NSM

Helhetlig IKT-risikobilde 2017

Helhetlig IKT-risikobilde skal bidra til å øke bevisstheten om og motivere til bedre IKT-sikkerhet i offentlige og private virksomheter. Rapporten henvender seg til ledere og personell med sikkerhetsoppgaver i alle sektorer. Begrepet helhetlig innebærer at rapporten omhandler problemstillinger knyttet til individer, virksomheter og til samfunnet som helhet. Rapporten tar særlig for seg risiko som følge av uønskede hendelser som skyldes bevisste, ondsinnede handlinger, men omhandler også risiko knyttet til utilsiktede feil, ulykker og tilfeldige hendelser.

IKT-risikobildet er i stadig endring som følge av samfunns- og teknologiutviklingen. I rapporten ser vi på trender i trusselbildet og endringer i sårbarhetsbildet som følge av digitalisering og teknologiutvikling for å vurdere hvordan dette påvirker norske virksomheters informasjon, digitale tjenester, systemer og infrastruktur.

Innhold

IKT-risikobildet – overordnet vurdering

Nasjonal sikkerhetsmyndighet erfarer at norske virksomheter blir stadig mer oppmerksomme på sikkerhetsutfordringer ved bruk av IKT. Det samme bildet ser vi i flere internasjonale undersøkelser. Det er langt mellom uønskede IKT-hendelser som får alvorlige konsekvenser for tjenesteproduksjon i Norge. NSMs data og analyser viser imidlertid at det fortsatt er mye å rette på i en verden der risikobildet endrer seg raskt.

Målrettede digitale spionasjeoperasjoner og løsepengevirus vedvarer

NSM registrerer et jevnt trykk av målrettede digitale spionasjeoperasjoner fra fremmede stater mot norske virksomheter.

Trusselaktørenes metoder er i stadig endring. Det utfordrer vår evne til å forebygge, oppdage og håndtere hendelser. Informasjonsoperasjonene i forbindelse med det amerikanske presidentvalget i 2016 viste at digital spionasje og nettverksoperasjoner kan sette demokratiske prosesser under press.

Større løsepengeviruskampanjer har fått store konsekvenser på verdensbasis i 2017, både for virksomheter og samfunnsfunksjoner. Vi forventer at slike angrepskampanjer vil fortsette og i enda større grad kunne treffe Norge, også med nye metoder som utnytter andre sårbarheter.

NSM ser fortsatt en overvekt av e-post som angrepsmetode, og det er en økning i målrettede e-poster med skadevare til personers private adresser. Vi forventer at trykket mot norske virksomheter vil vedvare og gi økte samfunnsmessige konsekvenser.

Komplekse verdikjeder gir redusert kontroll

Tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan gi bedre sikkerhet og mer stabile og tilgjengelige tjenester, lavere og mer forutsigbare kostnader og bidra til fokusering på virksomhetens kjerneaktivitet. Det kan imidlertid føre til økt risiko på grunn av redusert kontroll over stadig mer komplekse verdikjeder. I 2017 har trusselaktører forsøkt å få tilgang til IT-tjenesteleverandørers kunder og deres data. NSM er bekymret for risiko knyttet til konsolidering av store mengder nasjonale data. Virksomheter må aktivt etablere organisatoriske, prosessuelle, tekniske og juridiske sikringstiltak.

Digitalisering utfordrer risikoaksepten

Digitaliseringen gjør at stadig flere arbeidsprosesser utføres eller støttes av digitale verktøy. Kunnskap om, eller muligheten for å gjennomføre, manuelle rutiner forsvinner. Med økt digitalisering følger også økte krav til tilgjengelighet for viktige IKT-systemer. Dette er helt sentrale faktorer når nye, sikre digitale løsninger skal planlegges og implementeres.

En annen viktig faktor er behovet for tillit til digitale løsninger. Et eksempel på dette er Stortingsvalget 2017. Det å lykkes i både implementeringen av og kommunikasjonen om en digital tjeneste vil være avgjørende i tiden fremover. Digitale løsninger kan bygges sikre, men risikostyring og risikoaksept

vil alltid være en del av en digitaliseringsprosess. Dette må kommuniseres på en slik måte at brukerne har tillit til løsningen.

Mangelfullt vedlikehold skaper unødvendige sårbarheter

Mange IKT-produkter har i 2017 god innebygget teknisk sikkerhet, og vi forventer at den teknologiske utviklingen vil gjøre det enklere å etablere sikre løsninger. Nye operativsystemer og ny programvare har ofte gode sikringsmekanismer, noe som kan heve sikkerheten i egen virksomhet og i verdikjedene virksomheten er en del av. NSM erfarer imidlertid at økte muligheter innen teknisk sikring ikke alltid utnyttes og at mangelfullt teknisk vedlikehold av systemer, eksempelvis manglende sikkerhetsoppdateringer, skaper unødvendige sårbarheter.

Fortsatt manglende tilgjengelighet på sikkerhetskompetanse

Et økende gap mellom tilgjengelighet og behov for sikkerhetskompetanse utgjør en nasjonal sårbarhet. Fokus på IKT-sikkerhet ser imidlertid ut til å øke blant ledere i offentlig og privat sektor. NSM registrerer økt etterspørsel fra ulike ledernivåer som ønsker råd og veiledning, og fra virksomheter som ønsker inntrengingstest av sine IKT-systemer. Stadig flere sektorer utarbeider risikovurderinger, noe som over tid vil bidra til et bedre og mer fullstendig IKT-risikobilde.

Sårbarhetsflaten øker

Sårbarhetsflaten øker som følge av at digitale verdikjeder blir mer uoversiktlige, og av at stadig nye enheter og prosesser kobles til internett. Utviklingen der «alt henger sammen med alt» er en strukturell samfunnsmessig sårbarhet på flere måter. Virksomhetene er avhengige av digitale tjenester levert av andre for egen produksjon eller aktivitet. Sårbarheter og feil forplanter seg raskt mellom leddene i verdikjeden og kan få uante og uforutsette konsekvenser. Tjenester, systemer, virksomheter og infrastrukturer arver sårbarheter av hverandre. Det vil derfor være svært krevende å holde oversikt over sårbarheter gjennom hele verdikjeden. Når vi i tillegg ser at trusselaktørene utvikler sine metoder raskere enn vi utvikler og tar i bruk mottiltak, vurderer NSM at risikobildet forverres og forventer at samfunnskonsekvensene av IKT-hendelser vil øke.


rbeidsprosesser

Trusler

Norske virksomheter står overfor en rekke trusler som kan medføre økonomiske tap, at informasjon kommer på avveie eller tjenester blir utilgjengelige, og i verste fall konsekvenser for liv og helse. Tilfeldige, uønskede hendelser har også betydning for risikobildet. Nasjonal kommunikasjonsmyndighet (Nkom) viser til at Norge i 2016 hadde tre tilfeller av ekstremvær som forårsaket skader på infrastruktur som ga utfall av kraft og elektronisk kommunikasjon (ekom).[1] Uønskede hendelser kan også oppstå som følge av menneskelige feil, uten at det ligger ondsinnede intensjoner bak. Eksemplene på feilkonfigurering av IKT-utstyr, uforvarende aktivering av skadevare og andre handlinger som i god tro forårsaker uønskede hendelser, er mange.

TRUSLENE SOM TREFFER OSS

I IKT-trusselbildet for 2017 ser vi vedvarende trender fra foregående år, og enkelte nye, viktige utviklingstrekk. Vi erfarer et jevnt trykk av målrettede digitale spionasjeoperasjoner fra statlige aktører mot norske offentlige og private virksomheter. Spionasje mot høyteknologi, forsvarsinteresser, virksomheter knyttet til kritisk infrastruktur så vel som nettverksoperasjoner mot politiske, økonomiske og militære mål, vedvarer også i 2017.[2]

I tillegg til nettverksoperasjoner mot primærmål registrerer vi i økende grad målrettede operasjoner mot underleverandører og kontraktører. Dette er virksomheter som gjerne har svakere sikkerhetsmekanismer og derfor utnyttes bevisst som en inngang for å nå det egentlige målet. I 2017 er det registrert operasjoner som har til hensikt å få tilgang til IT-tjenesteleverandørers kunder og deres data.

Vi har de siste årene også sett at trusselaktører kompromitterer tilfeldige systemer for å utnytte disse videre i nettverksoperasjoner mot andre mål. Dette betyr at god grunnsikring av nettverk og servere er viktig, selv om man ikke anser egen virksomhet å være et attraktivt mål i seg selv. Din infrastruktur kan bli brukt som plattform i angrep mot en tredjepart.

Nettverksoperasjoner utført av aktører med økonomiske hensikter eller hacktivister har også stort skadepotensial. Cyberkriminelle topper listen over de mest aktive trusselaktørene globalt[3] og har også gjort seg gjeldende i Norge i 2017. Bruk av ormer i løsepengeviruskampanjer, slik som WannaCry-kampanjen, har fått globale konsekvenser, selv om de nasjonale konsekvensene var begrensede. ENISA registrerer at cyberkriminelle i 2017 fremstår med større grad av operasjonell kapasitet enn tidligere, og at operasjonene konsentreres rundt løsepenge- og utpressingskampanjer.[4] Vi forventer at slike viruskampanjer vil ramme Norge på nytt, men også med nye metoder som utnytter andre sårbarheter enn det som ble observert i mai i år. Finanstilsynet uttaler for sin sektor at de har observert et færre antall hendelser med uønskede konsekvenser i 2016, men at tapene som følge av hendelsene har økt. Nettverksoperasjoner med formål å forstyrre eller gjøre informasjon og tjenester utilgjengelig, er forventet å vedvare i tiden fremover.

METODENE SOM BRUKES MOT OSS

Foten i døren: E-post og vannhull

NSM erfarer fortsatt at digitale angrep så godt som alltid innledes med bruk av ulike varianter av skadevare distribuert via e-post, og at denne typen angrep fremstår med økende grad av profesjonalitet. I de fleste saker som NSM NorCERT har håndtert i 2016 og 2017, ser vi at trusselaktøren sender e-poster som er målrettet utformet for å lure mottakeren (såkalt spearphishing). E-postens innhold og utforming fremstår som relevant og legitim for mottakeren. Eksempler på dette er nyhetsbrev fra kjente avsendere eller innkallinger til møter og konferanser med vedlegg. Lenkene eller vedleggene inneholder ondsinnet kode som aktiveres ved at mottaker klikker på eller åpner vedlegget.

For å levere slike e-poster benyttes flere ulike metoder. I noen tilfeller oppretter trusselaktør egen infrastruktur med domenenavn som etterligner kjente tjenester. Vi har også observert forfalskede nettadresser og kompromitterte e-postkontoer. Det kan være utfordrende å oppdage

[1] Nasjonal kommunikasjonsmyndighet (Nkom), *EkomROS 2017.*

[2] Politiets sikkerhetstjeneste: Trusselvurdering 2017 og Etterretningstjenesten: *Fokus 2017.*

[3] European Union Agency for Network and Information Security (ENISA), *Threat Landscape Report 2016.*

[4] ENISA, *Threat Landscape Report 2016, s. 69.*

kompromitterte e-postkontoer, da trafikk fra disse er vanskelig å skille fra legitim trafikk.

I tilfeller hvor e-posten inneholder en ondsinnet lenke, havner brukeren ofte i et såkalt vannhull, en tilsynelatende legitim nettside som leverer skadevare til utpekte mål. Det kan være ulike forutsetninger for at skadevaren leveres. Typisk vil være krav som at brukeren oppsøker vannhullet fra en spesifikk bedrift, maskin, nettleser eller lignende. I finanssektoren er svindel ved bruk av vannhull observert som en ny utvikling.

I 2017 har det vært en økning i spearphishing mot private e-postadresser. Målet med disse e-postene kan være å lure til seg innloggingsinformasjon til andre systemer, som for eksempel e-postkonto på personens arbeidsplass eller skylagringstjenester. Dette kan være en fremgangsmåte for å unngå å bli oppdaget av sikkerhetsmekanismer i disse systemene.

Cyberangrep mot demokratene i USA

Høsten 2016 ble en større og sammensatt angrepskampanje avdekket i forbindelse med det amerikanske presidentvalget. Private e-postkontoer tilhørende brukere med knytning til Det demokratiske partiet i USA ble kompromittert ved hjelp av målrettede angrep. Sensitivt innhold fra e-postene ble senere lekket til offentligheten. Rapporten fra et samlet amerikansk etterretningsmiljø vurderer det som sannsynlig at kompromitteringen og den påfølgende lekkasjen av sensitiv informasjon var del av en omfattende kampanje, iscenesatt av en fremmed makt, for å påvirke den amerikanske presidentvalgkampen.

Utilgjengeliggjøring: Kryptering og tjenestenekt

Så langt i 2017 har løsepengevirus og krypteringsvirus hatt store konsekvenser på verdensbasis. Europol vurderer at slike virus er den skadevaretrusselen med størst samfunnskonsekvenser.[5] Et krypterende virus gjør filene på en brukers klient utilgjengelige. Angrepsmetodene kan være flere, både e-post med ondsinnet vedlegg, vannhull og ormer. NSM understreker viktigheten av å ha gode sikkerhetskopier, fordi det i mange tilfeller er svært vanskelig å hente tilbake krypterte filer.

