NASJONAL
SIKKERHETSMYNDIGHET

Nasjonalt digitalt risikobilde 2021

Nasjonalt digitalt risikobilde er vår årlige 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, og tar opp problemstillinger knyttet til samfunnssikkerhet, statssikkerhet og individsikkerhet innenfor det digitale domenet.

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 cyberoperasjoner. NCSC har et spesielt fokus på rådgiving og krav innen forebyggende tiltak, tekniske sikkerhetsløsninger og yter bistand ved håndtering av digitale hendelser.

Sammendrag

Digital sikkerhet har utviklet seg fra å handle om det tekniske, til å bli et strategisk viktig tema som adresseres globalt. Leverandørkjedeangrepet mot IT-selskapet SolarWinds er et kjent eksempel som førte til omfattende konsekvenser for de virksomhetene og funksjonene som ble rammet. Slike globale hendelser viser at cyberoperasjoner rammer i stor skala og har et bredt nedslagsfelt. Samtidig kan de ha en styrkende effekt på hvordan likesinnede land svarer på slike hendelser. Globale trusler krever samlet respons. Cyberoperasjoner påvirker samfunnsfunksjoner og fører til betydelige tap av verdier for de som rammes.

Vi står overfor et taktskifte innenfor digital risiko i Norge. Antall alvorlige hendelser registrert hos Nasjonalt cybersikkerhetssenter (NCSC) i NSM i 2020 var tre ganger så mange som i 2019. NCSC har observert en vesentlig økning i hendelser knyttet til krypteringsvirus og økonomisk motivert kriminalitet på nett det siste året. Samtidig er det fremdeles avanserte aktører som utfører komplekse spionasjeoperasjoner mot norske mål, inkludert der våre viktigste verdier forvaltes. Dette har konsekvenser for Norges stats- og samfunnssikkerhet. Cyberoperasjonene mot Stortinget viser alvorlighetsgraden i det nasjonale digitale risikobildet.

Samfunnets digitalisering og introduksjon av stadig nye teknologier har ført til at skillelinjer mellom Forsvaret og det sivile samfunn blir mindre. Digitaliseringen medfører økt effektivisering og innovasjon, men samtidig introduseres nye sårbarheter, avhengigheter og konsentrasjonsrisikoer som kan utnyttes og derfor må håndteres. Komplekse systemer og eierforhold skaper nye sårbarheter og aktualiserer behovet for samarbeid om sikkerhet i totalforsvaret.

Tekniske sikkerhetstiltak alene vil ikke stoppe trusselaktører, det er nødvendig med gode prosesser i virksomheten og god sikkerhetskultur hos brukere av systemer og virksomhetens ansatte. Dette øker robusthet, men også bevissthet og forståelse for sikkerhet hos den enkelte.

Stadig flere prioriterer det digitale sikkerhetsarbeidet. NSM ser likevel at for mange norske virksomheter ikke har et forsvarlig sikkerhetsnivå for å beskytte viktige verdier. Vi opplever for eksempel at mange virksomheter som rammes av løsepengevirus i liten grad har vært forberedt. Økt bevissthet om digital risiko har ofte ikke blitt omsatt til handling. Dette bør være et tema i alle styrerom og ledergrupper.

For alle norske virksomheter er det forebyggende sikkerhetsarbeidet med på å redusere digital risiko. Med det utfordrende risikobildet, hvor konsekvensene av cyberoperasjoner blir mer alvorlige, haster det mer enn tidligere å implementere risikoreduserende tiltak.

Noen digitale tjenester og leveranser er kritiske for samfunnet og vil kreve nasjonal digital autonomi. Datasenter står sentralt i vår felles digitale grunnmur og må adresseres på en grundig måte. Militær og sivil sektor vil i økende grad benytte felles digital infrastruktur da tjenestene vil bli levert fra de samme kommersielle aktørene. NSM har derfor valgt å rette oppmerksomhet mot norske datasentre og digital autonomi i en egen temarapport i høst.

«Nasjonalt digitalt risikobilde 2021» ser på hvilke typer digitale hendelser som rammer norske virksomheter og konsekvensene av disse for vår felles digitale sikkerhet. Rapporten gir også en status over nasjonale og internasjonale satsninger innen digital sikkerhet og retning for det videre sikkerhetsarbeidet. Som i 2020, har flere av NCSCs partnere gitt innspill til årets rapport 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 nasjonalt bilde av digital risiko i Norge. ■

1.
Det digitale risikobildet

Norge står overfor et komplekst digitalt risikobilde der statlige og kriminelle aktører forsøker å utnytte sårbarheter i funksjoner, virksomheter og systemer ved bruk av et bredt utvalg digitale virkemidler.

I dag understøttes samfunnet av en rekke digitale kritiske funksjoner som må fungere til enhver tid. En uønsket hendelse mot en eller flere av disse kan få store konsekvenser og føre til synlige og negative samfunnseffekter. Vi ser at det gjøres mye godt sikkerhetsarbeid i mange virksomheter, og stadig flere får opp bevisstheten rundt og fokuset på digital sikkerhet. Men arbeidet må forsterkes betydelig. Det kreves et taktskifte i forebyggende arbeid og beredskap.

