NASJONAL
SIKKERHETSMYNDIGHET

Helhetlig digitalt risikobilde 2019

Helhetlig digitalt risikobilde er en årlig rapport som har til hensikt å øke bevisstheten og motivere til bedre digital sikkerhet i offentlige og private virksomheter. Rapporten henvender seg til ledere og personell med sikkerhetsoppgaver i alle sektorer.

Begrepet helhetlig betyr at rapporten handler om problemstillinger knyttet til individer, virksomheter og til samfunnet som helhet.

Årets rapport vil utdype angrepstrender i 2019, utfordringer og muligheter som kommer med de store teknologitrendene, risikoen ved digitalisering av kritisk infrastruktur, individets trygghet på nett og Norges avhengighet til det digitale, internasjonale samfunnet.

Innhold

NASJONAL SIKKERHETSMYNDIGHET (NSM)
er Norges ekspertorgan for informasjons- og objektsikkerhet. Direktoratet er det nasjonale fagmiljøet for digital sikkerhet og varslings- og koordineringsinstans for alvorlige digitale angrep og sikkerhetshendelser.

NASJONALT CYBERSIKKERHETSSENTER (NCSC)
er en del av NSM og skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot digitale angrep. Senteret vil ha et spesielt fokus på rådgiving og krav innen forebyggende tiltak, tekniske sikkerhetsløsninger og yte bistand når uhellet er ute.

1. Situasjonsbildet

Digitaliseringen skyter fart både innen forbrukersfæren, kritisk infrastruktur og offentlige og private tjenester. Nye trender som 5G, tingenes internett (IoT), kunstig intelligens samt virtuell og utvidet virkelighet vil gi oss smarte byer, hus, virksomheter og tjenester og vil bidra til å videreutvikle samfunnet.

Den teknologiske utviklingen gjør Norge mer avhengig av det digitale internasjonale samfunnet. Samtidig har globaliseringen gjort sikkerhetsutfordringene mer komplekse. Med digitaliseringen får vi flere og lengre verdikjeder og blir mer avhengige av digitale løsninger. Disse løsningene er igjen avhengige av andre tjenester, virksomheter og produkter, som ofte er utenlandske. Program- og maskinvare er digitaliseringens grunnmur, men lite av den er utviklet i Norge. Flere norske virksomheter tjenesteutsetter IKT-miljøet sitt til utlandet.

Statlig etterretning og kriminelle aktører utgjør de største digitale truslene mot Norge. NSM ser et jevnt trykk av digitale angrep mot norske mål, inkludert virksomheter som ivaretar viktige samfunnsfunksjoner. Digitale operasjoner blir vanskeligere å oppdage og metodene er sammensatte. Digitaliseringen åpner også nye veier inn i organisasjonene, blant annet via IoT-enheter og privat utstyr.

Virksomheter er ofte uforberedt på alvorlige hendelser. Det gjør det utfordrende å redusere skadeomfanget og gjenopprette forsvarlig sikkerhetsnivå når hendelsen inntreffer, særlig dersom en trusselaktør først har fått fotfeste.

Det er når viktige samfunnsfunksjoner blir digitalisert og sårbare for digitale trusler at vi har mest å tape. Digitale angrep mot tjenester innen elektronisk kommunikasjon (ekom) og kraft kan få store konsekvenser, men disse sektorene har høyt fokus på sikkerhet. NSMs oppfatning er at vi likevel er sårbare for alvorlige digitale angrep mot viktige samfunnsfunksjoner. Hendelser som strømutfall og bortfall av ekomtjenester som følge av digitale angrep kan skje i Norge. Dette vil videre kunne få store konsekvenser for mange andre samfunnssektorer.

I sum ser NSM at hovedtrendene er de samme som tidligere år. Den digitale risikoen øker: Det er flere verdier som skal passes på, og vi utfordres av profesjonelle og målrettede trusselaktører. Samtidig finnes det betydelige digitale sårbarheter i samfunnet og hos norske virksomheter. Virksomheter som arbeider systematisk og godt med sikkerhet vil kunne holde risikoen for sine digitale systemer på et akseptabelt nivå.

Norske virksomheter har blitt mer sikkerhetsbevisste. De identifiserer mange tiltak og iverksetter dem raskere enn før.

De viktigste virkemidlene for sikker digitalisering beskrev vi i *IKT-risikobilde 2018, Et sikkert digitalt Norge*. De gjelder fortsatt.

NSM opplever at norske virksomheter har blitt mer sikkerhetsbevisste. De identifiserer mange tiltak og iverksetter dem raskere enn før. Dette er positivt, men arbeidet må fortsette. Digitalt sikkerhetsarbeid dreier seg ikke bare om tekniske tiltak. Det krever i tillegg god ledelse og organisatoriske og prosessuelle tiltak for å forebygge alvorlige digitale angrep. Ved å implementere NSMs *grunnprinsipper for IKT-sikkerhet*[1] står virksomheter bedre rustet til å møte fremtidens digitale sikkerhetsutfordringer.

Norge må møte den storstilte digitaliseringen vi står overfor på en sikker måte. For å klare dette lanserte regjeringen i januar 2019 en ny nasjonal strategi for digital sikkerhet.[2] Samtidig kom en nasjonal strategi for digital sikkerhetskompetanse med fokus på styrkning av forskning og utdanning.[3] Digitaliseringen legger press på både samfunn og virksomheter. Ny sikkerhetslov og etableringen av Nasjonalt cybersikkerhetssenter (NCSC) i NSM og Nasjonalt cyberkrimsenter (NC3) i Kripos skal bidra til å styrke og konsolidere innsatsen mot digitale trusler. For å støtte sikkerhetsarbeidet i norske virksomheter vil NSM gjennom NCSC ha et spesielt fokus på rådgiving og krav innen forebyggende tiltak, tekniske sikkerhetsløsninger og å yte bistand når uhellet er ute.

I sum ser NSM at hovedtrendene er de samme som tidligere år. Den digitale risikoen øker.

DIGITALISERINGEN SKYTER FART

Endring og videreutvikling av organisasjoner og IKT-systemer vil alltid medføre risiko. Vi må akseptere en viss risiko for å få de nødvendige gevinstene, men hastigheten må tilpasses forholdene. NSM erfarer for ofte at farten medfører høyere risiko enn virksomheten selv er klar over, og vi ser alvorlige eksempler på manglende kontroll. Digitaliseringen krever riktig bruk av gass og brems. Stor fart forutsetter kompetanse og en investering i sikkerhet.

[1] *Grunnprinsipper for IKT-sikkerhet, versjon 1.1,* https://www.nsm.stat.no/publikasjoner/andre-publikasjoner/grunnprinsipper-for-ikt-sikkerhet/

[2] *Nasjonal strategi for digital sikkerhet,* https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

[3] *Nasjonal strategi for digital sikkerhetskompetanse,* https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/

SENTRALE GREP FOR SIKKER DIGITALISERING

- Prioriter kompetanse innen IKT og digital sikkerhet.
- Adresser digital sikkerhet systematisk på alle nivåer i virksomheten.
- Prioriter sikkerhet og sørg for at virksomheten gjennomfører risikovurderinger og følger anerkjente rammeverk, for eksempel NSMs grunnprinsipper for IKT-sikkerhet.
- Sørg for å ha en moderne, oppdatert og ryddig IKT-portefølje.
- Ha et tilpasset og profesjonelt IKT-miljø som leverer nødvendige tjenester. Sikkerhet må være en naturlig del av tjenesteutsetting gjennom hele tjenestens livsløp. Virksomheter må få på plass god IKT-arkitektur og automatisere sikkerhetsarbeidet.
- Tilby sluttbrukerne løsninger som fjerner eller reduserer risikoen for brukerfeil.

2. Sikkerhetsarbeidet nytter

NSM ser at stadig flere virksomheter iverksetter gode tiltak. Mange virksomheter fokuserer bevisst på å forbedre sikkerheten gjennom å modernisere, automatisere, konsolidere og profesjonalisere sine IKT-porteføljer. Fortsatt er det slik at hendelser kunne vært avverget eller fått mindre konsekvenser dersom virksomhetene jobbet mer strukturert og helhetlig med digital sikkerhet. NSM anbefaler derfor at myndigheter og forvaltere av regelverk av betydning for digital sikkerhet bruker NSMs *grunnprinsipper for IKT-sikkerhet* i sitt utviklings- og veiledningsarbeid. NSM anbefaler videre at alle virksomheter bruker de samme grunnprinsippene i sitt digitale sikkerhetsarbeid.