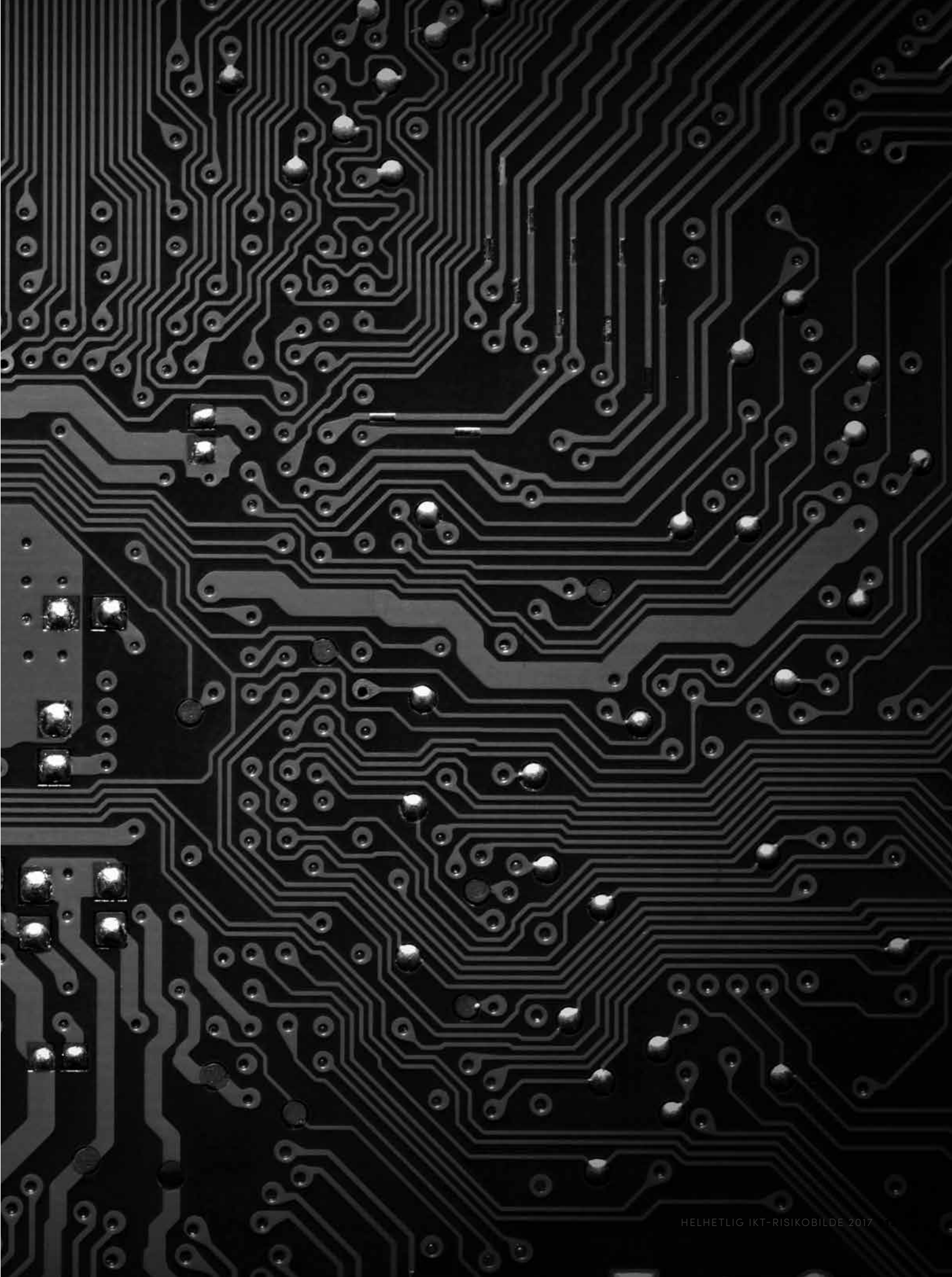
I juni i år så vi at et enkeltstående angrep mot en IT-underleverandør kan ha svært store konsekvenser. En ukrainsk leverandør av programvaretjenester ble kompromittert, og tilsynelatende legitime programvareoppdateringer til kundene ble deretter infisert med skadevare. Denne skadevaren krypterte innholdet på kundenes klienter og spredte seg som en orm i nettverkene. Fem norske virksomheter, underlagt selskaper som også hadde kontorer i Ukraina, ble rammet av denne ormen.

Tjenestenektangrep overbelaster en tjeneste med trafikk slik at tjenesten lammes og dermed blir gjort utilgjengelig for de som trenger den. Tjenestenekt er et svært enkelt angrep å iverksette, men vanskelig å beskytte seg mot.

Døråpneren: Innsidere

En innsider er en bruker som misbruker legitim tilgang til IKT-nettverket til illegitime formål. Det finnes flere typer innsidere; infiltratøren som er utsendt fra en trusselaktør med en klar oppgave, en ansatt som på et tidspunkt er vervet av en trusselaktør, en ansatt som handler på eget initiativ, og den uforvarende innsideren som ikke har til hensikt å kompromittere. For systemer som er adskilt fra omverdenen, vil en sentralt plassert innsider være et svært effektivt virkemiddel for å nå målet om å kompromittere et ellers godt beskyttet nettverk.

[5] Europol (2017). *Serious and organised crime threat assessment.*



Sårbarheter

For å kunne sikre norske virksomheters IKT-systemer og -infrastrukturer er det viktig å kartlegge svakheter som kan forårsake feil eller utnyttes av ondsinnede aktører. Sårbarheter finnes i nær sagt alle virksomheter, systemer og infrastrukturer, både av teknisk, organisatorisk og menneskelig art. Digitalisering og teknologiutvikling bedrer i mange tilfeller sikkerheten, men sammenkobling av stadig nye systemer og enheter utvider samtidig sårbarhetsflaten. Sårbarheter gjør systemer, infrastrukturer og verdikjeder utsatt for hendelser som kan få konsekvenser både for enkeltindivider, den enkelte virksomhet og samfunnet som helhet.

ALT HENGER SAMMEN MED ALT – SÅRBARE VERDIKJEDER

Ifølge finske Etlatieto har Norge nå passert Finland og er det mest digitaliserte landet i verden. Digitaliseringen har gjort det enklere og mer effektivt å styre samfunnsfunksjoner, tjenester, produksjon og infrastrukturer. Utviklingen skaper imidlertid nye sårbarheter. Mobile enheter, tjenesteutsetting og internasjonalisering knytter et flyktig, flerdimensjonalt, internasjonalt og dermed uoversiktlig nett av sårbarheter til produksjon av mange tjenester.

Mobile IKT-enheter som kobles til ulike offentlige og private nettverk, utgjør en økende utfordring. Ved å koble mobiltelefonen eller nettbrettet til hjemmenettet eller nettverk på offentlige steder kan sårbarheter i et svakt sikret nettverk utsette et i utgangspunktet godt sikret nettverk på arbeidsplassen for risiko.

Økende internasjonalisering innebærer sårbarhet overfor uønskede hendelser som inntreffer utenfor landegrensene og dermed utenfor norsk kontroll, og rammer produksjon av norske tjenester. Nkom vurderer at forringelse av nasjonal kontroll over kritisk tjenesteproduksjon og et uforutsigbart sikkerhetspolitisk bilde utgjør økende risiko innen ekom.

Norsk nett rammet av feil i Sverige

Telias norske mobilnett har kjernenettfunksjoner i Sverige. Sommeren 2016 falt deler av nettet ut som følge av feilkonfigurering i forbindelse med planlagt vedlikeholdsarbeid i Sverige. 63.000 abonnenter ble rammet av nettutfallet, som varte i en time. Dette illustrerer at norske tjenester kan være sårbare overfor og rammes av uønskede hendelser som forplanter seg på tvers av landegrenser.

Det digitale sårbarhetsutvalget skriver i sin rapport (NOU 2015:13) at på grunn av kompleksiteten i de digitale verdikjedene er det ingen virksomheter som har full oversikt over egne sårbarheter. Utvalget vurderer at fordi IKT-systemer er bærere av svært mange viktige samfunnsfunksjoner, er den digitale sårbarheten for mange slike funksjoner stor. Verdikjedene er sårbare for alle typer uønskede hendelser, både de som skyldes bevisste handlinger og de som skyldes feil eller ulykker. Konsekvensene av hendelser i digitale verdikjeder kan ramme oss på alle nivåer, fra enkeltindividet til samfunnssikkerheten i stort.

For en enkeltperson kan en feil eller en sikkerhetsbrist i et ledd i verdikjeden kunne medføre midlertidig bortfall av en viktig digital tjeneste, som at nettbanken er nede eller at mobiltelefonen mister nettilkoblingen. I ytterste konsekvens kan gjensidige avhengigheter og sårbarheter i de digi-

tale verdikjedene påvirke samfunns- og statssikkerheten, dersom kritisk infrastruktur eller samfunnsfunksjoner rammes av uønskede hendelser i et slikt ledd i en verdikjede.

Tjenester innen kraft og ekom er særlig viktige for å opprettholde digitale tjenester og verdikjeder. Tjenesteutfall innen disse sektorene vil derfor kunne ha store konsekvenser fra individnivå til samfunnet som helhet. Norges vassdrags- og energidirektorat (NVE) vurderer at risikoen for alvorlig svikt i viktige IKT-systemer øker på grunn av stadig mer sammenkoblede og komplekse infrastrukturer, herunder industrielle kontrollsystemer, intelligente rørledninger, smarte nett og digitale anlegg. Svikt kan skyldes både utilsiktede feil og menneskeskapte målrettede cyberangrep. I en undersøkelse om informasjonssikkerhet i energiforsyningen i 2017 oppgir over halvparten av de 88 virksomhetene som svarte at de har hatt uønskede IKT-sikkerhetshendelser siste 12 måneder. Blant de som svarte på spørsmålet om den mest alvorlige hendelsen, oppga 34 prosent at løsepenge- eller krypteringsvirus var mest alvorlig. Den mest alvorlige hendelsen fikk for 19 prosent av virksomhetene konsekvenser i form av driftsavbrudd.[6]

Angrep mot nettleverandør utnyttet IoT-sårbarheter

Stadig nye typer enheter kobles til internett. Hendelser der IoT-enheter (Internet of Things, tingenes internett) brukes for å angripe infrastrukturer eller systemer, illustrerer hvordan sårbarheter i et ledd av en verdikjede kan utnyttes for å ramme funksjonalitet. I oktober 2016 ble den amerikanske nettleverandøren Dyn rammet av et omfattende tjenestenektangrep (også kalt DDoS-angrep, Distributed Denial of Service). Trusselaktøren brukte et såkalt botnet som bestod av hundretusener av IoT-enheter, deriblant webkameraer, digitale videospillere, rutere og babycaller som var infisert med skadevare. Botnetet bombarderte Dyns infrastruktur med trafikk, noe som førte til at nettsidene til blant andre Twitter, Netflix, Spotify, Airbnb, CNN, The Guardian og The New York Times var midlertidig utilgjengelige. Dyn skal etter hendelsen ha mistet om lag 8 prosent av internettdomenene som benyttet dem som leverandør, tilsvarende mer enn 14.000 domener.

Helsedirektoratet vurderer manglende oversikt, lange verdikjeder og gjensidige avhengigheter blant de viktigste digitale sårbarhetene i sin sektor. Et komplekst aktørbilde forsterker sårbarheten i verdikjedene, fordi ansvaret for ulike løsninger, produkter og verdikjeder er uoversiktlig og fragmentert. Drifts- og forvaltningsansvaret er plassert hos både offentlige og private leverandører. Dette gjør det utfordrende å skaffe oversikt over og drive god styring av risiko og sårbarhet for IKT i sektoren.[7]

Samfunnet og stadig flere verdikjeder har de siste par tiårene blitt mer avhengig av satellittbaserte tjenester. Som individ tar du blant annet i bruk teknologien når du navigerer med mobiltelefonen. Fly vil om kort tid bruke satellittbasert navigasjon som primær navigasjonskilde under landing og avgang. Forsvaret bruker tjenester fra rommet i sine operasjoner for blant annet kommando og kontroll og for styring av våpen. Kommunikasjon med satellittene er sårbare for interferens og cyberangrep. Romrelatert infrastruktur er sårbar for både fysiske og logiske anslag. Også utilsiktede hendelser som solstormer og ulykker kan ramme satellitter og andre viktige verdier.

[6] Studentrapport, NVE, 11. august 2017. *Undersøkelse av informasjonssikkerhetstilstanden i energiforsyningen.*

[7] Helsedirektoratet (2017). *Overordnede risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren.*

Bortfall av datasystemer ga stans i lufttrafikken

British Airways opplevde store problemer lørdag 27. mai 2017 ved at viktige datasystemer ikke fungerte. Rundt 800 flygninger og 75.000 passasjerer ut fra Heathrow og Gatwick lørdag og søndag ble rammet, idet både bagasjehåndtering og kommunikasjonssystemer falt ut. Kostnadene for British Airways anslås til å være på om lag 61 mill. EURO. Årsaken skal ha vært bortfall av strøm ved et lokalt nettsenter i et slikt omfang at det fikk konsekvenser for backupsystemer. Foreløpig er det ingenting som tyder på at hendelsen som forårsaket bortfallet av datasystemer var tilsiktet. Selv om det i Norge ikke har vært hendelser av tilsvarende alvorlighetsgrad, mener Luftfartstilsynet det er grunn til å peke på potensialet som ligger i å ramme elektroniske informasjonssystemer.

NSM vurderer at denne utviklingen, der «alt henger sammen med alt», utgjør en strukturell samfunnsmessig sårbarhet. Sårbarheten er dels knyttet til at virksomheter og tjenester er avhengige av andre for å opprettholde sin produksjon eller aktivitet. Et utfall av en tjeneste i en verdikjede vil dermed kunne lamme andre virksomheter. Sårbarheten er også dels knyttet til sammenkoblingen i seg selv, ved at sårbarheter arves og feil forplanter seg raskt fra en tjeneste eller virksomhet til en annen. Fordi verdikjedene i mange tilfeller strekker seg over flere sektorer og ofte også over flere land, kan det være utfordringer knyttet til at det er ulike regulatoriske forhold og lovverk som slår inn.

Flyktigheten i det digitale markedet, der leverandører byttes ut, selskaper kjøpes opp, ny teknologi oppstår og gammel raskt byttes ut, bidrar til å komplisere bildet ytterligere. Kompleksiteten i avhengighetene mellom tjenestene den enkelte brukeren ser og de underliggende infrastrukturene som tjenestene baserer seg på, vil bare fortsette å øke. Konsekvensene av en slik strukturell sårbarhet er til dels uoverskuelige og uforutsigbare, men økende grad av sammenkobling gjør at risikoen for at enkelthendelser får følgekonsekvenser, øker.

DINE DATA I ANDRES HENDER – TJENESTEUTSETTING

Mange offentlige og private virksomheter tjenesteutsetter hele eller deler av sin IKT-portefølje. Ifølge Statistisk sentralbyrå (SSB) har andelen norske foretak med ti eller flere ansatte som kjøper skytjenester, økt fra 40 til 48 prosent fra 2016 til 2017.

I digitaliseringsrundskrivet for 2017, som gjelder alle statlige virksomheter, anbefaler Kommunal- og moderniseringsdepartementet å ta i bruk skytjenester når det ikke foreligger spesielle hindringer for det, som for eksempel særskilte krav til sikkerhet. Nasjonal strategi for bruk av skytjenester slår fast at offentlige virksomheter skal (og private virksomheter bør) gjennomføre risikovurderinger ved større endringer, som etablering av nye digitale tjenester. Dette gjelder også alle virksomheter som behandler personopplysninger. For virksomheter som er underlagt sikkerhetsloven, gjelder regelverket om sikkerhetsgraderte anskaffelser. Her foreligger det detaljerte krav i lover, forskrifter og veiledninger.