Et taktskifte innenfor digital risiko

I 2020 og 2021 har Nasjonalt cybersikkerhetssenter i NSM opplevd en markant vekst i aktivitetsnivå i det digitale rom sammenlignet med tidligere år. Antall alvorlige hendelser registrert hos NCSC i 2020 var tre ganger så mange som i 2019. Flere av disse var omfattende operasjoner hvor flere virksomheter var berørt. I noen tilfeller har disse hatt forgreninger til internasjonale operasjoner. I tillegg får cyberoperasjoner mot norske virksomheter synligere konsekvenser. Hendelser knyttet til krypteringsvirus øker og blir mer avanserte. Aktørene bruker flere metoder som pressmiddel for å få betalt løsepenger, slik som trusler om publisering av sensitive data. Samlet sett utgjør disse forholdene et taktskifte. Cyberoperasjonene mot Stortinget viser alvorlighetsgraden i det digitale risikobildet vi nå står overfor.

Både Etterretningstjenesten og Politiets Sikkerhetstjeneste (PST) har påpekt at utenlandsk etterretnings- og påvirkningsaktivitet rettet mot både offentlig og privat sektor forblir en betydelig trussel mot Norge og norske interesser. Etterretningstrusselen retter seg mot stadig flere sektorer. Informasjon om utforming av norsk politikk, særlig innenfor forsvars-, utenriks- og sikkerhetspolitikk, er av vedvarende interesse. Erfaringer NSM har gjort det siste året underbygger disse vurderingene.

Det digitale rom er også en arena for samhandling og informasjonsutveksling på tvers av land, sektorer, virksomheter og borgere. Denne arenaen gir mulighet til fremmede staters påvirkningsoperasjoner og spredning av feilinformasjon, som kan skape usikkerhet, så splid, undergrave tillit, og påvirke det offentlige ordskiftet. Kompromittering av kontoer i sosiale medier kan også gi tilgang til privat kommunikasjon som kan brukes til å utøve press på enkeltpersoner.

Internasjonale cyberhendelser har fått mye oppmerksomhet i 2020 og 2021. Utnyttelse av sårbarheter i Microsoft Exchange og

Cyberoperasjonene mot Stortinget viser alvoret vi nå står overfor.

Mange digitale løsninger kom på plass under pandemien. Digitale sårbarheter fulgte med på lasset.

leverandørkjedeangrepet mot IT-selskapet SolarWinds er to eksempler som er kjent for mange. Felles for dem var at de førte til omfattende konsekvenser for de som ble rammet. Slike globale hendelser viser at cyberoperasjoner rammer i stor skala og har et bredt nedslagsfelt, samtidig som de kan ha en styrkende effekt på hvordan likesinnede land svarer på slike hendelser. Globale trusler krever samlet respons. Stadig flere innser at cyber-operasjoner kan påvirke samfunnsfunksjoner og føre til betydelige tap av verdier. Dette gjelder for individer, for den enkelte virksomhet og for samfunnet.

Lavt digitalt sikkerhetsnivå på ett område kan forplante seg som sårbarheter på andre områder fordi funksjoner har avhengigheter til hverandre. Derfor må sikkerhetsfokus omfatte både tekniske, organisatoriske og menneskelige nivå. Sårbarheter på ett område er nok til å øke sjansen for at digitale operasjoner lykkes i å ramme våre verdier. Det er viktig å opprett-holde et tilstrekkelig sikkerhetsnivå i egen organisasjon og ivareta IKT-drift og beredskap på en forsvarlig måte. Dette er et kontinuerlig arbeid. NSM publiserer jevnlig råd, veiledere og tiltak som hjelper norske virksomheter med å forhindre uønskede digitale hendelser.

COVID-19 har skapt digitale sårbarheter
Ved publisering av fjorårets rapport sto det norske samfunnet midt i en pandemi. Situasjonen akselererte bruken av nye digitale løsninger, og endret måten vi jobbet og

FOTO: NTB SCANPIX / MONICA STRØMDAHL / AFTENPOSTEN

Erna Solberg ledet regjeringens koronautvalg fra hjemmekontoret i statsministerboligen.

Digital sikkerhet har vokst fra å handle om det tekniske til å bli et tema som adresseres globalt.

kommuniserte med hverandre. Utstrakt bruk av hjemmekontorløsninger skapte samtidig nye digitale sårbarheter. NCSC observerte at ulike trusselaktører tilpasset seg den endrede situasjonen og utnyttet disse sårbarhetene, for eksempel ved å benytte COVID-19 tematikk i svindelforsøk og målrettet phishing.

Sårbarhetsflaten ble større med løsninger som var ment å være midlertidige, men som nå har blitt permanente. Pandemien førte også til økt press mot enkelte sektorer og samfunnsfunksjoner, eksempelvis helse- og forskningssektoren. Med nye digitale sårbarheter kom også behov for nye risikoreduserende tiltak. Gjennom året har vi tilpasset råd, varsler og veiledere til den nye digitale hverdagen. Vi mener at både offentlig og privat sektor har vist evne til mobilisering i ekstraordinære situasjoner for å sette fokus på digital sikkerhet. Mange digitale løsninger og sårbarhetsflater fremskyndet av pandemien har kommet for å bli, også når vi igjen befinner oss i en ny normal hverdag.

Sammen utgjør vi et økosystem for digital sikkerhet i Norge

Alle virksomheter har ansvar for å ivareta egen digital sikkert. Likevel kan hverken myndigheter, virksomheter eller borgere håndtere de digitale utfordringene alene. Den raske teknologiske utviklingen øker også den gjensidige avhengigheten mellom Forsvaret og sivilsamfunnet. For å ivareta totalforsvarsevnen må det digitale sikkerhetsarbeidet følge den raske digitaliseringen. Strukturert samarbeid med relevante nasjonale og internasjonale partnere og på tvers av sektorer er avgjørende for å lykkes i å motvirke, avdekke og håndtere digitale hendelser som rammer våre nasjonale verdier.