Risikoen øker ved at vi digitaliserer verdiene våre samtidig som trusselaktørene blir mer avanserte. Med den teknologiske utviklingen kommer også nye utfordringer, sårbarheter og konsekvenser. Derfor må vi innrette oss for å sikre oss best mulig, også mot fremtidige utfordringer. Det er mulig å digitalisere sikkert, men å bygge opp motstandsevne mot sofistikerte operasjoner fra trusselaktører og å være robuste i møte med tilfeldige hendelser krever kontinuerlig arbeid, evne og vilje. For å forsvare det digitale Norge må vi ha kompetanse om alle byggeklossene som utgjør samfunnet vårt, samt dyp, teknisk forståelse og evnen til å se helhetsbildet. Det er gledelig at forskning og undervisning innen digital sikkerhet nå introduseres ved flere universiteter og høyskoler.

Digitaliseringen legger press på samfunn og virksomheter. Norske myndigheter jobber for å ta fram gode regelverk og arenaer for samhandling.

Regulering av nasjonal sikkerhet og digital sikkerhet

Myndighetene tar digital sikkerhet på alvor. En revidert og modernisert sikkerhetslov[4] trådte i kraft 1. januar 2019. Ny lov er mer dynamisk, mer fleksibel og tar konsekvensen av at det norske samfunn og totalforsvaret er preget av høy grad av offentlig og privat samhandling. Loven setter myndigheter og virksomheter i bedre stand til å sikre nasjonale sikkerhetsinteresser mer helhetlig med et trussel- og risikobilde i stadig og rask endring.

Et sentralt virkemiddelet i loven er departementenes identifisering av *grunnleggende nasjonale funksjoner* (GNF) for sine sektorer. GNF-er utledes blant annet fra de nasjonale sikkerhetsinteressene. Basert på GNF-ene skal departementene identifisere virksomheter hvis tjenester og/eller produksjon er av en slik betydning at et helt eller delvis bortfall vil få konsekvenser for statens evne til å ivareta

Nasjonalt cybersikkerhetssenter skal styrke innsatsen mot digitale trusler.

[4] *Lov om nasjonal sikkerhet (sikkerhetsloven)*, https://lovdata.no/dokument/NL/lov/2018-06-01-24

nasjonale sikkerhetsinteresser. Dette inkluderer utpeking og klassifisering av skjermingsverdige objekter og infrastruktur. Virksomheter som forvalter slike, og andre skjermingsverdige verdier som skjermingsverdige informasjonssystemer og skjermingsverdig informasjon, omfattes av sikkerhetsloven ved enkeltvedtak.

Informasjonssystemer som behandler sikkerhetsgradert informasjon er skjermingsverdige. Etter ny lov er også informasjonssystemer som er av avgjørende betydning for GNF-er også skjermingsverdige. Skjermingsverdige informasjonssystemer skal sikres slik at tilgjengelighet, integritet og konfidensialitet ivaretas. Som følge av endringene i ny sikkerhetslov vil trolig flere IKT-systemer omfattes av lovreguleringen.

Sikkerhet i informasjonssystemer reguleres på mange måter. Reguleringen vil være avhengig av systemenes funksjon og innhold, og inkluderer blant annet sektorovergripende regelverk som personopplysningsloven, sektorspesifikke regelverk, kontraktuelle forpliktelser og strategier for hvordan vi skal skape god sikkerhet. Plikt til sikring etter sikkerhetsloven gjelder kun for de systemer som er viktigst for Norge i fred, krise og krig.

IKT-sikkerhetslovutvalget[5] anbefalte at det etableres en ny IKT-sikkerhetslov som skal skape et gjennomgående sikkerhetsnivå for informasjonssystemer som ikke omfattes av sikkerhetslovens bestemmelser. Ny IKT-sikkerhetslov anbefales også å inkludere implementeringen av EUs NIS-direktiv.

Nasjonalt cybersikkerhetssenter

Nasjonal sikkerhetsmyndighet har et tverrsektorielt oppdrag med å legge til rette for og følge opp nasjonal digital sikkerhet. For å styrke arbeidet med digital sikkerhet etableres Nasjonalt cybersikkerhetssenter som en del av NSM. NCSC vil blant annet ivareta flere av NSMs eksisterende oppgaver. Videre er etableringen av NCSC et viktig bidrag til oppfølgingen av nasjonal strategi for digital sikkerhet[6] ved at det fremmer samhandling. Senteret skal bidra til tettere samarbeid internt i offentlig sektor og med næringsliv, akademia og internasjonale partnere. NSM ønsker at alle disse aktørene arbeider sammen, med utgangspunkt i et felles risikobilde og med samme situasjonsforståelse. Senteret er et viktig steg i videreutviklingen av det offentlig-private samarbeidet innen digital sikkerhet.

Ny sikkerhetslov setter myndigheter og virksomheter i bedre stand til å sikre nasjonale sikkerhetsinteresser.

[5] *NOU: 2018:14 IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet,* https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/

[6] *Nasjonal strategi for digital sikkerhet,* https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

«Samhandling», sier Bente Hoff når hun blir spurt om senterets viktigste oppgave.

Hun leder det nye nasjonale cybersikkerhetssenteret som ligger flott plassert i Oslo havnelager, like ved sjøen og med operaen som nærmeste nabo. Hoff gleder seg til å ta imot nye samarbeidspartnere og besøkende i senteret.

«Sektorvise responsmiljøer, samfunnskritiske virksomheter og andre som jobber med digital sikkerhet kan komme hit for å utveksle informasjon og samarbeide med senterets egne fagfolk», sier hun. «Her kan man møte eksperter fra andre virksomheter tilknyttet senteret og dele erfaringer. Herfra skal vi sammen gi norske virksomheter råd, ansikt til ansikt, men også digitalt slik at vi når enda flere.»

NSM NorCERT, Norges nasjonale responsfunksjon som håndterer digitale angrep mot samfunnskritisk infrastruktur og informasjon, har blitt en del av senteret.

«Det stemmer», sier Hoff. «De største, mest alvorlige digitale hendelsene i Norge kommer til å bli håndtert her i senteret. Selv om noe av arbeidet må skje bak lukkede dører ønsker vi å dele kunnskapen, informasjonen og den praktiske kompetansen med resten av Norge. Velkommen til oss!»

Det Nasjonale cybersikkerhetssenteret ligger i Oslo havnelager.

Nasjonalt cyberkrimsenter

Ettersom vi i større grad lever livene våre og flytter verdiene våre over på nettet, øker den digitale kriminaliteten. Vi blir ofre for hets og trakassering, ID-tyveri og overgrep. Norske virksomheter blir utsatt for blant annet direktør-svindel, løsepengevirus og krypto-mining hvor skadevare utvinner kryptovaluta på fornærmedes IKT-utstyr.

NC3 i Kripos er Norges nye spydspiss i kampen mot digital kriminalitet og trusler. Senteret skal være drivkraften for å sikre og utnytte digitale spor og utvikle nye, framtidsrettede etterforskningsmetoder. NC3 skal få over 200 ansatte og vil bli det teknologiske navet i politi-Norge. Herfra skal de spre kunnskap og kompetanse videre til politidistriktene og den enkelte politimann og -kvinne.

Store, profesjonelle IKT-miljøer – tjenesteutsetting og konsolidering

For å være konkurransedyktige og ivareta digital sikkerhet må norske virksomheter være oppdatert på ny teknologi, på hvordan den kommer til å påvirke oss og på hvordan folk og vaner endrer seg. Gårsdagens teknologiske utfordringer forsvinner ikke, de har bare fått selskap av nye sårbarheter og angrepsmetoder. Derfor må virksomhetene bygge ny kompetanse, innføre nye arbeidsmetoder og øke motstands-evnen ved å ta gode strategiske og organisa-toriske valg – i tillegg til de tekniske.

NSM anbefaler konsolidering til større, profesjonelle IKT-miljøer med egne sikkerhetsmiljøer og 24/7-bemanning av responsfunksjoner. Det innebærer at miljøer med høy kompetanse tilbyr færre tjenester, med god kvalitet for flere aktører. De må jobbe med kontinuerlig oppdatering av kompetanse, verktøy og organisasjon. NSM har etablert en kvalitetsordning for bruk av leverandører av tjenester for håndtering av IKT-hendelser.[7]

I det offentlige pågår det nå konsolidering på mange plan. Det blir innført felles, tekniske sikkerhetstjenester, for eksempel for DNS og e-post, samt sikre nett for kommunikasjon innen offentlig forvaltning. I tillegg har vi fått en digitaliseringsstrategi for offentlig sektor[8] som skal understøtte digital transformasjon i hver enkelt virksomhet og i offentlig sektor som helhet.

Ofte vil konsolidering innebære tjeneste-utsetting. Det er det mange gode grunner til, inkludert tilgang til store, profesjonelle sikkerhetsmiljøer hos leverandøren. Samtidig stiller utsetting andre krav til kompetanse hos

God IKT-sikkerhet er et resultat av langsiktig, kontinuerlig og strukturert arbeid.