Riksrevisjonens revisjoner viser at det er lav bevissthet rundt krav til og oppfølging av informasjonssikkerhet ved utsetting av IKT-tjenester og utveksling av data med samarbeidspartnere.

I 2017 har vi flere eksempler i Norge og Sverige på beslutninger om tjenesteutsetting, der risikovurderingene knyttet til sårbarheter har vært mangelfulle eller manglende. Disse sakene har blitt slått stort opp i media og har i ettertid fått store konsekvenser for noen av de sentrale beslutningstakerne. I saken knyttet til Nødnett besluttet NSM å åpne tilsynssak mot det som da var Direktoratet for nødkommunikasjon (DNK) og som 1. mars ble innlemmet i Direktoratet for samfunnssikkerhet og beredskap (DSB).

Transportmyndigheten i Sverige – tjenesteutsetting til IBM med drift og forvaltning fra Romania, Tsjekkia, Kroatia og Serbia

Den svenske Transportstyrelsen inngikk i 2015 en avtale med IBM Sverige om driften av myndighetens IT-systemer. Ifølge Transportstyrelsen besluttet daværende generaldirektør Maria Ågren at det i forbindelse med tjenesteutsettingen kunne gjøres unntak fra krav i Säkerhetsskyddslagen, Personuppgiftslagen og Offentlighets- och sekretesslagen. Saken ble svært betent for svenske myndigheter da det kom frem at teknisk personell uten sikkerhetsklarering hadde tilgang til Transportstyrelsens registre, blant annet i IBMs datterselskap i Romania, Tsjekkia, Kroatia og Serbia. Ifølge svensk presse skal personell i utlandet ha hatt tilgang til førerkortregisteret og to av politiets hemmelige nettverk, og personell i Serbia skal ha kunnet følge trafikk mellom Transportstyrelsen og 34 svenske myndigheter gjennom det ekstra sikre nettet Swedish Government Secure Internet (SGSI). Säkerhetspolisen (SÄPO) gjennomførte tilsyn av Transportstyrelsen og fant at myndigheten ikke har etterlevd sitt sikkerhetsansvar, ved å unnlate å gjennomføre og dokumentere sikkerhetsanalyser og sikkerhetstiltak og ved bevisst å ha avveket fra sikkerhetslovgivningen. Maria Ågren ble i januar 2017 avskjediget som sjef for Transportstyrelsen, og statsminister Stefan Löfven ble sommeren 2017 tvunget til å omrokkere sin regjering som følge av IT-skandalen.

Sårbarhetene til en virksomhets IKT-tjenester kan ved en tjenesteutsetting øke om ikke kompenserende tiltak iverksettes. Svak bestillerkompetanse innen IKT-sikkerhet gjør det vanskelig å komme opp med gode nok krav overfor en leverandør. Dermed øker virksomhetens sårbarhet. Ifølge Direktoratet for forvaltning og IKT (Difi) er det fortsatt slik at utilstrekkelig kompetanse kan medføre at enkelte virksomheter anskaffer skytjenester uten tilstrekkelig kartlegging av behov og uten å ha gjennomført risikovurderinger i forkant. Dette understøttes også av Finanstilsynet i deres årlige risiko- og sårbarhetsanalyse for sektoren. I flere tilfeller oppfyller ikke virksomhetene kravene i IKT-forskriften ved tjenesteutsetting.[8]

I en undersøkelse om informasjonssikkerhetstilstanden i energiforsyningen fremgår det at 74 prosent av virksomhetene er middels eller sterkt avhengig av støtte fra IKT-leverandøren for å håndtere hendelser.[9]

Sårbarhetene knyttet til tjenesteutsetting er ofte relatert til at virksomheten får redusert kontroll på sitt eierskap, sikringstiltak og tilgangen til sine data. Dette er en generell utfordring som forsterkes når data lagres og driftes utenfor Norge. Her vil gjeldende lover og regler i det aktuelle landet være av stor betydning. En virksomhet står veldig svakt om leverandørstatens nasjonale lover overstyrer den inngåtte anskaffelseskontrakten med krav om for eksempel innsyn og logging.

Tjenesteutsettingsmarkedet domineres av store

[8] Finanstilsynet (2016). *Risiko- og sårbarhetsanalysen (ROS) 2016.*

[9] Studentrapport, NVE, 11. august 2017. *Undersøkelse av informasjonssikkerhetstilstanden i energiforsyningen.*

globale selskaper, hvor de fleste leveransene skjer som skytjenester. Norske selskaper supplerer ofte sine egne leveranser med videresalg av skytjenester fra de store globale selskapene som Google, Microsoft, Apple og Amazon. Sårbarheten i slike leveransemodeller vil forsterkes gjennom uoversiktlige leverandørkjeder og veldig komplekse verdikjeder.

Resultater fra Datatilsynets tilsyn med kommuner i 2016 viste vesentlige avvik knyttet til informasjonssikkerhet. Eksempelvis ble det avdekket at virksomheter ikke har tilstrekkelig fokus på å ivareta personvernet og på å oppfylle pliktene i personopplysningsloven knyttet til internkontroll og informasjonssikkerhet. Dette omfattet virksomheter med ansvar for digitaliseringsprosesser, men også for virksomheter som i økende grad benytter nye digitale løsninger. Datatilsynet vurderer det som viktig for virksomhetene å ha et akseptabelt nivå på internkontroll og informasjonssikkerhet før store digitaliseringsprosesser starter opp.

Konsekvenser av mangelfulle risikovurderinger

- I mai ble det kjent at et titalls IKT-arbeidere i Asia og Øst-Europa har hatt tilgang og utvidete rettigheter til datasystemet til Helse Sør-Øst. En av årsakene til dette var etter Datatilsynets vurdering manglende risikovurdering ved tjenesteutsetting.
- Datatilsynet ga i 2016–2017 fire kommuner og en fylkeskommune overtredelsesgebyr på til sammen 475 000 kroner som følge av at sensitive personopplysninger ble publisert på nett.
- Sosialistisk Venstreparti (SV) og Miljøpartiet De Grønne (MDG) ble ilagt overtredelsesgebyr i 2017 som følge av mangelfull sikring. En inntrenger utnyttet svake autentiseringsmekanismer og klarte å ta over brukerkontoer i systemene, for så å skaffe seg tilganger og rettigheter. Konsekvensen av mangelfulle sikkerhetstiltak ble i dette tilfellet at uvedkommende fikk tilgang til medlemsopplysninger.

SIKKERHET UTEN PLAN OG STYRING

Mange virksomheter har betydelige sårbarheter innen sikkerhetsbevissthet og sikkerhetskompetanse. Disse svakhetene kan utnyttes av en trusselaktør, eller de kan føre til uønskede utilsiktede hendelser som kan skade virksomheten selv eller andre. Næringslivets Sikkerhetsråds «Mørketallsundersøkelsen 2016» viser at kun halvparten av de mest alvorlige hendelsene i virksomhetene ble fanget opp av intern overvåkning, kontroll og revisjon. NSMs tilsyn og en studie fra FFI[10] viser at mange sikkerhetshendelser skyldes organisatoriske svakheter.

NSM erfarer fortsatt at virksomhetenes IKT-avdeling kan ha implementert gode og fornuftige sikringstiltak, men at tiltakene ikke er forankret i ledelsen. Sikkerhetsarbeidet blir dermed ikke prioritert som del av den totale styringen av virksomheten. Ledelsen vet derfor heller ikke hvilken risiko de tar på vegne av virksomheten. Resultatet kan være at sensitiv informasjon og infrastruktur ikke er godt nok beskyttet. Mangel på helhetlig vurdering ved valg av tiltak kan føre til at sikringstiltakene totalt sett ikke oppnår hensikten. Det er ikke tilstrekkelig at sikringstiltakene er riktig implementert, det må også være de riktige sikringstiltakene som er implementert på rett sted.

Gjennomføring av risikovurderinger er en utfordring både for offentlige og private virksomheter. Mange virksomheter har utilstrekkelige risikovurderinger, noe også Nkom og Finanstilsynet

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

understreker i sine årlige ROS-analyser. Riksrevisjonens funn viser at styringssystem for informasjonssikkerhet er innført i varierende grad, og at sammenhengen mellom risikovurderinger og sikringstiltak kan være vanskelig å se. Oppfølgingen av om iverksatte sikringstiltak har ønsket effekt er mangelfull. I Mørketallsundersøkelsen 2016 fremgår det at manglende investering i og prioritering av sikkerhetsarbeidet står bak en betydelig andel av virksomhetenes sikkerhetshendelser.[11]

I Næringslivets Sikkerhetsråds (NSR) Kriminalitets- og sikkerhetsundersøkelse i Norge (KRISINO) fremgår det at en stadig større andel virksomheter dokumenterer sine risikovurderinger av kriminalitet, herunder IKT-kriminalitet, i eller mot virksomheten.[12] Andelen har økt fra 20 prosent i 2009 til 28 prosent i 2017. Det kan tyde på at det er flere som ser nytten av slike vurderinger, selv om flere myndighetsorganer påpeker at analysene fortsatt er mangelfulle. Det er fremdeles en langt større andel av offentlige virksomheter (46 prosent) som har en skriftlig dokumentert risikovurdering, enn private (24 prosent). Blant de private virksomhetene er det også en tydelig forskjell på små og store virksomheter. Ikke uventet er det store private virksomheter som i størst grad dokumenterer sine risikovurderinger.

Fokus på IKT-sikkerhet ser heldigvis ut til å øke blant toppledere i offentlig og privat sektor. NSM erfarer en økning i etterspørsel fra ulike ledernivåer som ønsker råd og veiledning, blant annet i form av informasjon og foredrag.

Det er flere faktorer som påvirker denne utviklingen, deriblant en økende grad av risikoerkjennelse knyttet til digitalisering gjennom økt mediedekning og åpenhet om nasjonale og internasjonale hendelser som rammer norske virksomheter. WannaCry, direktørsvindel, løsepengevirus og hacking av det amerikanske presidentvalget er saker som direkte og indirekte gir økt bekymring og fokus på IKT-sikkerhet.

Hovedfunn fra NSMs tilsyn med virksomheters styring av sikkerhetsarbeidet i virksomheter underlagt sikkerhetsloven:

- Mangelfulle rutiner eller svak oppfølging – sikkerhet følges ikke opp systematisk.
- Implementering av de fire store hovedtiltakene innen sikkerhetsstyring – verdivurdering, risikoanalyser, internrevisjon og ledelsesevaluering – er krevende for mange virksomheter.
- Virksomhetene ville ha avdekket de fleste avvik som vi avdekker under tilsyn hvis de hadde gjennomført gode interne sikkerhetsrevisjoner.
- Manglende tilgangsstyring og soneinndeling – i datasystemer og fysisk sikring av lokaler.
- En del virksomheter mangler grunnleggende sikkerhetsfaglig kompetanse eller benytter ikke tilgjengelig sikkerhetsfaglig kompetanse systematisk og i tilstrekkelig grad.
- Mange virksomheter har ikke kompetanseplaner eller annen oversikt over den sikkerhetsfaglige kompetansen i virksomheten.
- Få virksomheter synes å registrere og rapportere sikkerhetstruende hendelser, kompromittering av skjermingsverdig informasjon og grove sikkerhetsbrudd.
- Oppfølgingstilsyn viser at virksomheter iverksetter tiltak på bakgrunn av påviste mangler. Dette er positivt.

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

[12] Næringslivets Sikkerhetsråd (NSR), *KRISINO 2017*.

Kompetanseutfordringer på flere plan

Det er tydelig for NSM gjennom tilsyn og annen aktivitet at det er betydelige svakheter innen sikkerhetsbevissthet og sikkerhetskompetanse. Mangelfull kompetanse er en utfordring ikke bare for enkeltindividet, men også for virksomheter og samfunnet. Mangelfull kompetanse har konsekvenser blant annet for hvordan IKT-systemer og -programmer er designet og koblet sammen, og hvordan rutiner og styringssystemer er utformet og fulgt opp sikkerhetsmessig.

NSM har tidligere påpekt at det i Norge utdannes for få personer innen IKT-sikkerhet. Tall fra en NIFU-rapport konkluderer med at det i 2030 vil være en estimert etterspørsel på 15.000 personer med IKT-sikkerhetskompetanse, mens tilgangen samme år vil være på knapt 11.000.[13] Forskere mener tilbudssiden må økes med vel en tredel for å dekke gapet. Det vil innebære en nødvendig økning av antall studieplasser innen dette fagområdet.

Holdningskampanjer som Nasjonal sikkerhetsmåned, kurs og foredrag bidrar til økt oppmerksomhet og kompetanse som er verdifullt for arbeidet i virksomhetene. NSM vurderer at økende gap mellom tilbud og behov for sikkerhetskompetanse i årene fremover kan utgjøre en nasjonal sårbarhet. Særlig SMB-markedet og virksomheter som ikke er lønnsledende, kan få utfordringer med å rekruttere og beholde nødvendig kompetanse. Mangelfull IKT-sikkerhetskompetanse hos tilsynsmyndigheter kan medføre at sårbarheter ikke avdekkes under tilsyn hos virksomheter, og at disse sårbarhetene dermed ikke blir utbedret. NSM erfarer at virksomheter unnlater å rapportere alvorlige sikkerhetshendelser. Det forhindrer oss å fra å lære av feilene vi gjør.

Lysneutvalget trekker frem øvelser som et virkemiddel for å redusere den digitale sårbarheten.[14] Gjennom øvelser kan kompetansemangler avdekkes og både den enkelte virksomhet og samfunnet kan bli bedre til å forebygge, avdekke og håndtere uønskede hendelser. For å få best mulig læringseffekt bør alle hendelser og funn fra en øvelse evalueres.