NCSC vedlikeholder et oppdatert risikobilde i det digitale rom. Et sentralt virkemiddel er å utnytte potensialet som ligger i et styrket offentlig-privat samarbeid. Forebyggende arbeid reduserer digital risiko og sammen utgjør vi et økosystem for digital sikkerhet i Norge. Vårt felles mål må være å skape robusthet gjennom forebyggende tiltak og evne til å avverge, oppdage og forebygge. Uten et velfungerende digitalt økosystem vil resultatet være bortfall av viktige samfunnsfunksjoner.

Flere og flere virksomheter erkjenner at cyberoperasjoner kan ramme alle og NCSC erfarer at stadig flere prioriterer det digitale sikkerhetsarbeidet. Vi ser likevel at mange norske virksomheter ikke har et forsvarlig sikkerhetsnivå for å beskytte viktige verdier. Økt bevissthet om digital risiko har ofte ikke blitt omsatt i handling. Dette bør være et tema i alle styrerom og ledergrupper.

Erfaringer og lærdom etter hendelser er viktige bidrag for å bygge motstandsdyktighet mot digitale trusler og sårbarheter. Informasjonsdeling på tvers av sektorer og landegrenser, samt forebyggende tiltak bidrar også til å bygge en slik robusthet. Det er samtidig viktig å informere om svakheter og sårbarheter i tjenester og produkter *før* hendelser inntreffer. Her er varsling og informasjonsutveksling sentralt for å kunne møte risikoene vi sammen står overfor. Digital sikkerhet har vokst fra å handle om det tekniske til å bli et tema som adresseres globalt. ■


NASJONAL

2. Cyberoperasjoner får alvorlige konsekvenser

Både statlige og kriminelle aktører har intensjon og kapasitet til å utføre cyberoperasjoner mot norske virksomheter. Slike operasjoner har konsekvenser for Norges stats- og samfunnssikkerhet. Felles Cyber-koordineringssenter[1] (FCKS) peker på at russiske og kinesiske etterretnings- og sikkerhetstjenester er de mest aktive aktørene. Vi er kjent med at disse har gjennomført operasjoner mot Norge og Norges allierte i det digitale rom. Aktørene disponerer avanserte verktøy og metoder, og måten de opererer på tyder på en ressurs- og kapasitetssatsning i domenet.

Flere avanserte aktører opererer i norsk infrastruktur over tid. NCSC observerer store og komplekse operasjoner mot flere mål og på tvers av sektorer, hvor aktøren benytter avanserte metoder og angrepsvektorer for å lykkes. Dette er en endring fra tidligere, hvor vi i større grad observerte enkeltstående operasjoner mot ett mål. Slike omfattende hendelser krever betydelig ressursbruk over tid for å kunne håndteres.

Det er sannsynlig at enkelte avanserte aktører ønsker å oppnå et varig fotfeste i norske virksomheter med formål om å hente ut informasjon som vil være av etterretningsverdi på kort og lang sikt. Slike aktører er det siste året observert som aktive mot mål i blant annet forskning- og utdanningssektoren, sentralforvaltningen, innenfor høyteknologi og mot forsvarssektoren.

Aktører får tilgang til norske mål på ulike måter

Phishing, der en aktør sender en e-post for å få mottaker til å åpne et ondsinnet vedlegg eller lenke, brukes fortsatt som inngangsmetode i cyberoperasjoner. NCSC blir regelmessig kontaktet av virksomheter som har mottatt phishing-e-poster. Det siste året er det sett flere tilfeller av phishing-operasjoner fra det

OPERASJON MOT FORSKNINGS- OG UTDANNINGSSEKTOREN

Som i fjorårets rapport peker NSM også i 2021 på et økt fokus mot forsknings- og utdanningssektoren. NCSC har i 2020-2021 håndtert flere hendelser tilknyttet denne sektoren i Norge.

Operasjonen omfatter en rekke virksomheter tilhørende forsknings- og utdanningssektoren, blant annet Norges arktiske universitet UiT (UiT) som i desember 2020 informerte om at de var rammet av et datainnbrudd.

NCSC og Uninett CERT[2] har siden desember bistått UiT med hendelseshåndtering.

Analyse har avdekket både kompromitterte servere og brukerkontoer, hvor veien inn har vært sårbare systemer og manglende multifaktorautentisering. UiT har fortløpende iverksatt en rekke risikoreduserende og skadebegrensende tiltak.

Det har vært observert kartleggingsaktivitet mot en rekke virksomheter i saken, samt enkelte påloggingsforsøk hvor formålet ser ut til å være knyttet til informasjonsinnhenting. NCSC og de sektorvise responsmiljøene i andre sektorer har fortløpende varslet og vært i dialog med berørte virksomheter.

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

[2] *Uninett CERT er sektorvist responsmiljø for utdanningssektoren.*

som sannsynligvis er avanserte aktører mot viktige norske mål. Phishingforsøkene er ofte svært godt tilpasset til hvert enkelt mål. Vi er kjent med at trusselaktører bruker offentlig tilgjengelig informasjon for å skreddersy e-poster som sendes virksomheter. Virksomheter bør derfor vurdere hvor mye informasjon om ansatte som skal ligge tilgjengelig på internett.