[7] *Kvalitetsordning for bruk av leverandører av tjenester for handtering av IKT-hendelser,* https://www.nsm.stat.no/om-nsm/tjenester/leverandorforhold/kvalitetsordning-for-bruk-av-leverandorer-av-tjenester-innen-ikt-hendelseshandtering/

[8] *Én digital offentlig sektor - Digitaliseringsstrategi for offentlig sektor 2019-2025,* https://www.regjeringen.no/no/dokumenter/en-digital-offentlig-sektor/id2653874/

virksomheten. Den får blant annet mindre kontroll og oversikt over tjenestene den kjøper og blir avhengig av tilbyder. Gode råd finnes i NSMs *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting*.[9] Tjenesteutsetting trenger ikke alltid være løsningen. Dette gjelder særlig store virksomheter som allerede har tunge IKT-miljøer. Det kan være vel så kostnadseffektivt å ha sitt eget datasenter og dermed beholde kontrollen over systemer og informasjon.

Digital sikkerhetsstyring

Sikker digitalisering krever helhetlig styring av sikkerhetsarbeidet. Virksomhetens styre må være orientert om sikkerhetstilstanden. Ledelsen må integrere digitalt sikkerhetsarbeid i prosesser og styring. Digital sikkerhet må prioriteres i budsjettene. Virksomheten må ha rett kompetanse. Næringslivets Sikkerhetsråds Mørketallsundersøkelse fra 2018[10] avdekker at tilfeldigheter og uflaks blir oppgitt som årsak til hendelser i to tredjedeler av tilfellene, fulgt av menneskelige feil og mangel på sikkerhetsbevissthet. En undersøkelse Norges vassdrags- og energidirektorat (NVE) gjennomførte i 2017 om IKT-sikkerhetstilstanden i kraftsektoren viste at rundt halvparten av virksomhetene som svarte, hadde hatt uønskede hendelser. Undersøkelsen viste videre at 40 % av virksomhetene som hadde hendelser de kategoriserte som deres alvorligste hendelse, ikke gjorde noen endringer i organisasjonen som følge av dette.[11]

God digital sikkerhet er et resultat av langsiktig, kontinuerlig og strukturert arbeid. Verdivurderinger og risikovurderinger må gjennomføres og digital sikkerhet må inn i alle prosesser og strategier. Virksomheten må ha en tydelig policy, en klart definert arkitektur for IKT-miljøet sitt og en god sikkerhetskultur. Et styrings- eller ledelsessystem for sikkerhet og digital sikkerhet er noe av det viktigste en virksomhet kan innføre for å bedre sikkerheten både i møte med tilsiktede og utilsiktede handlinger. NSM har publisert flere relevante veiledninger om temaet.[12] Systemet må følges opp i alle ledd i virksomheten og virksomhetens internrevisjon bør inkludere IKT-revisjon. Sikkerheten bør deretter verifiseres av eksterne, uhildede parter, for eksempel gjennom ytterligere IKT-revisjon og inntrengningstester.

[9] *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting*, https://www.nsm.stat.no/globalassets/dokumenter/temahefter/tjenesteutsetting2018v1.1_web.pdf

[10] *Mørketallsundersøkelsen - informasjonssikkerhet og datakriminalitet*, https://www.nsr-org.no/moerketall/

[11] *Informasjonssikkerhetstilstanden i Energiforsyningen*, http://publikasjoner.nve.no/rapport/2017/rapport2017_90.pdf

[12] *Sikkerhetsstyring*, https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/

[13] *Mediebrief fra NSM*, https://www.nsm.stat.no/om-nsm/mediebrief-fra-nsm/

[14] *Sikkerhetsbloggen*, https://www.nsm.stat.no/blogg/

NSM SIKKERHETSBLOGG OG PODKAST

NSM har en rekke nyttige publikasjoner på sine nettsider. Her kan du abonnere på NSMs daglige mediebrief[13] eller lese NSMs sikkerhetsblogg[14], et uformelt nettsted med hovedvekt på digital sikkerhet og andre tema innen forebyggende sikkerhet. NSM har også en ukentlig podkast. Her diskuterer NSM-ansatte og inviterte gjester ulike aktuelle tema innen sikkerhet. Du finner den på bloggen vår, på Spotify, Soundcloud og iTunes.

3.
Digitale angrep

Internett består av et utall enheter av forskjellige slag og bruksområder, koblet sammen ved hjelp av stadig flere typer nettverk og tjenester. Det finnes sårbarheter innen alle områder: Maskinvaren, programvaren, protokollene, algoritmene, verdikjedene, organisasjonene, rutinene og menneskene har alle sårbarheter. Med mindre det gjøres riktig skapes det nye sårbarheter når alle disse elementene settes sammen.

Til tross for iherdig innsats for å tette sikkerhetshull kommer det stadig nye til, samtidig som flere verdier står på spill. En virksomhet som skal sikre seg er nødt til å tenke helhetlig: På organisasjon, mennesker og teknologi. Den må forstå at verden utenfor har en direkte, økende påvirkning på virksomhetens verdier.

Fremmede stater søker blant annet etter høyteknologi og forretningshemmeligheter, i tillegg til statshemmeligheter, når de gjennomfører digitale etterretningsoperasjoner mot norske virksomheter. Etterretningstjenesten[15] og Politiets sikkerhetstjeneste (PST)[16] peker på at statsforvaltningen og virksomheter innen forsvar, rom, maritim, medisinsk forskning, petroleum og kraft er utsatt. I tillegg til informasjon ønsker fremmede stater å ha mulighet til å påvirke norske beslutningsprosesser gjennom eierskap, samarbeid og handel. Disse aktørene har store ressurser og jobber med langsiktige målsettinger.

De vinningskriminelle har også blitt digitale. Avanserte verktøy og kriminelle tjenester er til salgs på nettet og pengene våre kan bli stjålet uten at gjerningsmennene har satt en fot på norsk jord.

Det er ofte vanskelig å finne ut hvem som står bak en digital operasjon og enda vanskeligere å kunne bevise det. Dette gjelder enten det er politiet som etterforsker en straffesak eller det er mistanke om at en statlig aktør står bak. Forskjellige aktører samarbeider, benytter samme verktøy, prøver å etterlikne andre aktører, legger ut falske spor og bruker avanserte anonymiseringsteknikker.

NSM ser gjennom Felles Cyberkoordineringssenter (FCKS), et samarbeid mellom Etterretningstjenesten, Kripos, PST og NSM, hvordan norske virksomheter blir utsatt for mange typer digitale operasjoner. Det kan være etterretning, kartlegging, eller svindel- og utpressingsforsøk som kryptomining og løsepengevirus. I tillegg blir intetanende, norske virksomheter kompromittert og brukt som del av komplekse infrastrukturer i operasjoner mot mål helt andre steder i verden.

NSM NCSC erfarer at trusselaktører kommer seg inn i norske virksomheter på en rekke måter:

NSMS GRUNNPRINSIPPER FOR IKT-SIKKERHET

definerer et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer. Prinsippene hjelper virksomheter med å velge ut de riktige sikkerhetstiltakene, gir en begrunnelse for hvorfor tiltakene bør implementeres og viser hvilke tiltak NSM mener bør prioriteres. Utvikling av gode sikringstiltak er en kontinuerlig prosess, og NSM vil videreutvikle grunnprinsippene i tråd med trussel- og sårbarhetsbildet, samt den teknologiske utviklingen i samfunnet.

Godt sikkerhetsarbeid dreier seg om solid håndverk.

[15] *Fokus 2019*, https://forsvaret.no/fokus

[16] *Trusselvurdering 2019*, https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2019/

Hvorfor utnytte en nulldagssårbarhet når det finnes så mange gamle å ta av?

E-post med vedlagt skadevare eller ondsinnede lenker er fortsatt den mest brukte inngangsvektoren. Selv om masseutsendelser fortsatt blir benyttet, ser vi særlig bruk av e-poster rettet spesifikt mot enkeltpersoner i en virksomhet. Disse e-postene kan være skrevet på korrekt norsk eller engelsk. Hensikten er enten å svindle oss eller virksomhetene våre, eller få oss til å installere skadevare. E-post er et grunnleggende usikkert kommunikasjonsverktøy som allmennheten har gitt altfor stor tillitt.

