 INTERNASJONALT SAMARBEID

De fleste virksomhetene som har med IKT-sikkerhet å gjøre, deltar i forskjellige former for internasjonale fora, for eksempel EU, NATO, FN, OECD og diverse fagfora. I noen tilfeller koordineres deltagelsen nasjonalt.

NSM NorCERT deltar blant annet i European Government CERTs Group (EGC), som er et samarbeid mellom nasjonale CERTer i Europa og i Nordic CERT Cooperation (NCC). Det er også et samarbeid med NATOs CERT (NCIRC) og bilaterale samarbeid med en rekke land. ⊙

[112] UNINETT CERT innspill.

[113] Nkom innspill.



7.

Risikobildet

Risikobildet har blitt mer komplekst. Det forvaltes store verdier i Norge i dag, som andre kan ha interesse av å tilegne seg for egen vinning eller å skade. På flere områder er trusselen høy og økende. Norske interesser utsettes daglig for cyberangrep og mange er alvorlige.

7.1 METODISK GRUNNLAG

Et risikobilde er summen av verdier, trusler og sårbarheter i samfunnet vårt. Terminologien er definert i Norsk Standard[114].

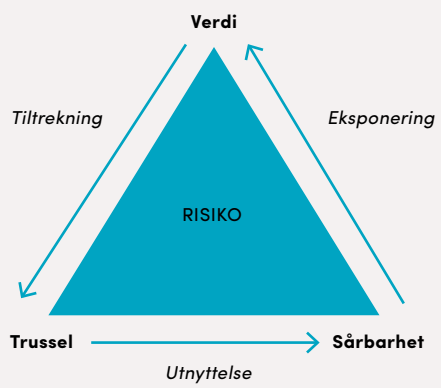
Risiko for uønskede tilsiktede handlinger kan illustreres som en trekant, hvor det finnes sammenhenger mellom faktorene verdi, trussel og sårbarhet:

Uavhengig av hvor samfunnet velger å legge et akseptabelt risikonivå, er det avgjørende å være kjent med egne verdier og sårbarheter, samt trusler mot disse, når slike beslutninger fattes.

For å kunne beskytte samfunnets verdier, må det tas tak i det som det kan gjøres noe med, det vil si å redusere samfunnets *sårbarhet*. Arbeidet med å redusere sårbarheter må styrkes på alle nivåer i samfunnet, i det offentlige, i næringslivet og hos den enkelte.

Erfaringer i forbindelse med kriser og hendelser er at man i mange tilfeller ikke kan forvente at det vil være en varslingstid som gir mulighet til å iverksette ytterligere tiltak. Derfor må det prioriteres å ha en god grunnsikring og evne til å håndtere hendelser. God risikostyring er et viktig virkemiddel.

FIGUR 1: VERDI TILTREKKER TRUSSEL, TRUSSEL UTNYTTER SÅRBARHET, SÅRBARHET EKSPONERER VERDI.



7.2 VERDIER OG INTERESSER

Norske statlige og private virksomheter har betydelige verdier som er ettertraktet for trusselaktørene. Trusselaktørene gjør gode vurderinger av hva som er informasjon av høy verdi. De siste årene er datanettverksoperasjoner mot norsk forsvars-, sikkerhets- og beredskapssektor, politiske prosesser, norsk kritisk infrastruktur og enkeltvirksomheter eksempelvis innen petroleum, kraft, romfart, shipping og tele blitt oppdaget. Dette viser hva aktørene er ute etter.

7.3 FARER OG TRUSLER

Det en vedvarende økning av uønskede hendelser og handlinger via IKT og internett. Utbredelse av og kompleksiteter i IKT fører til økende utfordringer alene. Feil og mangler knyttet til internett og bruken av det har global spredning. Uønskede handlinger fortsetter å øke i antall og kompleksitet. I 2014 varslet og håndterte NSM totalt 88 alvorlige dataangrep, mot 51 i 2013. Dette tallet er sunket til 13 hittil i år. Samtidig har vi registrert 13.773 saker og håndtert 2.943 saker pr. 31. august 2015, mot henholdsvis totalt 17.662 registrerte og 5.066 håndterte saker i hele 2014. Det antas at dette blant annet gjenspeiler at truslene er blitt mer avanserte og vanskelige å oppdage.

De mest kraftfulle vedvarende truslene på nettet dreier seg hovedsakelig om spionasje. Flere omfattende spionasjeoperasjoner er blitt kjent gjennom åpne kilder.

Sabotasje eller terrorisme over internett i fremtiden kan ikke utelukkes, spesielt ikke hvis mindre rasjonelle aktører tilegner seg relevante teknologier. Potensialet for sabotasje mot norske interesser, politiske myndigheter og kritisk infrastruktur anses som en alvorlig trussel.

7.4 SÅRBARHETER

NSM finner store sårbarheter i det norske samfunnet med hensyn til IKT.

[114] Norsk Standard NS 5830:2012 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger. Terminologi. Se ordliste for nærmere definisjon av begrepene risiko, risikobilde, verdi, trussel og sårbarhet.

Det er store mangler i det forebyggende IKT-sikkerhetsarbeidet. Dette ser NSM på bakgrunn av de hendelsene vi bidrar til å håndtere, og gjennom andre aktiviteter som for eksempel inntrengningstesting. Ofte er det grunnleggende mangler som gjør det lett for trusselaktørene. Dersom virksomheter på alle nivåer hadde gjennomført grunnleggende IKT-sikkerhetstiltak, slik som NSMs 10 (4+6) anbefalte grunnleggende tiltak[115], ville sårbarhetsnivået vært betydelig lavere og lettere å håndtere.

Det finnes menneskelige sårbarheter som kan utnyttes, gjerne i kombinasjon med tekniske sårbarheter. Sosial manipulering er et eksempel på dette. Gjennom egne undersøkelser og kunnskap om konkrete hendelser har NSM sett eksempler på store sårbarheter som andre kan ha interesse av å utnytte for å nå sine egne mål. Mange av sårbarhetene er av en slik art at nesten hvem som helst kan utnytte dem. Det gjør det for lett for alle som har onde hensikter. NSM har gjennom sikkerhetsfaglig råd identifisert en rekke sårbarheter på nasjonalt nivå. Mange av disse har relevans for IKT-risikobildet. Det er kritiske mangel på kompetanse innenfor IKT-sikkerhet og IKT-sikkerhetsspesialister. Rolleforståelse, anerkjennelse av roller og tydelig kommunisering av disse er også viktig. Den samlede nasjonale håndteringskapasiteten er heller ikke robust nok. Det gjelder både på sentralt nivå i NSM NorCERT, og i håndteringsmiljøene i de enkelte sektorer.