FORSØMTE SYSTEMER

Trusselaktørene utnytter i stor grad kjente sårbarheter, og nye sårbarheter oppdages daglig. NSM har over flere år anbefalt fire effektive sikringstiltak som stopper opp mot 90 prosent av alle kjente dataangrep. Ikke alle virksomheter opplever dem som enkle å implementere. Argumentene varierer fra at det kan være et styringssystem som ikke kan oppdateres, infrastrukturen er for gammel uten tilgjengelige sikkerhetsoppdateringer til at virksomheter ikke har ressurser til å håndtere tiltakene. Det er imidlertid et faktum at det store flertallet av alvorlige hendelser mot norsk kritisk infrastruktur kunne vært forhindret hvis tiltakene ble implementert. Fellesnevneren er mangelfullt vedlikehold av IKT-systemer og -tjenester. Dette understreker betydningen av at vedlikehold både må planlegges, finansieres og gjennomføres helt fra IKT-systemet implementeres.

Riksrevisjonens funn viser at sikkerhetstilstanden ikke har endret seg vesentlig fra foregående år. I likhet med NSM opplever Riksrevisjonen at det i mange virksomheter er vesentlige svakheter i grunnsikringen av IKT-systemene, og de ser med bekymring på dette i en situasjon hvor trusselnivået er høyt og digitaliseringen leder til økende avhengighet av IKT-systemer. Blant annet finner de mangler i hva som logges, i tillegg til at loggene som oftest er svært mangelfulle.

NSM erfarer gjennom inntrengingstester at sikkerheten i virksomhetenes klienter blir stadig bedre, og dermed vanskeligere å trenge inn i. Vi ser også at systemer der sikkerhet har vært en viktig del av planleggingen og implementeringen, generelt er vanskelige å trenge inn i. På serversiden erfarer

[13] Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU), *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud. Arbeidsnotat 2017:8.*

[14] NOU 2015: 13 *Digital sårbarhet – sikkerhet samfunn.*

vi imidlertid at systemene i mange tilfeller bruker eldre eller ikke-oppdaterte operativsystemer, ofte på grunn av applikasjoner på serverne som ikke vil takle nye OS-versjoner. Dette gjør serverne sårbare for inntrenging. Vi ser også at passordsikkerheten i mange av virksomhetene vi tester, har klare svakheter, noe som gjør systemene enkle å bryte seg inn i. Når det gjelder passordsikkerhet, ser vi ingen tegn til forbedring. Det kan videre i noen tilfeller være enkelt å få fysisk tilgang til infrastruktur som er plassert på andre lokasjoner enn i virksomhetens hovedbygg. Dette kan tyde på at man er mest opptatt av å sikre det man fysisk sett har nærhet til, mens andre, mer perifere lokasjoner oppfattes som mindre viktige å sikre. NSM ser med bekymring på utviklingen der virksomheter kobler stadig flere IoT-enheter, som ikke er sikkerhetsmessig «herdet» og ikke designet med tanke på sikkerhet, til nettene sine og til internett.

Hendelsen WannaCry tidligere i år synliggjorde at vedlikehold av IKT-systemene kan være kritisk – ikke bare for virksomheter, men også privatpersoner. Konsekvensene hendelsen fikk, i form av utilgjengelige helsetjenester og ekom-tjenester, ble en vekker for mange virksomheter. I Mørketallsundersøkelsen oppga 22 prosent av virksomhetene manglende oppdatering av utstyr eller konfigurasjoner som medvirkende faktor til at deres mest alvorlige sikkerhetsbrudd oppstod.[15] Sikker drift kan være krevende, og med mindre systemene moderniseres fortløpende, risikerer man å sitte med systemer som ikke lar seg oppdatere. Det blir ofte oppdaget nye sårbarheter i gammel programvare etter at produsentene har sluttet å vedlikeholde disse. Brukerstøtte og oppdateringer for Windows XP ble avsluttet i 2014. Konsekvensen av dette er at brukere av alle versjoner av Windows XP ikke lenger vil motta sikkerhetsoppdateringer som beskytter mot skadelig programvare. Likevel valgte Microsoft etter WannaCry-hendelsen å utgi en sikkerhetsoppdatering av Windows XP. Dette ble gjort i erkjennelsen av at mange fortsatt brukte XP tre år etter at oppdateringene ble avsluttet.

Mangelfullt oppdaterte systemer årsak til innbruddsforsøk

Tjenesten Allvis NOR i NSM bidrar til å kartlegge sårbarheter i offentlige virksomheter og hos eiere av kritisk infrastruktur. NSM har flere års erfaring med sanntidsdeteksjon av innbruddsforsøk i samfunnskritiske informasjonssystemer. Erfaringsmessig lykkes mange innbruddsforsøk på grunn av feilkonfigurerte eller mangelfullt oppdaterte systemer. Erfaring viser også utpreget bruk av enkle passord, og utstyr med standardpassord. Allvis NOR kan avdekke trivielle, men alvorlige, sårbarheter eksponert for internett, samt gi en økt evne til raskt å kartlegge utbredelsen av nye sårbarheter. Under spredningen av løsepengeviruset WannaCry ble Allvis NOR videreutviklet til å kunne avdekke den spesifikke sårbarheten som ble utnyttet.

INDIVIDET – ET SÅRBART LEDD

Individets rolle som utvikler, vedlikeholder og bruker utgjør en mulig sårbarhet ved IKT-systemer. Mennesker som er gitt fysisk tilgang eller nettverkstilgang til et arbeidsområde, kan svekke effekten av sikringstiltak. Antallet brukere av et system kan være høyt. Enhver bruker er en potensiell døråpner til IKT-systemers sikkerhetsinfrastruktur.

IKT-systemer er sårbare overfor innsidere. En innsider er en bruker med legitim tilgang til IKT-nettverket, som utnytter tilgang og tillit vedkom-

[15] Næringslivets Sikkerhetsråd (NSR), *Mørketallsundersøkelsen 2016*.

mende er gitt av virksomheten til uautoriserte formål. Vedkommende vil kunne være rekruttert, presset, motivert eller lokket av en trusselaktør til å eksponere, kompromittere eller skade IKT-systemet. Vedkommende vil også kunne være målrettet plassert i virksomheten med slike formål. Mørketallsundersøkelsen viser at bevisst misbruk av systemer var medvirkende årsak til at 7 prosent av de alvorligste hendelsene oppstod. Innsidere som har personlig motivasjon (egen vinning) til å forårsake uønskede hendelser er ifølge ENISA nummer to på listen over de mest aktive aktørgruppene globalt. Dette er bak cyberkriminelle, men foran hacktivister og statlige aktører.

Uhell, uaktsomhet og mangel på sikkerhetsbevissthet er ofte medvirkende til at, uønskede hendelser oppstår. Utnyttelse av menneskelige sårbarheter forbundet med bruk av IKT-systemer eksponerer og legger til rette for utnyttelse av andre, ofte teknisk artede, sårbarheter i disse systemene. En bruker kan ubevisst avsløre brukernavn og passord til IKT-systemer ved besøk av kompromitterte nettsteder (vannhull). Risiko forbundet med dette vokser vesentlig ved gjenbruk av passord på tvers av plattformer og systemer. NSM erfarer jevnlig forsøk på illegitim innhenting av passord og tilfeller av at passord på avveie har blitt utnyttet i angrep mot norske virksomheter. En bruker kan ubevisst aktivere skadevare som er målrettet lenket til eller levert via e-post som tilsynelatende er legitim og ufarlig (spearphishing).

Mangler i vedlikehold av systemer kan medføre at tekniske sårbarheter eksponeres ved at menneskelige sårbarheter utnyttes. Et eksempel er e-poster med skadelig innhold som slipper gjennom til bruker, og at skadevare ikke stoppes når den aktiveres av en uforvarende bruker. Slike tekniske sårbarheter kan skyldes svikt og mangelfulle rutiner eller systemer for oppfølging. I noen tilfeller vil sårbarhetene kunne tilskrives uaktsomhet eller mangel på sikkerhetsbevissthet hos den eller de som drifter systemet. Finanstilsynet rapporterer at ansatte ofte utgjør det svakeste ledd i sektorens nettverkssikkerhet og at økning i spearphishing-angrep er én av årsakene til at digital kriminalitet utgjør den største trusselen mot finansnæringen. Mørketallsundersøkelsen viser at mangler i sikkerhetsbevissthet og -kompetanse var medvirkende årsak til at 47 prosent av virksomhetenes mest alvorlige hendelser oppsto. NSM avdekker og utnytter jevnlig slike sårbarheter i inntrengingstester som gir tilgang til IKT-systemer.

Menneskelige feil, særlig i forbindelse med endringsaktiviteter, utgjør sårbarheter ved IKT-systemer. Slike feil er direkte opphav til uønskede hendelser. Nkom viser til flere tilfeller det siste året av feilprogrammering som har fått konsekvenser for kritisk infrastruktur, og konkluderer med at planlagt arbeid i ekom-systemer er den hyppigste utløsende årsaken til at slike hendelser oppstår i sektoren. Den siste mørketallsundersøkelsen viser at menneskelige feil var medvirkende til at 60 prosent av virksomhetenes alvorligste sikkerhetshendelser oppstod.

IKT-hendelser som rammer privatpersoner, kan også få store konsekvenser for virksomheter vedkommende er tilknyttet og i ytterste konsekvens for samfunnet. Bilder, video og annen sensitiv personlig informasjon som er egnet til å sverte, krenke, presse eller svindle kan komme på avveie via bruk av internett og tilkoblede enheter. En person som trues med spredning av slik sensitiv personlig informasjon, vil kunne la seg presse til å fungere som innsider. Individet vil dermed kunne utgjøre en betydelig risiko. NorSIS ser en økning på 8,8 prosent i antall henvendelser til tjenesten slettmeg.no[16] som omhandler uønsket spredning av bilder og videoer, mobbesaker, hevnporno og utpressingssaker på nett. Falske og hackede profiler i sosiale medier utgjør til sammen 7,4 prosent av henvendelsene. NorSIS rapporterer at sakene spenner fra tilfeldige enkelthendelser til hendelser

[16] Slettmeg.no er en råd- og veiledningstjeneste for personer som føler seg krenket på nett.

som fremstår som organiserte med et gjenkjennbart mønster i fremgangsmåte, samt at de som står bak har mer kunnskap om teknologi og er mer utspekulert i sine metoder. Opplevelse av krenkelse, maktesløshet og rettsløshet er ifølge NorSIS vanlige personlige konsekvenser. Slettmeg.no er en viktig tjeneste for befolkningen, da den fanger opp tilfellene som er i gråsonen mellom etikk og kriminalitet.

Utilsiktede IKT-hendelser forårsaket av menneskelige feil på virksomhetsnivå kan få store konsekvenser på individnivå. Nkom vurderer utilsiktede logiske feil i kjerne- og transportnett som den type feil som potensielt har de største konsekvensene for brukere og tilbydere av tjenester som er avhengige av ekom.

ALT VI IKKE SER – ET UFULLSTENDIG RISIKOBILDE

Mørketallsundersøkelsen 2016 viser at nær halvparten – 46 prosent – av virksomhetenes mest alvorlige hendelser ikke ble fanget opp av rutiner, kontroller og revisjoner, men snarere ble oppdaget ved en tilfeldighet. Dette tilsier at mange alvorlige hendelser som treffer virksomhetene, trolig går upåaktet hen. For å kunne bedre sikkerhetstilstanden og styre risiko må man ha god kjennskap til egne systemer og sårbarheter i disse. God sikkerhetsstyring og planmessig sikkerhetsarbeid krever oversikt over egne sårbarheter og egen sikkerhetstilstand. Dette gjelder både for den enkelte virksomheten, for hver samfunnssektor og ikke minst nasjonalt.

Flere kilder kan gi opphav til oversikt over sårbarheter og sikkerhetstilstand. Risikovurderinger og andre analyser, slik som pålitelighetsanalyser, vil gi kunnskap om virksomhetens utsatte prosesser uten at hendelser har inntruffet. Også tilsyn gjennomført av sektormyndighet bidrar til dette bildet. Samtidig vil et hendelsesbilde, og erfarte sårbarheter gjennom dette, utgjøre svært nyttig informasjon om hvilke verdier som er verdt å sikre.

Mange virksomheter gjennomfører risikovurderinger, og det er også stadig flere sektormyndigheter som lager egne aggregerte risikovurderinger for hele sektoren. Dette gir også grunnlag for en stadig bedre nasjonal oversikt over sårbarhetene i kritisk infrastruktur og scenarioene det vil være mest hensiktsmessig å sikre seg mot.

En viktig kilde til kunnskap om sårbarheter i ulike sektorer er tilsyn. Sektorvis og nasjonalt gjennomfører ulike sektormyndigheter tilsyn av sikkerhetsarbeidet i virksomheter både innenfor og utenfor sikkerhetslovens virkeområde. Dette arbeidet bidrar til å avdekke og tette sårbarheter i kritisk infrastruktur, men IKT-tilsyn i sektorene har fortsatt mangler. Det er derfor grunnlag for å si at det nasjonale IKT-risikobildet har mangler på grunn av dette. Lysneutvalget uttrykte gjennom sin utredning i 2015 at det er behov for å styrke IKT-sikkerhetskompetansen innen flere sektortilsyn. Dette skyldes både kapasitets- og kompetansemangel. Justis- og beredskapsdepartementet vurderer i stortingsmeldingen om IKT-sikkerhet at knapphet på IKT-sikkerhetskompetanse gjør dette utfordrende å få til i alle sektortilsyn. Som en konsekvens skal NSM derfor i løpet av 2017 etablere en felles arena for informasjons- og kompetanseoverføring mellom de mest sentrale tilsynsmyndighetene. Hensikten er å øke kvaliteten på sektorenes tilsyn med IKT-sikkerhet. Erfaringer gjennom tilsyn vil bidra til en mer helhetlig oversikt over samfunnets samlede sårbarheter, og i større grad gjøre det mulig å si noe om utviklingen over tid.

For å kunne se hendelser i sammenheng og avgjøre omfang og alvorlighetsgrad, er det ofte nødvendig å aggregere dette på nasjonalt nivå. Manglende innrapportering, eller lav kvalitet på det som innrapporteres, vil gi et mangelfullt trussel- og sårbarhetsbilde. Hemmelighold rundt hendelsene fratar samfunnet muligheten for læring og bedre sikkerhet, og den preventive effekten for

andre virksomheter begrenses. For virksomheter underlagt sikkerhetsloven gjelder lovpålagt rapporteringsplikt av sikkerhetstruende hendelser til NSM. Mørketallsundersøkelsen fra NSR og NSMs erfaring indikerer at det i dag er en underrapportering av hendelser.

Trusler innen IKT kan også utgjøre deler av en bredere kampanje sammensatt av en rekke virkemidler, ofte omtalt som hybride trusler. For å kunne identifisere og imøtegå slike trusler er det avgjørende at IKT-hendelser rapporteres og sammenstilles med andre hendelser for å sikre et helhetlig situasjonsbilde.