✓ All kjørbar kode som er lastet ned via e-post bør undersøkes for skadevare og holdes unna virksomhetens kjernenett. NSM har gitt ut noen grunnleggende tiltak for sikring av e-post.[17]

NSM NCSC ser flere forsøk på digitale innbrudd via internetteksponerte tjenester. Mange løsninger blir sporadisk oppdatert og kan ofte ha utgåtte lisenser. I nesten alle situasjoner er det eldre sårbarheter som blir utnyttet. Trusselaktører kan skaffe seg oversikt over, og tilgang til, eldre tredjeparts programvare hos målene sine for så å finne sårbarheter de kan utnytte.

✓ Operasjoner mot internetteksponerte tjenester er en organisatorisk, ikke bare en teknisk, utfordring. Ved å følge NSMs grunnprinsipper for IKT-sikkerhet vil virksomheten kunne vite hvilke eksponerte tjenester den har, om de er herdet og oppdatert, hvor i nettverkene de står og hvilke tilganger de har. Bruk av flerfaktor-autentisering og fjerning av standard-passord på komponenter reduserer angrepsflaten. Virksomheten bør overvåke nettverkstrafikk og aktivitet på egne systemer. Godt sikkerhetsarbeid dreier seg om solid håndverk.

Trusselaktører benytter også andre inngangsvektorer som opprettelse av ondsinnede vannhullsider, kompromittering av andre nettsteder med skadevare-skript, og installasjon av skadevare på mobiltelefoner som sluttbrukerne så kobler til virksomhetens interne tjenester. Trusselaktører som har mulighet til å operere fysisk kan distribuere minnepinner med skadevare, koble seg til åpne trådløse nett og finne nettverkspunkter som befinner seg utenfor fysiske sperringer.

✓ Tiltakene nevnt over er også relevante her, men digital sikkerhet er gjensidig avhengig av fysisk og personellsikkerhet. NSM har publisert flere veiledninger om tema innen helhetlig sikkerhet.[18]

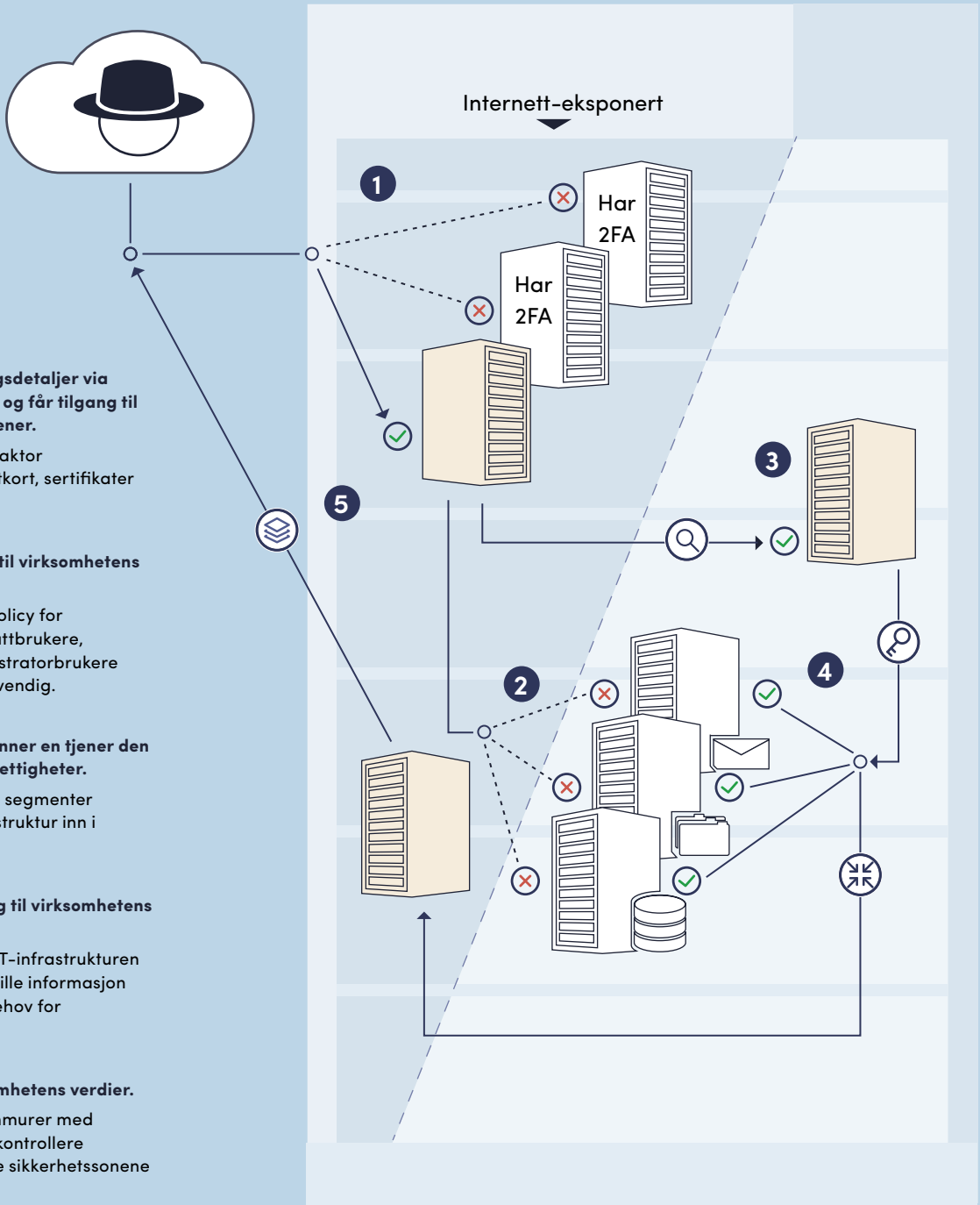
Har trusselaktørene først kommet seg inn i virksomhetens nettverk er det viktig å hindre dem i å spre seg og skaffe seg utvidede rettigheter. NSMs inntrengningstestere ser ofte usegmenterte og usikrede nettverk, tjenere og nettverksutstyr som ikke er herdet eller oppdatert samt tilkoblede maskiner virksomheten ikke har oversikt over. Den tekniske arven bare øker, og ofte vil man ikke oppdatere kritiske tjenere av bekymring for at disse da vil slutte å fungere. Hvorfor utnytte en nulldagssårbarhet når det finnes så mange gamle å ta av?

[17] *Grunnleggende tiltak for sikring av e-post,* https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/u-02-grunnleggende-tiltak-for-sikring-av-e-post---en-delig.pdf

[18] *Publikasjoner,* https://www.nsm.stat.no/publikasjoner/

Angrep mot norsk virksomhet – et typisk forløp.

Hendelsesforløpet under illustrerer teknikker trusselaktører har brukt mot norske virksomheter. Tiltakene under er hentet fra NSMs Grunnprinsipper for IKT-sikkerhet versjon 1.1.



1. Aktør finner påloggingsdetaljer via kartlegging på internett og får tilgang til en internetteksponert tjener.

Tiltak 2.5.5: Bruk multi-faktor autentisering, som smartkort, sertifikater eller engangspassord.

2. Aktør får ikke tilgang til virksomhetens verdier.

Tiltak 1.3.2: Etabler en policy for aksesskontroll; ikke gi sluttbrukere, servicekonti eller administratorbrukere flere privilegier enn nødvendig.

3. Aktør kartlegger og finner en tjener den kan utnytte og får fulle rettigheter.

Tiltak 2.4.1: Segreger og segmenter virksomhetens IKT-infrastruktur inn i nettverk og soner.

4. Aktøren har nå tilgang til virksomhetens verdier.

Tiltak 2.2.5: Segreger IKT-infrastrukturen i sikkerhetssoner for å skille informasjon med ulik verdi og ulikt behov for brukertilgang.

5. Aktøren stjeler virksomhetens verdier.

Tiltak 2.7.1: Benytt brannmurer med logging for å filtrere og kontrollere trafikken mellom de ulike sikkerhetssonene og mot internett.

Under inntrengningstester utnytter NSM menneskelige sårbarheter med stort hell.

Den gode nyheten: Enkle grep nytter, som for eksempel NSMs fire viktige tiltak mot digitale angrep.[19] I tillegg vil implementering av NSMs grunnprinsipper for IKT-sikkerhet kunne stoppe de aller fleste angrep. Ny og oppdatert programvare er ofte designet med sikkerhet i tankene og trenger gjerne færre privilegier. Flåtestyring, flerfaktor-autentisering og hvitlistingsløsninger er viktige tiltak, men kun effektive hvis vi konfigurerer dem rett og husker at de også er angrepsmål. Virksomheter bør automatisere oppdatering, konfigurasjonsstyring og brukerhåndtering, sentralisere loggløsninger, og stille samme krav til autentisering på interne som på internett-eksponerte tjenester.