7.5 NSMS VURDERING AV IKT-RISIKOBILDET

NSM vurderer at alle viktige trender som påvirker IKT-risikobildet vil fortsette. Noen av dem har preg av gjennombrudd, for eksempel den teknologiske utviklingen, og vil utvikle seg raskt. Teknologiutviklingen har ført til store endringer i evnen til å behandle store mengder data. Kapasitetsutviklingen vil fortsette, stordatatrenden vil øke og vil bli utnyttet til kapasitetsgrensen, for forskjellige formål. Alle som bruker og beveger seg på internett har, på godt og ondt, global rekkevidde og tilgjengelighet.

Teknologiutviklingen vil gjøre det lettere for trusselaktørene å gjennomføre sine forsetter enn det vil bli for IKT-sikkerhetsmiljøene å hindre dem. Alle trusselaktører kan i prinsippet operere hvor som helst i verden. Det er for eksempel lite som hindrer utvikling av store transnasjonale kriminelle nettverk.

Svært mye av den fysiske virkeligheten er tilgjengelig gjennom internett, i form av informasjon eller i form av muligheter for direkte styring av fysiske prosesser. Informasjon i informasjonssamfunnet er blitt et mer omfattende begrep enn det folk har vært vant til. Penger på en bankkonto eksisterer for eksempel i form av elektronisk informasjon og ikke i form av fysiske informasjonsbærere som sedler og mynter.

7.5.1 RISIKOBILDET PÅ NASJONALT NIVÅ

Sett i lys av at samfunnets verdier øker, at truslene mot dem øker og at det finnes betydelige sårbarheter knyttet til IKT-sikkerhet, finner NSM grunn til å fremsette følgende vurderinger om IKT- risikobildet på nasjonalt nivå slik det fremstår høsten 2015:

Vedrørende kunnskap:

- Det er betydelig langsiktig risiko forbundet med at det ikke utdannes tilstrekkelig antall personer som har relevant kompetanse innen forebyggende sikkerhet på IKT-området, på alle nivåer i undervisningskjeden og ute i virksomhetene. Dette hemmer evnen til å gjennomføre gode IKT-sikkerhetstiltak og tekniske IKT-tilsyn. Det vil også hemme evnen til å forbedre risikobevissthet hos brukere av IKT-systemer. Denne risikoen vil øke dersom det ikke tas tak i den.
- Det er stor og akutt risiko forbundet med at det ikke utdannes tilstrekkelig antall personer med spesialistkompetanse innen hendelseshåndtering på IKT-området. Dette vil sannsynligvis føre til at det nasjonalt ikke vil finnes tilstrekkelig antall ressurspersoner til å håndtere større IKT-angrep, eksempelvis mot kritisk infrastruktur. Risikoen er allerede stor og forventes å øke inntil tilstrekkelig og relevant undervisningskapasitet er godt etablert.

[115] Se kapittel 8.

- Det er risiko forbundet med manglende kapasitet i NSM og eventuelt i andre IKT-sikkerhetsmiljøer til å følge med på konsekvensene av den teknologiske utviklingen for IKT-sikkerhetsområdet. Dette kan føre til at raske teknologiendringer ikke fanges opp til rett tid i politikkutformingen.

Vedrørende overordnet styring:
- Det er risiko forbundet med rolleforståelsen mellom styrende organer og mellom utøvende organer. Dette kan føre til utilstrekkelig koordinering både av politikkutformingen og av gjennomføring av forebyggende tiltak. Videre kan dette være en hemsko under krisehåndtering. Det viser seg for eksempel at evnen til samvirke på IKT-området i krisesituasjoner ikke er tilstrekkelig utviklet. Situasjonen vil vedvare uten ytterligere tiltak.
- Det er risiko forbundet med bruk av styringsdokumenter som kan fremstå som ikke tilstrekkelig oppdaterte eller utilstrekkelig utviklet, slik som Nasjonal strategi for informasjonssikkerhet av 2012.
- Det er risiko forbundet med at utvikling, forvaltning, og drift av offentlige IKT-løsninger ikke er bedre samordnet. Dette fører til forskjellige tilnærminger til IKT-sikkerhet og kan skape svake ledd i den forebyggende sikkerheten.

Vedrørende forebyggende evne:
- Det er stor risiko forbundet med at store og små virksomheter ikke tar i bruk grunnleggende tiltak for å sikre sine IKT-systemer, jf NSMs anbefaling om 10 grunnleggende tiltak[116].
- Det er betydelig risiko forbundet med mangel på fellesløsninger for IKT-systemer for sensitiv, lavgradert og høygradert informasjon. Dette er en utfordring for den forebyggende sikkerheten og fører ofte til dårlig informasjonssikkerhet. Denne mangelen kan være kritisk i en krisesituasjon.
- Det er risiko forbundet med at ugraderte elektroniske kommunikasjoner i liten grad blir kryptert. Terskelen for vellykket avlytting blir unødvendig lav og ugradert sensitiv informasjon kan kompromitteres. I den grad sikkerhetsgradert informasjon kommer over på ugraderte nett, er risikoen betydelig.
- Det er betydelig risiko for at mangelfull rapportering av alvorlige IKT-hendelser vil svekke evne til forbedring og læring innen forebyggende IKT-sikkerhet.
- Det er risiko forbundet med at viktige virkemidler for forebyggende IKT-sikkerhet ikke er tilstrekkelig utviklet eller tilstrekkelig tatt i bruk. Dette gjelder bruk av inntrengningstesting, digitale sertifikater og akkreditering av leverandører av IKT-sikkerhet. Dette kan føre til at forebyggende evne svikter og til unødvendig belastning på miljøer for hendelseshåndtering.

Vedrørende operativ evne og evne til krisehåndtering:
- Det er stor risiko forbundet med at den nasjonale CERT-funksjonen, sammen med sektorvise håndteringsmiljøer, ikke er robust nok til å møte fremtidens utfordringer. Inntil dette forbedres, er det sannsynlig at eventuelle store IKT-angrep mot kritisk infrastruktur og andre sentrale nasjonale interesser ikke blir tilfredsstillende håndtert.
- Det er stor risiko forbundet med at den nasjonale evnen til å detektere IKT-hendelser ikke er tilstrekkelig videreutviklet. Dette kan føre til at betydelige IKT-angrep ikke blir oppdaget på rett tidspunkt og at mottiltak kommer for sent.

7.5.2 RISIKO FOR VIRKSOMHETER OG INDIVIDER

Store virksomheter er utsatt for mye av den samme risiko som nasjonen. Store næringslivsaktører med store verdier må i tillegg regne med risiko med hensyn til forsøk på:
- Tyveri av elektronisk tilgjengelige aktiva.
- Industrispionasje og andre former for tyveri av kunnskap og intellektuell kapital.
- Generering av driftsavbrudd eller annen form for sabotasje.

[116] Se kapittel 8.

- Å bringe virksomheten i vanry.
- Illojal konkurranse gjennom å skaffe seg informasjonsfordeler.

