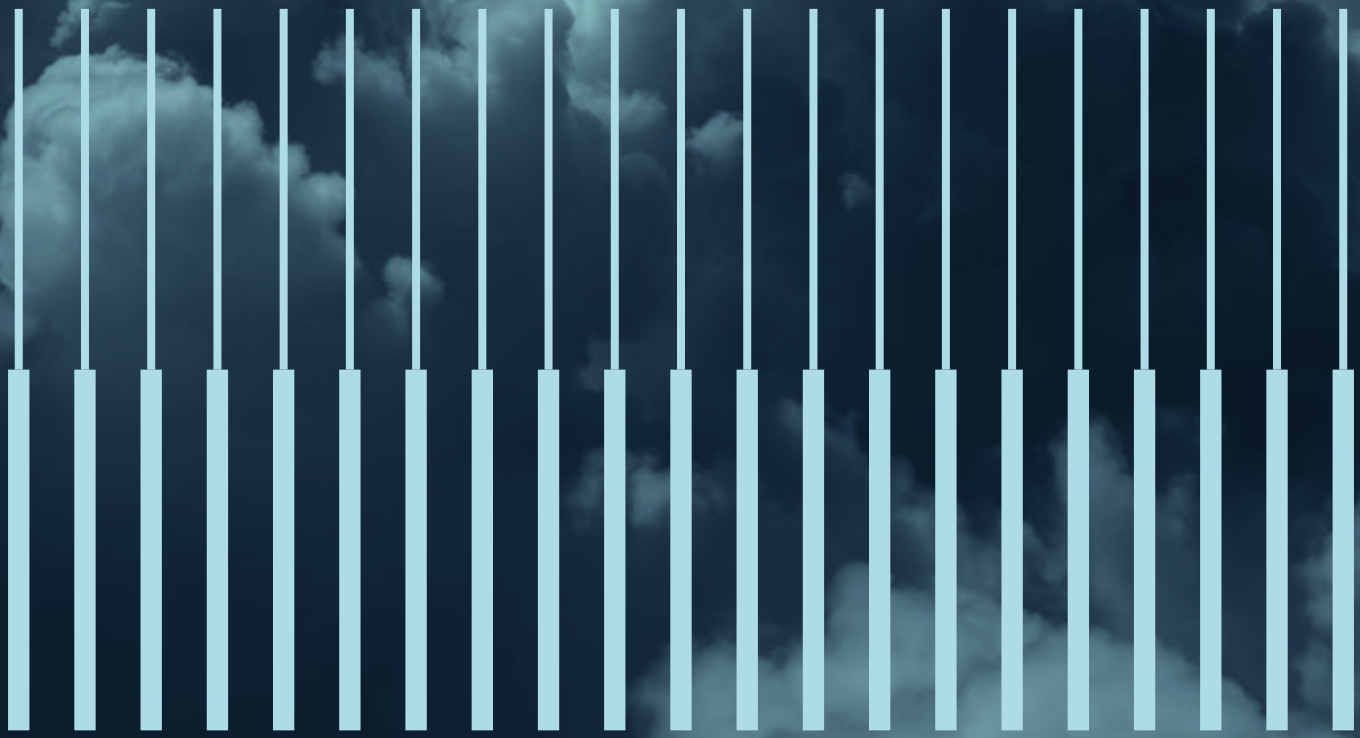
NASJONAL
SIKKERHETSMYNDIGHET

Helhetlig digitalt risikobilde 2020



Helhetlig digitalt risikobilde er en årlig rapport som skal 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.

Tema for årets rapport er muligheter og utfordringer som kommer med skytjenester og tjenesteutsetting. I tillegg omtales hvilke typer digitale hendelser som rammer norske virksomheter og metodene som benyttes mot oss. Rapporten gir også en status over nasjonale tiltak innen digital sikkerhet og retning for det videre sikkerhetsarbeidet.

Innhold

NASJONAL SIKKERHETSMYNDIGHET (NSM)

er Norges ekspertorgan for forebyggende sikkerhet. 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 samtidig et partnerskap mellom NSM og ulike offentlige og private virksomheter. Senteret skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot digitale angrep. NCSC har et spesielt fokus på rådgiving og krav innen forebyggende tiltak, tekniske sikkerhetsløsninger og yter bistand til hendelseshåndtering når uhellet er ute.

Sammendrag

COVID-19 har vist at ekstraordinære situasjoner og kriser påvirker det digitale domenet i større eller mindre grad, men pandemien har likevel ikke endret hovedlinjene i det digitale risikobildet mot Norge. Nasjonalt cybersikkerhetssenter (NCSC) i NSM observerer ulike typer digitale operasjoner mot norske mål, inkludert mot virksomheter som ivaretar viktige samfunnsfunksjoner.

En gjennomgående erfaring er at digitale operasjoner blir mer sofistikerte og komplekse, og at hendelseshåndtering er tid- og ressurskrevende. En annen erfaring er at løsepengevirus i økende grad rammer norske virksomheter. NSM har i flere år rapportert om at det er kjente sårbarheter som benyttes for å gi uautorisert tilgang til systemer og nettverk. Det digitale risikobildet preges fremdeles av dette.

NSM erfarer at mange virksomheter fortsatt mangler risikoreduserende tiltak helt eller delvis, og dette utgjør en bekymring. NSM er av den oppfatning at norske virksomheter er bedre rustet mot uønskede digitale hendelser hvis de følger rådene i NSMs *Grunnprinsipper for IKT-sikkerhet*. Erfaringer det siste året underbygger denne vurderingen.

NSM er positive til at virksomheter benytter skytjenester såfremt virksomheten har gjort gode og riktige vurderinger rundt dette. Fordelene er større enn ulempene for de aller fleste. Men det er viktig å understreke at virksomheten fortsatt har det hele og fulle ansvaret for sikring av egne verdier, selv ved bruk av skytjenester. Det er viktig at virksomheten har god bestillerkompetanse og utøver god sikkerhetsstyring.

Økt bruk av skytjenester bringer også med seg nye sårbarheter og økt risiko utover virksomhetens eget domene. NSM er bekymret for den samlede nasjonale avhengigheten av utenlandske skytjenesteleverandører, og hvordan denne avhengigheten kan spille ut i hele krisespennet. For noen virksomheter bør bruk av skytjenester derfor vurderes opp mot nasjonal kontroll og nasjonal beredskap.

Forebyggende sikkerhetsarbeid reduserer digital risiko. Sikkerhetsstyring har nå blitt enda viktigere i møte med komplekse verdikjeder og et samfunn preget av internasjonalisering og teknologisk utvikling. En helhetlig tilnærming til sikkerhet inkluderer både prosessuelle, organisatoriske og tekniske tiltak.

NSM erfarer at stadig flere virksomheter prioriterer IKT-sikkerhetsarbeidet. Norske private og offentlige virksomheters arbeid med sikring av digitale verdier øker samfunnets totale robusthet mot sikkerhetstruende hendelser. Digital sikkerhet er et felles ansvar, og det må tas på alvor. ■

NSM erfarer at mange virksomheter fortsatt mangler risikoreduserende tiltak helt eller delvis, og dette utgjør en bekymring.

1. Det digitale risikobildet

Situasjonsbildet i det digitale rom var ved inngangen til 2020 preget av hendelser mot norske virksomheter som spente bredt både i omfang og alvorlighetsgrad. Dette er i samsvar med bildet erfart de siste årene. Da COVID-19 inntraff i Norge viste det at ekstraordinære situasjoner og kriser også påvirker det digitale domenet. COVID-19-situasjonen har utfordret oss på mange måter – hvordan vi kommuniserer med hverandre og hvordan vi jobber. Den har tvunget frem og akselerert bruk av nye og digitale løsninger for hele samfunnet. Pandemien har også medført flere digitale sårbarhetsflater og risikoområder. Hva betyr helhetlig digital sikring i en slik kontekst?

COVID-19 forsterker digitale sårbarheter

NSM har erfart at ulike aktører utnytter COVID-19-tematikk som et mulighetsrom for svindelforsøk og digitale operasjoner på nett. Enkelte sektorer med viktige verdier ble satt under økt press som følge av situasjonen. Operativ evne og funksjonalitet var kritisk, og disse sektorene var dermed sårbare for ondsinnede digitale operasjoner. Flere sårbarhetsflater og sikkerhetshull knyttet til utstrakt bruk av hjemmekontorløsninger, som utnyttelse av sårbarheter i fjernaksessløsninger, førte til behov for økt årvåkenhet og bevisstgjøring rundt IKT-sikkerhet. NSM har gjennom året gitt ut flere varsler, råd og tiltak om COVID-19-situasjonen og det digitale rom.

Forebygging og risikoreduserende tiltak må være på plass i forkant av en krise. Det har COVID-19-situasjonen vist oss. Langsiktig forebyggende arbeid begrenser skadeomfanget og konsekvensene av sikkerhetstruende virksomhet. Kartlegging av verdier, digitale avhengigheter og verdikjeder er helt sentrale elementer i det forebyggende sikkerhetsarbeidet. Å være forberedt på enhver eventualitet og etablere evne til å håndtere hendelser er viktig for raskt å kunne gjenopprette sikkerheten.

COVID-19-situasjonen har likevel ikke endret hovedlinjene i det digitale risikobildet mot Norge. Nasjonalt cybersikkerhetssenter (NCSC) i NSM observerer fortsatt ulike typer digitale operasjoner mot norske mål, inkludert mot virksomheter som ivaretar viktige samfunnsfunksjoner. Til tross for at aktivitetsnivået som er observert så langt i 2020 i hovedsak samsvarer med normalbildet i det digitale rom, ser vi enkelte utviklingstrekk. En gjennomgående erfaring er at digitale operasjoner blir mer sofistikerte og komplekse, og at hendelseshåndtering er tid- og ressurskrevende. En annen erfaring er at løsepengevirus i økende grad rammer norske virksomheter. Dette er en utvikling NSM har pekt på i flere år.

Digitale verdikjeder og avhengigheter

Den teknologiske utviklingen har ført til en digital transformasjon. Store samfunnsverdier

NSM har erfart at ulike aktører utnytter COVID-19-tematikk som et mulighetsrom for svindelforsøk og digitale operasjoner på nett.

legges over i det digitale domenet. Digitale verdikjeder vokser og har sterke avhengigheter til hverandre. Fra et samfunnsperspektiv er det viktig å vurdere og forstå hvilken risiko et eventuelt utfall av henholdsvis kraftforsyning, ekom eller satellittbaserte tjenester utgjør for andre verdikjeder i samfunnet. Dersom kraftforsyningen faller ut, vil store deler av samfunnet stoppe opp. Utfall av ekom vil ha umiddelbar konsekvens for mobiltjenester, nettilgang, informasjons- og nyhetsformidling og digital samhandling over internett. Utfall av satellittbaserte tjenester vil få konsekvenser for blant annet Forsvaret, redningstjenester, skips- og luftfart, deler av finansnæringen, så vel som kraft og ekom.

Alle sektorer er risikoutsatt som følge av økt digitalisering. Grunnen kan være ekstraordinære situasjoner som fører til økt press på enkelte sektorer, som under COVID-19, fordi verdiene i økende grad befinner seg i det digitale rom, eller fordi avhengigheter mellom sektorer og funksjoner blir sterkere.

Digitalisering vil alltid innebære risiko, for samfunnet, for virksomheter og for individet. En helhetlig tilnærming til sikkerhetsarbeidet og tiltak for å redusere sårbarheter og håndtere hendelser når de inntreffer, hjelper oss å digitalisere på en sikker måte. NSM vurderer at *sårbarhetsbildet* stadig blir mer komplekst.

Innen det digitale risikobildet er sårbarhetsreduserende tiltak helt sentralt for å forhindre, eller minimere effekten av, sikkerhetstruende virksomhet i det digitale rom. Virksomheter må adressere sine egne sårbarheter.

Det er viktig å se digital sikkerhet som del av en helhet. En virksomhet må beskytte sine verdier mot trusselaktører som vil lete etter sårbarheter for å nå disse verdiene. Digitale virkemidler er én vei inn. Andre er bruk av innsidere og fysisk tilgang til verdier. Det er dermed viktig å se sikkerhetstiltak i sammenheng, og få til et godt samspill mellom disse gjennom god sikkerhetsstyring.

Digitaliseringen fører også til økte avhengigheter til utlandet. Disse komplekse verdikjedene blir stadig viktigere for å ivareta norske samfunnsfunksjoner. Flere virksomheter tar i bruk skytjenester og tjenesteutsetter sin IKT-portefølje. Mulighetene og utfordringene ved skytjenester og tjenesteutsetting er mange og blir stadig mer aktuelle. Derfor har NSM valgt skytjenester og tjenesteutsetting som tema for årets rapport. I tillegg vil rapporten omtale digitale hendelser som treffer norske virksomheter og hvilke metoder trusselaktørene benytter for å kompromittere systemer og nettverk. Observasjoner og funn fra NCSC fremkommer i teksten som «NCSCs» egne, ellers er vurderinger og standpunkter gjennom rapporten gjort av NSM som helhet. ■

Mulighetene og utfordringene ved skytjenester og tjenesteutsetting er mange og blir stadig mer aktuelle.

Nasjonalt cybersikkerhetssenter – en del av NSM

Det har nå gått et knapt år siden Nasjonalt cybersikkerhetssenter (NCSC) offisielt ble åpnet i november 2019. Senteret ivaretar det oppdaterte risikobildet i det digitale rom og gir ut råd, veiledninger og andre tiltak på NSMs nettsider. NCSC skal være en autoritativ stemme innen digital sikkerhet i Norge.