Ofte er det vi mennesker som er sårbarheten som blir utnyttet. Det er vi som utvikler, kjøper, setter opp, bruker og vedlikeholder datamaskiner, nettverk og tjenester. Det er vi som lar oss presse eller kjøpe, som slurver, som tar snarveier og som ikke mottar eller tilegner oss opplæring. Vi klikker fortsatt på lenker i e-poster, putter fortsatt minnepinner i maskiner og velger dårlige, gjenbrukte passord. Dette vet også trusselaktørene. NSM NCSC ser at brukernavn, e-postadresser og passord blir samlet inn ved innbrudd og observerer hvordan phishing-operasjoner blir mer målrettede. Under inntrengningstester utnytter NSM menneskelige sårbarheter med stort hell.

Det er lett å rope høyt om brukerfeil, men systemer basert på eldre teknologi som ikke er utviklet med sikkerhet i tankene skaper sårbarheter. Teknologien må bidra til å hjelpe brukeren slik at feil unngås eller at man hindrer uønskede konsekvenser. I tillegg peker undersøkelsen *Nordmenn og digital sikkerhetskultur*[20] fra NorSIS på at to av tre av oss ikke har fått opplæring i digital sikkerhet de siste to årene, selv om vi oppgir at kompetanseheving hjelper. Kontinuerlig kompetansebygging, opplæring og bevisstgjøring vil gjøre oss tryggere.

En innsider er en person som utnytter sin legitime tilgang til en virksomhets verdier for å utføre handlinger som påfører virksomheten skade eller tap. En innsider kan være en nåværende eller tidligere ansatt, en konsulent, kontraktør eller en annen person som har eller har hatt tilgang til virksomhetens informasjon, objekter eller andre verdier. En innsider vil ofte kunne omgå de fleste logiske og fysiske sikkerhetsmekanismene en virksomhet har implementert. Særlig for IKT-systemer som er adskilt fra andre nettverk, kan en innsider være et virkemiddel for å kompromittere et system som ikke kan nås med andre digitale inngangsvektorer. Dersom virksomheten har mangelfulle loggmuligheter i sine IKT-systemer kan en potensiell innsider operere uten risiko for å bli oppdaget.

NSM er fagmyndighet for personellsikkerhet innenfor sikkerhetslovens virkeområde, og publiserer veiledninger, rapporter og håndbøker om temaet.[21] I 2017 ble det i samarbeid med andre myndigheter utgitt en veiledning om sikkerhet ved ansettelsesforhold. NSM har også publisert en ny temarapport om innsidere i 2019.[22]

[19] *Anbefalte tiltak for å øke virksomheters egenevne (side 32),* https://www.nsm.stat.no/virksomhetssikkerhet/fire-enkle-tiltak-stopper-90-prosent-av-dataangrep/

[20] *Nordmenn og digital sikkerhetskultur 2018,* https://norsis.no/nordmenn-og-digital-sikkerhetskultur-2018/

[21] *Nasjonal sikkerhetsmyndighet,* https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/

[22] *Ny veileder: Sikkerhet ved ansettelsesforhold,* https://www.nsm.stat.no/aktuelt/ny-veileder-om-innsideproblematikk/

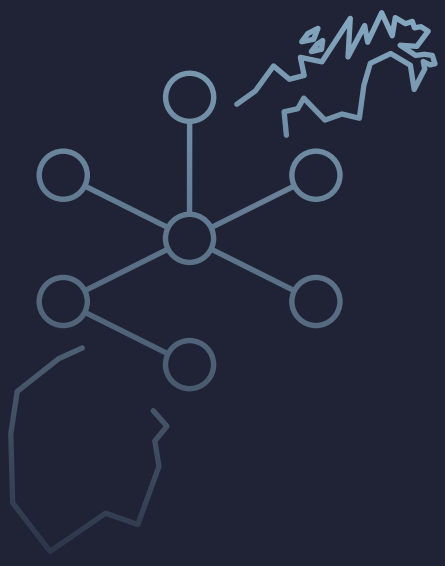
HYDRO-SAKEN

I mars ble Hydro rammet av løsepengeviruset «LockerGoga» som krypterer filer, inkludert systemfiler, på det infiserte systemet.

Hendelsen påvirket drift og produksjon i flere av selskapets forretningsområder. Hydro valgte å ikke betale løsepengesummen.

«Åpenhet har vært viktig for Hydro og vi valgte også umiddelbart å varsle NSM og anmelde dataangrepet til Kripos» sier Halvor Molland, informasjonsdirektør i Hydro. «Ved å dele kunnskap om slike angrep med andre bedrifter og å samarbeide på tvers kan vi bidra til å forhindre eller avgrense fremtidige angrep.»

Mens Hydro jobbet for å gjenopprette systemene sine, samarbeidet Kripos og NSM om etterforskning, hendelseshåndtering og analyse. Det er gledelig at Hydro valgte å informere bredt om hendelsen og dermed rette søkelys mot denne type angrep på virksomheter. Dette bidro til at norske myndigheter kunne avdekke forberedelser til innbruddsforsøk også mot andre virksomheter. Slike løsepengevirus vil kunne ramme flere norske virksomheter fremover. For å unngå og begrense skaden etter slike hendelser er det viktig at aktørene i det digitale sikkerhetsmiljøet er åpne om hendelser, deler informasjon og samarbeider seg imellom.



4.
Viktige samfunns-funksjoner på nett

Våre aller mest sentrale, livsnødvendige samfunnsfunksjoner blir styrt av datamaskiner. Datamaskiner sørger for at vi har strøm i huset, at togene går og flyene letter, at bilene kjører trygt på veiene, at varer blir levert, at vi får helsehjelp og at forsvar og nødetatene kan være der de trengs og gjøre det de skal. Disse systemene har sterke avhengigheter og hendelser, enten det er en naturkatastrofe eller et digitalt angrep, kan ha store konsekvenser.

PST rapporterer i sin trusselvurdering at andre lands etterretningstjenester vil videreføre kartleggingsoperasjoner for å avdekke funksjoner og sårbarheter innen norsk kritisk infrastruktur, krisehåndtering og sikkerhet og beredskap. Andre, mindre alvorlige og tilfeldige hendelser, som for eksempel en skadevare-infeksjon, vil kunne overbelaste eller forstyrre kritiske systemer. De siste årene har andre nasjoners industrisystemer blitt rammet av alvorlige digitale operasjoner. Slike hendelser kan også inntreffe i Norge.

Industrielle kontrollsystemer er gjerne ikke designet for å motstå digitale angrep, men for integritet og leveringspålitelighet. De er ofte basert på utdatert, usikker teknologi. Rådgivere og inntrengningstestere fra NSM ser flere eksempler på tekniske sårbarheter i slike systemer. Leverandører kan kreve tilgang gjennom kundens brannmur for å vedlikeholde og oppdatere systemene sine og ofte brukes svake, kjente passord. Sikkerhetsløsningene i industrielle kontrollsystemer kan være fra 90-tallet, der alle brukere har administrator-rettigheter og brannmurer er slått av for å kunne kjøre leverandørens programvare.

I nasjonal strategi for digital sikkerhet fokuseres det på at eiere av kritisk, digital infrastruktur skal gjennomføre risikovurderinger og identifisere avhengigheter. Myndighetene skal ha oversikt over kritisk digital infrastruktur, stille krav til sikkerheten og føre tilsyn. Øvelser trekkes også fram som et tiltak. Sikkerhetsstyring, rammeverk for intern kontroll, test og ekstern revisjon av IKT-miljø, samt monitorering og inntrengningstesting kan brukes for å vurdere sikkerhet på alle nivå. Hvitelisting er et effektivt tiltak som er relativt lett å vedlikeholde på industrisystemer, ettersom dette er systemer som sjelden endres.

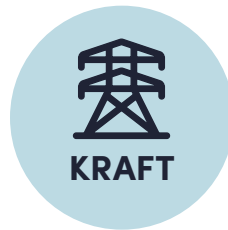
Endringene i den nye sikkerhetsloven innebærer et bedre grunnlag for å skape sikkerhet for våre viktigste informasjons-systemer gjennom et utvidet virkeområde, utvidelse av begrepet skjermingsverdig informasjonssystem og introduksjonen av begrepet skjermingsverdig infrastruktur.

Ekom- og kraftsektorene er absolutte avhengigheter for de fleste andre samfunns-funksjoner, i tillegg til å være gjensidig avhengig av hverandre. Romsektoren blir også stadig viktigere for samfunnet.

Våre aller mest sentrale, livsnødvendige samfunnsfunksjoner blir styrt av datamaskiner.