For små virksomheter er ofte den største risikokomponenten deres egen sårbarhet. Digital sorgløshet er nevnt som en viktig faktor. For små virksomheter og individer er det risiko særlig med hensyn til:

- Identitetstyveri og mulige konsekvenser av dette, for eksempel at gjerninger begås i ditt navn.
- Tap av eierskap eller kontroll over til din egen informasjon, for eksempel bankkonto, navn, personnummer eller eiendomsskjøter.
- Økonomiske tap som ikke kan bæres.
- Tap av privatliv og personlig informasjon.
- Tap av ditt gode rykte.

De enkelte virksomheter har begrenset evne til å vurdere risiko utover den virksomheten selv direkte står overfor, eksempelvis risiko knyttet til funksjonen virksomheten har i et større samfunnsperspektiv. Virksomhetene selv og myndighetene har begrenset kapasitet til å oppdage ondsinnede handlinger, og det er for stor forsinkelse fra man eventuelt oppdager hendelser til effektiv skadereduserende respons blir gjennomført.

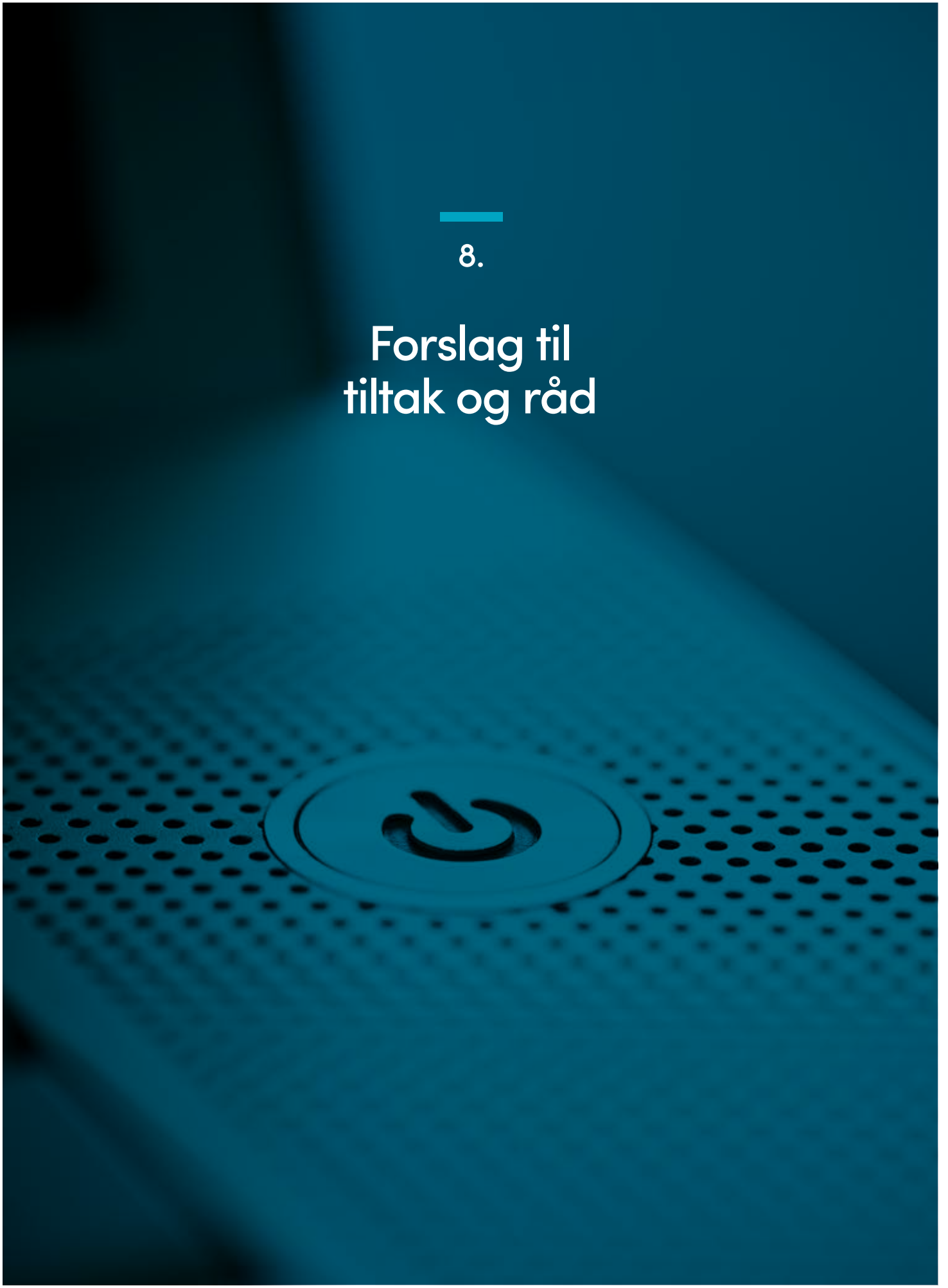
7.6 OVERORDNET VURDERING AV IKT-RISIKO

NSMs overordnede vurdering av IKT-risikobildet er at det er stor risiko forbundet med bruk av IKT. Det gjelder på alle nivå i samfunnet.

Trusselen er høy og økende, og det er store sårbarheter i norske IKT-systemer. Konsekvensen av mangelfull IKT-sikkerhet er at store verdier kan gå tapt, i et spenn fra individets gode navn og rykte, til nasjonal selvstendighet.

Helt grunnleggende sikkerhetstiltak er ofte ikke gjennomført eller mangelfullt implementert.

For å redusere risikoen er det behov for en omfattende nasjonal satsning på IKT-sikkerhet i årene som kommer.



8.

Forslag til tiltak og råd

NSM har fått i oppgave å utarbeide et sikkerhetsfaglig råd (SFR) til Forsvarsministeren. Forsvarssjefen er også gitt i oppdrag å fremme et militærfaglig råd (FMR). Disse rådene skal danne grunnlag for en ny langtidsplan for perioden 2017-2020 for forsvarssektoren og for en melding til Stortinget om samfunnssikkerhet.

Mange av tiltakene i dette kapitlet er hentet fra relevante deler av NSMs sikkerhetsfaglige råd. Disse tiltakene er forkortet, og det henvises til sikkerhetsfaglig råd for detaljer. Andre tiltak retter seg mot virksomheter og individer. Det vises her til veiledninger for mer informasjon, både hos NSM og hos andre virksomheter.

Formålet med dette kapitlet er å bidra til at forebyggende sikkerhet på IKT-området blir forstått og å formidle løsninger.

8.1 NASJONALE TILTAK, FORSLAG

Grunnlaget for dette delkapitlet er NSMs sikkerhetsfaglige råd, hvor NSM blant annet foreslår en rekke tiltak for å styrke IKT-sikkerheten på nasjonalt nivå.