Senteret har et klart formål om å utnytte potensialet som ligger i et styrket sektorovergripende og offentlig-privat samarbeid. Så langt har i overkant av 40 norske virksomheter blitt partnere i cybersikkerhetssenteret, og flere har meldt sin interesse. Ulike myndighetsorganer og næringsliv samarbeider her om å utveksle informasjon, dele erfaringer og sammen bidra til et helhetlig situasjonsbilde. Flere partnere har gitt innspill til årets *Helhetlig digitalt risikobilde* gjennom å dele risikovurderinger og annen relevant informasjon, samt gjennom å bidra med konkrete eksempler og erfaringer. Samarbeidet setter oss i stand til å gi et helhetlig bilde av digital risiko i Norge.

«NSM er av den oppfatning at norske virksomheter blir mer sikkerhetsbevisste. Likevel opplever vi at flere av de som utsettes for digitale hendelser hverken har nødvendige forebyggende tiltak på plass eller kompetanse og kapasitet til å avdekke, håndtere eller begrense skadeomfang ved dataangrep. Hendelser NCSC har håndtert det siste året kunne vært avverget eller begrenset dersom virksomhetene hadde fulgt rådene i *NSMs Grunnprinsipper for IKT-sikkerhet*», sier Bente Hoff.

Bente Hoff, Avdelingsdirektør Nasjonalt cybersikkerhetssenter, NSM

Nasjonalt cybersikkerhetssenter ligger i Oslo havnelager

2. Utvikling og trender innen digitale hendelser – hva rammer norske virksomheter?

Aktivitetsnivået NCSC har sett hittil i 2020 samsvarer i hovedsak med det som er blitt normalbildet i det digitale rom de siste årene. NCSC ser at flere uønskede digitale hendelser har hatt store konsekvenser for berørte virksomheter, og hvor håndtering har tatt tid og krevd mye ressurser.

Norske virksomheter blir rammet av ulike typer nettverksoperasjoner

Gjennom samarbeidet i Felles cyberkoordineringssenter (FCKS)[1] ser NSM at både statlige og kriminelle aktører utfører digitale operasjoner og datainnbrudd mot mål i Norge. Fremmede stater søker blant annet etter statshemmeligheter, høyteknologi og forretningshemmeligheter når de gjennomfører digitale operasjoner mot norske virksomheter. Disse aktørene har omfattende ressurser til rådighet og jobber med langsiktige målsettinger. Organiserte kriminelle utnytter det digitale rom for økonomisk vinning, slik som utpressing med løsepengevirus, datatyveri og svindelforsøk.

NSM vurderer som tidligere år at forvaltningen og en rekke sektorer i Norge er risikoutsatt for digitale operasjoner. Dette inkluderer særlig virksomheter innen sektorene forsvar, romvirksomhet, maritim, petroleum, ekom og kraft. I tillegg observerer NCSC at andre sektorer i økende grad er risikoutsatt. Det siste året har NCSC hatt økt fokus innen sektorene samferdsel, forskning og høyere utdanning samt helse. Det er en risiko for at sektorer som er under økt press kan være mer sårbare for vellykkede nettverksoperasjoner, slik som under COVID-19-situasjonen.

Trusselaktører utfører rekognosering og informasjonsinnhenting mot mål i Norge. NCSC ser digital kartlegging av norske virksomheters infrastruktur og digitale innhentingsoperasjoner hvor aktøren bak lykkes i å kompromittere en virksomhet for deretter å hente ut data fra systemene. Kartlegging av sårbarheter i infrastruktur kan i tillegg være forberedelse til fremtidige sabotasjehandlinger ved en eventuell eskalering i krisespennet.

Videre observerer NCSC også andre typer nettverksoperasjoner. Virksomheter utsettes for eksempel for utpressingsforsøk ved bruk av løsepengevirus, der trusselaktørene lammer digitale systemer gjennom kryptering og krever løsepenger for å låse opp krypteringen. I mange tilfeller er løsepengevirusangrep utført av aktører med høy digital kompetanse, på eget initiativ eller på oppdrag fra andre. Det er et undergrunnsmarked for kjøp og salg av løsepengevirus («ransomware as a service»). I tillegg er løsepengevirus under konstant

Det siste året har NCSC hatt økt fokus innen sektorene samferdsel, forskning og høyere utdanning samt helse.

[1] *FCKS består av Forsvarets etterretningstjeneste, Politiets sikkerhetstjeneste, NSM og Kripos.*

NSM forventer en fortsatt økning i løsepengeangrep mot norske virksomheter i tiden fremover.

utvikling, hvor verktøy og metoder stadig endres. Det er en trend at angripere krever penger for å ikke auksjonere bort dataene eller lekke disse. De siste årene har det vært sett løsepengevirus rettet mot bedrifter og virksomheter med større betalingsevne enn enkeltpersoner. Løsepengevirus kan også benyttes som en avledning med den hensikt å skjule faktisk intensjon utover økonomisk vinning.

Allerede tidlig under COVID-19 så NCSC en økning i rapportering av løsepengevirus mot norske virksomheter. Flere av partnerne har rapportert om et høyt trykk av forsøk på bruk av løsepengevirus den siste tiden. DNB omtaler blant annet krypteringsvirus som en økende trend i sin trusselvurdering for 2020[2] og trenden er også observert i kraftbransjen. Det norske mediebildet[3] og rapportering internasjonalt gjenspeiler også dette. NSM forventer en fortsatt økning i løsepengeangrep mot norske virksomheter i tiden fremover. Å være forberedt på slike hendelser, vite hva en skal gjøre dersom det inntreffer, samt forebyggende arbeid gjør virksomheter bedre rustet til å håndtere løsepengevirus.

Svindelforsøk i form av direktørsvindel og misbruk av infrastruktur til utvinning av kryptovaluta rammer også mange norske virksomheter. Dette rapporteres også av flere av partnerne i NCSC samt fra internasjonale samarbeidspartnere. COVID-19-tematikk ble også benyttet i svindelforsøk mot norske mål i 2020.

Verdikjedene blir mer komplekse og avhengighetene mellom ulike ledd i verdikjedene øker i takt med digitaliseringsprosessen. Programvare- og tjenesteleverandører kan utnyttes av trusselaktører for å få innpass i systemene til selskapets kunder. Leverandørkjedeangrep, hvor aktøren rammer en tredjepart eller tilgrensende virksomhet, forkommer også i Norge. NSM observerer at virksomheter lengre nede i verdikjedene rammes av sikkerhetstruende virksomhet, enten som mål i seg selv eller som ledd i å nå mål høyere opp i verdikjedene. På bakgrunn av dette anser NSM det som sannsynlig at angrep på leverandørkjeder vil øke. Dette synet deles av aktører i flere sektorvise responsmiljøer.

BESKYTT DEG MOT LØSEPENGEVIRUS

Sammen med Kripos har NSM utarbeidet en temarapport[4] om løsepengevirus. Temarapporten beskriver hva løsepengevirus er og gir råd om hvordan man kan beskytte seg mot slike angrep, blant annet om hvordan man kan hindre skadevaren i å kjøre og begrense konsekvensene skadevaren kan påføre.[5]

[2] *DNB trusselvurdering 2020:* https://www.dnb.no/dnbnyheter/no/samfunn/trusseletteretning_sparer_kundene_for_enorme_summer

[3] *Medieomtale fra 2020 viser at virksomheter som har blitt rammet er alt fra små familiebedrifter til store tjenesteleverandører og produsenter som for eksempel Garmin, Vard, Webmercs, Honda og Fresenius Kabi.*

[4] *Løsepengevirus – temarapport:* https://nsm.no/getfile.php/133208-1591778522/Demo/Dokumenter/Rapporter/temarapport-losepengevirus-200218.pdf

[5] *Løsepengevirus – råd og anbefalinger:* https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger/losepengevirus

Direktørsvindel – et eksempel fra samferdselssektoren

Virksomheten har gjennom Covid-19-perioden opplevd stor pågang av svindel, særlig via e-post.

«Et tilfelle vi hadde av direktørsvindel var profesjonelt gjennomført. Her hadde svindlerne gjort grundig forarbeid og med stor sannsynlighet kartlagt ansatte i administrasjonen. De hadde tilegnet seg informasjon om ansatte innen økonomi og controlling, personer som ikke er profilerte eller har gjort seg bemerket utad, men som likevel har et økonomisk mandat og tilganger til å gjennomføre økonomiske transaksjoner. Svindelen ble utført på en dag hvor adm.dir. kun periodevis kunne nås via mobil.

Økonomikontrollere spredt ut på hjemmekontor ble kontaktet med en e-post som tydeligvis kom fra en mobiltelefon. E-posten bestod av korte, presise og konkrete setninger hvor avsender (adm.dir.) ba om å få hastebetalt en faktura. Det var viktig at fakturaen måtte betales umiddelbart. Teksten og formen i e-posten var ikke ulik den form som kan bli benyttet av adm.dir. når e-post sendes fra mobiltelefonen. Det som avslørte svindelen var først og fremst at adm.dir. i selskapet ikke ville gått frem på denne måten. Det andre er at de interne rutinene for økonomistyring og fakturabetaling ville stoppet denne type betaling.

Saken ble raskt sendt til IT-ansvarlig som konstaterte svindel, og medarbeidere innen økonomi og regnskap ble informert om hendelsen. Adm.dir. konstaterte at han aldri hadde sendt en slik e-post og heller aldri kommer til å gjøre dette. Saken ble publisert på intranett for å vise at svindelsaker kan ramme virksomheten, og med formaning om varsomhet og nettvett. Saken ble oversendt IT-leverandøren innen sikkerhet som undersøkte saken. Hendelsen ble politianmeldt for å få registrert saken, og ble senere henlagt.»

I 2020 er også COVID-19-tematikk blitt benyttet i ulike phishing-kampanjer mot norske virksomheter.

KraftCERT, eksempelvis, har håndtert saker som involverer produsenter og tredjepartsleverandører i både kraftbransjen og oljesektoren, og anser angrep via leverandørkjeder som en stor trussel.

Norske mål utsettes for kartleggingsaktivitet

NCSC har gjennom det siste året observert ulike kartleggingsaktiviteter mot norske mål. I noen tilfeller observeres brede rekognoseringskampanjer mot hele sektorer og i flere land. Her benyttes generiske skanneverktøy for å finne ulike sårbarheter eller sikkerhetshull som er eksponert mot internett og som kan utnyttes. Dette er enkle verktøy som baserer seg på fritt og lett tilgjengelig programvare. De er tilstrekkelige for å rekognosere tilgjengelig infrastruktur og for å finne sårbarheter. I tillegg gjør generiske verktøy det vanskelig å avdekke hvem som står bak.

Kartlegging kan også være målrettet mot enkelte virksomheters infrastrukturer. I kartleggingsøyemed kan detaljert informasjon om både virksomheten og ansatte legges til grunn for målrettede digitale operasjoner. Eksempler på dette kan være informasjon publisert på sosiale medier, virksomhetens hjemmeside og artikler i media. Derfor bør virksomheter gjennomføre en verdivurdering av egen virksomhet og av informasjonen de deler åpent om den. Les mer i NSMs *Håndbok i verdivurdering av informasjon*.[6]

Målrettet kartlegging kan også avdekke internetteksponerte sårbarheter eller andre sikkerhetshull i virksomhetens infrastruktur. Disse kan utnyttes for å kompromittere virksomhetens systemer.

LØSEPENGEVIRUS («RANSOMWARE») – ET EKSEMPEL FRA FINANSSEKTOREN

En søndag høsten 2019 gikk kontorstøttesystemene til en finansiell virksomhet i Norge offline da de ble angrepet av en aktør som aktiverte ransomware. Virksomhetens kunde- og forretningssystemer ble ikke berørt av selve hendelsen da de var adskilt fra kontorstøttesystemene, men likevel reduserte hendelsen virksomhetens evne til å operere effektivt og betjene sine kunder.

Virksomheten hadde konsesjon fra Finanstilsynet, som blant annet medfører at de er pliktig til å følge IKT-forskriften for sektoren. Den stiller krav til å drive systematisk risikobasert sikkerhetsarbeid i henhold til god praksis, som inkluderer å ha gode rutiner og systemer for å håndtere avvik, med fungerende backup-rutiner. Disse tiltakene medførte at den totale nedetiden for virksomheten var begrenset. Hendelsen er et eksempel på at sikkerhetsarbeid etter god praksis fungerer.

NSMs Grunnprinsipper for IKT-sikkerhet er et godt utgangspunkt for videreutvikling av sikkerhetsarbeidet i alle sektorer og virksomheter.

[6] *Håndbok i verdivurdering av informasjon:* https://nsm.no/getfile.php/133657-1592813304/Demo/Dokumenter/Veiledere/handbok-i-verdivurdering-av-informasjon---032020.pdf

I kartleggingsøyemed kan detaljert informasjon om både virksomheten og ansatte legges til grunn for målrettede digitale operasjoner.

E-post benyttes som inngangsvektor

Phishing-kampanjer brukes fortsatt som inngangsvektor i hendelser mot norske mål. Phishing er en metode aktører benytter ved å utnytte en ansatt for å skaffe seg uautorisert tilgang til en virksomhet. Phishing kan gjøres på ulike måter. De mest benyttede metodene er ved å lure en mottaker til å oppgi påloggings-detaljer eller å få mottaker til å laste ned skadevare via vedlegg eller link i en e-post. Dette kan gi aktøren tilgang til systemet for videre kompromittering.

Slike kampanjer kan være målrettet mot sektorer, mot enkelte virksomheter eller enkeltpersoner i en spesifikk virksomhet. Andre ganger ser vi brede generelle phishing-kampanjer hvor norske mål inngår som en del av målbildet på tvers av virksomheter, sektorer og land.