Direktoratet for samfunnssikkerhet og beredskap (DSB) har analysert flere krisescenarioer i rapporten *Alvorlige hendelser som kan ramme Norge*[23], og et av de mest kritiske er et angrep mot sentrale noder i Telenors transportnett, der både maskin- og programvare blir ødelagt. All kommersiell elektronisk kommunikasjon lammes. Dette kan føre til dødsfall, alvorlig skadde og syke samt tap på flere milliarder kroner. Tilsvarende mener Nasjonal kommunikasjonsmyndighet (Nkom) at tjenestenektangrep rettet mot sentrale elementer i ekominfrastrukturen kan få store konsekvenser. Fremtidens konsekvenser kan bli enda større: Neste generasjons nødnett planlegges implementert i de kommersielle mobilnettene med basis i 5G. Forsvaret ser også på muligheten for å realisere noe av sitt kommunikasjonsbehov på en tilsvarende måte.

Nkom foreslår i sin årlige risikovurdering *ekom*ROS 2019[24] økt diversitet i nett og tjenester, forbedret responsevne og håndtering av digitale operasjoner, økt beredskap for å håndtere uforutsette hendelser, samt forbedret sikkerhetskompetanse hos aktørene. Innføring av 5G vil føre til sikrere systemer, men også til at mobilnettene vil være eksponert for et bredere omfang av angrepsmetoder og trusselaktører. Sikkerheten i 5G vil derfor være kritisk fra utbyggingsstart.



Kraftbransjen blir digitalisert. Digitalisering av kraftnettet (smarte nett), smarte vern, automatisert styring og overvåking samt markedssystemet for kjøp og salg av kraft må alle fungere for å kunne levere strøm. Med økt digitalisering har det blitt mer utfordrende å drifte kraftsystemet manuelt, men kraftbransjen har lang tradisjon for å arbeide for god beredskap på dette området. Kraftbransjen har krav om at industrielle kontrollsystemer skal være separerte fra internett og andre kontornettverk. I en normalsituasjon vil kraften flyte i henhold til fysiske lover, men i situasjoner der det oppstår feil eller brudd, for eksempel ved trefall over linjen, trengs det oversikt for å kunne identifisere og reparere feilen. Mangel på oversikt kan forsinke reparasjonsarbeidet og medføre store, langvarige strømbrudd, inkludert utkobling av større områder.

Kraftbransjen har tydelig fokus på digital sikkerhet. Kraftberedskapsforskriften[25] gjør NVE i stand til å styre sektoren inn mot et ønsket sikkerhetsnivå. Kraftbransjen er blitt mer moden på digital sikkerhet de siste årene. Gjennom samarbeid mellom NVE, NSM, Energi Norge og Norges teknisk-naturvitenskapelige universitet (NTNU) tilbys opplæring i kraftberedskapsforskriften og NSMs *grunnprinsipper for IKT-sikkerhet*. Etter siste revisjon av kraftberedskapsforskriften bygger noen av kravene i forskriften på grunnprinsippene.

[23] *Hva er de mest alvorlige hendelsene som kan ramme Norge?* https://www.dsb.no/reportasjearkiv/hva-er-de-mest-alvorlige-hendelsene-som-kan-ramme-norge/

[24] *EkomROS 2019: Den digitale grunnmuren,* https://www.nkom.no/aktuelt/nyheter/_attachment/42430?_ts=16b4a976ad8

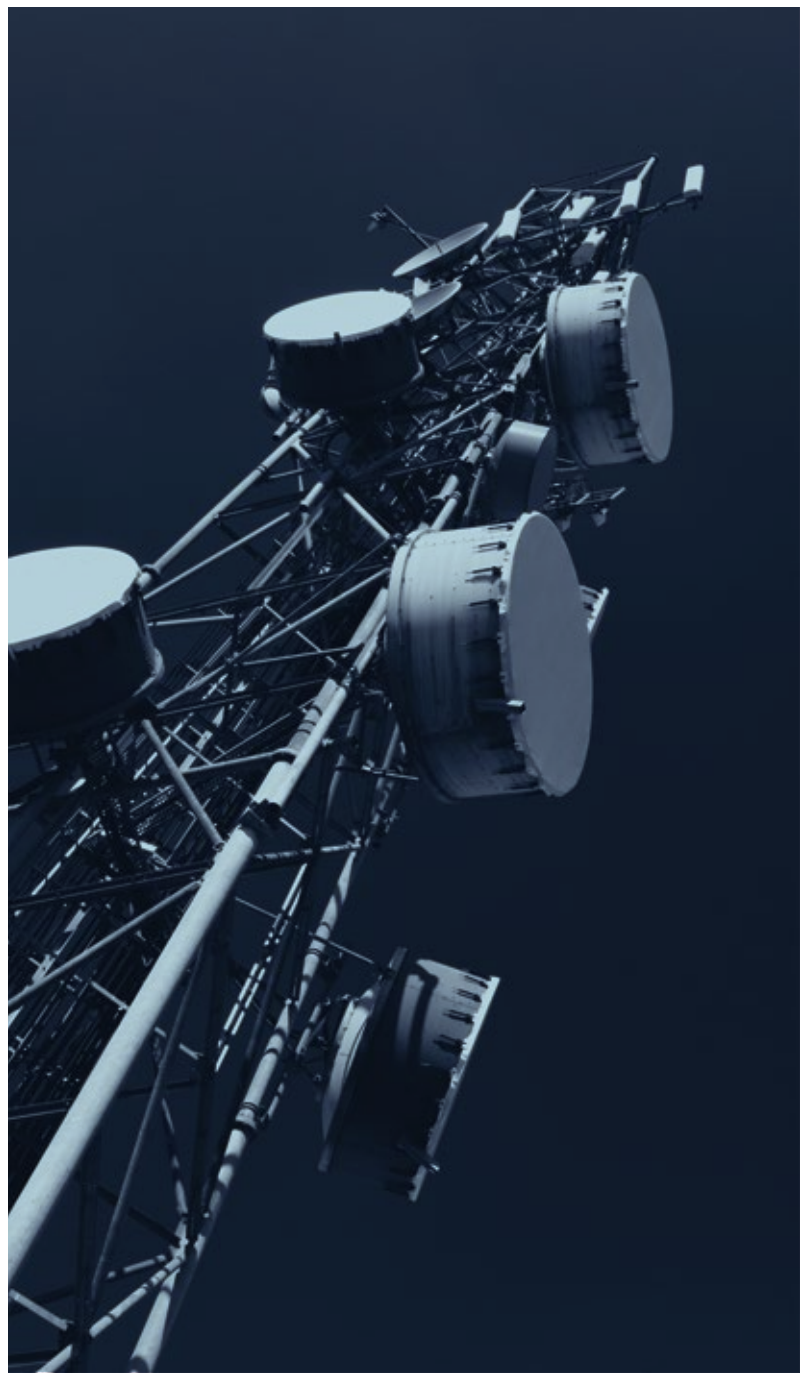
[25] *Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften),* https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

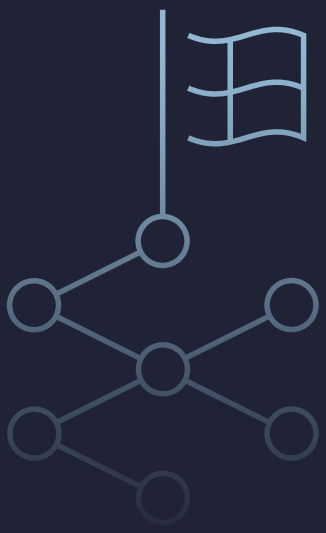
[26] *På rett sted til rett tid - Nasjonal strategi for posisjonsbestemmelse, navigasjon og tidsbestemmelse,* https://www.regjeringen.no/contentassets/abd1dec7647a4c22aaef7d93046e3f2b/pa-rett-sted-til-rett-tid.pdf

ROM

Romsektoren understøtter sentrale områder som posisjon, navigasjon og tid (PNT), i tillegg til kommunikasjon og jordobservasjon. Dette er tjenester som er sentrale for både sivile og militære formål. Flere samfunnsfunksjoner er avhengig av at disse tjenestene fungerer, som person- og godstransport, elektronisk kommunikasjon, kraftforsyning, finansielle tjenester og krisehåndtering. Romvirksomhet er en forutsetning for å kunne ivareta stats- og samfunnssikkerhet og må beskyttes med det som utgangspunkt. Bakkestasjoner som er koblet mot nett har de samme sikkerhetsmessige utfordringene som annen IKT-infrastruktur og kan benyttes som inngang for å kompromittere satellitter og informasjon.

Det er viktig å forebygge både tilsiktede og utilsiktede forstyrrelser av satellittsignalene, håndtere forstyrrende signaler og sørge for fysisk og digital sikkerhet for rombasert infrastruktur. Samferdselsdepartementet har utarbeidet en nasjonal strategi for posisjonsbestemmelse, navigasjon og tidsbestemmelse.[26] Den foreslår en rekke tiltak knyttet til bedre sikring av PNT-infrastruktur, som forebyggende tiltak, hendelseshåndtering og beredskap, herunder også tiltak som reduserer konsekvensene ved svikt. Det samme vil være nødvendig for infrastruktur for satellittkommunikasjon og jordobservasjon.