I noen tilfeller sendes e-posten fra en kompromittert virksomhet eller bruker, som det egentlige målet har en relasjon eller tillitsforhold til. Innholdet i e-posten er ofte relevant for sluttmålet. Dette øker sannsynligheten for at mottaker vil åpne vedlegg eller lenker i e-posten. NCSC observerer også at høsting av brukernavn og passord («credential harvesting») kan utføres ved hjelp av målrettede phishing-e-poster for å lure en mottaker til å oppgi påloggingsdetaljer. Noen aktører bruker skytjenester som «Drop-box» i sine cyberoperasjoner. I en norsk organisasjon fikk ansatte lekket brukerdetaljer etter å ha mottatt en phishing e-post med «Drop-box»-tematikk med beskjed om at en bruker ville dele et dokument. Avsender utga seg for å være en samarbeidspartner målet samarbeidet tett med.

Digital årvåkenhet og sikkerhetskultur blant ansatte er viktig, men alene vil det ikke være tilstrekkelig for å sikre seg mot phishing-eposter. NCSC anbefaler robuste tekniske sikkerhetsløsninger og -tiltak som kan forhindre eller redusere skadene ved phishing. Oftest gjelder det å fjerne sårbarheter. Det gjelder for eksempel sårbarheter i nettverksarkitekturen og sårbarheter med styring av brukerkontoer og brukerrettigheter. Dette inkluderer særlig multifaktorautentisering for å hindre misbruk av brukernavn og passord som kan komme på avveie etter vellykket phishing. Regelmessig oppdatering av tjenester og programvare er også et godt forebyggende tiltak mot flere ulike typer uønskede hendelser.

Det observeres jevnlig kartlegging og automatisert skanning av digitale tjenester og programvaresårbarheter som er tilgjengelige på internett. Utnyttelse av sårbarheter i tjenester, som Exchange, Web-logic og annen serverprogramvare har vært en gjenganger det siste året, også i Norge. Virksomheter kan redusere egen sårbarhetsflate ved å være bevisst hvilke tjenester og verdier som er eksponert mot internett. For å sikre internetteksponerte tjenester anbefales det å 1) legge tjenesten bak fjernpåloggingsløsninger (for eksempel VPN), 2) aktivere multifaktorautentisering på tjenesten, og gjerne også det underliggende operativsystemet, og 3) begrense mengden eksponerte tjenester der dette er mulig. Videre bør man 4) ha logging og systemovervåkning som fanger opp (og varsler om) store mengder feilpåloggingger.

Virksomheter bør vurdere hvor mye informasjon om ansatte som skal ligge tilgjengelig på internett.

Sårbarheter i Microsoft Exchange

I mars 2021 publiserte Microsoft informasjon om syv sårbarheter i Exchange-servere. Fire av disse var nulldagssårbarheter og hadde vært aktivt utnyttet mot sårbare virksomheter siden tidlig i januar.

Som en konsekvens av at utnyttelseskoden ble offentlig tilgjengelig ble det rapportert om aktiv utnyttelse av sårbarhetene av ulike trusselaktører. Flere virksomheter meldte om bred kartlegging og vilkårlig utnyttelse av sårbarhetene, i tillegg til målrettede angrep.

NCSC varslet bredt om sårbarhetene til våre varselmottakere og på NSMs nettsider i dagene etter Microsofts publisering. Vi anslo på dette tidspunktet at svært mange norske virksomheter kunne være berørt.

Utnyttelse av sårbarhetene kunne gi tilgang til virksomheters infrastruktur og kontroll over nettverket. Ulike aktører tilpasser seg raskt denne type mulighetsrom, og denne tilgangen kunne utnyttes til avanserte spionasjeoperasjoner eller kryptering av systemer med påfølgende krav om løsepenger.

NSM iverksatte en sårbarhetskartlegging av norske IP-adresser for å få oversikt over antallet virksomheter i Norge som potensielt kunne utnyttes gjennom Microsoft Exchange.

Norske virksomheter rapporterte om lite skade som følge av sårbarhetene, men flere virksomheter fikk installert bakdør i sine systemer før sikkerhets-oppdateringer ble installert.

Skanningen av norske IP-adresser resulterte i et mer detaljert nasjonalt sårbarhetsbilde enn det NSM normalt besitter. Ved å kartlegge IP-adresser ble flere mulige datainnbrudd hos norske virksomheter avdekket og avverget. Rask varsling og sikkerhetsoppdatering kan ha spart samfunnet for store kostnader. Den omfattende nasjonale varslingen og skanningen har hatt god forebyggende effekt.

FOTO: COLOURBOX

Stortinget ble rammet av cyberoperasjoner i 2020 og 2021.

NCSC har observert hendelser knyttet til automatiserte påloggingsforsøk, såkalt «brute-force», på digitale tjenester. Her brukes verktøy for å teste et stort antall brukernavn- og passordkombinasjoner i et høyt tempo. Det kan for eksempel være gjentakende påloggingsforsøk på en e-postserver som Microsoft Exchange for å få tilgang til brukeres kontoer. Dette er en effektiv metode, men samtidig er den lett å oppdage. Vi understreker viktigheten av å ikke gjenbruke påloggingsdetaljer på tvers av tjenester – dersom en aktør får påloggingsdetaljer til en e-postkonto og samme detaljer benyttes ved fjernpåloggingsløsninger, slik som VPN, vil en aktør enkelt kunne omgå dette sikkerhetstiltaket.