NCSC har det siste året sett en rekke forsøk på målrettede phishing-kampanjer mot norske virksomheter. I disse tilfellene er tema for e-posten relevant for mottaker, og vedlegg eller lenker i e-posten er spisset for mottaker og dens arbeidsoppgaver. Slike skreddersydde e-poster øker sannsynligheten for å lykkes. I 2020 er også COVID-19-tematikk blitt benyttet i ulike phishing-kampanjer mot norske virksomheter.

Påloggingsdetaljer kan kjøpes, tilegnes ved hjelp av phishing eller gjettes av aktøren selv. De kan være innhentet ved hjelp av tidligere e-poster hvor brukeren har blitt lurt av en falsk nettside til å oppgi sine opplysninger, eller de kan være hentet ned fra store databaser som samler på kompromitterte brukernavn og passord. NCSC ser også kompromitteringer av legitime nettsider hvor en aktør utnytter sårbarheter som ligger på den. Aktøren kan legge til funksjonalitet på nettsiden for å omdirigere brukere, eller laste opp skadevare

TILGANG TIL E-POST GJENNOM PHISHING

De siste årene har det vært skrevet mye om såkalt *Microsoft 365*-phishing. NSM har eksempler på at en aktør fikk tilgang via fjernpålogging til en e-postserver og deretter hadde mulighet til å laste ned alt innhold fra den aktuelle e-postkontoen. For en virksomhet kan e-postinnhold bestå av potensielt sensitiv informasjon om kundeforhold, kilder eller pågående arbeid.

Ofte vet hverken NSM eller virksomheten hvordan aktøren har fått tilgang til virksomhetens e-postkonti. Manglende logg-grunnlag og overvåkning av eget nettverk hos virksomheten er en viktig årsak til at NSM og virksomheten ikke klarer å avdekke hvordan kontoen ble kompromittert i utgangspunktet. Gode passordrutiner og flerfaktor-autentisering ville også i mange tilfeller hindret uautorisert tilgang til e-post og øvrige IKT-systemer.

eller utnyttelseskode direkte til nettsiden slik at den blir et «vannhull»[7]. Dette kan igjen ramme andre brukere av tjenesten.

Trusselaktører vet at mennesker er vanedyr og erfaring tilsier at vi gjenbruker passord fordi det gjør det lettere å huske. Et tidligere eksponert passord kan prøves flere steder, og én tapt konto kan fort bli flere. For virksomheter kan dette bli et problem hvis ansatte bruker samme passord på private tjenester og i jobbsammenheng.

Myndigheter og sikkerhetsindustrien har advart mot phishing i flere år. Mange har derfor blitt mer bevisst på mistenkelige e-poster og tenker seg om før de åpner et vedlegg eller klikker på lenker. Mørketallsundersøkelsen 2020 viser at 77 % av virksomhetene i løpet av det siste året har gjennomført tiltak for å øke de ansattes bevissthet rundt sikkerhet. Det er imidlertid sannsynlig at flere kompromitteringer av norske mål forblir uoppdaget hvert år. Enkelte aktører sender e-poster som er svært godt utformet og dermed vanskelig å oppdage. Gode sikkerhetstiltak for å forhindre at uønsket e-post kommer frem bør derfor implementeres. Opplæring og tiltak for økt sikkerhetsbevissthet blant de ansatte er viktig da det å klikke på lenker eller åpne vedlegg er en menneskelig sårbarhet som aktører vil fortsette å utnytte.

Kjente sårbarheter utnyttes

I de aller fleste tilfeller ser NCSC at det er tekniske sårbarheter som utnyttes for å kompromittere datasystemene til norske virksomheter. Tekniske sårbarheter kan for

MÅLRETTET PHISHING-KAMPANJE – ET EKSEMPEL

NCSC varslet sine mottakere i juni 2020 om en phishing-kampanje rettet mot ansatte på et personlig nivå, men som antageligvis var ment for å kompromittere virksomheten. Kampanjen ble først observert i perioden september til desember 2019 mot mål i Europa og Midtøsten, og ble i juni observert mot mål i Norge.

Aktøren bak kampanjen utgav seg på LinkedIn for å jobbe innen HR hos store forsvars- eller luftfartsselskaper, og gav informasjon om ledige stillinger. Etter å ha fått kontakt sendte aktøren en ondsinnet fil som skulle inneholde informasjon relatert til stillingsutlysningen. Disse filene ble delt direkte gjennom meldingstjenesten på LinkedIn, eller over e-post med en OneDrive-link. Kjøring av den ondsinnede filen ville gi aktøren tilgang til maskinen.

NSM anbefaler å være forsiktig med å åpne filer med ukjent opphav, være kritiske til uoppfordret kontakt over både e-post og sosiale medier, samt minner om at privatutstyr kan være like utsatt som utstyr eid av arbeidsplassen.

[7] *Et vannhull er en tilsynelatende legitim nettside som leverer skadevare til utpekte mål.*

Myndigheter og sikkerhetsindustrien har advart mot phishing i flere år.

eksempel være feil i nettverks-, klient- og server-konfigurasjon, svake autentiseringsmekanismer, svak styring av rettigheter og manglende sikkerhetsoppdatering. NSM har i flere år rapportert om at det er kjente sårbarheter som benyttes for gi uautorisert tilgang til systemer og nettverk. Det digitale risikobildet preges fremdeles av dette.

Manglende oppdateringer av systemer og tjenester kan gi en aktør uautorisert tilgang til virksomhetens systemer. Direkte innbrudd i sårbare, internetteksponerte tjenester er en vanlig inngangsvektor. NCSC har bistått flere virksomheter med hendelser, hvor manglende oppdateringer er direkte årsak til kompromittering.

NCSC sender jevnlig ut sårbarhetsvarsler til sine mottakere. Fra januar til august 2020 ble det sendt ut over 55 slike varsler, som er tilnærmet likt antallet for samme periode i 2019. Norske virksomheter oppfordres til å melde seg på denne varslingslisten ved å kontakte NCSC.

SÅRBARHETSKARTLEGGING – ALLVIS NOR[8]

Allvis NOR er NSMs automatiserte sårbarhetskartlegger. Tjenesten tilbys offentlige virksomheter og eiere av kritisk infrastruktur, og består i hovedsak av regelmessig kartlegging og sårbarhetsundersøkelse av innmeldte IP-adresser som er tilgjengelige på internett.

Allvis NOR gir NSM et mer helhetlig situasjonsbilde og er et viktig bidrag i videreutvikling av sikkerhetsarbeidet.

NSM anbefaler at alle virksomheter som ivaretar grunnleggende nasjonale funksjoner benytter seg av Allvis NOR.

PHISHING-KAMPANJE – ET EKSEMPEL FRA FORSKNINGS- OG UTDANNINGSSEKTOREN

Forsknings- og utdanningssektoren har gjennom 2020 vært mål for en avansert, utenlandsk aktør. Angrepene bruker e-post og falske nettsider tilpasset den enkelte virksomhet, og har som mål å «høste» brukernavn og passord som gir tilgang til interne ressurser. Aktøren retter seg mot universiteter og forskningsmiljø i flere vestlige land, og samarbeid mellom sikkerhetsmiljø på tvers av landegrensene har vært avgjørende for å forstå framgangsmåten i Norge. Som sektorens responsmiljø, har Uninett CERT jobbet tett med sektoren og internasjonale samarbeidspartnere for å oppdage, forhindre og ikke minst bedre forstå kampanjene. Dette har gjort det mulig å flere ganger sette i gang forebyggende tiltak før angrepene kommer.

[8] *Allvis NOR:* https://nsm.no/tjenester/allvis-nor/

NCSC observerte i 2020 at avanserte aktører kartla sårbarheter i enkelte tjenester for fjernpålogging, og at aktiv utnyttelse inntraff flere måneder etter.

De fleste leverandører varsler jevnlig om nye sårbarheter i sine produkter og tjenester. De aktuelle produkter og tjenester må oppdateres for å redusere risiko og lukke sårbarheten så raskt som mulig. NCSC erfarer at det er et kort tidsrom fra en sårbarhet varsles til den kan utsettes for aktiv utnyttelse av trusselaktører.

NCSC har i 2020 sett aktiv utnyttelse av kjente sårbarheter i ulike fjernaksessløsninger, for eksempel ved hjemmekontorløsninger, og ser at løsninger for fjernaksess er en vedvarende sårbarhet for norske virksomheter i alle sektorer. NSM har hatt spesielt fokus på dette i 2020 og under COVID-19-situasjonen. Fjernaksessløsninger til et virksomhets nettverk hjemmefra gir lik eller tilnærmet lik tilgang til virksomhetens interne tjenester og applikasjoner. Flere aktører har utnyttet sårbarhetene i slike løsninger og kan legge igjen bakdører for å beholde tilgang til systemene etter at sårbarhetene er lukket. Fjernaksessløsninger må kontinuerlig oppdateres og sikres forsvarlig. Finanstilsynet skriver også i sin *Risiko og sårbarhetsanalyse* 2020 at sårbarheter for uønskede hendelser kan øke ved bruk av hjemmekontor.[9]

NCSC observerte i 2020 at avanserte aktører kartla sårbarheter i enkelte tjenester for fjernpålogging, og at aktiv utnyttelse inntraff flere måneder etter. En slik tålmodighet i angrepsprosessen får konsekvenser for virksomhetene og hendelseshåndtering i ettertid. For å kunne håndtere hendelsen er det avgjørende at virksomheten har overvåkning av sitt nettverk i perioden fra virksomheten var sårbar til tidspunktet for aktiv utnyttelse.

SÅRBARHETER I CITRIX NETTVERKSUTSTYR – ET EKSEMPEL FRA FINANSSEKTOREN

Produkter fra Citrix brukes av mange også i finanssektoren. Mange medlemmer av Nordic Financial CERT (NFCERT) gjorde tidlig tiltak, inkludert oppdatering etter at sårbarheten i Citrix-systemer ble kjent sent i 2019. Likevel opplevde noen av disse å få enkelte Citrix-enheter kompromittert tidlig i 2020 da utnyttelseskode ble publisert og benyttet på internett. Disse kompromitteringene ble oppdaget og håndtert raskt av den enkelte finansinstitusjon, noe som forhindret at angrepene fikk spre seg lenger inn i virksomheten. Ingen av hendelsene fikk nevneverdige konsekvenser – utover behovet for hendelseshåndtering og opprydding.

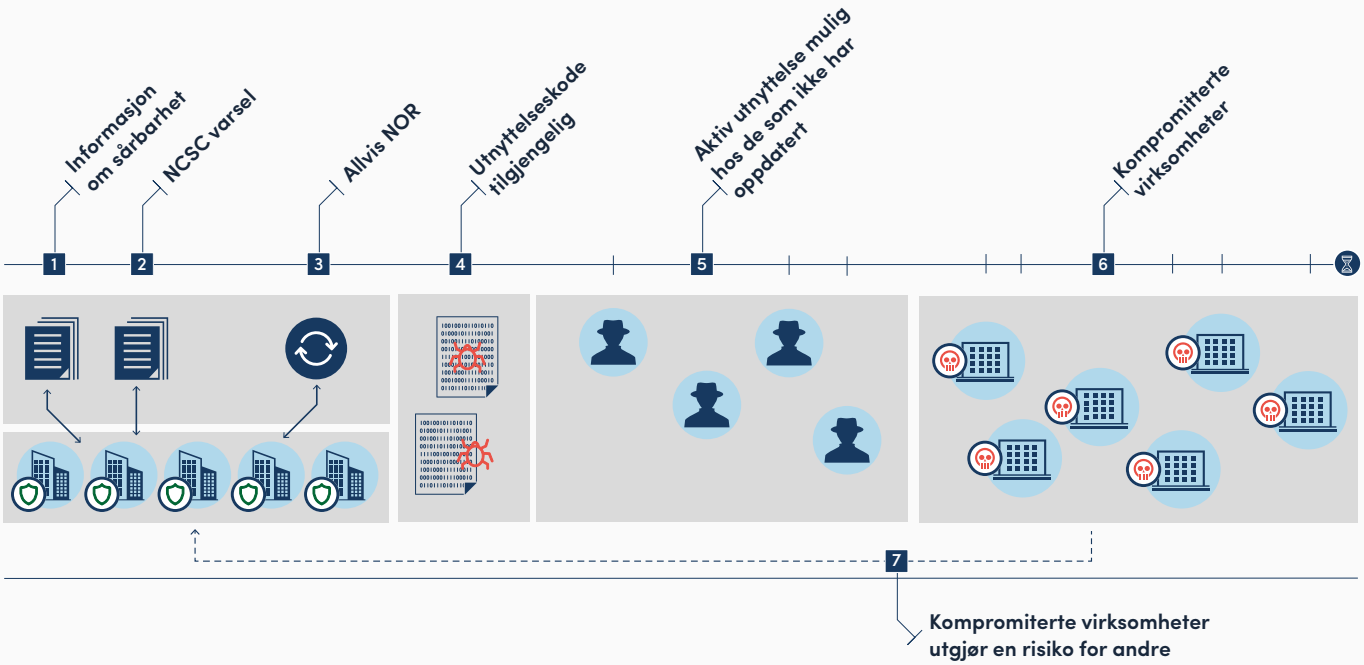
Til tross for at virksomhetene hadde rutiner for oppdatering og vedlikehold av kritiske systemer, ble de kompromittert. Disse hendelsene viser at evne til rask deteksjon og respons er en viktig del av et godt dybdeforsvar mot cyberangrep.