NSMs viktigste budskap er at det er behov for en omfattende nasjonal satsing på IKT-sikkerhet i årene som kommer.

NSMs sikkerhetsfaglige råd foreslår til sammen 72 ulike tiltak på områder som organisering, ledelse og koordinering, IKT-sikkerhet, personellsikkerhet, fysisk sikkerhet, samarbeid med næringslivet, kompetanse, og tiltak for å øke Forsvarets operative evne. Her presenteres de viktigste tiltakene som har relevans for IKT-sikkerhet.

Universiteter og høyskoler må satse sterkere på utdanning innen IKT-sikkerhet, blant annet gjennom å etablere bachelor- og mastergrader i IKT-sikkerhet, men også ved å ta inn IKT-sikkerhet som et obligatorisk fag for alle som utdanner seg innen IKT. IKT-sikkerhet bør også bli en del av lærerutdanningen.

NSM anbefaler ikke at det gjøres endringer i organisering og struktur for samfunnssikkerhet og beredskap slik den fremstår etter 22. juli-hendelsen. Derimot må det gjøres noe for å få denne strukturen til å fungere bedre. Det er nødvendig med bedre koordinering og samarbeid. NSM foreslår *å tydeliggjøre roller, og utvikle rolleforståelsen*. Nasjonal evne og vilje til samarbeid er avgjørende. Til dette hører også å anerkjenne hverandres oppgaver og ulike roller.

NSM foreslår flere tiltak som har til formål å styrke samarbeidet og koordineringsevnen. Eksisterende arenaer foreslås videreutviklet og det foreslås også at det etableres nye arenaer i en formalisert og helhetlig struktur. Det gjelder spesielt på IKT-sikkerhetsområdet.

Justis- og beredskapsdepartementets samordningsrolle for sivil samfunnssikkerhet må *tydeliggjøres ytterligere*. Det er spesielt viktig at Justis- og beredskapsdepartementets koordinerende rolle blir anerkjent. Andre departementer og sektormyndigheter må akseptere den rollen Justis- og beredskapsdepartementet har. Ansvarsforholdene må kommuniseres på en måte som gir bred forståelse i samfunnet.

NSM foreslår en rekke tiltak for å styrke evnen til å stoppe cyberangrep mot Norge. Grovt sett kan tiltakene deles i to: For det første de som har til hensikt å etablere motstandsdyktighet, ofte benevnt forebyggende tiltak. For det andre de som har som formål å avdekke og håndtere hendelser når de skjer, ofte kalt beredskapstiltak. Noen av dem løftes frem her:

- *Kryptering* er ett av de mest effektfulle enkelttiltakene som anbefales for å øke motstandsevnen. Det bør stilles nasjonale krav om bruk av kryptering av sensitiv informasjon, og det anbefales utstrakt bruk av kryptering i forvaltningen.
- *Inntrengningstesting* bidrar til å identifisere faktiske sårbarheter i egne systemer, og gir et godt grunnlag for å målrette ulike sikringstiltak. Det bør i enkelte tilfeller stilles krav til inntrengningstesting i systemer som behandler sensitiv informasjon.
- Det er i ferd med å etableres et *sikrere offentlig nett*. Arbeidet har fått arbeidsnavnet SON. Hensikten er blant annet å få kontroll på antall tilganger til internett, slik at sårbarheten for den enkelte systemeier reduseres. Dette er et meget godt sikringstiltak og NSM anbefaler at dette videreutvikles og styrkes så det kan omfatte større deler av offentlig forvaltning.

- Det er behov for flere *felles IKT-løsninger med ulike sikringsnivåer*, spesielt i offentlig forvaltning. Dagens fragmenterte løsninger svekker både funksjonaliteten og sikkerheten og er kostbart. Fellesløsninger kan ha stordriftsfordeler, bidra til forenkling og vil bidra til økt sikkerhet. NSM foreslår også at antall utviklings- og forvaltningsorganisasjoner i offentlig sektor reduseres for å skape mer robuste og kompetente miljøer.
- NSM foreslår å utvikle *nasjonale anbefalinger og minimumskrav til IKT-sikkerhet*. NSM har spilt inn flere forslag til lovendringer, blant annet forslag til lov om sikring av sensitiv informasjon og informasjonsinfrastruktur.

Evnen til å håndtere cyberangrep og andre sikkerhetstruende hendelser er en betydelig utfordring. Den nasjonale evnen til å *oppdage* alvorlige cyberangrep mot norske interesser må styrkes: Sensornettverket VDI må styrkes for å kunne gi et tilstrekkelig bilde av den nasjonale IKT-sikkerhetstilstanden. I dag er deltagelse basert på frivillighet og evne og vilje til å betale for deltakelsen. NSM mener at det er for stor risiko forbundet med dette. Utvikling, anskaffelse og drift av sensornettverket bør fullfinansieres av det offentlige og deltakelse i samarbeidet må formaliseres og gjøres obligatorisk for virksomheter som har kritisk IKT-infrastruktur eller viktige samfunnsfunksjoner.

Den nasjonale evnen til å *varsle og koordinere håndteringen* av cyberangrep, NSM NorCERT, må styrkes betydelig. NSM NorCERT skal ivareta den nasjonale koordineringen, men samtidig jobbe tett sammen med, og gjennom, responsmiljøene i sektorene, eiere av kritisk IKT-infrastruktur og viktige samfunnsfunksjoner når noe skjer. Alle ledd i denne verdikjeden må styrkes. Det er også behov for formaliserte samhandlingsarenaer mellom disse aktørene. Slike arenaer er viktige for deling av informasjon før, under og etter hendelser. For å dele hendelsesinformasjon mest mulig effektivt og i sann tid, er det behov for automatiserte løsninger for alle aktører.

NSM ønsker å legge til rette for at private bedrifter i større grad kan kvalifiseres til å supplere de oppgaver som NSM har, slik at den samlede leveranseevnen kan økes. Kvalifisering gjennom *akkrediteringsordninger* vil gjøre det lettere for virksomheter å velge kvalitetssikrede leverandører av sikkerhetstjenester og -produkter. Det anbefales også å forbedre informasjonen om det offentliges behov for sikkerhetstjenester og -produkter, og dermed legge bedre til rette for næringslivets fremtidige markedsmuligheter.

For nærmere detaljer henvises til til NSMs sikkerhetsfaglige råd.