En positiv utvikling er at det utarbeides stadig flere sektorvise risikovurderinger som gjøres tilgjengelig på tvers av sektorer. Dette er som tidligere beskrevet en forutsetning for å iverksette de riktige sikringstiltakene, og kan også tyde på en større bevissthet rundt IKT-sikkerhet og konsekvensene av utilstrekkelig sikkerhet.

Testing av rapporteringsrutiner – øvelse IKT-16

Alvorlige cyberangrep kan ramme flere sektorer samtidig. Under slike store hendelser er det helt nødvendig at håndteringsarbeidet er godt koordinert og at samarbeidet mellom sektorene fungerer. Angrep forekommer heldigvis sjelden, og øvelser er derfor et godt virkemiddel for å ruste seg mot dem. I november 2016 ble øvelse IKT16 avholdt i regi av Direktoratet for samfunnssikkerhet og beredskap (DSB). Formålet var å sette Norge bedre i stand til å håndtere større tverrsektorielle IKT-hendelser. Et utkast til *Nasjonalt rammeverk for digital hendelseshåndtering* ble lagt til grunn for øvelsen.

Øvelsen ga mange gode erfaringer, men foreløpige funn fra DSBs evaluering identifiserer et forbedringspotensial på noen områder. Rammeverket fungerte relativt sett godt, men flere virksomheter opplevde noe uklare rapporteringslinjer. Derfor ble erfaringene fra øvelsen brukt til å forbedre utkastet til rammeverk.

En del virksomheter meldte også tilbake at informasjon fløt oppover i systemet, men at det var begrenset hva som kom ovenfra. Det kan forklares med at IKT-hendelsen spilt under øvelse IKT16 går under kategorien tilsiktet hendelse. Informasjonsdeling blir i denne sammenheng mer komplisert enn ved utilsiktede hendelser. Det er flere hensyn som må vurderes med tanke på hvem som bør få tilgang til informasjon og graden av detaljer som skal distribueres, ettersom innholdet kan være sensitivt og gradert. Dette innebærer at virksomhetenes ønske om et utfyllende situasjons- eller trusselbilde i noen tilfeller vil måtte vike av hensyn til for eksempel rikets sikkerhet.

Teknologitrender og sikkerhetsutfordringer

Den pågående digitaliseringen av samfunnet blir drevet fremover og gjort mulig av teknologiutvikling. Ny teknologi kan gjøre det mulig å lage sikrere løsninger, men kan også medføre økt kompleksitet, introduksjon av nye sårbarheter og økt behov for sikkerhetskompetanse.

TJENESTEUTSETTING VANSKELIGGJØR KONTROLL PÅ KOMPLEKSE VERDIKJEDER

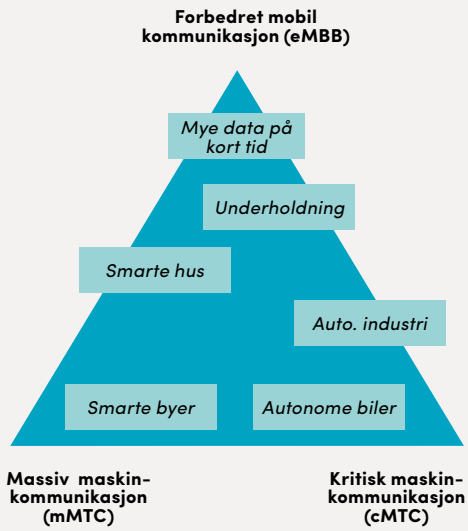
Den største og mest betydningsfulle trenden er vekst i bruken av tjenesteutsetting, inkludert skytjenester. Bruk av tredjepartstjenester og underleverandører, som igjen benytter andre tredjepartsløsninger og underleverandører, skaper et komplekst avhengighetsbilde på tvers av sektorer og på samfunnsnivå. Dette resulterer i mer komplekse og uoversiktlige digitale verdikjeder. Kompleksiteten gjør det også vanskeligere å ha kontroll med hvilken informasjon vi gir fra oss, hvor informasjon til enhver tid befinner seg og hvordan denne er sikret.

Økt bruk av tjenesteutsetting har også gjort det mulig å konsolidere og samle store mengder informasjon og IKT-tjenester på få datasentre. Dette er en utvikling vi forventer vil fortsette. Økt konsolidering av informasjon og IKT-tjenester vil muliggjøre og åpne opp for mer utstrakt bruk av automatiserte sikkerhetstiltak, men vil også åpne for automatisert håndtering av underliggende teknologier og tjenester. Konsekvensen er at virksomhetene får redusert mulighet til å kontrollere sine digitale verdikjeder. Ett av områdene der dette er relevant er innen ekom-tjenester.

NY TEKNOLOGI KREVER NY SIKKERHETSKOMPETANSE – IOT, 5G OG KUNSTIG INTELLIGENS

En mengde nye og ulike enheter kobles til internett. IoT vil være en bestanddel i en rekke nye teknologiske fremskritt, som for eksempel smart grid, smarte byer, smarte hus og autonome biler og skip. Enhetene er gjerne små og kan inneha relativt kraftig dataprosesseringskapasitet og må ses i kombinasjon med fremveksten av neste generasjons mobilnett (4G/5G). Kombinasjonen av smarte enheter og et mye raskere mobilnett vil medføre et generasjonsskifte i tilgjengelig funksjonalitet, men også medføre nye sårbarheter. Kommunikasjon på 5G vil i større grad foregå fra maskin til maskin, og virksomheter som velger å benytte teknologien, må skaffe seg kunnskap om nye sårbarheter og sikkerhetsmekanismer.

EKSEMPLER PÅ TJENESTER SOM KAN TILBYS GJENNOM 5G. KILDE: FFI.



Økende bruk av stordata og algoritmer for kunstig intelligens gir muligheter for tilpasset informasjon til brukerne. Dette kan også brukes til å skreddersy

ensidige nyhetsmeldinger til ulike befolkningsgrupper for å endre opinionen i samfunnet. I ytterste konsekvens vil dette være en trussel mot vårt demokratiske system.

Kunstig intelligens vil også innta tjenesteproduksjon i datasentre og i ekom-sektoren innenfor en femårs-periode, men muligens ikke i full skala før nærmere 2025. Det er i hovedsak to utviklingstrekk som driver frem bruk av kunstig intelligens innenfor ekom og databehandling:

- Programvaredefinerte nettverk og virtualisering
- Kompleksitet i moderne ekom- og datasystemer

Mange prosesser som tidligere krevde menneskelig interaksjon, er nå fullstendig automatisert. Samtidig ser vi at fremtidens ekom, og særlig utviklingen mot 5G med maskin-til-maskinkommunikasjon, får en kompleksitet og skala som gjør det nær umulig å bruke manuelle prosesser i drift og vedlikehold. De nye kommunikasjonsnettverkene krever avansert nettverksstyring i stor skala, som blir muliggjort ved hjelp av virtualisering av nettverksfunksjoner og kunstig intelligens.

Mulige effekter av kunstig intelligens

Valget i USA i 2016 synliggjorde en industri som spesialsyr informasjon mot forbrukere i hensikt å påvirke meninger. Underliggende teknologier er både stordata og forskjellige former for kunstig intelligens. I USA-valget ble dette brukt direkte for å påvirke velgere som med stor sannsynlighet lot seg påvirke av rettet informasjon. Teknologien kan også brukes for opinionspåvirkning innen andre områder enn politikk. Effekten av denne teknologien er sannsynligvis ikke fullt utforsket ennå, og vi forventer mer bruk av slik teknologi i fremtiden. Denne typen teknologi er blitt mulig fordi personopplysninger har blitt en handelsvare på det åpne markedet.

Når kunstig intelligens styrer nettverk og datasystemer vil dette medføre ikke-verifiserbare systemer. Dagens regime for sikkerhetsgodkjenning blir utfordret når et systems oppførsel kan endres basert på automatiserte algoritmer. Kompleksiteten i moderne og kommende ekom- og datasystemer er så høy at det heller ikke er mulig for menneskebaserte prosesser å ha full kontroll over systemet til enhver tid. Målet må være at kunstig intelligens gir bedre kontroll over sikkerhetsutfordringer enn menneskebaserte prosesser. Alternativt må menneskene fortsette å kontrollere sikkerheten, eventuelt kompleksiteten reduseres.

Utvikling av algoritmer for kunstig intelligens krever høy kompetanse, samtidig som behovet for dagens driftsingeniører blir redusert. Det er mulig at slik kompetanse kun vil være tilgjengelig hos et fåtall spesialiserte firmaer på global basis. Et pågående initiativ i Telenor, i samarbeid med NTNU, har som mål å utvikle nasjonal kompetanse innenfor dette feltet.

Virtualisering

Målet med virtualisering er å separere en tjeneste logisk fra maskinvaren som kjører tjenesten. Funksjonalitet flyttes fra maskinvare til programvare, noe som blant annet vil gi stor gevinst ved utrulling og realisering av nye tjenester. Endringene kan gjøres i programvare istedenfor at fysiske komponenter byttes ut. Virtualisering har en rekke konsekvenser innenfor sikkerhet og er en viktig

byggekloss i de andre trendene. Skytjenester er antagelig den mest kjente anvendelsen av virtualiseringsteknologi. En positiv effekt er at økning i bruk av virtuelle arbeidsflater vil generelt kunne øke IKT-sikkerheten i bedrifter ved at mulige angrepsflater blir redusert. Liten til ingen datalagring på lokale datamaskiner reduserer sårbarheten.

VIKTIGHETEN AV TILLITSSKAPENDE TEKNOLOGIER ØKER

Den teknologiske utviklingen kan gi nye muligheter når det gjelder sikkerhet. Med tillitsskapende teknologier mener vi teknologier og teknologiutvikling som påvirker særlig personvern og samfunnets tillit til både teknologi og forskjellige aktører, men også IKT-sikkerhet generelt.

Ny EU-forordning om personvern (General Data Protection Regulation (GDPR)) vil gi skjerpede krav til både behandling av personopplysninger og krav til varsling ved eventuelle brudd på sikring av personopplysninger. I tillegg vil det komme straff i form av bøter. I det nye regelverket stilles det blant annet krav om innebygd personvern (bygge personvern inn i løsninger og at personvern skal være standardinnstilling), og at virksomheter må gjøre en vurdering av personvernkonsekvenser blant annet når det behandles sensitive personopplysninger i stor skala, ved profilering og ved utstrakt overvåking av offentlig område.[17]

Store selskaper har ikke råd til å få dårlig omtale av egen sikkerhet og vern av kundenes data og har meget stort fokus på egen sikkerhet. De må sikre sin egen virksomhet mot uheldig omtale og direkte påvirkning av egne datasystemer. Det er også indikasjoner på at de store selskapene bedre vil regulere og kontrollere hvordan samarbeidspartnere bruker og utveksler sensitiv informasjon. Det er derfor grunnlag for å påstå at personvernet blir bedre fremover. Likevel ønsker mange forbrukere tjenester som er personlig tilpassede, og de gir dermed mer eller mindre bevisst fra seg informasjon om seg selv til tjenestetilbydere og «app-er». I andre tilfeller kan brukeren bli «tvunget» til å gi fra seg informasjon til tredjeparter for å kunne benytte enkle tjenester på telefonen. Mengden informasjon vi frivillig gir fra oss, vil mest sannsynlig fortsette å øke. Dette medfører at store selskaper mottar store mengder informasjon om enkeltpersoner, som brukes for å tilpasse tjenestene til brukerne.

Oppdateringer av operativsystemer, applikasjoner og liknende har tidligere gjerne vært overlatt til brukerne. I de nyeste operativsystemene er det en trend at leverandørene overtar dette ansvaret selv gjennom at sikkerhetsoppdateringer blir tvunget på brukerne. De store leverandørene er avhengig av brukernes tillit til sikkerhet i sine produkter, og tvungen sikkerhetsoppdatering av produkter vil fjerne mange eldre sårbarheter. Ulempen for brukerne er at slike oppdateringer kan endre oppførselen til et system uten at brukerne får et forvarsel. NSM vurderer at denne trenden i stor grad vil øke datasikkerheten i konsumentmarkedet og i små og mellomstore bedrifter.

KVANTEDATAMASKINER UTFORDRER DAGENS KRYPTERINGSMEKANISMER

En viktig langsiktig trend innen utviklingen av IKT er stadig økende regnekapasitet. Fysiske og økonomiske begrensninger på konvensjonell silikonbasert teknologi har bremset utviklingen. Innen standardisering av kryptoteknologi har vi til nå klart å forutse og ta høyde for den økte regnekraften gjennom å benytte tilstrekkelige sikkerhetsmarginer eller ved å utfase eldre teknologi i tide.

Kvantedatamaskiner har vært under utvikling i mange tiår. De fungerer etter andre prinsipper enn tradisjonell digital teknologi, og når kvante-

[17] Datatilsynet (2017). *Programvareutvikling med innebygd personvern.*

datamaskiner med tilstrekkelig kapasitet og stabilitet realiseres, vil dette føre til en svært stor kapasitetsøkning innenfor noen, men viktige beregningsproblemer som er relevante i et kryptografisk perspektiv. Dette vil innebære et paradigmeskifte, og vil gjøre forskjellige typer kryptoteknologi utdatert over natten.

Mange av de kryptografiske mekanismene som er vanlig i bruk i dag, vil bli knekt av kvantedatamaskiner. Det er ikke mulig i praksis å videreutvikle alle disse mekanismene slik at de blir robuste nok. En må ta høyde for at krypterte data lagres av en motstander for senere forsering den dagen en kvantedatamaskin blir tilgjengelig. Det haster derfor med å komme frem til nye standarder som er resistente mot kvantedatamaskiner. NSM har satt i gang arbeid som er relevant for videreutvikling av krypteringsteknologi for nasjonale graderte systemer. For det ugraderte domenet har det anerkjente internasjonale standardiseringsorganet National Institute of Standards and Technology (NIST) satt i gang et større standardiseringsarbeid.

Eiere av krypteringsløsninger eller nøkkelinfrastruktur (PKI) må ta høyde for den kostnaden det vil innebære å bytte ut kryptoteknologi som er sårbar overfor kvantedatamaskiner. Eiere med et langsiktig beskyttelsesbehov må ta denne kostnaden tidligere enn de med et kortsiktig beskyttelsesbehov.