[9] *Finanstilsynet – risiko og sårbarhetsanalyse 2020:* https://www.finanstilsynet.no/contentassets/816cd5c4576a484ab41749a3ff985a69/risiko--og-sarbarhetsanalyse-2020.pdf

Oppdag og lukk dine sårbarheter

En åpen sårbarhet eksponert på internett kan utnyttes av ulike trusselaktører. Systemet må da oppdateres for å lukke sårbarheten. Sårbarheter kan brukes for å kompromittere et system eller nettverk hos en virksomhet, enten som et mål i seg selv eller for å kompromittere andre virksomheter.

Tiltakene er hentet fra NSMs Grunnprinsipper for IKT-sikkerhet 2.0.



1. Informasjon om sårbarhet
2. NCSC varsel (virksomheter lukker sårbarhet)
   - Tiltak 3.1 Oppdag og fjern kjente sårbarheter og trusler
   - Tiltak 3.1.1 Gjennomfør jevnlig sårbarhetskartlegging
   - Tiltak 3.1.2 Abonner på tjenester relatert til sårbarhetsetterretning
3. AllvisNor skanner etter sårbarhet
   - Tiltak 3.4.3 Benytt verktøy for sårbarhetskartlegging og angrepsverktøy
4. Utnyttelseskode gjøres tilgjengelig
5. Aktiv utnyttelse mulig hos de som ikke har lukket sårbarhet (sårbarhet nå åpen)
   - Tiltak 2.3.1 Etabler et sentralt styrt regime for sikkerhetsoppdatering
6. Trusselaktører kan kompromittere virksomheter med åpen sårbarhet
7. Rammede virksomheter kan brukes til å kompromitere virksomheter som har lukket sårbarheten, med andre inngangsmetoder

NCSC har i 2020 sett operasjoner med påloggingsforsøk av internetteksponerte tjenester ved hjelp av såkalt «brute-force», hvor en aktør prøver å logge inn med ofte brukte brukernavn og passord. Det anbefales å sørge for at virksomhetene har sikkerhetssystemer som fanger opp store mengder feilpåloggінger, aktiverer flerfaktor-autentisering og begrenser mengden eksponerte tjenester der dette er mulig. Systemer for å oppdage «mistenkelige» påloggінger, som for eksempel kan forby pålogging fra utenlandske IP-adresser har vist seg effektive for å minimere konsekvensen dersom brukernavn og passord kommer på avveie. NSM har gitt ut råd om sikre passord på sine nettsider.[10]

NSM er bekymret for et økende antall sårbarheter i mobile enheter og IoT-enheter («tingenes internett»).[11] Internasjonalt har man sett eksempler på kompromitteringer av godt sikrede IKT-systemer hvor sårbarheten som ble utnyttet var enkle IoT-enheter tilknyttet nettverket. IoT-enheter er utviklet med et funksjonalitets- og kostnadsfokus, og er ofte dårlig sikret. Slike enheter kan ha iboende sårbarheter og svak grunnkonfigurasjon, hvor for eksempel standardpassord ikke er endret. Når de kobles opp mot godt sikrede IKT-systemer, introduserer de nye sårbarheter i eksisterende infrastruktur. Virksomheter må sørge for forsvarlig sikring av IoT-enheter, eller implementere andre sikringsmekanismer for å minimere risikoen. NSM forventer at utnyttelse av sårbarheter i slike enheter vil øke i tiden fremover.

Utvikling i modus operandi

Hovedtrekkene i det digitale risikobildet sammenfaller i stor grad med trendene observert de siste årene. Likevel ser NCSC utvikling i metodene som benyttes mot norske mål.

Verktøykassen til en trusselaktør kan være stor og variert. Verktøy kopieres, etterliknes og gjenbrukes av ulike aktører. Dette gjør det utfordrende å vite hvem som står bak en nettverksoperasjon. Noen verktøy er fritt tilgjengelige på internett. Andre verktøy baserer seg på åpen tilgjengelig kildekode, men blir endret og tilpasset av aktøren før bruk. I tillegg finnes det verktøy som er spesialutviklet til et angrepsmål.

Både tilpassede og spesialutviklede verktøy er observert mot norske mål i 2020. Et eksempel er verktøy som en aktør kan benytte for å skjule lateral bevegelse i nettverket til en virksomhet. I tillegg har det vært observert at eldre verktøy

Tidligere har NCSC sett utstrakt bruk av infrastrukturer som var gjenkjennbare fra tidligere. Det siste året har NCSC sett at infrastruktur i noen tilfeller ikke gjenbrukes, men etableres på nytt for hver nettverksoperasjon.

[10] *Passordråd for personer og virksomheter:* https://nsm.no/aktuelt/passordrad-for-personer-og-virksomheter

[11] *13 råd om sikkerhet på mobile enheter:* https://nsm.no/aktuelt/13-rad-om-sikkerhet-pa-mobile-enheter

brukes mot eldre operativsystemer som ikke er oppdatert.

Trusselaktører bruker ofte komplekse digitale infrastrukturer for å utøve digitale operasjoner mot norske virksomheter. Det er slik aktørene kan kompromittere sine mål, utføre kommando- og kontroll av operasjonene, få tilgang til å plassere skadevare, eller på annen måte utnytte sårbarheter og hente ut informasjon fra systemene. I noen tilfeller øker trusselaktørene egen operasjonssikkerhet og reduserer risiko for å bli oppdaget eller identifisert ved å bruke kryptert kommunikasjon. Tidligere har NCSC sett utstrakt bruk av infrastrukturer som var gjenkjennbare fra tidligere. Det siste året har NCSC sett at infrastruktur i noen tilfeller ikke gjenbrukes, men etableres på nytt for hver nettverksoperasjon. Disse forholdene vanskeliggjør arbeid med å avdekke nye operasjoner.

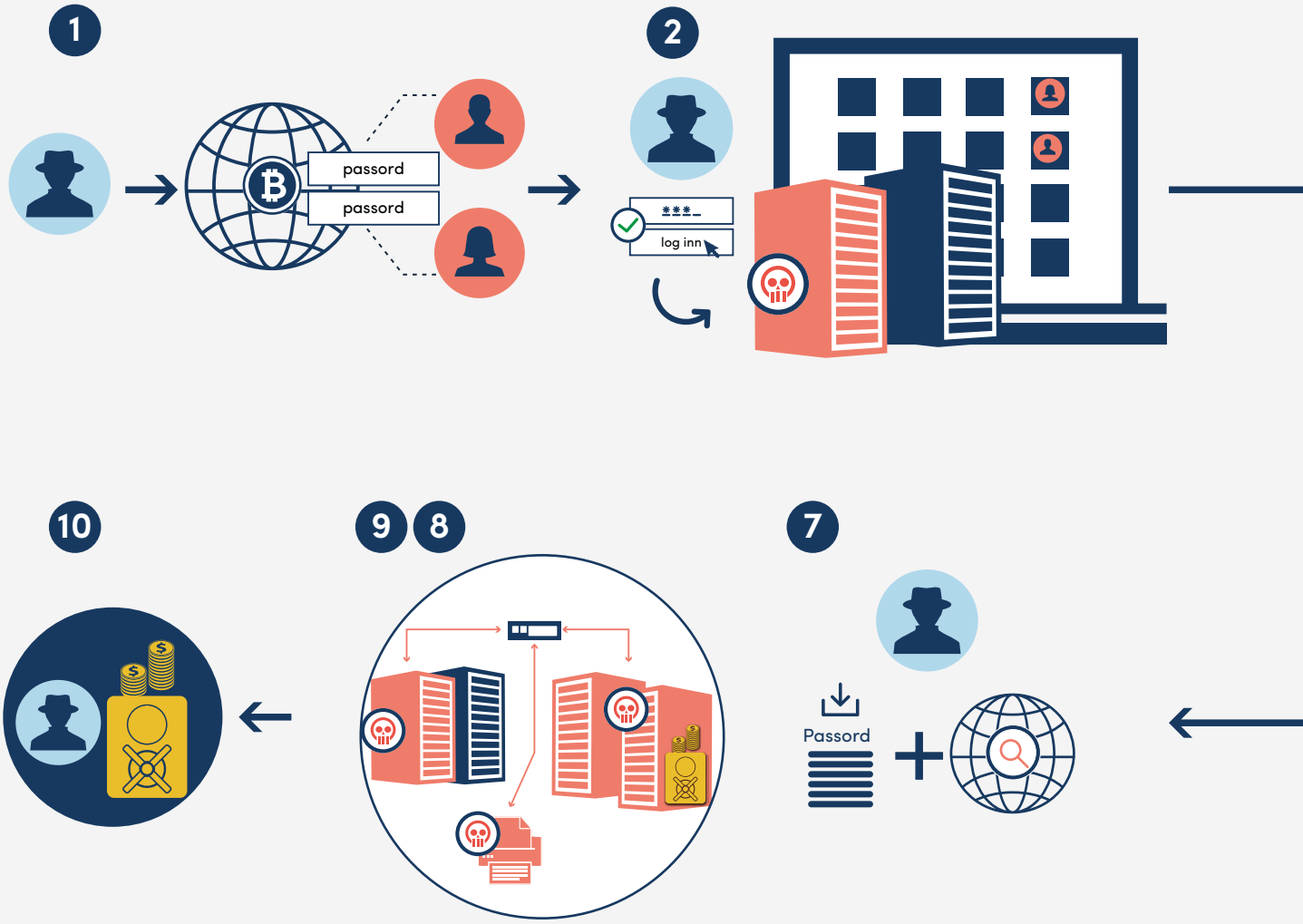
Det har vært tilfeller hvor intetanende norske virksomheter blir brukt som en del av komplekse infrastrukturer i operasjoner mot mål i andre land. Det er også eksempler på at ondsinnede aktører benytter infrastruktur som har vært fremleid i mange ledd, såkalt «bullet proof hosting», i sine nettverksoperasjoner. I datahaller med utleie av infrastruktur, servere og serverkapasitet er det per i dag ikke krav om at det føres oversikt over fremleie. Vertstjenester kan leie ut serverplass til en kunde som deretter kan fremleie plassen til andre, og infrastruktur kan være fremleid i flere ledd. Dette gjør det utfordrende å spore bakmenn, og potensielt alvorlig kriminalitet vil i praksis ha lav oppdagelsesrisiko. Manglende synlighet og oversikt vanskeliggjør håndtering ved denne typen misbruk.

Måten skadevare blir brukt på er under utvikling. NCSC erfarer at aktører benytter skadevare for å få initiell tilgang til et IKT-system og oppnå administratorrettigheter. Deretter kan aktørene bruke legitime verktøy som allerede ligger på systemet for videre aktivitet. For eksempel kan det benyttes legitime administratorverktøy for å slette eller endre logger på systemene for å vanskeliggjøre deteksjon. NSM anbefaler at slike verktøy kun er tilgjengelige der det er et reelt behov.

NCSC understreker at utviklingstrekkene er basert på observert aktivitet mot norske mål. Det er grunn til å tro at flere digitale operasjoner forblir uoppdaget hvert år. Likevel kan observasjonene være en indikator på hvor utviklingen går i det digitale domenet. Samarbeid med virksomhetene på tvers av sektormyndigheter samt partnersamarbeid er derfor vesentlig for å kunne vurdere det helhetlige situasjonsbildet.

Det må forventes at utviklingen av digitale trender vil utnyttes av aktører og at dette vil forsterkes i tiden fremover. Et eksempel er at IoT-enheter i økende grad vil kunne utnyttes av aktører for å etablere infrastruktur som brukes i nettverksoperasjoner mot mål i Norge. I slike systemer er IoT-enheter koplet til samme infrastruktur som mer avanserte enheter, som igjen har tilgang til systemer som bearbeider, systematiserer og analyserer informasjonen. Dermed introduseres sårbarheter i systemer som for eksempel kan benyttes til samfunnskritiske funksjoner. Verdiene som forvaltes i systemer der tjenester digitaliseres og automatiseres er store, og konsekvensen ved kompromitteringer kan bli alvorlige.