8.2 RÅD TIL STORE OG SMÅ VIRKSOMHETER

8.2.1 DEN GRUNNLEGGENDE STYRINGEN

IKT-sikkerhet må inn på agendaen i styrerommene[117]. Det bør innføres god selskapsledelse også for forebyggende IKT-sikkerhet, det vil si å sikre en hensiktsmessig rolle- og ansvarsfordeling i forbindelse med kontroll og styring av organisasjonen. Et vesentlig element av god selskapsledelse er risikostyring og revisjon. Iverksett grunnleggende sikkerhetsstyring i virksomheten[118], herunder disse overordnede elementene:

- **Forankring:** Styring av sikkerhet må *forankres* hos virksomhetens ledelse. Ledelsen må sette mål for sikkerhet, tildele nødvendige ressurser, og evaluere sikkerhetstilstanden i virksomheten årlig. Basert på evalueringen kan ledelsen sette nye mål og ambisjoner for sikkerhetsarbeidet.
- **Forpliktelse:** Virksomheten må *forplikte* seg og dokumentere klare føringer for sikkerhetsarbeidet. Det må etableres en tydelig ansvarsfordeling og klare rapporteringslinjer for å sikre at alle oppgaver i realiteten gjennomføres.
- **Forståelse:** Det må arbeides kontinuerlig med å bevisstgjøre, motivere, *øke forståelsen* og heve kompetansen innen sikkerhet på alle nivåer i virksomheten. En virksomhet er avhengig av at støttefunksjoner, som eksempelvis IT-drift og HR fungerer, og det må settes mål og krav til disse som er i samsvar med hovedmålene også innen sikkerhet.

IKKE gjør den enkelte medarbeider de facto eneansvarlig for virksomhetens IKT-sikkerhet. Test egen sikkerhet. Vær åpen om angrep og angrepsforsøk, så andre kan lære av det. Ha gode og oppdaterte tilgangskontroller, gi administratorrettigheter kun til

[117] Cisco ibid.

[118] Google NSM, Veileder i sikkerhetsstyring, 10. mars 2015.

noen få navngitte personer i forbindelse med definerte oppgaver, logg og analysér aktivitet, ha arbeidsdeling slik at ikke en angriper kan benytte en og samme bruker til å utsette virksomheten for store tap eller stor fare, samt kjenne trafikkmønstre slik at avvik lettere kan oppdages[119]. Behold tilstrekkelig kompetanse i virksomheten med hensyn til kravspesifikasjon og leveransekontroll når du utkontrakterer.

I små virksomheter, hvor mange funksjoner blir samlet på få personer, er det kanskje ekstra viktig med god sikkerhetskultur og høy sikkerhetsbevissthet. For å sikre virksomhetens verdier og redusere sårbarheter må både ledere og ansatte ha nødvendig kompetanse.

8.2.2 DE GRUNNLEGGENDE TILTAKENE

Samtidig som metoder hele tiden utvikles og forbedres, benyttes fortsatt enkle angrep når det er tilstrekkelig for å nå målet. Mange angrep vil derfor kunne avverges ved hjelp av helt grunnleggende tiltak[120].

Selv store og/eller profesjonelle virksomheter legger ofte ikke tilstrekkelig vekt på å gjennomføre disse 10 (4+6) tiltakene. I enkelte tilfeller må de betale dyrt for det, i form av tap av store pengesummer eller tap av tillit til at de er i stand til å gjennomføre sitt samfunnsoppdrag.

NSM anbefaler at følgende grunnleggende IKT-sikkerhetstiltak[121] gjennomføres:

Disse fire tiltakene stopper 80-90 % av internettrelaterte angrep:

- **Oppgrader program- og maskinvare.** Nyere produktversjoner har tettet flere sikkerhetshull enn eldre versjoner og de har ofte flere og bedre sikkerhetsfunksjoner.
- **Installer sikkerhetsoppdateringer så fort som mulig.** Selv de beste produktene har feil og sårbarheter som kan bli utnyttet av angripere. Systemeiere bør etablere et sentralt styrt regime for oppdatering av applikasjoner, operativsystemer og firmware (f. eks. BIOS-kode).
- **Ikke tildel sluttbrukere administratorrettigheter.** De fleste sluttbrukere har ikke behov for administratorrettigheter. I et sentralt administrert system kan sluttbrukere få den programvaren de trenger fra et felles distribusjonspunkt.
- **Blokker kjøring av ikke-autoriserte programmer («hvitelisting»).** La brukerne bare kjøre godkjente applikasjoner ved å bruke verktøy som Windows AppLocker. Blokker spesielt programmer utenfor godkjente mapper og på flyttbare media, som for eksempel på CD'er og minnepinner.

Seks tilleggstiltak:

- Aktiver kodebeskyttelse mot ukjente sårbarheter for å styrke systemet mot sårbarheter i applikasjoner og operativsystemet, selv når det ikke finnes en oppdatering.
- Herde applikasjoner for å begrense skadeomfanget ved kompromittering. Deaktiver unødvendig mobil kode og makroer.
- Bruk klientbrannmur. Windows Firewall eller tilsvarende blokkerer all ubedt innkommende trafikk og logger sikkerhetsrelevante hendelser i brannmuren. Inspiser loggfilene regelmessig.
- Bruk sikker oppstart og diskkryptering. Windows Secure Startup og Windows BitLocker vil oppdage manipulering av oppstartsprosessen og forhindre tap av data fra stjålne eller tapte PCer.
- Bruk antivirus / anti-skadevare. Antivirus blokkerer kjent skadevare som blant annet utnytter sårbarheter i epost-programmer og dokumentlesere.
- Ikke ta i bruk flere applikasjoner og funksjoner enn nødvendig. Enhver ny applikasjon og funksjon øker mulighetene for angrep og må herdes og oppdateres.

Disse tiltakene stopper lavnivå trusler, men ikke målrettede angrep fra APTer.

Under gjennomføring av IKT-tilsyn har NSM erfart at få virksomheter har implementert alle de fire mest effektive overnevnte tiltakene, og de færreste har implementert tiltakene på en effektiv måte. Videre erfaringer tilsier at svært få, om noen, har effektivt implementert de 10 overnevnte tiltakene.

8.2.3 OM NETTSKYEN

Dersom man vurderer å ta i bruk en skyleverandør, bør man i vurderingen ta hensyn til hvilke land dataene passerer ved lagring, transport og behandling.

[119] Finanstilsynet ibid.

[120] Varianter av en slik tipunktsliste utgis av myndighetene i flere land, for eksempel i USA og Storbritannia.

[121] NSM, Veileder, Ti viktige tiltak mot dataangrep, se også NSM lenke Veiledning for systemteknisk sikkerhet for detaljer.

Dette blir særdeles viktig dersom dataene passerer leverandører eller IKT-infrastruktur i land vi vanligvis ikke sammenligner oss med. Momenter man bør ta hensyn til vil for eksempel være: Sikkerhetspolitiske betraktninger, vertslandets samfunnsforhold og stabilitet, hvorvidt det eksisterer en god handelsavtale med Norge, hvorvidt landet er underlagt regelverk knyttet til sikkerhet og personvern, hvorvidt leverandøren er seriøs i et lengre tidsperspektiv, og hvorvidt IKT-sikkerhet er ivaretatt i leverandørens virksomhetsprosesser. Videre er det avgjørende å inngå en solid og utfyllende leiekontrakt (Service Level Agreement, SLA) – spesielt med tanke på eierskapet til egen informasjon og metadata, tilgangskontroll til data, samt IKT-spesifikke krav (oppetid, konfidensialitet, krypto-nøkkelhåndtering, backup, exit-strategi og autonomi-krav).