NSM anser i dag at eiere med kortsiktige beskyttelsesbehov bør ha migrert til kvanteresistent kryptoteknologi i løpet av 2025–2030.

Tiltak

En helhetlig tilnærming for å beskytte risikoutsatte verdier inkluderer både forebyggende tiltak og tiltak for å håndtere hendelser dersom de inntreffer. Forebyggende sikkerhetsarbeid skal bidra til å beskytte viktige verdier og skape motstandsdyktighet. Tiltak for å øke evnen til å håndtere hendelser er vesentlig for å redusere konsekvensene dersom hendelser inntreffer. Anbefalingene som gis i årets rapport, må ses i sammenheng med NSMs tidligere anbefalinger i *Risiko 2017* og *Helhetlig IKT-risikobilde 2016*. Tiltakene retter seg i hovedsak mot virksomheter. Enkeltpersoner kan søke råd gjennom NorSIS eller tjenesten Nettvett.no, som er et tverrsektorielt pilotprosjekt mellom NorSIS, Nkom og NSM for å heve kompetanse om og jobbe forebyggende med IKT-sikkerhet.

Ansvaret for å forebygge uønskede IKT-hendelser hviler først og fremst på virksomheten selv. I første rekke handler det om å øke robusthet ved å avdekke og lukke sårbarheter tilknyttet egne IKT-systemer. Dette innebærer rutinemessig kontroll av verdier og sikringstiltak, tilgangsstyring, bevisstgjøring av hver enkelt ansatt om at alle har felles ansvar for sikkerhet, og aksept for at det å si fra om hendelser og avvikende oppførsel er helt nødvendig for å beskytte virksomheten. Det hviler også et forebyggende ansvar på virksomhetene om å rapportere IKT-hendelser til overordnet myndighet. Dette kan bidra til å øke robusthet i andre virksomheter og er en forutsetning for at nasjonale myndigheter skal kunne avdekke og imøtegå ulike trusler.

Hva gjør myndighetene for å redusere vår samlede nasjonale risiko?

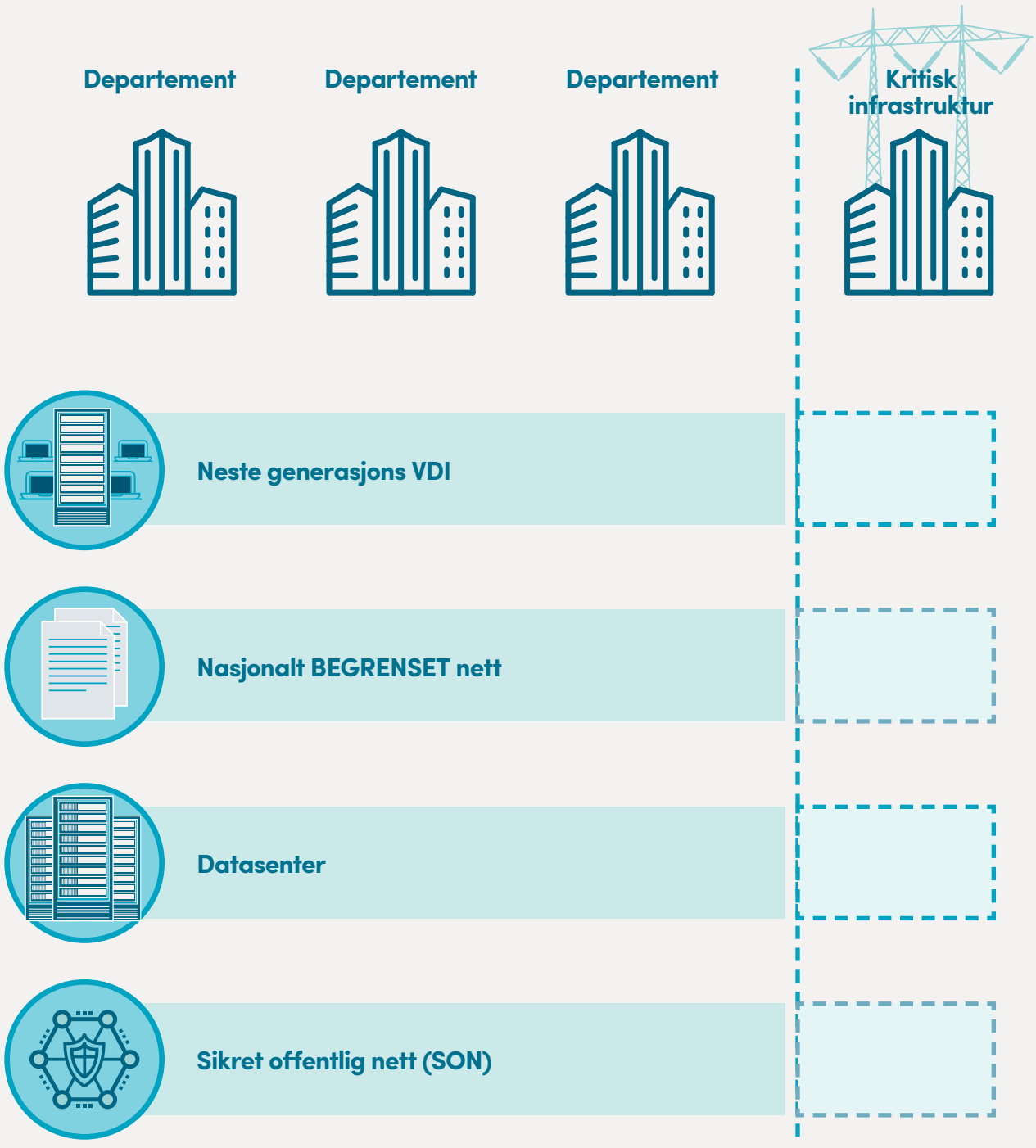
Norge klassifiseres som ett av 21 «ledende land» i FN-organet International Telecommunication Unions (ITU) *Global Cybersecurity Index* (GCI), som måler medlemslandenes engasjement og innsats (*commitment*) innen IKT-sikkerhet.[18] Sommeren 2017 utga Justis- og beredskapsdepartementet for første gang en egen stortingsmelding om IKT-sikkerhet med tiltak for å avbøte en rekke tverrsektorielle utfordringer.[19] Samtidig ble også forslag til modernisert sikkerhetslov fremlagt av Forsvarsdepartementet. Den nye loven tar høyde for at flere private virksomheter har avgjørende betydning for grunnleggende nasjonale funksjoner og at det er gjensidige avhengigheter mellom ulike samfunnssektorer.

Ett av satsingsområdene fremover blir å styrke den nasjonale evnen til å avdekke og håndtere digitale angrep. Dette skal skje gjennom videreutvikling av det nasjonale varslingssystemet for digital infrastruktur (VDI) og gjennom rammeverket for digital hendelseshåndtering. I tillegg står informasjonsdeling mellom offentlige og private virksomheter sentralt for å bedre samarbeidet, samt å effektivisere og automatisere deling av informasjon. NSM skal i 2017 bidra til dette ved å utvikle løsninger for automatisert deling av varsler og teknisk informasjon med responsmiljøene i de ulike sektorene. Felles cyberkoordineringssenter (FCKS) ble opprettet 31. mars 2017, og har som oppdrag å styrke nasjonal evne til effektivt forsvar mot og håndtering av alvorlige hendelser i det digitale rom. Dette er et viktig tiltak, som blant annet vil bidra til koordinert bruk av nasjonale ressurser og utvikling av et helhetlig beslutningsgrunnlag innen cyberhendelser mot Norge.

[18] International Telecommunications Union (2017), *Global Cybersecurity Index (GCI)*.

[19] Meld. St. 38 (2016-2017). *IKT-sikkerhet – Et felles ansvar.*

NY ROBUST OFFENTLIG INFRASTRUKTUR



Illustrasjonen viser hvordan en rekke iverksatte prosjekter til sammen vil bidra til å skape et nytt offentlig nett med god robusthet. Det er besluttet at Nasjonalt BEGRENSET nett (NBN) skal være felles plattform for departementene med underliggende etater. Dette vil derfor bli en nøkkelkomponent i å realisere prosjektene.

Sikkerhet trekkes frem som en viktig innsatsfaktor for innovasjon og produktivitet i stortingsmeldingen Digital agenda for Norge, som gir en tydelig retning for regjeringens hovedmål og -prioriteter innenfor IKT-området.[20] Digitaliseringen av det offentlige Norge er inne i en kritisk fase. De utfordringene som er beskrevet tidligere i rapporten, omfanget av sårbarheter og hvordan disse utnyttes av ulike trusselaktører, kan ikke løses utelukkende ved hjelp av sikkerhetstiltak basert på dagens teknologi. Nytenkning, sammen med en tydelig visjon om hvordan funksjonalitet, effektivisering og sikkerhet kan kombineres for å gi tjenester med høy grad av tillit, er avgjørende for at vi skal klare å digitalisere samfunnet på en sikker måte.

REGJERINGENS TVERRSEKTORIELLE TILTAK FOR STYRKET IKT-SIKKERHET

Forebyggende sikkerhet - virksomheters egenevne	Avdekke og håndtere digitale angrep	IKT-sikkerhetskompetanse	Kritisk IKT-infrastruktur
• utrede rettslig regulering på IKT-sikkerhetsområdet • legge bedre til rette for at virksomheter kan vurdere og prioritere tiltak innenfor IKT-sikkerhet • utvikle og vedlikeholde et godt og tilgjengelig kunnskapsgrunnlag som gjør enkeltindivider, virksomheter og myndigheter i stand til å treffe riktige tiltak for å opprettholde tilstrekkelig sikkerhet i sine IKT-systemer	• videreutvikle det nasjonale varslingssystemet for digital infrastruktur (VDI) • videreutvikle et nasjonalt rammeverk for digital hendelseshåndtering • etablere et informasjonsdelingsarbeid for å bedre samarbeidet mellom offentlige og private virksomheter • utrede hvordan en form for digitalt grenseforsvar kan etableres og lovreguleres • gjøre politiet bedre i stand til å bekjempe kriminalitet i det digitale landskapet • videreutvikle samarbeidet mellom E-tjenesten, NSM, PST og politiet for øvrig • forbedre NSMs evne til å analysere alvorlige digitale angrep	• etablere en nasjonal kompetansestrategi for IKT-sikkerhet, • vurdere hvorvidt IKT-sikkerhet er tilstrekkelig inkludert i den grunnleggende digitale kompetansen elevene skal tilegne seg • styrke IKT-sikkerhetskompetansen i tilsyn • legge vekt på systematisk oppfølging og læring etter både øvelser og hendelser, også ved digitale hendelser	• prioritert midler til etablering av en pilot for alternativt kjernenett, jf. Meld. St. 33 (2016– 2017) Nasjonal transportplan 2018–2029 • arbeide videre med konkretisering av mulige statlige tiltak som kan bidra til å legge til rette for flere fiberkabler til utlandet • arbeide for et sterkt kommunikasjonsvern i Norge
Fellestiltak • utarbeide ny nasjonal strategi for IKT-sikkerhet • etablere forum for offentlig-privat samarbeid • videreutvikle Nettverk for informasjonssikkerhet • videreutvikle totalforsvaret og øke motstandsdyktigheten i samfunnskritiske funksjoner			

[20] Meld. St. 27 (2015-2016). *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet.*

Når cyberangrepet bare er begynnelsen

De siste årene har sammensatte operasjoner (ofte omtalt som hybride trusler) fått stor oppmerksomhet. Ved sammensatte operasjoner inngår cybertrusselen som ett element blant andre virkemidler. Et hybrid angrep kan foregå ved en kombinasjon av eksempelvis cyberoperasjoner, fysiske angrep, oppkjøp av eierandeler i kritisk infrastruktur, verving av innsidere og påvirkning av beslutningstakere og opinion. En kartlegging av tiltak andre europeiske land har iverksatt mot cyberangrep, viser bredde i tiltakene mot dette. Langt på vei de fleste tiltakene iverksettes for å forebygge hendelser. Blant disse tiltakene er digitalt grenseforsvar, offensiv cyberkapasitet og cybersikkerhetsstrategier iverksatt i flere av landene. Flere land etablerer også ulike organer (eksempelvis råd og senter) for overvåking, analyse og håndtering av cyberangrep på ulike nivå i statsforvaltningen. Det er også flere land som iverksetter tiltak i form av informasjon og bevisstgjøring om trussel og ansvarsforhold, særlig bevisstgjøring om private virksomheters egenevne innen IKT-sikkerhet. For å kunne håndtere sammensatt virkemiddelbruk er det avgjørende at IKT-hendelser rapporteres og sammenstilles med andre hendelser, for å sikre et helhetlig situasjonsbilde. Også norske myndigheter har iverksatt prosesser for å styrke mekanismene for å forebygge og håndtere cyberangrep.

ETABLERING AV GRUNNPRINSIPPER FOR IKT-SIKKERHET

Vi ser ofte at det mangler en rød tråd mellom de prioriteringene som toppledelsen gjør og de faktiske sikringstiltakene som iverksettes i IKT-systemene og i organisasjonen. Forretnings- og IKT-ledere skal omsette toppledelsens prioriteringer til rammeverk og retningslinjer som virksomheten må følge.

I august 2017 lanserte vi første versjon av NSMs grunnprinsipper for IKT-sikkerhet[21]. Her definerer vi et sett med grunnprinsipper for å beskytte verdier og leveranser i en virksomhet. De beskriver hva en virksomhet bør gjøre og hvorfor. Dette vil hjelpe de ulike virksomhetene å velge ut og prioritere sikringstiltak, og gi regelverksforvaltere et rammeverk de kan vise til i sin kravstilling og veiledning. Det vil samtidig være til hjelp for å bedre risikokommunikasjonen mellom toppledelsen og implementasjonspersonell i virksomheten.

Arbeidet er basert på anerkjente standarder og rammeverk sett i sammenheng med erfaringer fra NSM og våre samarbeidspartnere. Grunnprinsippene for IKT-sikkerhet skal være et verktøy for å:

- velge ut de riktige sikringstiltakene
- gi en begrunnelse for hvorfor tiltakene bør implementeres
- vise hvilke tiltak NSM – på bakgrunn av gjeldende risiko – mener særlig bør prioriteres

Grunnprinsippene er strukturert i fire kategorier. Hvert grunnprinsipp har underliggende sikringstiltak som beskriver hva som bør gjøres, og understøttes av en begrunnelse for hvorfor dette bør gjøres. Grunnprinsippene kompletterer, men erstatter ikke en virksomhets sikkerhetsstyringsarbeid. Utvelgelse av sikringstiltak bør baseres på det ordinære risikoarbeidet, men grunnprinsippene vil hjelpe virksomhetene å velge ut riktige sikringstiltak.