Trusselaktører får digitalt fotfeste

Når en aktør har fått tilgang til et mål kan det etableres et fotfeste i målets systemer. Gjennom fotfestet kan en trusselaktør bruke tilgangen for å installere skadevare. Skadevare kan kartlegge et system, installere bakdører for kjøring av kommando- og kontroll, og gi muligheter til å hente ut data fra virksomheten.

Flere typer verktøy og skadevare som aktørene bruker i sine cyberoperasjoner regnes som «hyllevare» og er åpent tilgjengelig på internett. Noen verktøy er derimot spesifikt utviklet av avanserte aktører. Ofte er skadevare en kombinasjon av hyllevare og egenutviklede verktøy. Trusselaktører benytter også legitime verktøy, for eksempel administrasjonsverktøy, for å utføre handlinger på målet. Dette bidrar til å maskere den ondsinnede aktiviteten som legitim, som igjen kan gjøre deteksjon og attribusjon vanskeligere.

For å utføre cyberoperasjoner har trusselaktører sannsynligvis etablert et nettverk av operasjonell infrastruktur i forkant. Denne infrastrukturen er ofte bygget opp i flere lag slik at det er flere hopp tilbake til aktør. Dette reduserer risikoen for å bli oppdaget. Infrastrukturer kan bygges opp ved hjelp av anonymiseringstjenester eller bestå av et nettverk av kompromitterte servere.

En node som inngår i en større operasjonell infrastruktur kan tilhøre en intetanende virksomhet som ikke selv vet at nettverket deres er kompromittert. Her blir virksomheten brukt som virkemiddel i en aktørs cyberoperasjoner mot et sluttmål. Det er eksempler på at kompromitterte hjemmerutere brukes i slike operasjonelle infrastrukturer. I alle disse tilfellene er det viktig å ha kontroll på sårbarhetsflaten og på hvilke tjenester, funksjoner og enheter som er tilgjengelige på internett.

For å utføre cyberoperasjoner etablerer trusselaktører ofte et nettverk av operasjonell infrastruktur i forkant.

Utnyttelse av nulldagssårbarheter har preget internasjonalt risikobilde siste år.

Sårbarheter utnyttes for å få tilgang til norske mål

Vi står fremdeles overfor et komplekst og stadig skiftende sårbarhetsbilde. NCSC ser at kjente, tekniske programvaresårbarheter er den vanligste veien inn for få uautorisert tilgang til en virksomhets digitale systemer. Dette er samme erfaring som i 2020. I 2021 har vi sett bred utnyttelse av sårbarheter i mye brukte tjenester, som for eksempel e-postløsningen Microsoft Exchange (se tekstboks s. 15). Dette har vært gjort av både avanserte og ikke-avanserte trusselaktører.

Utnyttelse av nulldagssårbarheter har preget det internasjonale risikobildet det siste året. En nulldagssårbarhet er en sårbarhet som ikke er kjent for leverandøren av programvaren, og som kan utnyttes av en trusselaktør. Koden for å utnytte en nulldagssårbarhet er vanligvis lite kjent før den er avdekket. Leverandøren må da utvikle en sikkerhetsoppdatering *før* de som visste om nulldagssårbarheten slipper utnyttelseskoden bredt, for å unngå at den utnyttes av alle som har kompetanse til det. En leverandør vil bruke noe tid på å utvikle en sikkerhetsoppgradering for å lukke sårbarheten. Det vil også gå tid fra en sikkerhetsoppgradering er tilgjengelig til brukere av programvaren installerer oppgraderingen. Virksomheter som ikke har rukket å installere sikkerhets-oppdateringer vil dermed fortsatt være sårbare.

Løsepengehendelser rammer bredt og vilkårlig

Norske virksomheter blir jevnlig rammet av krypteringsvirus med krav om løsepenger, såkalt løsepengevirus, og flere av disse forvalter

– Vår etterretnings-informasjon er at dette dataangrepet ble gjennomført fra Kina. Der kan det være mange ulike aktører, men vi har basert oss på den etterretnings-informasjonen vi har, sa sa daværende utenriks-minister Ine Eriksen Søreide til pressen 19. juli i år.

CYBEROPERASJONENE MOT STORTINGET 2020 OG 2021

Sent i august 2020 ble det kjent at Stortinget var rammet av en alvorlig cyberoperasjon. Dette var en del av en omfattende cyberoperasjon som rammet virksomheter i flere land. PSTs etterforskning konkluderte med at det var sannsynlig at den russiske, militære etterretningstjenesten GRU stod bak. Dette er første gang norske myndigheter offentlig har attribuert en slik cyberoperasjon til et annet land.

Trusselaktøren benyttet automatisert gjetting av passord på et stort antall e-post-kontoer. Forsøkene fortsetter til de lykkes eller til de blir avvist av sikkerhetsløsninger. Om man har tilstrekkelig logging på systemet, kan slike angrep bli avdekket. Slike angrep kan karakteriseres som støyende og lite sofistikerte.

Våren 2021 ble det kjent at Stortinget hadde vært utsatt for nok en cyberoperasjon. Nulldagssårbarheter i Stortingets Exchange-servere ble utnyttet for å få tilgang til Stortingets systemer. Senere gikk regjeringen Solberg offentlig ut og pekte på at operasjonen ble gjennomført fra Kina. NATO, EU og en rekke allierte land attribuerte utnyttelsene i Exchange-serverne også andre steder i verden til statlige kinesiske aktører. Dette var første gang en så stor samling av allierte stod sammen og attribuerte en cyberoperasjon.