I tillegg bør man undersøke om informasjonen man ønsker å plassere i skyen er underlagt lovpålagte eller virksomhetsinterne krav til å ha fysisk kontroll og synlighet på hvor informasjonen fysisk er lagret. I noen tilfeller kan sikkerhetsløsninger i nettskyen være bedre og enklere å forholde seg til enn mindre gode sikkerhetsløsninger i den enkelte virksomhet. I så fall må det inngås kontrakter og utvikles løsninger som gir virksomhetene en fornuftig grad av kontroll over egen sikkerhet.

Skytjenester innebærer at flere ulike virksomheter leier delte IKT-ressurser hos en kommersiell leverandør, såkalt multi tenancy. I slike scenarier er det viktig at IKT-sikkerheten er justert for å tilby sterk gjennomgående kundeseparasjon, eksempelvis innen datanettverk, servere og lagring.

8.2.4 OM BRUK DITT EGET UTSTYR (BYOD)

En bedre løsning på *Bring Your Own Device* er at medarbeidere får med seg arbeidsgivers IKT-utstyr til hjemmekontor eller reisebruk. De samme fordelene som nevnt i kapittel 3 kan oppnås gjennom velg ditt eget utstyr. Dette vil si at arbeidstaker velger utstyr godkjent av arbeidsgiver og at dette utstyret enten er dedikert utelukkende for virksomhetsrelevant bruk og/eller har installert såkalt konteinerisering. Dette vil si at virksomhetens informasjon lagres i en egen passordbeskyttet og kryptert virtuell boks i utstyret, som kan fjernslettes av arbeidsgiver ved behov, og forhåpentligvis før profesjonelle etterretningsaktører rekker å knekke passord og dekryptere innhold[122]. Dette forutsetter at trusselaktør ikke har hatt fysisk adgang til å modifisere utstyr og at det er installert sterk logisk sikring i det.

8.2.5 OM UHELL OG ULYKKER[123]

Om det er mulig, bør virksomheten sikre seg at viktige funksjoner kan videreføres uten IKT eller med redusert kvalitet på IKT. Det bør sikres reservestrømløsninger og redundante kommunikasjonsløsninger for slike funksjoner. Det bør finnes en plan B, jf. kraftforsyningens planer om bemanning av nøkkelpunkter. Viktige komponenter bør plasseres slik at risiko for fysisk skade gjøres så liten som mulig.

8.2.6 OM ANSATTE SOM ER SPESIELT UTSATT

Virksomheten bør etablere tiltak for ansatte som i kraft av stilling eller andre egenskaper bør antas å være potensielle mål for personlig, målrettet IKT-angrep, spesielt en APT[124]. Disse personene skal være utstyrt med og bruke IKT-utstyr som er levert og kontrollert av virksomheten og skal ha fått relevant opplæring og instruks. Det bør være spesiell oppmerksomhet rundt risiko forbundet med reisevirksomhet.

[122] Se imidlertid også nedenfor.

[123] DSBs innspill.

[124] Advanced Persistant Treath, se ordliste.

Vedlegg 1
Ordliste

APT 28
Skadevaresett, sannsynlig russisk aktør (se Fireeye i litteraturliste).

APT 30
Skadevaresett, sannsynlig kinesisk aktør (se Fireeye i litteraturliste).

Autentisering
Verifisere identiteten og andre egenskaper til en bruker. Sterk autentisering / to-faktor-autentisering = autentisering ved bruk av flere metoder, f.eks. minst to av pinkode, passord, fingeravtrykk.

Autorisering
Privilegert tilgang til IKT-system for autentisert bruker.

Avanserte vedvarende trusler (Advanced Persistent Threats, APT)
Vedvarende og målrettet angrep på systemer med formål å etablere bakdører, plante og spre skadevare og hente ut fortrolig informasjon. Angriperen er gjerne ressurssterk, bruker avansert skadevare og opererer langsiktig. Også betegnelse på aktøren bak et slikt angrep.

Bakdør
Skadevare som gir angriper uautorisert adgang til og mulighet til å kontrollere systemer.

BFI
Beredskapsutvalget for finansiell infrastruktur; ledes av Finanstilsynet og koordinerer krisehåndtering i finanssektoren. Se også FinansCERT.

BIOS/UEFI
Basic Input/Output System, erstattes av Unified Extensible Firmware Interface. Fastvare (innebygd program) for oppstart av datamaskin.

Bitcoin
Eksempel på virtuell valuta, det vil si et elektronisk betalingsmiddel som omgår bankvesenet og er utenfor myndighetskontroll.

Border Gateway Protocol (BGP)
Internettets «telefonsentral». Protokoll (regelsett) for å forbinde internettdomener med hverandre.

Botnett
Et nettverk av infiserte og samarbeidende datamaskiner som kan styres av en angriper, ofte for ulovlige formål. Eieren av en infisert datamaskin vet ikke at den er infisert. Botnettet kan f.eks. brukes til tjenestenektangrep, spam eller phishing.

Bring your own device (BYOD)
Bruk ditt eget utstyr. Bruk av privat IKT-utstyr på arbeidsgivers nettverk.

Computer Emergency Response Team (CERT)
Ekspertgruppe som håndterer uønskede hendelser på internett.

Computer Security Incident Response Team (CSIRT)
Se CERT.

Cyberkriminalitet
Type kriminalitet hvor IKT-system eller -infrastruktur er middel eller mål for kriminaliteten.

Datanettverksoperasjoner
Datatangrep, datainnbrudd via internett.

Defacing
Defacing er en type vandalisme mot websider der noen bytter ut et element, tekst og/eller bilder på en webside, ofte med angriperens eget budskap.

Difi
Direktoratet for forvaltning og IKT.

DNSSEC
DNS Security Extensions (DNSSEC) er et sett utvidelser til DNS som føyer til autentisering og integritetskontroll.

Domain Name System (DNS)
Internettets «telefonkatalog». DNS forbinder domenenavn (f.eks. www.nsm.stat.no) på internett med internettprotokoll(IP)-adresser (tallkode analogt med et telefonnummer).

ENISA
European Union Agency for Network and Information Security. Den europeiske etaten for nettverks- og informasjonssikkerhet.

EOS
Etterretning, Overvåking, Sikkerhet.

E-tjenesten
Etterretningstjenesten (utenlandsetterretning).

FD
Forsvarsdepartementet.