5.
«Too big to fail» – Utenlandske selskaper bærer norske samfunnsfunksjoner

Hvor mange av appene våre slutter å fungere hvis de ikke får koblet seg opp mot tjenester i utlandet? Kan vi fortsatt betale for varer og tjenester? Hva vil skje hvis mobiltelefonene våre ikke får snakket med Google eller Apple? Vil virksomhetene våre lammes hvis saksbehandlingssystemet, kunderegisteret og e-postklientene ikke har kontakt med utenlandske datasentre? Hva betyr det når utenlandske virksomheter eier norsk, kritisk infrastruktur? Står Norge langt nok framme i køen for å få hjelp hvis hele verden blir rammet av en skadevare? Hva gjør vi hvis vi ikke lenger stoler på maskin- eller programvaren vi bruker?

Selv om det kan være lønnsomt for en norsk virksomhet å tjenesteutsette store deler av IKT-miljøet til utlandet, påvirker det også nasjonal risiko hvis majoriteten av store, norske virksomheter gjør dette. Spesielt hvis alle velger en av de få, ledende aktørene på markedet.

Norge har råderett over eget forsvar, transportsystem, kraftnett og vannforsyning, men ikke over avhengighetene til utlandet. Verdikjedene vokser og vi får flere lag med tjenesteutsetting og tjenestebruk, hvor hver tjeneste baserer seg på en rekke andre tjenester.

En pågående debatt dreier seg om i hvilken grad komponenter og tjenester fra utenlandske selskaper kan brukes for å bygge ny digital infrastruktur som Norge vil være avhengig av i fred, krise og krig. Debatten aktualiserer leverandøravhengighet. Innen flere bransjer er det kun noen få, store aktører som leverer den nødvendige teknologien. Vi blir prisgitt de store leverandørene når vi skal planlegge, sette opp, drifte og vedlikeholde infrastrukturen vår.

Eksempelvis må ekom-aktørene ha de beste og nyeste tekniske løsningene, både for å konkurrere internasjonalt og for at Norge ikke skal sakke akterut i det teknologiske kappløpet. Neste generasjons nødnett og alle leverandører av mobilnett er avhengig av support og kompetanse fra utlandet og det meste av utviklingen av ekomnettene skjer utenfor Norge. Når det gjelder kraftsektoren er den avhengig av noen få, utenlandske utstyrsprodusenter med store markedsandeler. Innen de andre sektorene er bildet det samme, med utvidet bruk av tjenester fra utenlandske leverandører. Internasjonale verdikjeder og tjenester blir stadig viktigere for å ivareta viktige samfunnsfunksjoner i Norge.

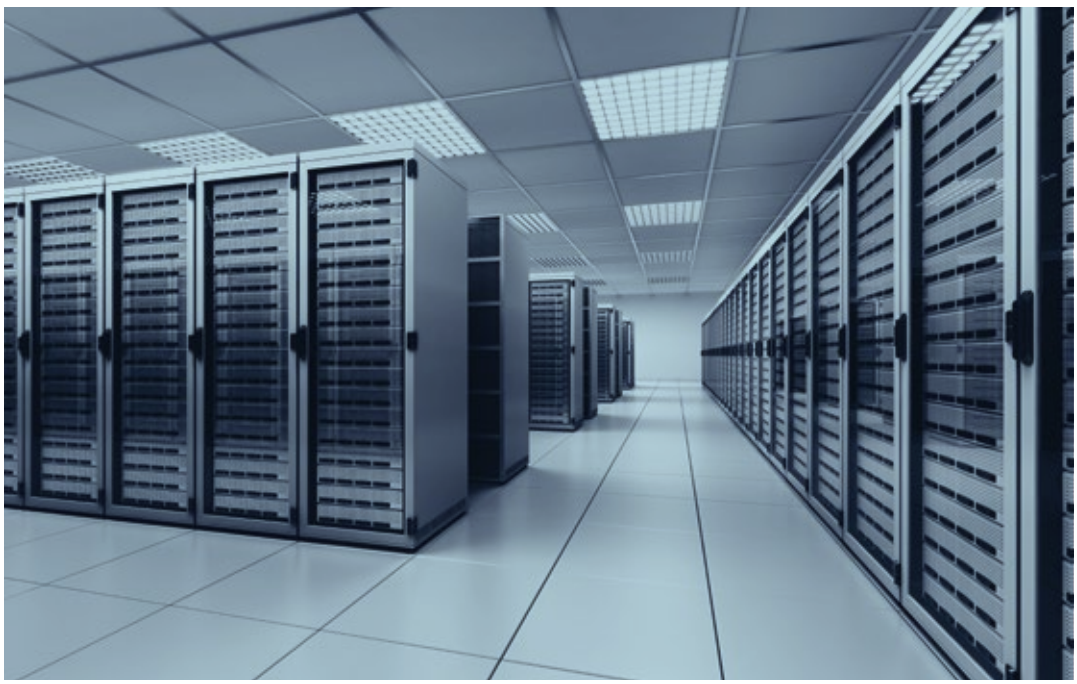
Avhengighetene til utlandet øker.

Innen flere bransjer er det kun noen få, store aktører som leverer den nødvendige teknologien.

Regulering er et av virkemidlene myndighetene har for å sørge for at vi er mer selvforsynt med digitale tjenester. Nasjonal lovgivning er viktig for å sikre nasjonale verdier, men i tillegg må virksomhetene selv ha et bevisst forhold til hvordan de setter krav om sikkerhet i kontrakter med sine leverandører. Norsk regulering skal også harmoniseres med EU i den grad det er EØS-relevant.

Mer komplekse bruksområder og teknologi kommer til å drive behovet for, og ønsket om, økt bruk av datasentre. De fleste store leverandørene av slike tjenester har ikke datasentre i Norge. Dermed lagres og foredles norske data i utlandet, av utenlandsk personale. Disse dataene vil samlet sett ha stor verdi og kan være sensitive for samfunnet, virksomheter og enkeltpersoner.

Norske virksomheter kan stille krav til, og i enkelte tilfeller ha en plikt til å kreve, at datasentre plasseres i Norge. Flere store leverandører er i ferd med å gjøre dette. I framtiden vil nye sanntidsapplikasjoner innen tingenes internett, for eksempel selvkjørende, kommuniserende biler, kreve at enkelte datasentre plasseres fysisk nær applikasjonene for å unngå forsinkelser. Norske virksomheter bør bygge arkitekturer som beskytter oss mot både interne og eksterne, inkludert internasjonale, hendelser. Vi må vurdere alternative løsninger, redundans og muligheten for å opprettholde tjenester med redusert ytelse og kvalitet. Mulighet for manuell overstyring av visse funksjoner bør alltid vurderes.



Syv viktige teknologiske trender fra et sikkerhetsperspektiv

1 

Automatisering
Automatisering fører til standardisert oppførsel og færre menneskelige feil. Eksempler på anvendelser er flåtestyring, oppdatering, konfigurering, monitorering og verifisering.

2 

Skytjenester
Skytjenester er den nye virkeligheten. Vi kan spare på drift og investeringer og får et mer fleksibelt miljø. De fysiske klientene trenger sjelden ha data lagret lokalt. Bruk av virtuelle nettverk øker.

3 

5G
Utbyggingen av 5G-nettet vil innebære en betydelig endring i hvordan ekom-nettene vil understøtte andre samfunnsfunksjoner. Det vil gi oss muligheter vi ennå ikke kan tenke oss. Utbyggingen vil tilrettelegge for IoT-revolusjonen og distribuerte sanntidssystemer.

4 

Kunstig intelligens
Manuell dataanalyse vil reduseres. Det er for dyrt, for tregt, for sårbart. Store, komplekse systemer vil kreve utstrakt bruk av kunstig intelligens i driften. Kunstig intelligens vil også brukes både til angrep og forsvar innen digital sikkerhet og vi kan få et digitalt våpenkappløp.

5 

Tingenes internett
Små, strømgjerrige, billige enheter får økt regnekraft og vil, med 5G, sette fart på tingenes internett. Enkle reguleringssystemer er blitt komplekse datamaskiner med ny og nyttig funksjonalitet, og er nå sårbare for de samme operasjonene som treffer konvensjonelle enheter. Forskjellen er at sikkerheten er dårligere og konsekvensene større.