[21] NSM (2017). *Grunnprinsipper for IKT-sikkerhet.*

NSMS GRUNNPRINSIPPER FOR IKT-SIKKERHET

KONTROLL MED TJENESTEUTSETTING

Utkontraktering av IKT-tjenester til profesjonelle aktører vil kunne gi bedre sikkerhet og mer stabile og tilgjengelige tjenester, lavere og mer forutsigbare kostnader og i større grad bidra til bedre fokus om virksomhetens kjerneaktivitet. Samtidig må virksomheten være bevisst hvilke verdier som eksponeres ved utkontraktering og iverksette tiltak som ivaretar disse. Behovet for konfidensialitet, integritet og tilgjengelighet bør særlig vektlegges i vurderingene, samt hvilke lover, krav og regler som gjelder for sektoren nasjonalt og internasjonalt.

Tjenesteutsetting kan imidlertid øke risikoen for at man ikke har god nok kontroll på eierskap, sikring og tilgang til data. Dette er en generell utfordring, men den forsterkes når data lagres eller driftes utenfor landets grenser. Med stadig mer kompliserte verdikjeder og leverandøravhengigheter trenger virksomhetene bedre bestillerkompetanse og

bedre oppfølging av underleverandører. En grunnleggende forutsetning er at det gjøres gode risikovurderinger. Eksempler på områder som må risikovurderes er:

- fysisk lokalisering av utstyr og driftspersonale
- hvem som har innsyn i virksomhetens informasjon
- hvor og hvordan informasjon behandles og lagres, samt hvordan informasjonen er adskilt fra andre kunder
- tilgangsstyring, inkludert kryptering, aktivitetslogging og fysisk og logisk sikkerhet
- rutiner for hendelseshåndtering, avviks- og sikkerhetsrapportering
- krise- og beredskapsplaner som skal harmonisere med virksomhetens egne planer
- bruk av underleverandører
- terminering av kontrakten, hvordan utføres tilbakeføring eller flytting av informasjon og sletting eller destruksjon av lagringsmedium

NSM anbefaler bruk av skytjenester, forutsatt at det gjøres en grundig risikovurdering. Det understrekes også at lagring og prosessering utenfor landets grenser krever særlig aktsomhet og kompetanse. Kritisk infrastruktur må være under nasjonal kontroll. Med nasjonal kontroll menes akseptabel nasjonal risiko, og fortrinnsvis at slik infrastruktur er lokalisert og driftet i Norge.

BESTILLERKOMPETANSE
Tjenesteutsetting krever gode risikovurderinger og høy bestillerkompetanse. Virksomheten må besitte nødvendig kompetanse til blant annet å gjennomføre selve anskaffelsen, følge opp i produksjonsfasen og gjennomføre en eventuell avvikling av kontrakten eller tjenesten. Dette krever i de fleste tilfeller en kompleks bestillerkompetanse som må dekke blant annet følgende områder:

Virksomhetskompetanse	Sikkerhetskompetanse	Integrasjonskompetanse	Kompetanse om anskaffelser	Juridisk kompetanse
- For å kunne definere behov og stille nødvendige krav	*- For å kunne vurdere risiko og stille riktige sikkerhetskrav. Dette gjelder alle områder av sikkerhet dvs. fysisk -, personell- og informasjonssikkerhet*	*- For å kunne forstå hvordan tjenestene skal kunne integreres i virksomheten på best mulig måte*	*- Slik at den kan gjennomføres på en måte som understøtter virksomhetens forretningsmessige og funksjonelle behov på best måte*	*- Slik at virksomhetens juridiske krav og behov ivaretas og at kontrakten kan oppfylles i produksjonen*

SIKKER DRIFT OG VEDLIKEHOLD

Helgen før 17. mai 2017 kom nyheten om at løsepengeviruset kjent som WannaCry var spredd til datamaskiner over hele verden. Det kritiske, men enkle, virkemidlet for å beskytte seg mot WannaCry var å installere siste oppdatering fra Microsoft, noe som fjernet sårbarheten som ble utnyttet. I dette tilfellet var skadeomfanget i Norge begrenset.

Det typiske angrepsmønsteret i det digitale rom er at virksomheten mottar en e-post med infisert skadevare. Selv om man lykkes med å etablere en god sikkerhetskultur og filtreringsmekanismer for mottak av e-post, vil en angriper før eller siden kunne komme seg på innsiden av IKT-systemene. Man må derfor iverksette tiltak som hindrer at skadevare etablerer seg eller kommer seg videre. NSM har siden 2014 anbefalt fire viktige tiltak for sikring av IKT-systemer mot denne typen trussel.[22]

[22] NSM (2016). S-01 *Fire effektive tiltak mot dataangrep.*

FIRE EFFEKTIVE TILTAK MOT CYBERANGREP

1

Oppgraderer program- og maskinvare

3

Ikke tildel sluttbrukere administratorrettigheter

2

Installer sikkerhetsoppdateringer så fort som mulig

4

Blokker kjøring av ikke-autoriserte programmer

Dette er tiltak som reduserer risiko i cyberdomenet, enten det dreier seg om spionasje, vandalisme, løsepengevirus eller annen kriminell adferd. Oppdaterte systemer krever at vedlikehold prioriteres, men også en moderniseringsplan for å unngå utdatert programvare. Sikker drift og vedlikehold må være en del av helhetlig virksomhetsstyring.

For brukere som ikke kan oppdatere maskinene sine, anbefales det å sikre seg så godt som mulig ved hjelp av andre sikkerhetsmekanismer, som for eksempel å skille gamle, og potensielt sårbare, maskiner fra øvrig infrastruktur ved hjelp av brannmurer eller tilsvarende teknologier.

Digitale verdikjeder har også en svært viktig fysisk dimensjon. Virksomheter må kartlegge og sikre fysisk infrastruktur de er avhengig av for å kunne utføre sin funksjon. Dette kan gjøres gjennom å opprette redundante løsninger, samt fysisk sikring av kritiske komponenter. Et viktig moment å ta med i vurderingen av sikringsbehovet er om tapte komponenter enkelt og raskt kan erstattes.

E-POSTSIKKERHET – TEKNISKE OG MENNESKELIGE TILTAK

E-post er fortsatt den foretrukne digitale kommunikasjonskanalen for norske offentlige og private virksomheter, selv om ny teknologi gjør det mulig å kommunisere elektronisk på andre måter. Ifølge en undersøkelse fra SSB benyttet 90 prosent av den norske befolkningen e-post i 2016. E-post er en attraktiv angrepsmåte for trusselaktører og har potensial til å ramme mange.

E-post er basert på en i utgangspunktet usikker teknologi, og er enkel å forfalske, avlytte og endre. Nye utvidelser og sikringstiltak rettet mot e-post har blitt utviklet for å imøtekomme det endrede trusselbildet. Fordi e-post er et svært vanlig angrepsvåpen, bør mottiltak som bygger robusthet mot denne type digitale angrep være høyt prioritert.

Virksomheten bør sikre e-post slik at ingen uvedkommende får tilgang til eller kan manipulere innholdet, at avsender verifiseres og at e-post ikke benyttes for å levere skadevare. NSM har anbefalt flere tekniske sikringstiltak for å begrense og stoppe uønsket og ondsinnet e-post.[23] Blant annet anbefaler vi å ta i bruk de åpne standardene SPF, DKIM og DMARC som begrenser mulighetene for å motta forfalsket e-post.[24]

I tillegg er det viktig å sørge for å etablere god sikkerhetskultur og regelmessig opplæring. Hvis en ondsinnet e-post likevel skulle havne i sluttbrukers innboks, bør en årvåken bruker generelt være varsom med å åpne vedlegg og klikke på linker i e-poster. Dessverre er enkelte ondsinnede e-poster svært vanskelig for ordinære brukere å identifisere. Sluttbrukers årvåkenhet kan derfor ikke bli en sovepute for driftspersonell som administrerer e-posttjenesten i virksomheten.

RAPPORTERING OG DELING AV INFORMASJON OM IKT-HENDELSER

Alvorlige digitale hendelser er ofte sammensatt av små enkelthendelser. For å kunne se hendelser i sammenheng og avgjøre omfang og alvorlighetsgrad, er det nødvendig å aggregere disse på nasjonalt nivå. NSM utviklet i 2017 et *Rammeverk for digital hendelseshåndtering* for å gi en helhetlig tilnærming til nasjonal hendelseshåndtering. Ambisjonen er å legge til rette for at samfunnet utnytter kompetanse og ressurser effektivt og koordinert for å håndtere alvorlige tverrsektorielle digitale hendelser. For å sikre et best mulig helhetlig trussel- og sårbarhetsbilde er det avgjørende at hendelser rapporteres og at kvaliteten på det som rapporteres er god. Rapporteringen er viktig av to grunner:

[23] NSM (2014). U-02 *Kryptering av e-postoverføring.*

[24] Se punkt 2.9 i NSMs Grunnprinsipper for IKT-sikkerhet.

[25] PST, NSM, Politiet og NSR (2017). *Sikkerhet ved ansettelsesforhold – før, under og ved avvikling.*

1. For å kunne bistå virksomheter i å håndtere sine hendelser er NSM og andre myndigheter og sentrale aktører avhengig av historiske data, fordi digital hendelseshåndtering i stor grad tar utgangspunkt i erfaringer fra tidligere hendelser. Derfor er det viktig at virksomheter og sektorvise responsmiljøer rapporterer alle hendelser, ikke bare de store hendelsene. Hendelser som håndteres i en virksomhet eller sektor, kan gjerne rapporteres etter at hendelsen er lukket internt i en virksomhet.

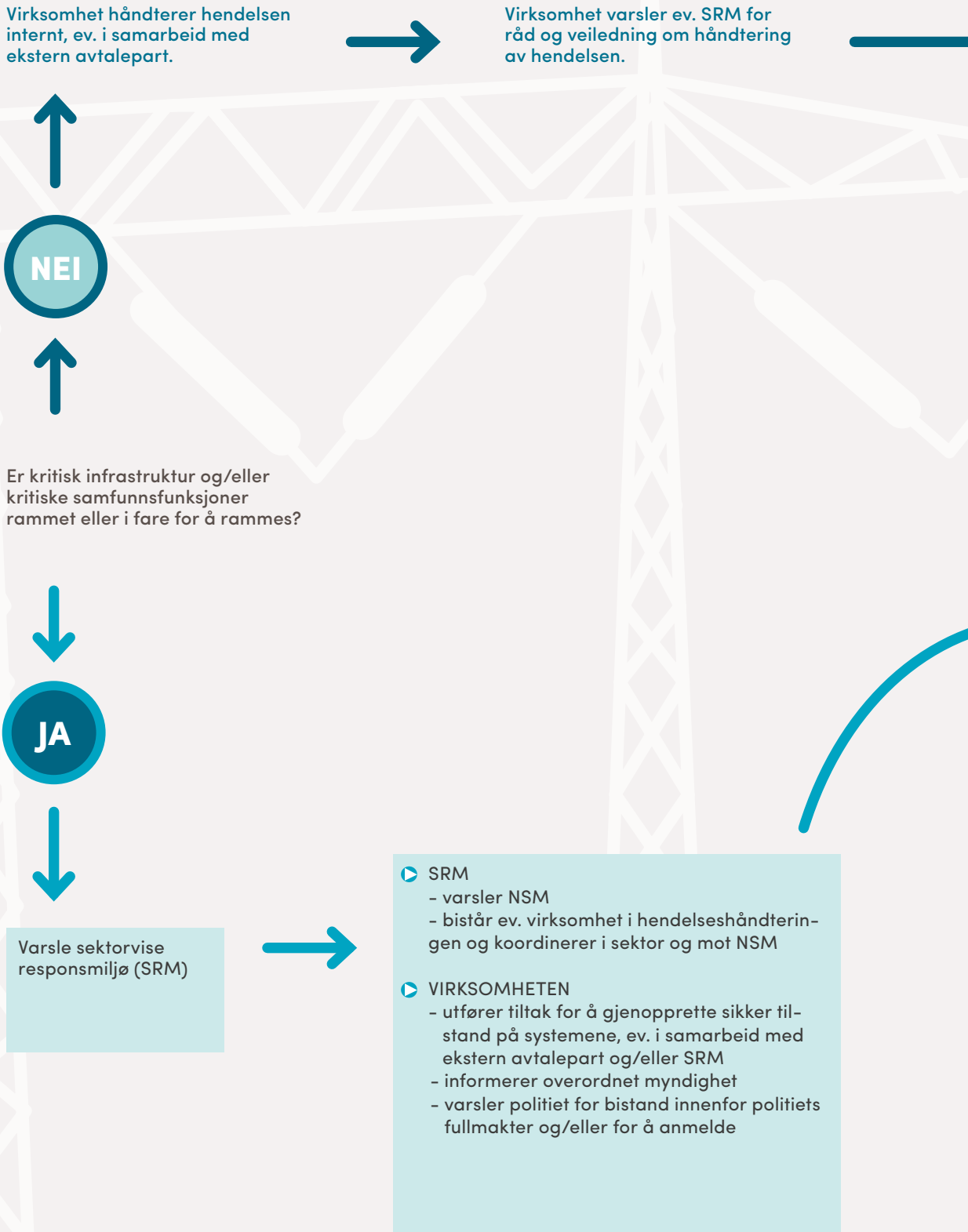
2. For å kunne avgjøre om hendelser skyldes en feil, et angrep eller en strategisk trussel, kreves ofte analyser på myndighetsnivå. Det er derfor anbefalt at det er en lav terskel for å varsle om hendelser.

Rammeverket gjelder for digitale hendelser og digital kriminalitet mot kritisk infrastruktur og kritiske samfunnsfunksjoner. Det er et sektoransvar å identifisere virksomheter som skal benytte dette rammeverket i sin digitale hendelseshåndtering. Dette bør skje gjennom risikovurderinger som identifiserer kritisk infrastruktur og kritiske samfunnsfunksjoner i sektor. Alle virksomheter har også en egeninteresse av å beskytte sin informasjon og sine systemer. Her er det verdt å merke seg at det er en forskjell på å vurdere risiko i et virksomhetsperspektiv og i et samfunnsperspektiv. En hendelse som har stor innvirkning på kritisk infrastruktur eller kritiske samfunnsfunksjoner, har ikke nødvendigvis store konsekvenser for bunnlinjen hos virksomheten som er rammet, og motsatt. Dette er en viktig erkjennelse for virksomheter som forvalter kritisk infrastruktur og kritiske samfunnsfunksjoner.