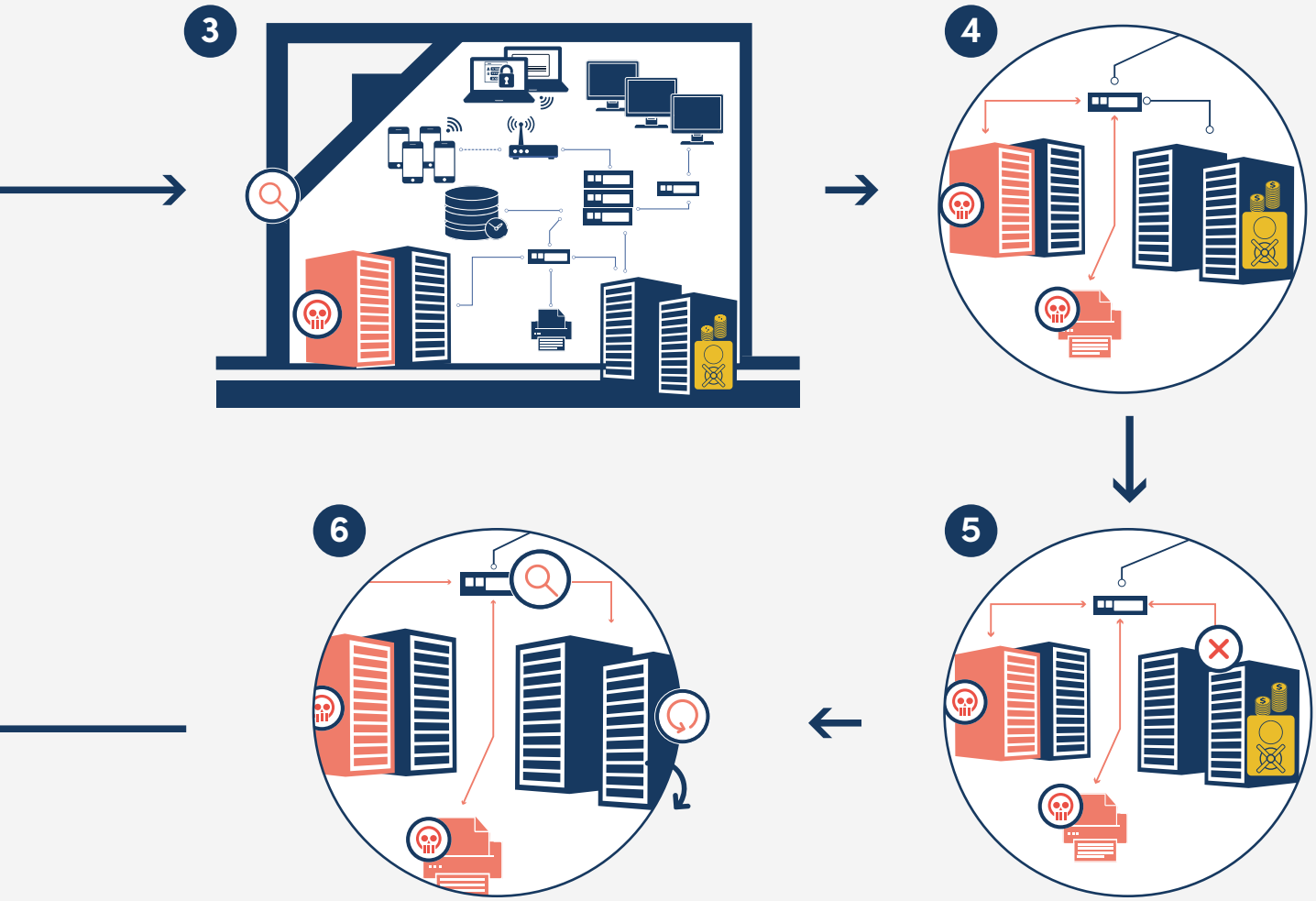
Digital operasjon mot norsk virksomhet



1. Aktør får tak i påloggingsinformasjon til to brukere for fjernaksessløsning ved hjelp av passorddump, kjøpt på Internett eller ved brute-force
   - Tiltak 2.6.6 Styr tilgang til enheter
   - Tiltak 2.6.7 Bruk multi-faktor autentisering
2. Aktør bruker påloggingsinformasjonen til å logge på fjernaksessløsning til virksomheten og får tilgang til virksomhetens nettverk
   - Se tiltak punkt 1
3. Aktør gjør initiell kartlegging av virksomhetens nettverk for videre lateral bevegelse
   - Tiltak 2.2.3 Del opp virksomhetens nettverk etter virksomhetens risikoprofil
   - Tiltak 2.5 Kontroller dataflyt
   - Tiltak 3.2 Etabler sikkerhetsovervåkning
   - Tiltak 3.3 Analyser data fra sikkerhetsovervåkning
4. Aktør utnytter gamle, offentlig tilgjengelige sårbarheter til «glemte» enheter eller som er dårlig sikret av IT
   - Tiltak 1.2 Kartlegg enheter og programvare
   - Tiltak 2.3.7 Endre alle standardpassord
   - Tiltak 2.3 Ivareta en sikker konfigurasjon
   - Tiltak 2.2 Etabler en sikker IKT-arkitektur
   - Tiltak 2.2.3 Del opp virksomhetens nettverk etter virksomhetens risikoprofil
5. Aktøren prøver å få tilgang til virksomhetens verdier (adskilt), men lykkes ikke
   - Tiltak 2.5 Kontroller dataflyt
   - Tiltak 2.6 Ha kontroll på identiteter og tilganger

Et typisk hendelsesforløp med teknikker trusselaktører har brukt mot norske virksomheter.

Tiltakene er hentet fra NSMs Grunnprinsipper 2.0.



6. Aktøren går tilbake til første tilgangspunkt (del av kontornettverk) og kartlegger mer
   - Tiltak 2.5.1 Styr dataflyt mellom nettverkssoner
   - Tiltak 3.2 Etabler sikkerhetsovervåkning
   - Tiltak 3.3 Analyser data fra sikkerhetsovervåkning
7. Aktøren finner nettverksenhet med leverandør-standardpassord som finnes på Internett, logger på nettverksenhet, henter konfigurering og får liste med brukernavn og passord
   - Tiltak 2.3.7 Endre alle standardpassord
   - Tiltak 2.1.2 Kjøp moderne og oppdatert maskin- og programvare
8. Aktøren beveger seg tilbake i nettverket via glemte enheter
   - Se tiltak punkt 3
9. Aktøren bruker passord hentet fra nettverksenheten og får tilgang til virksomhetens verdier
   - Tiltak 2.6 Ha kontroll på identiteter og tilganger
   - Tiltak 2.6.1 Etabler retningslinjer for tilgangskontroll
10. Aktøren kan endre/manipulere virksomhetens verdier og/eller hente ut verdiene
    - Tiltak 2.6 Ha kontroll på identiteter og tilganger
    - Tiltak 2.6.4 Minimer rettigheter til sluttbrukere og spesialbrukere
    - Tiltak 1.1.3 Identifiser virksomhetens prosesser for risikostyring knyttet til IKT

Mange virksomheter har blitt bedre – andre henger etter

Norske virksomheter blir mer sikkerhetsbevisste – de identifiserer tiltak og iverksetter disse i større grad. Ifølge Mørketallsundersøkelsen 2020 oppgir syv av ti virksomheter at de har et rammeverk eller et styringssystem for informasjonssikkerhet. Det er en økning fra 2016 og 2018, da rundt seks av ti virksomheter oppgav at de hadde det. Likevel, i møte med virksomheter der NCSC bistår i hendelseshåndtering, er det ofte gjentakende utfordringer som gjør håndteringen tidkrevende og komplisert. NSM mener at det er bekymringsfullt at mange virksomheter mangler risikoreduserende tiltak helt eller delvis. Dette gjør dem sårbare for digitale operasjoner.

Mange virksomheter mangler oppdatert oversikt over egne systemer og nettverk, og hvor virksomhetens verdier befinner seg.

NSM KVALITETSORDNING FOR HENDELSESHÅNDTERING

Med etableringen av sektorvise responsmiljøer og kvalitetsordning for hendelseshåndtering er evnen til bistand i håndtering av alvorlige IKT-hendelser forbedret. Dette muliggjør hendelseshåndtering, informasjons- og erfaringsutveksling på tvers av sektorer. Virksomheter som tilfredsstiller NSM sine krav til kvalitet innen hendelseshåndtering finnes til enhver tid på NSMs nettsider.

Hva finnes av enheter og programvare? Hvor finnes nettverkskartet? Nye systemer «legges oppå» eldre systemer som i kombinasjon kan introdusere nye sårbarheter i overgangene mellom systemene som det er vanskelig å ha kontroll over. Økende avhengighet til komplekse verdi- og leverandørkjeder gjør det utfordrende å ha oversikt over den totale sårbarhetsflaten.

INNSIDERRISIKO

Ved å utnytte menneskelige sårbarheter hos personer med de rette tilgangene, vil en trusselaktør kunne skaffe seg urettmessig tilgang til informasjon, informasjonssystemer eller andre verdier det er viktig å beskytte. For en virksomhet vil en potensiell innsider være en betydelig risikofaktor.

Les mer om innsidere i NSMs temarapport *Innsiderisiko*.[12]

Utnyttelse av menneskelige sårbarheter kan fungere som inngangsvektor i en nettverksoperasjon. I juli 2020 ble en rekke offisielle og profilerte konti på Twitter misbrukt til Bitcoin-svindel. Aktørene skal ha logget på en Twitter-ansatts konto og via denne fått tilgang til et administratorpanel som gjorde det mulig å ta over andres konti. Påloggingsdetaljene skal ha blitt innhentet i en målrettet phishing-kampanje mot ansatte med tilgang til interne systemer.

[12] *Innsiderrisiko – temarapport:* https://nsm.no/getfile.php/133153-1591706148/Demo/Dokumenter/Rapporter/Temarapport%20innsiderisiko.pdf

I flere tilfeller blir NCSC varslet om en hendelse fra tredjepart hvor aktiviteten fant sted tilbake i tid. Da vil manglende logging hos virksomheten være en utfordring. Manglende logging gjør det teknisk umulig å få full oversikt over hendelsen og omfanget av kompromitteringen. Virksomhetene må ha grunnleggende deteksjonsevne og evne til å agere på mistenkelig aktivitet.

Tjenesteutsetting kan bidra til kvalitetssikring og økt sikkerhet, men innen hendelseshåndtering og forebygging ser NCSC at det er viktig at virksomheten har god tilgang til egne logger og informasjon dersom de utsettes for uønskede hendelser. Derfor er et godt avtaleverk og en tydelig definert bestilling til tjenesteleverandøren viktig. Noen virksomheter mangler beredskapsplaner og er ikke rigget for å utøve operativ håndtering. Økt sikkerhetsbevissthet og god sikkerhetskultur er viktig. Fortsatt er det mennesker som utgjør en av de største sårbarhetene og som vitende eller uvitende tilrettelegger for et vellykket datainnbrudd.

NSMs *Grunnprinsipper for IKT-sikkerhet* versjon 2.0[13] ble lansert våren 2020 og beskriver hvordan virksomheter kan beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Dette er viktig for å ivareta god grunnsikring av digitale verdier og vil igjen føre til redusert skadeomfang dersom en hendelse inntreffer. NSM er av den oppfatning at norske virksomheter blir mer robuste i møte med uønskede digitale hendelser hvis de følger rådene i Grunnprinsippene. Erfaringer det siste året underbygger denne vurderingen. I de tilfeller der NSM har utført en inntrengingstest eller bistått med hendelseshåndtering, ville tiltak fra Grunnprinsippene stoppet eller redusert konsekvensene av hendelsen hos virksomheten. Regelverksforvaltere og sektormyndigheter oppfordres derfor til å bruke Grunnprinsippene aktivt i videreutviklingen av regelverk og instrukser om IKT-sikkerhet.

VARSLINGSSYSTEM FOR DIGITAL INFRASTRUKTUR – VDI

Sensornettverket VDI[14] er et viktig redskap for å sikre den nasjonale evnen til å detektere digitale angrep i kritisk infrastruktur og samfunnsviktige funksjoner. VDI-kapasiteten ble styrket våren 2020 for å anskaffe flere VDI-sensorer til samfunnskritiske sektorer og virksomheter med særlig beskyttelsesbehov som følge av COVID-19. I perioden fram til 2023 gjennomføres også en betydelig styrking og modernisering av VDI med et særskilt fokus på forsvarssektoren.

Flere virksomheter mangler oppdatert oversikt over egne systemer og nettverk, og hvor virksomhetens verdier befinner seg.

[13] *Grunnprinsipper for IKT-sikkerhet:* www.nsm.no/grunnprinsipper-ikt

[14] *Varslingssystem for digital infrastruktur.*

I de tilfeller der NSM har utført en inntrengingstest eller bistått med hendelseshåndtering, ville tiltak fra Grunnprinsippene stoppet eller redusert konsekvensene av hendelsen hos virksomheten.

Internasjonalisering øker kompleksiteten

Internasjonalisering utfordrer tradisjonell nasjonal tankegang og definerte sektorprinsipper. Internasjonale verdikjeder og komplekse digitale infrastrukturer gjør at operasjoner mot infrastruktur i ett land kan påvirke infrastrukturen i et annet. Dette gjelder særskilt for store virksomheter med omfattende nettverk og strukturer som spenner på tvers av flere landegrenser. Norske virksomheters verdier befinner seg ikke bare i Norge, men i et stadig mer integrert, omfattende og internasjonalt bilde. Selskapsstrukturer splittes i underselskaper med forgreininger over landegrenser. Vet vi hvor våre virksomheters verdier egentlig befinner seg? Det er en risiko for at norske verdier kan utsettes for nettverksoperasjoner langt utenfor våre landegrenser.

Som en del av dette bildet, med utgangspunkt i digitaliseringsprosessen og økende verdikjeder, er skytjenester og tjenesteutsetting helt sentrale momenter og tema for neste kapittel.

ERFARINGER FRA KRAFTBRANSJEN

Antall KraftCERT-relatert saker og henvendelser steg med 51 % til 2625 i 2019. Antallet utsendte varsler fra KraftCERT økte til 222 i 2019, der hvert varsel kan dekke flere saker.

Antallet hendelser der det ble iverksatt full hendelseshåndtering steg med 49 % til 168 i 2019, og KraftCERT har gjort følgende observasjoner:

- Det har vært et jevnt høyt nivå av kartlegging/rekognosering.
- Det har vært bruk av innlogginger med brute-force, mye mot *Microsoft-365*. Noen av angrepene benyttet brukernavn/passord som åpenbart stammet fra eldre lekkasjer, sannsynligvis de større og kjente lekkasjene (Linkedin, Yahoo osv.) De fleste hendelsene fikk ingen konsekvenser, men noen fikk konsekvens i form av kompromitterte brukerkonti.
- Vedlegg med skadevare inkludert lenker til skadevare. Noe slipper gjennom sikkerhetssystemene som skal stoppe og filtrere bort slike vedlegg.
- Det har vært flere hendelser med kompromitterte leverandører, alt fra små selskaper som elektrikerfirmaer, til produsenter av utstyr, tjenesteleverandører eller infrastrukturleverandører. Hvor sofistikert dette er, varierer fra e-post på et annet språk, til svært plausible norske emnefelt, eller kapring av eksisterende diskusjoner.
- Fakturasvindel og phishing via sosiale medier (profesjonsmedier).