FOTO: BEATE OMA DAHLE / NTB

viktige samfunnsverdier i Norge. Bruken av løsepengevirus fortsetter å øke i både omfang og antall, og har i flere tilfeller ført til store systemlammelser med utilgjengeliggjøring av funksjoner, varer og tjenester, samt sensitiv informasjon på avveie. Internasjonalt rapporteres det om en dramatisk økning i summen av løsepengekrav. Dette er tydelige eksempler på at løsepengevirus får synligere og mer alvorlige konsekvenser.

Løsepengevirus har blant annet som formål å hindre virksomheten i å bruke sitt eget IT-system, slik at virksomheten presses til å betale angriperen for å kunne opprettholde ordinær drift. Internasjonalt rapporteres det om at aktører benytter flere ulike metoder i sin utpressing av virksomheten. Særlig utbredt er de fire metodene kryptering, publisering, trakassering og tjenestenektangrep (RDDoS). Felles for metodene er at de brukes som pressmiddel for å få betalt løsepenger. Ved *kryptering* krever aktøren løsepenger for å dekryptere virksomhetens systemer, og ved *publisering* kan aktøren true virksomheten med å publisere data som er hentet ut fra virksomheten. Ved *trakassering* kan aktøren presse eller trakassere den rammede virksomhetens kunder eller interessenter. Ved *tjenestenektangrep* kan aktøren utsette virksomheten for et tjenestenektangrep med krav om løsepenger (RDDoS). NCSC har den siste tiden mottatt flere innrapporteringer av trusler om tjenestenektangrep med krav om løsepenger, men ønsker likevel å påpeke at det er få eksempler på at angrepene faktisk realiseres, noe som også gjenspeiles internasjonalt.

Det er en svært høy risiko for at flere norske virksomheter vil utsettes for løsepengevirus i løpet av 2022. Det er også mulig at norske virksomheter vil utsettes for løsepengevirus med omfattende konsekvenser.

Det er gjennom året sett flere eksempler på at løsepengevirus rammer tjenesteleverandører. Dette gir en ytterligere skadedimensjon til krypteringsangrep – nemlig at flere rammes gjennom hele kundesegment hos en virksomhet. Norske virksomheter trenger altså ikke nødvendigvis å være på en aktørs målliste, men kan rammes tilfeldig gjennom en leverandørkjede.

Globalt ser man at løsepengehendelser i større grad gjennomføres med bruk av «ransomware as a service» (RaaS), altså løsepengevirus som hyllevare. I en slik cyberoperasjon kan hovedaktøren gjennomføre krypteringen, og heller kjøpe tjenester som for eksempel utpressing og e-post-phishing fra andre tilbydere. Dette har medført en «forbedring» av enkelte tjenester fordi en aktør kan spesialisere seg på ett felt og kjøpe andre tjenester. Eksempelvis har metoder som e-post-phishing fått bedre språk og blitt bedre tilpasset mottakeren, noe som kan øke sjansene for at de lykkes.

[3] https://kommunecsirt.no/nyheter-og-artikler/digitalt-situasjonsbilde-for-f%C3%B8rste-kvartal-2021

Betaler du løsepenger er du ikke garantert hverken å få tilbake dataene eller å hindre at de selges videre.

En erfaring fra kommunal sektor

Østre Toten kommune ble i januar utsatt for et krypteringsvirus med krav om løsepenger som satte store deler av kommunens nettverk tilbake til manuell styring i lang tid. Kommunen melder om at enkelte systemer fortsatt er ute av drift et halvt år senere.

Kommune-CSIRT rapporterer[3] om at de lørdag 9. januar ble kontaktet av Østre Toten kommune som var rammet av et løsepengevirus med skadevaren PYSA. Hele den virtuelle serverparken til kommunen ble kryptert og låst ned. Også de internettbaserte sikkerhetskopiene ble kryptert og utilgjengeliggjort. Aktøren hadde også stjålet betydelige mengder data, og dobbel utpressing fremstod som et mulig scenario. Kommunens operative evne ble sterkt redusert da de aller fleste av kommunens digitale tjenester var nede. Situasjonen ble ytterligere forverret den 29. mars, da PYSA publiserte deler av dataene som var stjålet fra kommunen på det mørke nettet. Kommunen måtte håndtere sensitive personopplysninger på avveie, og informere og støtte personer som ble rammet.

På NSMs sikkerhetskonferanse 11. mars fortalte Østre Totens ordfører Bror Helgestad at hendelsen i praksis medførte at de eldres alarm-system på sykehjem ble erstattet med bjeller, låse-systemet på kommunens bygninger ikke fungerte, og at helsestasjonen for barn og unges journaler var utilgjengelige. Kommunen måtte operere manuelt i flere måneder uten fungerende IT-systemer.

FOTO: MAHLUM/WIKIPEDIA

Bedriften Norske VTC-tjenester (NoVTC AS) blir rammet av løsepengevirus

Bedrift Norske VTC-tjenester (NoVTC AS) utvikler og tilbyr videokonferanseløsninger for norske kunder. Dette har tradisjonelt vært en liten bedrift med noen få utviklere, men har vokst i størrelse under korona-pandemien. De har utviklet interne systemer selv, blant annet kildekode for videokonferansetjeneste, kundedatabase og regnskapssystem.