6 

Smarte byer
Når IoT-enheter kombineres med virtualisering, sanntidsstyring, 5G og kunstig intelligens vil vi kunne bruke automatisering og digitalisering til å skape smarte byer og samfunn. Dette realiseres av enheter, nettverk, datasentre, tjenester og grensesnitt som alle må fungere sammen og løse nye sikkerhetsutfordringer.

7 

Virtuell virkelighet
Virtuell og utvidet virkelighet er teknologier som har vært på trappene i noen år. De vil forenkle og trygge jobbene våre. En revolusjon innen området vil kunne skape helt nye interaksjonsformer mellom menneske og maskin, med de utfordringene det vil føre med seg.

6.
Sårbart menneske, sårbart samfunn

Norge er et trygt land å bo i. Vi lever i et liberalt demokrati med ytringsfrihet, personvern, rettssikkerhet og likeverd. Det digitale rom har gitt utfordringer på dette området. Bevisstgjøring og tiltak hjelper oss å navigere i den digitale verden.

Et demokratisk samfunn er avhengig av muligheten til åpen debatt og drøfting av tanker og meninger. Disse verdiene utfordres. Flere store aktører samler inn stadig mer informasjon gjennom nettbruken vår, og vi blir utsatt for skjult påvirkning. Enkelte av oss blir utsatt for krenkelser som ID-tyveri og spredning av personlig informasjon på sosiale nettverk. Andre blir trakassert for sine meninger, holdninger, ytringer og tro.

Svært mye av informasjonen vi utsettes for er forsøk på påvirkning. Dette ser vi gjennom reklame, medier og politisk kommunikasjon. Dette er legitime former for påvirkning. Stater, organisasjoner eller virksomheter som søker å påvirke vår befolkning for å oppnå egne strategiske målsettinger kan i noen tilfeller true våre nasjonale sikkerhetsinteresser. I disse tilfellene vil påvirkningen utgjøre sikkerhetstruende virksomhet. Forsøk på påvirkning skjer i det skjulte. Aktørene vil da operere på måter som er vanskelig å avdekke for de som blir utsatt for påvirkning og dermed også for myndighetene. Forsøk på påvirkning kan finne sted i alle sektorer og blant hele befolkningen. Den kan skje gjennom brede kampanjer i media, eller være målrettet mot enkeltpersoner eller virksomheter.

- Flere kommersielle aktører innen sosiale medier har gått aktivt inn for å stoppe falske nyheter. Det er i tillegg behov for økt informasjon og veiledning om hvilke trusler Norge utsettes for, hva det betyr for den enkelte person, virksomhet eller organisasjon og hvordan man kan gjenkjenne forsøk på påvirkning. Blant annet lanserte regjeringen ti tiltakspunkter for å hindre uønsket påvirkning i valggjennomføringen[27] i forbindelse med Kommunestyre- og fylkestingsvalget 2019.

- Vi som borgere har også et ansvar. Vi trenger opplæring i nettvett. Denne bør inkludere en gjennomgang av metoder som retorikk og sosial kontroll og eksempler fra den virkelige verden. Evnen til rasjonell og kritisk

DEEPFAKE

«Deepfake» er bruken av kunstig intelligens for å endre på mennesker i bilder og på film. For eksempel har en del kjendiser og andre blitt misbrukt i pornofilmer på denne måten. Politikere og andre samfunnsdebattanter kan bli framstilt som om de har sagt og gjort ting de ikke har. Falskt materiale vil kunne spres for å sverte nøkkelpersoner i avgjørende øyeblikk som valg, rettsaker eller kriser og kan bidra til å skape falske minner hos eksponerte individer. Slike falske sannheter vil kunne påvirke grunnleggende oppfatninger og være vanskelige å imøtegå i ettertid.

[27] *Ti tiltak for hindre uønsket påvirkning i valggjennomføringen,* https://www.regjeringen.no/no/aktuelt/ti-tiltak-for-hindre-uonsket-pavirkning-i-valggjennomforingen/id2661220/

Et demokratisk samfunn er avhengig av muligheten til åpen debatt, drøfting av tanker og holdninger.

tenkning, sjekk av kilder og en god dose sunn skepsis i møte med sensasjonelle «nyhetssaker» på nettet bør også inkluderes. Dette vil hjelpe hver enkelt til å være best mulig rustet til å håndtere informasjonsstrømmen. Som eksempel lanserte Medietilsynet, Faktisk.no og Utdanningsdirektoratet i 2018 et opplegg om kritisk medieforståelse for ungdomsskole-elever. Ifølge en undersøkelse[28] gjort av Medietilsynet er det de unge som er flinkest til å identifisere falske nyheter.

Den personlige informasjonen vi villig gir bort representerer samlet sett verdifulle opplysninger om norske borgere, virksomheter og samfunn. Mange tjenester fungerer som samhandlingsarenaer for norske borgere og mye av informasjonen som lagres har behov for beskyttelse.

Innføringen av personvernforordningen (GDPR) i EU har vært et viktig skritt i å regulere teknologiselskaper. Tilsvarende vil lover som motvirker monopoler kunne være effektive virkemidler for å balansere maktforholdet mellom samfunn og kommersielle aktører.

Hvis noen stjeler et passord eller en ulåst telefon, kan vi oppleve at pengene våre er borte, korrespondansen vår er lest, maskinen vår er hacket, meldinger og e-poster er sendt i våre navn, og at de private bildene våre brukes til å presse oss. Slike krenkelser er en tung belastning og kan føles som vanskelig å få gjort noe med. Mindre enn én av tre vil anmelde digital hets til politiet, rapporterer NorSIS.[29]

Nettsteder som nettvett.no og slettmeg.no gir gode råd som kan hjelpe privatpersoner. NorSIS rapporterer at de har hjulpet mange enkeltpersoner med å nå fram til de store tilbyderne, spesielt når de har hatt problemer med å bevise at de eier stjålne, digitale identiteter. Personvernforordningen har blitt et virkemiddel norske myndigheter kan bruke overfor aktører som ikke ivaretar personvernet vårt godt nok. Norske myndigheter deltar i internasjonalt politisamarbeid og samarbeider også med private aktører for å beskytte norske borgere og interesser.

HVA AVGJØR OM VI KAN MOTSTÅ PÅVIRKNING?

- Det første er samfunnets evne til å avdekke, varsle og motstå påvirkningsforsøk.
- Det andre er myndighetenes og politisk ledelses evne til å håndtere påvirkning og andre former for hybrid virkemiddelbruk.
- Det tredje er virksomheter og myndighetenes evne til å samarbeide og dele informasjon seg imellom, på tvers av sektorer.
- Det fjerde er økt bevissthet og kunnskap hos norske borgere.

[28] *Kritisk medieforståelse i den norske befolkningen*, https://medietilsynet.no/om/aktuelt/eldre-er-darligst-pa-a-gjenkjenne-falske-nyheter/

[29] *Nordmenn og digital sikkerhetskultur 2018*, https://norsis.no/nordmenn-og-digital-sikkerhetskultur-2018/

Store samfunnsendringer er på vei

De største truslene er etterretning og påvirkning fra statlige aktører, samt kriminelle.

Det er et jevnt trykk av digitale angrep mot norske mål. Trusselaktørene blir mer profesjonelle.

Digitale etterretningsoperasjoner og sabotasje mot viktige samfunnsfunksjoner vil ha størst påvirkning på den nasjonale sikkerheten.

De fleste viktige samfunnsfunksjoner og tjenester er totalt avhengig av IKT.

Avhengigheten til digitale tjenester og systemer har økt så mye at alvorlige hendelser kan få store konsekvenser for samfunnet. Dette gjelder blant annet virksomheter innen kraft, telekom og rom. Dette er også sektorer med høyt fokus på sikkerhet.

Det er et behov for økt bevissthet, digitale reserveløsninger og beredskapstiltak.

Helhetlig digitalt risikobilde 2019

Denne rapporten har til hensikt å øke bevisstheten om sårbarheter, trusler, verdier og tiltak innen digital sikkerhet og virkningen disse faktorene har på nasjonal sikkerhet.

Mange virksomheter mangler et helhetlig arbeid med digital sikkerhet.

Bevisstheten om digital sikkerhet øker i mange norske virksomheter og de iverksetter i økt grad gode tiltak.

Sårbarheter er ikke bare tekniske. Digital sikkerhet må være en del av virksomhetsstyringen, tilsatte må ha nødvendig kompetanse og det offentlig må tilby de rette tjenestene for å skape motstandsdyktighet.

Usikre systemer, små IKT-miljøer, mangelfull risikovurdering ved tjenesteutsetting og uoversiktlige verdikjeder skaper risikoer.

Avhengigheten til utenlandske tjenestetilbydere vokser.

Design: Redink
Manus: NSM
Foto: iStock, NSM og Colourbox

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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