Ingen av hendelsene NVE eller KraftCERT har registrert har ført til problemer med forsyningssikkerheten av elektrisitet eller fjernvarme.

Erfaringer fra NSMs inntrengingstesting 2019 – 2020

NSM har opplevd at en trusselaktør med tilgang til et spesifikt nettverk i en virksomhet kan utnytte sårbarheter for å få fotfeste i andre nettverk. Adskilte sikkerhetssoner i et nettverk, og implementasjon av tonivåløsning for tilgang til nettverk fra internett reduserer sårbarhetsflaten og gjør videre bevegelse i nettverket vanskeligere.

NSM har i sine inntrengingstester fått kontroll over virksomheters systemer ved bruk av ulike teknikker. Dette gjelder ikke bare ved bruk av egenutviklede angrepsteknikker, men også ved bruk av offentlig tilgjengelige teknikker. En trusselaktør med slik tilgang har i teorien mulighet til å endre data, hente ut beskyttelsesverdig informasjon, stjele passord og manipulere informasjon. Tilgang til sentralt nettverksutstyr kan gi en aktør mulighet til å sette deler av nettverket ut av spill. I mange tilfeller kan slike handlinger utføres over internett og krever ikke fysisk tilgang til nettverket.

Passordsikkerhet er en vedvarende utfordring. Gjenbruk av passord på ulike konti, som brukerkonti og administratorkonti, svekker sikkerheten. Sterke passordregimer er viktig, og det er viktigere å lære brukere å sette gode og sterke passord enn å kreve at brukere skifter passord ofte. NSM har empiri på at passord som må byttes ofte blir svakere fordi brukere lager enklere passord eller benytter mønstre som er enkle å huske. Mange tjenester og løsninger kommer ferdig med strandardpassord fra leverandøren. For en trusselaktør kan disse være enkle å gjette eller finnes på internett.

Inntrengingstester har avdekket tilfeller hvor virksomhetens servere mangler kritiske sikkerhetsoppdateringer. Eldre operativsystemer mangler ofte sikkerhetsfunksjonaliteter som finnes i nyere versjoner. Oppdaterte og oppgraderte klienter er bedre herdet enn de som ikke er det. Gjenbruk av passord på flere klienter og servere øker sårbarheten i et system.

Inntrengningstester det siste året har også avdekket sårbarheter og svakheter i støttesystemer. Dette kan gi en trusselaktør med begrenset tilgang, som utviklertilgang, muligheter til å utvide egne rettigheter for å oppnå tilgang til sentrale driftstjenester. Dette kan føre til ytterligere kompromitteringer i nettverk og systemer.

NSM utnytter kjente sårbarheter i applikasjoner og operativsystemer i sine inntrengingstester. I flere tester utført sist år fant NSM flere komponenter i virksomhetens infrastruktur som ikke lar seg oppdatere fordi supporten på produktet for lengst har opphørt.

I noen tilfeller har tester vist at tilfeldig utstyr ukritisk kan kobles til nettverket – dette svekker sikkerheten. Manglende sperrer mot å koble til uautorisert utstyr gjør systemer unødvendig sårbare, og setter større krav til fysisk sikkerhet.

Bruk av e-post som inngangsvektor lykkes fortsatt. E-post med lenke til nettside hvor brukeren oppgir brukernavn og passord muliggjør pålogging til systemer. E-post med vedlagt skadevare muliggjør kjøring av denne på klienter koblet mot interne nettverk hos virksomheten. Denne tilgangen kan benyttes for å gjennomføre videre kompromitteringer mot andre maskiner i nettverket fra internett.

Videre avdekker inntrengingstester også i år at virksomheter har mangelfull skjerming av konfigurasjonsdata og passord og at det er for lite oppmerksomhet og forståelse for dette. En trusselaktør som har inngående informasjon om et system, vil ha bedre forutsetning for å lykkes med et angrep enn en som ikke har det.

Erfaringer fra NSMs inntrengingstestinger en del av grunnlaget for rådene i *NSMs Grunnprinsipper for IKT-sikkerhet.*

Jørgen Botnan, seksjonssjef Inntrengningstesting, NSM

15 prioriterte tiltak fra *NSMs Grunnprinsipper for IKT-sikkerhet 2.0*

NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0 inneholder tilsammen 118 sikkerhetstiltak. NSM har registrert ønsker om hjelp med prioritering av disse sikkerhetstiltakene. NSM har derfor publisert et støtteprodukt som angir prioritet på tiltakene. Tiltakene er fordelt på 3 grupper, hvor gruppe 1 inneholder 15 tiltak som ansees å gi sikkerhetsmessig størst effekt.

1. Kartlegg enheter i bruk i virksomheten.
2. Kartlegg programvare i bruk i virksomheten.
3. Kjøp moderne og oppdatert maskin- og programvare.
4. Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.
5. Del opp virksomhetens nettverk etter virksomhetens risikoprofil.
6. Etabler et sentralt styrt regime for sikkerhets-oppdatering.
7. Konfigurer klienter slik at kun kjent programvare kjører på dem.
8. Deaktiver unødvendig funksjonalitet.
9. Endre alle standardpassord på IKT-produktene før produksjons-setting.
10. Minimer rettigheter til sluttbrukere og spesialbrukere.
11. Minimer rettigheter på driftskontoer.
12. Legg en plan for regelmessig sikkerhets-kopiering av alle virksomhetsdata.
13. Avgjør hvilke deler av IKT-systemet som skal overvåkes.
14. Beslutt hvilke data som er sikkerhetsrelevant og bør samles inn.
15. Etabler et planverk for hendelses-håndtering.

For mer informasjon se www.nsm.no/grunnprinsipper-ikt

3. Skytjenester og tjenesteutsetting – muligheter og utfordringer

Bruken av skytjenester er fortsatt en tydelig trend og forventes å øke. Når virksomheter skal fornye eller utvikle egen IKT-infrastruktur og egne tjenester er bruk av skytjenester ofte et foretrukket valg. Enkelte ganger står virksomheter overfor situasjoner hvor tjenestene kun tilbys fra skyen. Argumenter som taler for bruk av skytjenester er mange, og NSM erfarer at lavere og bedre kontroll på kostnadene ofte er en primærdriver. Det tradisjonelle datarommet kan være avleggs om få år for de fleste virksomheter. Skillet som vi i dag bruker mellom lokale «tradisjonelle» IKT-løsninger og skytjenester vil viskes ut. Bruk av skytjenester er kommet for å bli, men det er viktig å ikke se seg blind på lavere kostnader alene.

Begrepet «sky» og «skytjenester» favner vidt og benyttes for en rekke ulike teknologier, forretningsmodeller og leverandørkonstellasjoner. *Nasjonal strategi for bruk av skytjenester*[15] omtaler skytjenester som:

«…skalerbare tenester som blir leverte over nett. Den viktigaste forskjellen på skytenester og meir tradisjonell tenesteutsetting er forretningsmodellen, der kunden berre betaler for den kapasiteten han har brukt. Målet er å tilby kostnadseffektive, sikre, skalerbare IT-tenester til kundane.»

NSM er positive til at virksomheter i større grad benytter skytjenester såfremt virksomheten har gjort gode og riktige vurderinger i forkant av beslutningen. Fordelene er større enn ulempene for de aller fleste. Skyløsninger er ofte basert på ny teknologi med tilgjengelige sikkerhetsmekanismer, og skytjenesteleverandørene har kapasitet til nødvendig vedlikehold og oppdateringer. Skytjenesteleverandører har som regel et profesjonelt drevet driftsmiljø med egen sikkerhetsorganisasjon, utfører sikkerhetsrevisjoner og har tredjepartssertifiseringer. Kjøp av enkelte skytjenester kan være bedre enn å utvikle og vedlikeholde tjenestene selv i egen virksomhet. Alle virksomheter må imidlertid være bevisst på hva de tjenesteutsetter, gjøre gode verdivurderinger og vurdere hvilken risiko det innebærer.

Bedre digital sikkerhet hos virksomhetene gjør samfunnet mer motstandsdyktig mot det stadig skiftende trussellandskapet. Bruk av skytjenester kan i så måte bidra til å redusere risiko, spesielt for mindre virksomheter som ikke har kompetanse eller ressurser til digitalt sikkerhetsarbeid selv. NSM erfarer at flertallet av uønskede hendelser relatert til skytjenester ikke skyldes feil eller sårbarheter hos skytjenesteleverandøren, men skyldes mangler eller feil i konfigurasjon eller bruk av skytjenesten. Skytjenester må derfor brukes riktig, noe som krever kompetanse og ressurser.

Skyløsninger er ofte basert på ny teknologi med tilgjengelige sikkerhetsmekanismer, og skytjenesteleverandørene har kapasitet til nødvendig vedlikehold og oppdateringer.

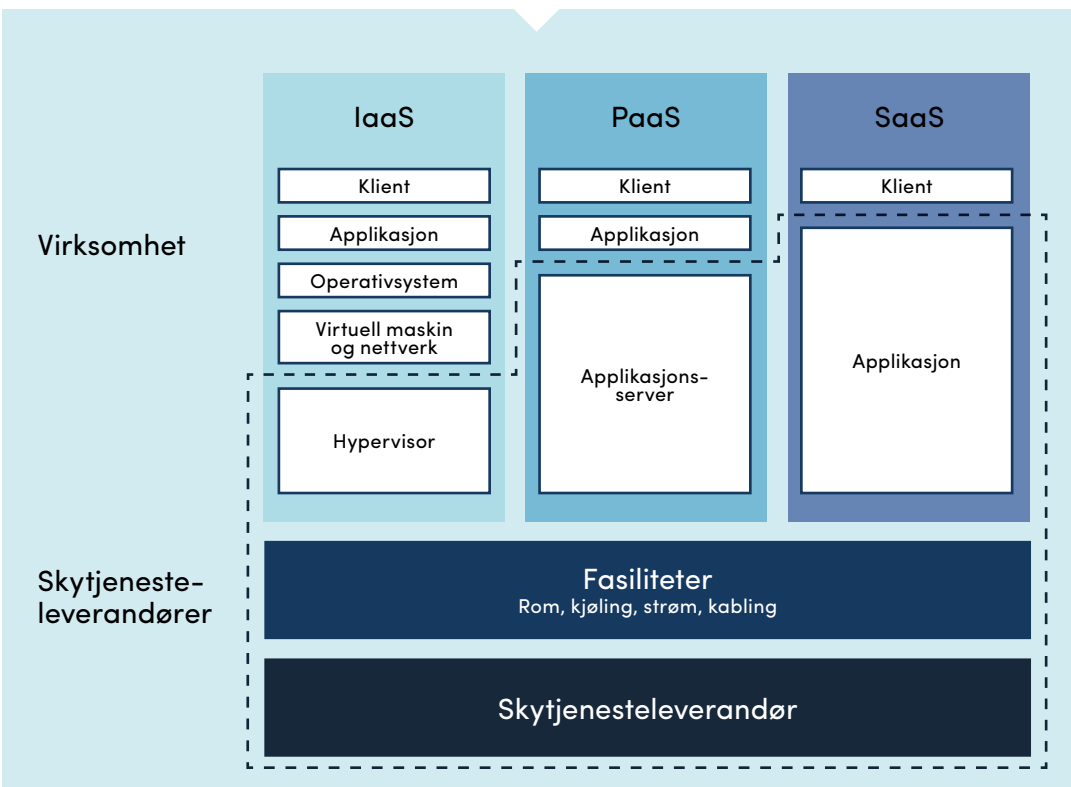
[15] *Nasjonal strategi for bruk av skytjenester:* https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-bruk-av-skytenester/id2484403/

Utenlandske skytjenesteleverandører bærer alt i dag viktige norske samfunnsfunksjoner.

Viktigheten av sikkerhetsstyring og bestillerkompetanse

Økt bruk av skytjenester bringer også med seg nye sårbarheter og økt risiko på andre områder. En migrering av eksisterende tjeneste («lift-and-shift») som er utdatert og sårbar er like sårbar om den kjører lokalt i datarommet eller om den kjører hos en skytjenesteleverandør. I enkelte tilfeller kan sårbarhetene *øke* ved bruk av skytjenester. Eksempelvis kan mange eldre IKT-tjenester, som ikke er laget for skyen, medføre økt sårbarhet og risikovandring ved å gi de økt eksponering fra en skytjeneste. Selv om eksisterende applikasjoner kan virtualiseres ved hjelp av relativt enkel lift-and-shift, er dette ikke alltid en like god løsning på lengre sikt. Virksomheten har i henhold til ansvarsprinsippet det hele og fulle ansvaret for sikring av egne verdier, også ved bruk av skytjenester, og vil selv ha et delansvar avhengig av hva slags tjenestemodell som benyttes:

- **Software-as-a-service (Saas):** Virksomheten har selv ansvar for å sikre data og tilgangsstyring.
- **Plattform-as-a-service (PaaS):** Virksomheten har selv ansvar for å sikre data, tilgangsstyring og programvare/applikasjoner.
- **Infrastructure-as-a-service (IaaS):** Virksomheten har selv ansvar for å sikre data, tilgangsstyring, programvare/applikasjoner, operativsystem og nettverkstrafikk.



Graden av kontroll mellom virksomhet og skytjeneste-leverandør avhenger av type skytjeneste. Alt utenfor den stiplede linjen må virksom-heten selv sikre.