Det interne nettverket er helt åpent og alle ansatte, servere og nettverksressurser er koblet på det samme interne nettet. Det er ingen soneinndeling eller interne grensesnitt som skiller de ulike ressursene fra hverandre.

Alle tiltakene under er hentet fra *«NSM Grunn-prinsipper for IKT-sikkerhet»*.

1

Aktør kompromitterer NoVTC via en e-post med vedlegg som inneholder skadevare.

TILTAK:

> 2.2. Etabler en sikker IKT-arkitektur

> 2.3. Ivareta en sikker konfigurasjon

> 2.5. Kontroller dataflyt

> 2.6. Ha kontroll på tilganger og identiteter

> 2.8. Beskytt e-post og nettleser

2

Aktøren har nå tilgang til nettverket til NoVTC. Den kartlegger nettverket og sprer seg videre ved å infisere filer, servere, databaser og back-up løsninger. Aktør legger igjen bakdører på systemet for videre kommunikasjon mellom seg selv og NoVTC.

TILTAK:

> 2.2. Etabler en sikker IKT-arkitektur

> 2.5. Kontroller dataflyt

> 3.2. Etabler sikkerhetsovervåkning

> 3.3. Analyser data fra sikkerhetsovervåkning

3

Aktøren heter data ut fra NoVTC' systemer.

TILTAK:

> 2.3. Ivareta en sikker konfigurasjon

> 2.4. Beskytt virksomhetens nettverk

> 2.5. Kontroller dataflyt

4

Aktøren aktiverer et krypteringsvirus på systemet til NoVTC og krypterer alt innhold. All data, tjenester og funksjoner på systemet til NoVTC er nå utilgjengelig.

TILTAK:

> 2.9. Etabler evne til gjenoppretting av data

> 4.1. Forbered virksomheten på håndtering av hendelser

5

En melding dukker opp på klientene til NoVTC med et løsepengekrav som skal betales i kryptovaluta. Aktøren truer NoVTC med følgende handlinger dersom NoVTC ikke innfrir løsepenge-kravet:

- Systemet til NoVTC forblir kryptert og utilgjengelig.
- Å selge innhentet data til en tredjepart.
- Å lekke innhentet data på internett, både virksomhetens egne data men også sensitive opplysninger om NoVTCs kunder.