FinansCERT
CERT for finanssektoren. Se også BFI.

Fjerntilgang
Tilgang til et ikke-offentlig IKT-system for autorisert bruker via internett.

Hacker
Person som på ulovlig vis forsøker å kompromittere et datasystems sikkerhet.

Hacktivisme
Politisk motivert hacking.

Heartbleed
Sårbarhet i Open SSL som er utnyttet av trusselaktører, f.eks. APT 18 (sannsynligvis kinesisk) som bl.a. har gått etter helseinformasjon.

HelseCSIRT
Norsk Helsenett SF sin CSIRT.

Identitetssvindel
Identitetssvindel er ervervelse av penger, varer, tjenester og andre fordeler eller unngåelse av økonomiske eller andre forpliktelser ved å utgi seg for å være en annen ved bruk av falsk identitet.

Identitetstyveri
Når noen anskaffer, overfører, besitter eller fremstår som rette innehaver av personlige opplysninger tilhørende en privatperson eller virksomhet på en uautorisert måte, med den hensikt å begå bedrageri eller annen kriminalitet.

IKT
Informasjons- og kommunikasjonsteknologi. Teknologi for innsamling, lagring, behandling, overføring og presentasjon av informasjon over elektronisk medium.

Inntrengningstest (penetrasjonstest, PENTEST)
Kontrollert forsøk på å trenge inn i et datasystem eller nettverk for å identifisere svake punkter i sikkerheten, med teknikker som i et reelt angrep. Gjennomføres av NSM med begrensninger som anført i sikkerhetslovens § 15

Innsider, innsideaktør
Individ eller gruppe innen en virksomhet som forårsaker IKT-sikkerhetshendelser innenfra.

Integritet
Pålitelighet. Korrekt, komplett, betimelig, autorisert. At informasjonen ikke blir endret i forhold til hva den skal være.

Internettprotokoll (IP)
Regelsett for korrekt adressering av datapakker slik at de når frem dit de skal.

JD
Justis- og beredskapsdepartementet.

Klartekst
Ukryptert tekst.

KMD
Kommunal- og moderniseringsdepartementet.

Konfidensialitet
At kun de som skal ha tilgang, får tilgang.

KraftCERT
CERT for kraftsektoren.

KRIPOS
Kriminalpolitisentralen (nasjonal etterforskningsressurs).

Kryptering
Koding av informasjon slik at den blir uleselig for uvedkommende.

Løsepengevirus (ransomware)
Løsepengevirus låser alle eller noen filer på ofrenes PC med sterk kryptering. Ofrene får krav om å betale løsepenger for å låse opp innholdet.

Maskinvare (hardware)
Fysiske komponenter i datamaskiner.

Motstandskraft (resilience)
Evne til å motvirke og absorbere negativ påvirkning.

Mykvare (software)
Program, programvare i datamaskiner.

NasjonalCERT (StatsCERT) (GovCERT)
CERT (se dette) som ivaretar nasjonale / statlige behov for håndtering av IKT-sikkerhetshendelser. I Norge: NorCERT.

Nettverksoperasjoner
Se Datanettverksoperasjoner.

NIS-direktivet
EU-direktiv som skal sikre høyt felles nivå på nettverks- og informasjonssikkerhet i EU. COM(2013) 48 final, datert 7.2 2013.

NIX
Norwegian Internet Exchange. Samtrafikkpunkt for norsk internettrafikk.

NorCERT
Funksjon i NSM; nasjonal CERT.

Norid
UNINETT Norid AS. Driver det sentrale registeret for norske domenenavn. Ansvarlig for driften av DNS for det nasjonale toppdomenet .no.

NSM
Nasjonal sikkerhetsmyndighet (cybersikkerhet, objektsikkerhet, personellsikkerhet).

Offshoring
Kjøp av tjenester utenfor landets grenser.

Open SSL
Open Secure Socket Layer. Gratis programvare med åpen kildekode som implementerer krypteringsprotokoller som TLS med mer. Open SSL er et av de mest brukte krypteringssystemene for sikker kommunikasjon på internett. Jf. Heartbleed.

Outsourcing
Utkontraktering. Kjøp av tjenester utenfor eget foretak.

Patche
«Lappe», oppdatere / reparere programvare, ofte regelmessig rutine ved hjelp av oppdateringer fra systemleverandør.

Phishing
Det å gi seg ut for å være en annen og i denne forkledning be en person om opplysninger for å kunne plante skadevare. Personens tillit til den originale avsenderen blir forsøkt utnyttet. Se spearphishing.

PlugX
Den mest brukte skadevaren internasjonalt i 2014.

PST
Politiets sikkerhetstjeneste (innenlandsetterretning).

Risiko
NS 5830:2012 Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen.

Risikobilde
NS 5830:2012 En tidsavgrenset beskrivelse av en entitets risiko. Innen forebyggende sikkerhet utgjør risikobildet en samlet vurdering av samfunnets verdier, truslene mot disse og sårbarheter som eksisterer i forhold til truslene.

SCADA
Supervisory Control And Data Acquisition. System eller nettverk som brukes til å kontrollere (industrielle) prosesser eller infrastrukturer.

Skadevare (Malware)
Skadelig programvare, f.eks. virus eller trojaner.

Skytjeneste (Cloud computing)
Distribuert databehandling via et nettverk. Mulighet for å kjøre program på mange sammenknyttede servere. Skytjenester kan være både private og offentlige, eller en blanding av disse. Brukes ulikt av ulike leverandører, leveres via internett.

Sosial manipulering (social engineering)
Angrepsteknikk som unytter menneskelige sårbarheter som nysgjerrighet, tillit eller grådighet for å få tak i sensitiv informasjon eller påvirke offerets handlinger.

Spam
Uoppfordret / uønsket epost med reklame.

Spearphishing
Se phishing; målrettet mot spesielle personer, ofte med unik skadevare.

SS7
Signalling system 7. Kommunikasjonsprotokoll for telefoni.

SSB
Statistisk sentralbyrå.

Stordata (big data)
Begrepet innbefatter store datamengder både i strukturert og ustrukturert form. Dette krever stor lagringskapasitet og stor prosesseringskraft for behandling om en skal trekke ut verdifull informasjon. Forventningene er at en derved skal kunne treffe velbegrunnede og raske beslutninger i vanskelige saker.

Stuxnet
Orm (type skadevare) som sprer seg via minnepinner ved å utnytte sårbarhet i Windows. Angriper Siemens WinCC SCADA-systemer.

Sårbarhet
NS 5830:2012 Manglende evne til å motstå en uønsket hendelse eller opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning.

The Onion Router (TOR)
Tjeneste som gir brukerne mulighet til anonym tilgang til internett ved å sende kryptert trafikk via datamaskinene til andre TOR-brukere.

Tilgjengelighet
At informasjon er tilgjengelig for rettmessig bruker når det er behov for det.