En underskog av skybaserte tjenester vokser nå frem, og disse er ofte leverandørspesifikke.

En underskog av skybaserte tjenester vokser nå frem, og disse er ofte leverandørspesifikke. Tjenester kan integreres, og muliggjør stor grad av innovasjon og kreativitet, som er kostnadsbærende selv for små virksomheter. Dette skaper også et uoversiktlig bilde av avhengigheter og verdikjeder for virksomheten selv. Kompleksiteten kan øke hvis virksomheten bruker og integrerer tjenester både fra ulike skytjenesteleverandører kombinert med noe «lokalt» og fra eget datasenter.

Ved utstrakt bruk av skytjenester er det lett å miste forståelsen av teknologien som bærer skytjenestene. I tillegg kan virksomhetens egen evne til å kravstille og følge opp leveransene svekkes. Det kan være krevende å forstå hvilken sikkerhetsfunksjonalitet som tilbys og om disse er relevante for virksomhetens behov. Når skytjenester understøtter virksomhetens forretningsprosesser, blir disse tjenestene strategisk viktig å ha kontroll på. Da er det særlig viktig å ha god sikkerhetsstyring og bestillerkompetanse ved bruk av skytjenester. For mer informasjon vises det til NSMs temahefte *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting*.[16]

Behovet for nasjonal kontroll

For noen virksomheter bør bruk av skytjenester også vurderes opp mot nasjonal kontroll og krisespennet. Med krisespennet mener vi i fred, krise, konflikt og krig. Vil tjenesten kunne fungere i hele krisespennet? Må den fungere i hele krisespennet? Kan tjenesten/verdiene flyttes raskt «hjem» ved en eskalering? Samtidig kan bruk av skytjenester med backup i andre land medføre fortsatt tilgjengelighet ved utfall av IKT-systemer innenfor landets grenser. Bildet er sammensatt.

Noen virksomheter vil sikkert måtte vurdere behovet for nasjonal kontroll allerede i en lavere del av krisespennet, mens andre vil se det som viktig først ved en eskalering. Noen IKT-systemer er så kritiske for samfunnet at de må fungere i hele krisespennet. Dette kan bety at det for enkelte typer tjenesteutsetting må stilles større krav til robusthet og tilgjengelighet enn det som tilbys i vanlige kommersielle skytjenester.

NSM er bekymret for den samlede nasjonale avhengigheten av utenlandske skytjenesteleverandører. Den første bekymringsaksen er hvorvidt virksomheten selv gjør gode og riktige vurderinger før de velger å tjenesteutsette. Her har NSM og andre kommet med gode råd og anbefalinger.[17] Selv om alle virksomheter følger våre råd og anbefalinger og gjør riktige vurderinger isolert sett, så vil mange virksomheter kjøpe skytjenester fra en håndfull store utenlandske private selskaper. De aller fleste av disse har ikke installasjoner på norsk jord og tilbyr sine tjenester fra utlandet. Selv ved etablering av datasentre på norsk jord vil utvikling og drift av disse ofte skje fra utlandet.[18]

Den andre bekymringsaksen er at resultatet over tid kan bli at flertallet av IKT-tjenestene til norske offentlige og private virksomheter leveres fra utlandet. Utenlandske skytjenesteleverandører bærer alt i dag viktige norske samfunnsfunksjoner. Konsentrasjonsrisikoen dette medfører kalles gjerne «too big to fail». Disse leverandørene har blitt så store i kraft av økonomisk styrke, markedsmakt og påvirkningsevne at de utgjør en betydelig maktfaktor. Flere viktige og kritiske samfunnsfunksjoner må fungere i hele krisespennet. Hvis samfunnsfunksjonene er avhengige av IKT-systemer som kjører på en utenlandsk skytjenesteleverandør, skaper det en strategisk sårbarhet som det må håndteres og planlegges for - både teknisk, juridisk og politisk.

[16] *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting:* https://nsm.no/getfile.php/133447-1591950720/Demo/Dokumenter/Rapporter/Temarapport%20Landvurdering%20tjenesteutsetting.pdf

[17] *Generelle råd for tjenesteutsetting og skytjenester:* https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/generelle-rad-for-tjenesteutsetting-og-skytjenester/skytjenesteutsetting-og-sikkerhet/

[18] *Landvurdering ved tjenesteutsetting av IKT-tjenester:* https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/landvurdering-ved-tjenesteutsetting-av-ikt-tjenester

Ved å tjenesteutsette IKT-systemer som bærer kritiske samfunnsfunksjoner, eksempelvis i form av skytjenester, kan vi komme til å svekke vår nasjonale beredskapsevne.

I takt med den økte digitaliseringen av samfunnet vil digital sikkerhet være vesentlig for å oppnå god stats- og samfunnssikkerhet. Ved å tjenesteutsette IKT-systemer som bærer kritiske samfunnsfunksjoner, eksempelvis i form av skytjenester, kan vi komme til å svekke vår nasjonale beredskapsevne. Virksomheter som benytter skytjenesteleverandører med datasentre i utlandet får dermed de fysiske installasjonene underlagt et annet lands jurisdiksjon. I tillegg vil kommunikasjonen til og fra datasentre kunne gå gjennom ett eller flere transittland. Ved eskalering i krisespennet kan det tenkes scenarioer hvor skytjeneste-leverandøren blir nødt til å omprioritere ressurser i henhold til vertslandets egne beslutninger, herunder nedprioritering av support og lagrings-/prosesserings-/nettverkskapasitet. Dette er realiteter som må hensyntas både i virksomhetens egen beredskapsplanlegging, men også i arbeidet med vår samlede nasjonale beredskap.

Samfunnssikkerhet og ny teknologi

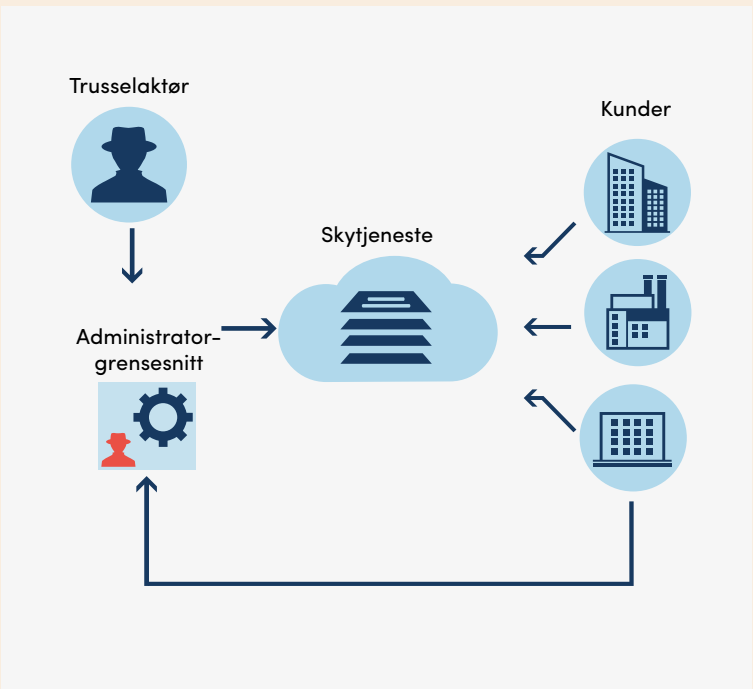
Mye av dagens, og i enda større grad morgendagens teknologileveranser, vil være avhengig av skytjenester. En rekke nye teknologitrender er på vei og vil gi virksomheter muligheter for

Skytjenester

Skytjenesteleverandøren utgjør en konsentrasjonsrisiko da de har ansvar for en rekke kunder. En attraktiv og mulig vei inn for en aktør er gjennom administratorgrensesnittet til skytjenesteleverandøren og at aktøren via denne får tilgang til skytjenesten hvor kundenes verdier befinner seg.

Kundens sikkerhetsarbeid må fortsette selv ved bruk av skytjenester. Skytjenesteleverandøren må også sørge for å ivareta forsvarlig sikkerhet av sine tjenester.

NSMs Grunnprinsipper for IKT-sikkerhet 2.0. lister en rekke tiltak som er relevante både for kunden og skytjenesteleverandøren.



Skytjenester vil være vesentlig for realisering av fremtidens teknologi og vil utgjøre sentrale bygge-klosser for morgendagens digitaliserte samfunn.

innovative digitaliseringsløft, det være seg alt fra IoT til kunstig intelligens/maskinlæring. Dette vil skape muligheter for vekst og effektivisering. Her vil bruk av skytjenester være sentralt, inkludert fremveksten av «edge computing»[19] i kjølvannet av 5G. Skytjenester vil være vesentlig for realisering av fremtidens teknologi og vil utgjøre sentrale byggeklosser for morgendagens digitaliserte samfunn. Det vil imidlertid være helt avgjørende at virksomheter vet hva de gjør og forstår konsekvensene ved bruk av skytjenester og en eventuell risiko for bortfall av disse. På et aggregert nivå vil dette ha konsekvenser for samfunnssikkerheten hvor summen av virksomheters «skyavhengighet» vil utgjøre en betydelig del av den samlede risikoen samfunnet vårt må ta innover seg. Skytjenester levert fra og med infrastruktur i Norge vil være en god start.

Arbeidet virksomhetene må gjøre for å styre egen IKT-sikkerhet, må fortsette selv ved økende bruk av skytjenester og tjeneste-utsetting. Bruk av NSMs *grunnprinsipper for IKT-sikkerhet* er et godt utgangspunkt for å øke sikkerheten ved norske virksomheters bruk av skytjenester. ■

[19] *Med edge computing her menes at neste generasjons mobilnett (5G) vil kunne tilby prosessering, lagring og nett-verkstjenester lokalt der den ønskes.*

4. Digitalisering krever styring og gode prosesser

Det stilles flere regulatoriske krav til samfunnet og virksomheter for å ivareta digital sikkerhet på en forsvarlig måte. Disse er ment for å sikre våre ulike verdier. Det er risiko knyttet til digitalisering, men denne kan håndteres ved å gjennomføre gode risikovurderinger og implementere tiltak som reduserer sårbarheter, eller reduserer konsekvenser av at sikkerhetstruende hendelser inntreffer. Det er fullt mulig å digitalisere på en sikker måte.

God forebyggende sikkerhet fordrer at virksomhetene har kunnskap om hvilke verdier som må beskyttes, enten av hensyn til egen virksomhet, andre virksomheter eller av nasjonale hensyn. Virksomhetene må avdekke egne sårbarheter og iverksette tiltak for å lukke disse sårbarhetene basert på en helhetlig risikovurdering, også utover de tiltak som regelverket stiller.

Regjeringen har iverksatt flere større tiltak for digital sikkerhet og tilrettelagt for samhandlingsarenaer på tvers av aktører. *Nasjonal strategi for digital sikkerhet*[20] med tilhørende handlingsplan, gir en god oversikt over sentrale nasjonale tiltak. Opprettelsen av NCSC i NSM og Nasjonalt cyberkrimsenter (NC3) i Kripos illustrerer myndighetenes satsning på digital sikkerhet. NCSC og NC3 skal komplementere hverandre og bidra til å konsolidere og styrke den nasjonale innsatsen i det digitale domenet.

Lovgivning om digital sikkerhet har blitt mer fleksibel

De siste årene har det kommet viktig ny lovgivning om digital sikkerhet, både i sektorlovgivning og i sikkerhetsloven. Felles for de ulike nasjonale tiltakene er at de skal gjøre virksomheter i bedre stand til å oppnå et forsvarlig sikkerhetsnivå. Lovverkene har en funksjonell innretning og gir rom for mer fleksibilitet enn tidligere.

Sikkerhetsloven baserer identifisering av sikkerhetstiltak på risikovurderinger. Følgelig er tilgang på relevant informasjon og kompetanse på gjennomføring av risikovurderinger en forutsetning for å oppnå forsvarlig sikkerhet. Økt fleksibilitet innebærer også at det stilles høyere krav til sikkerhetsfaglig kompetanse i virksomhetene. Dette innebærer at virksomheter må ha kunnskap nok til å innføre en kombinasjon av tekniske, organisatoriske og menneskelige tiltak for å oppnå en helhetlig og balansert sikring.

Grunnleggende nasjonale funksjoner

Sikkerhetsloven skal bidra til å forebygge, avdekke og motvirke tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. De nasjonale sikkerhetsinteressene er landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser.

Det er fullt mulig å digitalisere på en sikker måte.

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

Digitale verdikjeder krysser landegrenser, og koordinering og samarbeid foregår på tvers for å håndtere hendelser, utveksle informasjon og erfaringer.

Grunnleggende nasjonale funksjoner (GNFer) er *funksjoner* som, hvis de faller bort helt eller delvis, har betydning for statens evne til å ivareta disse nasjonale sikkerhetsinteressene.

Departementene skal identifisere og holde oversikt over GNFer og skal identifisere og holde oversikt over virksomheter som har avgjørende og/eller vesentlig betydning for GNFer i sine sektorer. Sektorenes arbeid med operasjonalisering av ny sikkerhetslov står sentralt i arbeidet med forebyggende sikkerhet i årene fremover. Objekter og infrastrukturer som blir utpekt som skjermingsverdige skal klassifiseres ut fra hvor alvorlige skadefølger bortfall av funksjonen kan få for grunnleggende nasjonale funksjoner. NSM bistår departementene med råd og veiledning i forbindelse med dette arbeidet.