Tiltak mot innsidevirksomhet

- **Kjenn dine ansatte**
  - Bakgrunnssjekk ved rekruttering
  - ID-sjekk på jobbintervju
  - Vær bevisst på avvikende oppførsel og hendelser
- **Styr tilganger**
  - Kontroll på hvem som har tilgang til hvilken type informasjon (tekniske tiltak)
  - Logg (tekniske tiltak)
- **Opprettholde god sikkerhetskultur**
  - Etabler tillitsforhold og vedlikehold dette
  - Bevisstgjør ansatte om trusselbildet
  - Styrk kompetanse om behov for å rapportere
  - Sørg for at avviksrapportering ikke får negative konsekvenser for den enkelte
  - Ha felles ansvar for sikkerhet
  - Gjennomfør rutinemessig kontroll
- **Evaluer skadeomfang etter hendelser**

NSM har nylig, sammen med andre myndigheter, utgitt en veileder om sikkerhet ved ansettelsesforhold.[25]


Virksomhet håndterer hendelsen internt, ev. i samarbeid med ekstern avtalepart.
Virksomhet varsler ev. SRM for råd og veiledning om håndtering av hendelsen.
NEI
Er kritisk infrastruktur og/eller kritiske samfunnsfunksjoner rammet eller i fare for å rammes?
JA
Varsle sektorvise responsmiljø (SRM)
SRM
- varsler NSM
- bistår ev. virksomhet i hendelseshåndteringen og koordinerer i sektor og mot NSM
VIRKSOMHETEN
- utfører tiltak for å gjenopprette sikker tilstand på systemene, ev. i samarbeid med ekstern avtalepart og/eller SRM
- informerer overordnet myndighet
- varsler politiet for bistand innenfor politiets fullmakter og/eller for å anmelde

Virksomhet anmelder forholdet til politiet.

Politiet kan be NSM om informasjon om tekniske indikatorer etc. i forbindelse med en etterforskning. NSM kan dele informasjon med politiet etter samtykke fra virksomhet.

Etter at angrepet er stanset og sikker tilstand gjenopprettet, bør virksomheten som har vært angrepet alltid gjøre følgende:

- Anmelde forholdet til politiet, dersom dette ikke allerede er gjort
- Rapportere hendelsen til NSM i henhold til rammeverk for digital hendelseshåndtering
- Evaluere virksomhetens håndtering av hendelsen og justere prosedyrer/beredskaps-planverk i henhold til læringspunkter

NSM

- Bistår SRM/virksomheter med analyser, koordinerer informasjonsdelingen og utarbeider nasjonalt situasjonsbilde som beslutningsgrunnlag til strategisk ledelse
- Leder og deltar i FCKS
- Rapporterer til JD, FD, lederdepartementet, FCKS, SRM, virksomheter tilknyttet VDI, ev. andre berørte virksomheter

PST

- Innhenter informasjon om personer og grupper som kan utgjøre en trussel, utarbeider analyser og trusselvurderinger samt etterforsker
- PST deltar i FCKS
- Rapporterer til JD, lederdepartementet og FCKS

POLITIET (KRIPOS)

- Bistår i gjenopprettelse av sikker tilstand gjennom håndtering av konsekvenser og bruk av tvangsmidler og/eller maktbruk for å stanse angrep
- Sikre tekniske spor, gjør beslag, pågripelser og etterforskning
- Kripos deltar i FCKS
- Rapporterer til JD, lederdepartementet og ev. til berørte virksomheter

SEKTOR-DEPARTEMENTET

- Samhandler med SRM for å etablere situasjonsbilde for egen sektor
- Vurdere behov for å iverksette tiltak i egen sektor
- Rapporterer til regjeringen eller lederdepartementet

- FCKS
- Koordinerer håndtering av hendelser under senterets arbeidsområder
- Utøver vurderinger av hendelser i innledende faser av håndtering
- Understøtter partenes operative oppgaveløsning
- Anbefaler håndterende part om hvilke spor og eventuelle tiltak som bør gjennomføres

Deling av informasjon om hendelser

NSM oppfordrer alle virksomheter til å dele mer informasjon om hendelser med hverandre. Dette vil legge til rette for læring i egen virksomhet og hos andre, gjennom at flere virksomheter blir bedre til å forebygge, avdekke og håndtere hendelser. Offentlighet rundt IKT-hendelser vil legge til rette for en åpenhetskultur og gjøre det enklere for andre virksomheter å informere om hendelser hos seg. Gjennom offentliggjøring blir det også lettere å oppnå aksept og forståelse for behovet for god informasjonssikkerhet i offentlige og private virksomheter og i samfunnet som helhet.[26]

Noen virksomheter vil synes det er problematisk å rapportere en hendelse på grunn av omdømmeproblematikk eller fordi dette vil avsløre sårbarheter. Noen ganger kan personvernhensyn gjøre det vanskelig å dele informasjon. Det er strenge bestemmelser for hvordan informasjon deles mellom myndigheter og hvilken informasjon som kan innhentes, lagres og benyttes blant myndighetene som har et ansvar på dette området. EOS-utvalget og Datatilsynet er viktige instanser for å kontrollere myndighetenes informasjonsinnhenting og håndtering.

IKT-hendelser bør være en integrert del av virksomheters øvelser i krisehåndtering. Virksomhetene anbefales å øve på håndtering av IKT-hendelser som del av scenarioer hvor målsettingen er å opprettholde drift og tjenesteleveranse. Åpenhet om IKT-hendelser bør inngå som et moment i slike øvelser for å bygge erfaring knyttet til vurderinger rundt dette.

Hva bør din virksomhet vurdere før dere beslutter å gå offentlig ut med en IKT-hendelse?

- Er hendelsen eller elementer av denne av en slik karakter at allmennheten bør kjenne til dette?
- Kan offentliggjøring bidra til å forebygge hendelser i andre virksomheter?
- Ønsker virksomheten selv å gå offentlig ut, eller er det mest hensiktsmessig at bransje- eller interesseorganisasjon eller sektorvise responsmiljø brukes som kanal for å unngå unødig eksponering av den aktuelle virksomheten?
- Risiko, og eventuelt skadepotensial knyttet til offentliggjøring, må vurderes før en hendelse offentliggjøres.
- Det bør vurderes om sårbarheter som førte til hendelsen fortsatt kan utnyttes.
- Det bør generelt sett utvises større varsomhet med offentliggjøring mens en hendelse pågår, herunder hvor detaljert informasjon som kan offentliggjøres, enn rundt informasjon om en avsluttet hendelse.
- Ved offentliggjøring av hendelser som skyldes tilsiktede handlinger bør det utvises varsomhet slik at detaljer om virksomhetenes og myndighetenes håndtering av hendelsen ikke eksponeres på en uønsket måte.
- Ved håndtering av hendelser der fremmede stater antas å stå bak, bør offentliggjøring skje etter samråd med EOS-tjenestene.
- Offentliggjøring bør ikke skje der dette kan skade muligheten for effektiv håndtering av hendelsen, eller politiets etterforskning.
- Er virksomheten i tvil om hendelsen bør offentliggjøres eller ikke, kontakt ekspertmiljøer som for eksempel egen sektor-CERT, NSM NorCERT eller NorSIS for å motta råd og veiledning.

[26] NSM, Difi, NorSIS, POD, NSR (2015), *Anbefalinger om åpenhet rundt IKT-hendelser.*

Ordliste

BEGREP	**BESKRIVELSE**
Alvorlig IKT-sikkerhetshendelse	Reelle uønskede tilsiktede hendelser eller trusler om slike hendelser i det digitale rom som er rettet mot kritisk infrastruktur og/eller kritiske samfunnsfunksjoner.
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.
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.
CERT	«Computer Emergency Response Team» er en koordinerende enhet for IKT-sikkerhet. CERT er en lisensbelagt tittel. Det er flere CERT-miljøer i Norge. NorCERT er nasjonal CERT.
CSIRT	Se CERT. CSIRT er ikke en lisensbelagt tittel.
Cyber	Benyttes om alt som er på internett og digitalt. Cyberspace refererer til en verden av sammenkoblede datasystemer og informasjonsressurser. Betegnelsen sidestilles i denne sammenheng med betegnelsen «IKT».
Deteksjon	Tekniske indikasjoner på angrep på IKT-system.
Digital hendelseshåndtering	Defensive tiltak ved alvorlige IKT-sikkerhetshendelser for å stanse, gjenopprette sikker tilstand for berørte systemer, skadevurdere og skadebegrense.
Grunnsikring	Permanent funksjonalitet og beskyttelse for å gjøre systemer mindre sårbare for uønskede hendelser.
Hacktivisme	Politisk motivert hacking.
Hybride trusler	Systematisk og synkronisert bruk av flere virkemidler iverksatt med formål om å påvirke en motpart og oppnå strategiske målsettinger. Den sammensatte virkemiddelbruken finner sted i en sikkerhetspolitisk kontekst og har vesentlig skadepotensial for den som rammes.

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.
Innsider, innsideaktør	En innsider er en person som utnytter eller har som intensjon å utnytte sin legitime tilgang for uautoriserte formål.
Inntrengingstest (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.
IKT-angrep	Handlinger med den hensikt å skade eller påvirke konfidensialiteten, integriteten eller tilgjengeligheten til et IKT-system.
IKT-hendelse	Situasjoner der IKT-systemer blir utsatt for tilsiktede handlinger.
IKT-sikkerhet	Beskyttelse av informasjon og systemer som er sårbare fordi de er koblet til, eller på annen måte er avhengig av IKT.
Integritet i IKT-systemer	Å sikre at IKT-systemer er korrekte, gyldige og fullstendige.
Konfidensialitet i IKT-systemer	Å sikre at IKT-systemer og informasjon i systemene bare er tilgjengelig for dem som skal ha tilgang.
Konsekvens	NS 5814:2008, Mulig følge av en uønsket hendelse.
Kritisk infrastruktur	De anlegg og systemer som er nødvendige for å opprettholde samfunnets kritiske funksjoner som dekker samfunnets grunnleggende behov og befolkningens trygghet.
Kritisk samfunnsfunksjon	De funksjonene som må opprettholdes i samfunnet for å sikre trygghet og basale fysiske behov for befolkningen.
Kryptering	Koding av informasjon slik at den blir uleselig for uvedkommende.
Orm	En orm er ondsinnet kode som replikererer seg selv på klienter og sprer seg til andre via nettverkstilkobling.
Passordadministrasjon	Rutine for å sikre at passord til blant annet IKT-systemer byttes med jevne mellomrom og er av tilstrekkelig kvalitet.
Patching	«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 be en person om opplysninger for å kunne plante skadevare. Personens tillit til den originale avsenderen blir forsøkt utnyttet. Se spearphishing.
Risiko	Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen (NS 5830:2012).
Risikobilde	En beskrivelse av risiko på et gitt tidspunkt. Innen forebyggende sikkerhet utgjør risikobildet en samlet vurdering av verdier, truslene mot disse og sårbarheter som eksisterer i forhold til truslene i en bestemt tidsperiode eller knyttet til en spesifikk hendelse (NS 5830:2012).
Risikovurdering	Risikovurdering er en helhetsvurdering basert på verdivurdering (eller konsekvensvurdering), trusselvurdering og sårbarhetsvurdering med mål om å angi en entitets risiko i en definert sikringsmessig kontekst (NS 5832).
Sannsynlighet	De vanligste definisjonene av sannsynlighet er frekvensbaserte, det vil si at antallet hendelser over en viss tid fremskrives som en sannsynlig fremtidig trend. Når det gjelder trusler, det vil si uønskede, tilsiktede handlinger, kan det være vanskelig å etablere trender. En alternativ definisjon er sannsynlighet basert på kvalitativ kunnskap. Synonymer til sannsynlig blir da mulig eller trolig. Jf. Etterretningsdoktrinens bruk av dette begrepet.
SCADA	Supervisory Control And Data Acquisition. System eller nettverk som brukes til å kontrollere (industrielle) prosesser eller infrastrukturer.
Skadevare (Malware)	Skadelig programvare (fra engelsk malicious software).
Skadevareanalyse	Analyse av det tekniske innholdet i skadevare.
Samfunnssikkerhet	Ivaretagelse av sivilbefolkningens liv, helse og trygghet, og sikre sentrale samfunnsfunksjoner og viktig infrastruktur mot angrep og annen skade.
Sikkerhetsrevisjon	Virksomhetens interne revisjon av (styringen av) eget sikkerhetsarbeid.
Sikkerhetstruende hendelse	Hendelse som truer en verdi, uansett om årsaken er handling fra trusselaktør eller et sikkerhetsbrudd i virksomheten.
Skytjeneste, nettskytjeneste (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.
Statssikkerhet	Sikkerhetsbehov knyttet til statens eksistens, suverenitet og integritet. Statssikkerhet har tradisjonelt vært særlig knyttet til forsvaret av territoriet (invasjonsforsvar).
Spam	Uoppfordret / uønsket e-post med reklame.
Spearphishing	Skadevare levert via målrettet e-post
Sårbarhet	Manglende evne til å motstå en uønsket hendelse eller opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning (NS 5830:2012).
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 botnet. Hensikten er å hindre normal tilgang fra ordinære brukere.
Trussel	Mulig uønsket handling som kan gi en negativ konsekvens for en entitets sikkerhet (NS 5830:2012).
Trusselaktør	En kjent eller ukjent entitet som forbindes med en trussel (NS 5830:2012).
Verdivurdering	Virksomhets vurdering av hvilke verdier den har som har sikkerhetsmessig betydning. Verdi: Ressurs som hvis den blir utsatt for en uønsket påvirkning vil utgjøre en negativ konsekvens for den som forvalter eller drar fordel av ressursen (NS 5830:2012).
Vannhull	I et vannhullsangrep kompromitterer en trusselaktør en internettside som hyppig besøkes av personer i en aktuell målgruppe slik at besøkende på nettsiden serveres skadevare. Sofistikerte aktører «hvitelister» vannhullene sine, noe som innebærer at kun besøkende i målgruppen vil bli servert skadevare
Virus	Skadevare (program) som infiserer andre programmer og reproduserer seg selv.

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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