Tingenes internett (Internet of things)
Om det fenomen at gjenstander inneholder datamaskiner, eventuelt sensorer, og kan kommunisere over internett.

Tjenestenekt-angrep (DoS, DDoS)
Et internettangrep som overbelaster en server ved at stor trafikk rettes mot serveren, gjerne ved bruk av et botnett. Hensikten er å hindre normal tilgang fra ordinære brukere.

TLS
Transport Layer Security. En protokoll som brukes til å kryptere meldinger og levere dem trygt, og forhindrer tyvlytting og «forfalsking» mellom epostservere.

Trojaner
Virus som utgir seg for et vanlig program, men som inneholder ondsinnet kode.

Trussel
NS 5830:2012 Mulig uønsket handling som kan gi en negative konsekvens for en entitets sikkerhet.

Trusselaktør
NS 5830:2012 En kjent eller ukjent entitet som forbindes med en trussel.

UNINETT CERT
CERT for universiteter og forskningsmiljøer.

VDI
Varslingssystem for digital infrastruktur (siden 1999), som driftes av NorCERT

Verdi
NS 5830:2012 Ressurs som hvis den blir utsatt for en uønsket påvirkning vil utgjøre en negativ konsekvens for den som forvalter eller drar fordel av ressursen.

Virus
Skadevare (program) som infiserer andre programmer og reproduserer seg selv.

WLAN
Wireless Local Area Network, dvs trådløs oppkoblingsmulighet

Vedlegg 2
Litteratur

ANSSI with the participation of the Afnic ,Internet Resilience in France 2013.

BDO; Nasjonale indikatorer for IKT-sikkerhet, 2015.

Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2014, November 2014.

Center for Media, Data and Society, Data Breaches in Europe: Reported breaches of Compromised Personal Records in Europe, 2005-2014 (2014), sitert i ENISA Threat landscape 2014.

Center for Strategic and International Studies, The Economic Impact of Cybercrime and Cyber Espionage, July 2013.

Center for Strategic and International Studies, Cyber Threat and Response, Combating Advanced Attacks and Cyber Espionage, James Andrew Lewis., Washington, DC, March 2014.

Center for Strategic and International Studies, June 2014, Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II.

Center for Strategic and International Studies, Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, Washington, DC, December 2008.

Center for Strategic and International Studies, Significant Cyber Events, oppdateres jevnlig (interaktiv versjon tilgjengelig på nett).

Chatham House (The Royal Institute of International Affairs), Cyber Security and Global Interdependence: What Is Critical? Dave Clemente, February 2013.

Cisco 2015 Annual Security Report.

Crowdstrike Global Threat Intel Report 2014.

DKCERT Trendrapport 2015, DeIC 2015.

Etterretningstjenestens vurdering, FOKUS 2015.
European Network and Information Security Agency (ENISA) "Annual Incidents Reports 2013" (ENISA, 2014).

European Network and Information Security Agency (ENISA) Threat Landscape 2014, Overview of current and emerging cyber-threats, December 2014.

European Network and Information Security Agency (ENISA) Threat Landscape and Good Practice Guide for Internet Infrastructure , January 2015.

European Union, Future & Emerging Technologies (FET) FP7 Projects Compendium 2007-2013, December 2013.

European Union, European Energy Security Strategy, COM(2014) 330 final.

European Union, The Network and Information Security (NIS) Directive, COM(2013) 48 final.

EUROPOL, socta 2013, EU Serious and Organised Crime Threat Assessment.

EUROPOL, The Internet Organised Crime Threat Assessment (iOCTA), 2014, European Police Office.

FFI-rapport 2014/00948 Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet.

Finanstilsynet, Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT), Risiko- og sårbarhetsanalyse 2014, April 2015.

Fireeye, APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? 2014.

Fireeye, APT30 AND THE MECHANICS OF A LONG-RUNNING CYBER ESPIONAGE OPERATION 2015.

Forsvarets Efterretningstjeneste, Efterretningsmæssig Risikovurdering 2014, En aktuel vurdering af forhold i udlandet af betydning for Danmarks sikkerhed, oktober 2014.

Forsvarsdepartementet, Et felles løft, Ekspertgruppen for forsvaret av Norge, 2015.

Kripos Trendrapport 2015, Den organiserte kriminaliteten i Norge.

Menon Business Economics: Den norske IKT-næringens verdiskapingsbidrag, rapport 2015 på oppdrag for IKT-Norge.

Microsoft Security Intelligence Report, Volume 17 | January through June, 2014.

Microsoft Security Intelligence Report, Volume 18 | July through December 2014 Regional threat assessment.

MIT Technology Review, July/August 2014, Hacking the Soul.

Myndigheten för samhällsskydd och beredskap (MSB), En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter, augusti 2014.

Myndigheten för samhällsskydd och beredskap (MSB), Informationssäkerhet – trender 2015.

Næringslivets sikkerhetsråd, Mørketallsundersøkelsen 2014.

National Cyber Security Centre, Cyber Security Assessment Netherlands, October 2014, CSAN-4.

National Intelligence Council, Global Trends 2030: Alternative Worlds, December 2012.

NorSIS, Trusler og trender 2015.

Norsk Standard NS 5830:2012 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger. Terminologi.

NOU 2006:6 Når sikkerheten er viktigst.

NSM årsrapport 2014, Økt risiko – styrket beredskap.

NSM, Sikringsrisikovurdering, høsten 2015.

NSM, Veileder i sikkerhetsstyring, 10. mars 2015.

NSM, Veileder, Ti viktige tiltak mot dataangrep, se også NSM lenke «Veiledning for systemteknisk sikkerhet» for detaljer.

OECD Digital Economy Outlook 2015.

OECD Reviews of Risk Management Policies, Future Global Shocks, Improving Risk Governance.

OECD Emerging Risks in the 21st Century, An Agenda for Action, 2003.

Peter Sommer, Information Systems and Innovation Group, London School of Economics, Ian Brown, Oxford Internet Institute, Oxford University, 14th January 2011, Reducing Systemic Cybersecurity Risk.

Politidirektoratet, Politiets omverdensanalyse, oktober 2012.

Politiets sikkerhetstjeneste, Åpen trusselvurdering 2015.

Statistisk sentralbyrå (SSB), Statistikkbanken: Bruk av IKT i næringslivet, diverse tabeller.

Statistisk sentralbyrå (SSB), Statistikkbanken: Bruk av IKT i staten, diverse tabeller.

Statistisk sentralbyrå (SSB), Statistikkbanken: Virksomheter.

Verizon 2014 Data Breach Investigations Report.

Verizon 2015 Data Breach Investigations Report.

Wikipedia (diverse, «List of emerging technologies» er et godt utgangspunkt).

World Economic Forum/Cornell University/INSEAD (eds.): The Global Information Technology Report 2015.

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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