Departementene skal også sørge for at det fattes vedtak om at loven helt eller delvis skal gjelde for virksomheter som faller inn under lovens kriterier. Dette vil gjelde dersom virksomheten råder over informasjon, informasjonssystemer, objekter eller infrastruktur eller driver aktivitet som har avgjørende betydning for GNFer, eller behandler sikkerhetsgradert informasjon. Felles for disse verdiene og aktivitetene er at de i de fleste tilfeller vil være avhengig av digitale verdikjeder og digitale informasjonssystemer som på ulike måter vil være sårbare.

Ved bruk av skytjenester og tjenesteutsetting kan det være vanskelig å imøtekomme sikkerhetslovens krav og få systemet sikkerhetsmessig godkjent hvis disse er levert fra utlandet. Det vil være avhengig av verdien til informasjonssystemet, om informasjonssystemet bærer skjermingsverdig informasjon og hvilke risikoreduserende tiltak som lar seg iverksette.

Virksomheten må vurdere ulike muligheter for å oppnå forsvarlig sikkerhet for sine skjermingsverdige informasjonssystemer. Virksomhetens risikovurdering vil ligge til grunn for valg av beskyttelsestiltak.

NSM har utarbeidet en rekke veiledere og håndbøker for å bistå virksomhetene med å etablere og opprettholde et forsvarlig sikkerhetsnivå. Disse er tilgjengelig på NSMs nettsider. For informasjonssystemsikkerhet anbefaler NSM at virksomheten tar utgangspunkt i NSMs *Grunnprinsipper for IKT-sikkerhet*. I tillegg har Justis- og beredskapsdepartementet utgitt et nasjonalt *Rammeverk for håndtering av IKT-sikkerhetshendelser*[21] for å avdekke, stanse og gjenopprette sikker tilstand etter at en hendelse inntreffer. Dette rammeverket er under revisjon av NSM, blant annet ved hjelp av sektorvise responsmiljøer og partnere i NCSC.

Samarbeid, tiltak og regelverk over landegrenser

Digitale verdikjeder krysser landegrenser, og koordinering og samarbeid foregår på tvers for å håndtere hendelser, utveksle informasjon og erfaringer. Eksempelvis er det både i Danmark, Nederland og Storbritannia etablert lignende cybersikkerhetssentre som NCSC hos NSM. For NCSC vil en viktig rolle fremover være koordinering mot disse organisasjonene.

EU tar en stadig større pådriverrolle i det digitale sikkerhetsarbeidet. Gjennom «Digital Europe Program» vil EU styrke medlemslandenes og EUs felles evne til å sikre sine digitale verdier. EU har også en aktiv rolle på den lovgivende siden med innføring av nytt harmonisert regelverk innenfor digital sikkerhet. Det er nå litt over to år siden **personvernforordningen** (GDPR) trådde i kraft i Norge og resten av Europa.

[21] *Rammeverk for håndtering av IKT-sikkerhetshendelser:* https://nsm.no/getfile.php/133853-1593022504/Demo/Dokumenter/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

Innføringen førte til økt oppmerksomhet rundt personvern, og hvordan virksomheter må arbeide for å sikre de personopplysningene de behandler. Dette har også ført til et styrket fokus på digital sikkerhet generelt. Også norske virksomheter rapporterer at de har gjort endringer i sin organisasjon som følge av GDPR. I Mørketallsundersøkelsen 2020 oppgir 84 % av virksomhetene at innføringen av nytt personregelverk (GDPR) har ført til at organisasjonen har gjort endringer og/eller forbedringer i arbeidet med personvern og informasjonssikkerhet. NCSC mener dette har bidratt til å øke den nasjonale digitale grunnsikringen. Skytjenesteleverandører har også måttet imøtekomme GDPR for sine skytjenester levert til kunder i Europa.

EU har også vedtatt **NIS-direktivet**[22] og **cybersikkerhetsforordningen (EU Cyber Security ACT)**. Begge regelverkene har trådt i kraft i EU, men arbeidet med norsk implementering pågår fortsatt. NIS-direktivet skal styrke den generelle digitale sikkerheten i Europa gjennom å kreve nasjonale responsfunksjoner (slik som NCSC), legge til rette for samhandling mellom disse og stille krav til hvordan operatører av kritisk infrastruktur sikrer sin infrastruktur og varsler ved digitale hendelser.

NIS-direktivet vil også styrke evnen til å koordinere deteksjon og håndtering av digitale kampanjer som rammer flere land. Dette vil øke situasjonsforståelsen på tvers og gi mulighet til å respondere på sikkerhetshendelser mer effektivt. Cybersikkerhetsforordningen styrker ENISAs[23] mandat og danner grunnlaget for et felles marked for sertifisering av produkter, tjenester og prosesser for cybersikkerhet.

STATSSIKKERHET OG PERSONVERN

Ofte kan statssikkerhet og personvern stå som motsetninger, for eksempel i diskusjonen rundt innføringen av tilrettelagt innhenting (TI). Samtidig kan det også være tilfeller hvor sikring av våre personopplysninger er nødvendig for å ivareta stats- og samfunnssikkerheten.

Dette kom godt til syne i NRK sine oppslag i 2020 rundt kjøp av geolokasjonsdata fra en britisk aktør. Ut i fra datapakker bestående av etter sigende anonyme data kunne NRK utlede identiteten til en rekke personer som jobbet ved militære avdelinger med behov for et høyt beskyttelsesnivå. Dette viser at det av og til kan være en sammenheng mellom hvor godt vi som samfunn klarer å beskytte opplysninger om innbyggerne våre, og hvor godt vi kan verne ressurser som har stor betydning for statssikkerheten.

[22] *Directive on Security of network and information systems.*

[23] *Det Europeiske byrået for nettverks- og informasjonssikkerhet (ENISA) er EUs ekspertisesenter for internettsikkerhet.*

NSM ser behov for en helhetlig tilnærming også til de teknologiområdene og digitale trendene som vil bli viktigere og viktigere fremover.

NATO Cyber Defence Pledge er ment å styrke alliansens prioritering av digital sikkerhet i nasjonale nettverk og infrastrukturer på tvers av sektorer i samfunnet og mellom land. Erklæringen forplikter blant annet medlemslandene årlig til å rapportere status på nasjonale tiltak som er iverksatt på feltet. Dette berører for eksempel opprettelsen av NCSC, styrking av sektorvise responsmiljøer og utvikling av et rammeverk for helhetsvurdering av verdikjeder.

Samlet sett viser de ulike initiativene at digital sikkerhet står høyt på den internasjonale agendaen. Tiltakene innenfor rammen av både EU og NATO underbygger viktigheten av digital sikkerhet i sivile og militære systemer.

Individet og digitalisering

Digitaliseringen påvirker i stor grad individet og samfunnet vårt. Både nasjonalt og i EU er det økt oppmerksomhet rundt regulering og tiltak mot desinformasjon og falske nyheter på sosiale medier. Flere tiltak er iverksatt i Norge for å avdekke falske nyheter, men her har vi alle et ansvar. Fremdeles er det viktig å utvise nettvett og være bevisst i møte med informasjon på nett.

I vårt gjennomdigitaliserte samfunn deler vi bevisst og ubevisst informasjon til enhver tid om våre bevegelser, handlinger, synspunkter og følelser. Dette kan innebære at vi lar aktører med ulike hensikter se oss i kortene – både i form av kommersielle selskaper som selger data

[24] *NOU 2020:6 Frie og hemmelige valg – ny valglov:* https://www.regjeringen.no/no/dokumenter/nou-2020-6/

PÅVIRKNING OG DESINFORMASJON KREVER ÅRVÅKENHET AV OSS ALLE

Åpne og liberale samfunn er sårbare for påvirkning og desinformasjon.

Informasjonen i det offentlige rom, sosiale medier eller på nyhetssider kan bli endret, og det kan være vanskelig å ivareta tilstrekkelig kildekritikk.

Påvirkningsaktivitet tar stadig nye former og kan være vanskelig å avdekke. Aktører har endret sin bruk av påvirkningsaktivitet gjennom sosiale medier, blant annet ved at polariserende temaer eller saker som løfter spesifikke budskap fra etablerte nyhetsplattformer, videreformidles.

Fremmede stater forsøker å påvirke norske beslutninger for å nå sine sikkerhetspolitiske og strategiske målsettinger. Slik påvirkning skjer både åpent og i det skjulte. Påvirkningsoperasjoner kan blant annet brukes for å svekke befolkningens tillit til myndigheter, valg og politiske prosesser. Slike operasjoner kan også ha som mål å påvirke opinionen i enkeltsaker eller styre samfunnsdebatten i en bestemt retning.

Viktige demokratiske prosesser kan bli utsatt for påvirkningsoperasjoner, og vi må alle være bevisst denne risikoen. Tiltak for å hindre uønsket påvirkning av valggjennomføringer har vært implementert, sist i forbindelse med kommunestyre- og fylkestingsvalget i 2019. Det blir viktig å ha et fortsatt fokus på dette i tiden frem til neste stortings- og sametingsvalg i 2021.

Valglovutvalget omtaler viktigheten av sikkerhet og teknologi særskilt i sin utredning fra juni 2020.[24]

Det kreves årvåkenhet mot falske nyheter og uønsket påvirkning.

om oss i markedsføringsøyemed og fremmede stater som samler informasjon til andre formål. Informasjonen du deler om deg selv og virksomheten du jobber i eller mobiltelefonen du bærer med deg overalt kan brukes som inngangsportal for en trusselaktør. Vær derfor bevisst på hvilken informasjon du deler, ikke minst gjennom sosiale medier og ulike digitale plattformer. Alle virksomheter bør gi ansatte klare retningslinjer og anbefalinger om hvordan de bør oppføre seg i det digitale rom.

Behov for regulering av teknologi i utvikling

Den pågående digitaliseringsprosessen vil påvirkes av fremtidige teknologiske drivere. Mange nasjonale tiltak for å bedre digital sikkerhet er iverksatt, men teknologi er i utvikling, og tiltakene må stadig videreutvikles. NSM ser behov for en helhetlig tilnærming også til de teknologiområdene og digitale trendene som vil bli viktigere og viktigere fremover. Nasjonale strategier knyttet til mulighetsrommet som 5G og IoT bringer med seg, adopsjon av moderne virtualisering og skyteknologier er eksempler på viktige områder i tiden fremover.

En av statens viktigste oppgaver er å beskytte og ta våre på sine innbyggere - i hele krisespennet. Satsning på digital understøttelse og opprettholdelse av samfunnskritiske funksjoner også oppover i krisespennet er et annet område som vil kunne få økt oppmerksomhet, spesielt i diskusjonen om bruk av skytjenester. Dersom vi velger å legge nasjonal kritisk infrastruktur og nasjonale digitale verdier ut i skyen, må vi være trygge på at tjenestene er tilgjengelige i hele krisespennet.

Datasenterbransjen består av aktører som tilbyr infrastruktur og tjenester i flere nivå, fra utleiere av lokaler til de som håndterer alt en virksomhet ønsker. I dag er kan noen av de tjenester og systemer som innplasseres i datasentre, være underlagt og regulert av statlige eller sektorvise lovverk. Bransjen i seg selv er ikke regulert av noe lovverk.

Flere nasjonale og internasjonale aktører i bransjen tilbyr leie av infrastruktur. Disse aktørene kan være alt fra sikkerhetsbevisste aktører som håndterer mye kritisk infrastruktur, til aktører med mindre midler og muligheter til å etablere sikre infrastrukturer. Disse kan i verste fall benyttes som brohode for ondsinnede aktører som vil infiltrere norske virksomheters infrastruktur. NSM erfarer at dagens bruk av leid infrastruktur medfører utfordringer for utøvelsen av hendelseshåndtering.

I og med at stadig flere virksomheter velger å anskaffe sine IKT-tjenester fra profesjonelle aktører, vil disse bli levert fra aktørenes datasentre. Antall aktører i markedet for datasentre i Norge kan ikke betraktes som stort, noe som kan innebære en konsentrasjon av verdier som samles i de samme datasentre. Dette er en problemstilling som bør kartlegges fremover.

I vårt gjennomdigitaliserte samfunn deler vi bevisst og ubevisst informasjon til enhver tid.

Forebyggende sikkerhetsarbeid reduserer digital risiko

Sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens verdier, med bakgrunn i risikovurdering. Da forsvarlig sikkerhet vil forandre seg over tid, på bakgrunn av endring av risiko, skal sikkerhetsstyring også ivareta prinsippet om kontinuerlig forbedring av sikkerhetsarbeidet i virksomheten.

Sikkerhetsstyring har blitt enda viktigere i møte med komplekse verdikjeder og et samfunn preget av internasjonalisering og teknologisk utvikling. Nye avhengigheter mellom virksomheter kan resultere i at sårbarheter i én virksomhet får konsekvenser for andre virksomheter.

God digital sikkerhet forutsetter et systematisk arbeid som er forankret i virksomhetens ledelse. En helhetlig tilnærming til sikkerhet inkluderer både prosessuelle, organisatoriske og tekniske tiltak.

Mange virksomheter er nok av den formening at de ikke har verdier som er attraktive for målrettede digitale operasjoner. Erfaring viser at alle kan bli brukt i både verdikjedeangrep mot andre mål eller rammes av mer vilkårlige trusler som direktørsvindel eller løsepengevirus. Derfor er det viktig at alle i virksomheten vet hva som skal gjøres når noe skjer. Virksomheten bør ha en beredskapsplan med definerte roller og ansvar og øve på denne jevnlig, samtidig som ledelsen må ha en plan for hvordan det skal løses.

God sikkerhetskultur er å erkjenne at dataangrep og andre sikkerhetshendelser kan ramme alle.

Det forebyggende sikkerhetsarbeidet må derfor være på plass for å redusere digital risiko.

Design: **Hyper**Redink
Manus: NSM
Foto: iStockphoto

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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