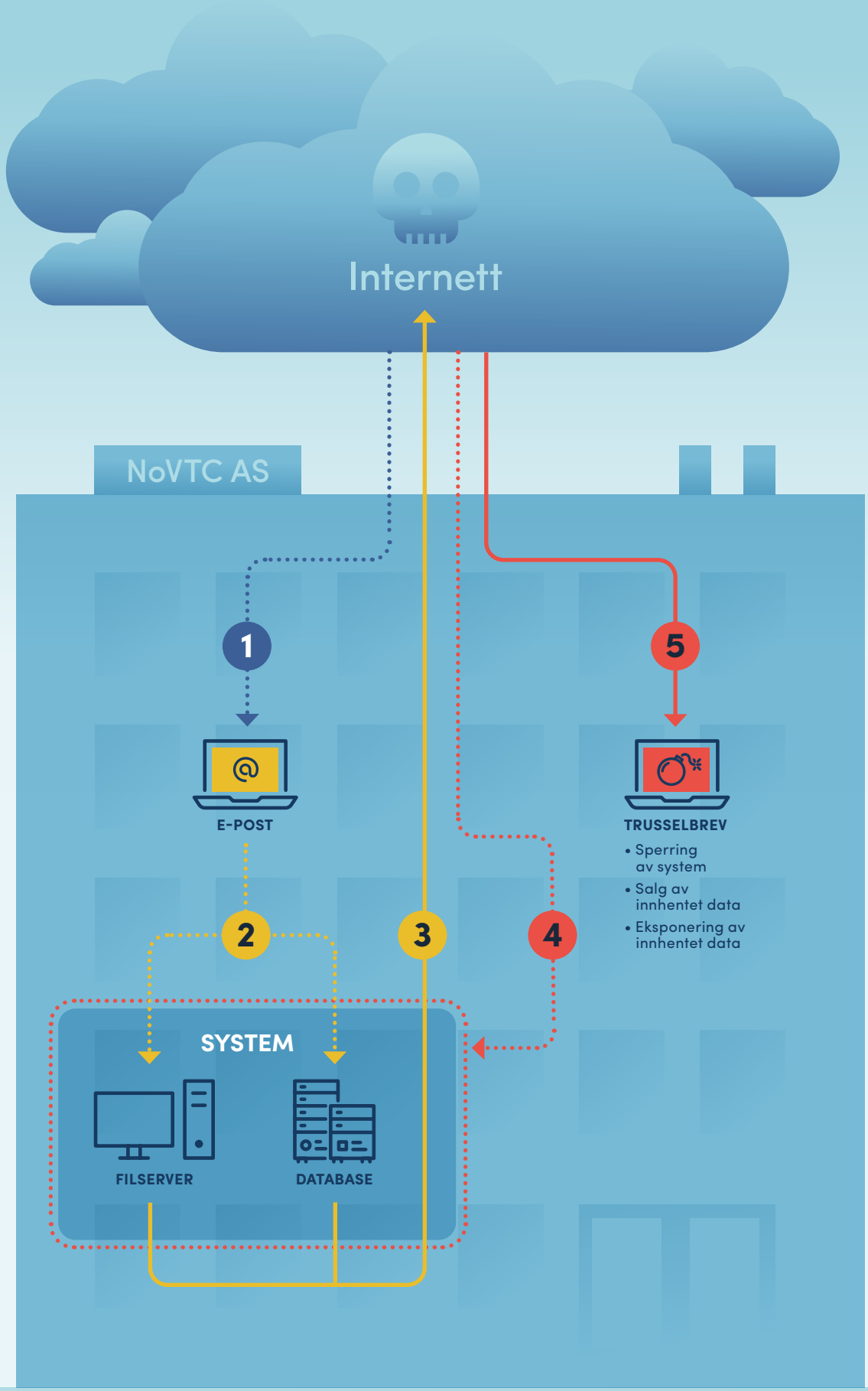
OVERORDNEDE TILTAK

> NSM vil at alle virksomheter skaffer seg god grunnsikring av digitale verdier og beskytter nettverk fra uønskede digitale hendelser. Da øker sannsynligheten for at man unngår krypteringsvirus og påfølgende datalekkasjer.

> På nsm.no beskrives 44 tiltak mot skadevare som virksomheter kan implementere for å vanskeliggjøre dataangrep og håndtere en hendelse hvis skaden først inntreffer. Tiltakene vil dermed 1) redusere sannsynligheten for å bli rammet av skadevare og løsepengevirus, 2) redusere spredningen av slik ondartet programvare og 3) redusere konsekvensene hvis man likevel blir rammet. Disse tiltakene er i stor grad hentet fra *«NSMs Grunnprinsipper for IKT-sikkerhet»*.

> NSM anbefaler på generelt grunnlag at man ikke betaler løsepenger.

** https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/skadevare/*


Internett
NoVTC AS
1
E-POST
2
3
4
5
TRUSSELBREV
• Sperring av system
• Salg av innhentet data
• Eksponering av innhentet data
SYSTEM
FILSERVER
DATABASE

Mange virksomheter som rammes av løsepengevirus har vært uforberedt.

Norsk senter for informasjonssikring (NorSIS) undestreker i sin rapport *Trusler og trender i 2021*[4] at det trolig er store mørketall knyttet til løsepengevirus. NCSC har observert flere ulike typer krypteringsvirus som har truffet en rekke ulike sektorer. Sektortilhørigheten til de ulike virksomhetene understreker et viktig poeng, nemlig at løsepengevirus rammer bredt. Det er en risiko for at sektorer som er under økt press er mer sårbare for krypteringsvirus og trusler om datalekkasjer. Erfaring viser også at trusselaktører raskt tilpasser seg aktuell tematikk. Særlig har COVID-19-situasjonen skapt en økt risiko for cyberoperasjoner for helsesektoren. Eksempelvis ble et psykoterapisenter i Helsinki utsatt for datainnbrudd i oktober 2020, hvor både virksomheten og enkeltpasienter ble utsatt for løsepengekrav med trusler om datalekkasje. Det er en risiko for tilsvarende operasjoner, med trusler mot enkeltpersoner, også i Norge.

At virksomhetene betaler løsepenger er ingen garanti for at stjålne data ikke selges videre, eller at krypterte data igjen blir tilgjengelige. NSM anbefaler å ikke betale løsepengekravet fordi dette direkte finansierer alvorlig kriminalitet. I tillegg viser det at virksomheten er betalingsvillig, noe som har vist seg å bli utnyttet gjennom flere utpressingsrunder.

Internasjonalt har årets store løsepengehendelser skapt større samfunnskonsekvenser enn tidligere. Hendelsene mot Coop Sverige, amerikanske Colonial pipeline og JBS spredte frykt for varemangel og gjorde tjenester

[4] *https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf*

[5] *Ifølge Microsoft.*

LØSEPENGEVIRUS STENGTE VITAL DRIVSTOFFLEDNING TIL DET NORDØSTLIGE USA – COLONIAL PIPELINE

Colonial Pipeline ble tidlig i mai offer for et løsepengevirusangrep hvor angriperne overførte og krypterte store datamengder fra selskapet. Kompromittert innloggingsinformasjon på en VPN-løsning, som skulle gjøre det mulig for ansatte å logge seg på hjemmefra, samt fravær av bruk av multifaktorautentisering skal være årsaken til at angriperne fikk tilgang til selskapets IT-systemer. Hendelsen medførte fem dagers stans i selskapets drivstoffdistribusjon til store deler av USAs østkyst. Stansen skapte frykt for økte oljepriser og drivstoffmangel i de berørte områdene, noe som førte til hamstring av drivstoff.

Colonial Pipeline valgte å betale løsepengene kort tid etter hendelsen. Imidlertid skal amerikanske myndigheter ha greid å gjenskaffe deler av beløpet.

Colonial Pipeline-saken har satt fokus på hackergrupper som ikke er direkte statssponsede, men som drar nytte av at staten de opererer fra ikke straffeforfølger dem for økonomisk kriminalitet i utlandet, herunder løsepengevirus. Amerikanske myndigheter pekte etter kort tid på gruppen DarkSide som ansvarlig for hendelsen, og at Russlands mangel på sanksjoner mot gruppen gjør dem medansvarlig.

Leverandørkjedeangrep mot amerikanske SolarWinds

Sent i desember 2020 ble det kjent at det amerikanske IT-selskapet SolarWinds hadde blitt utsatt for et leverandørkjedeangrep. Dette var en sofistikert og omfattende cyberoperasjon hvor trusselaktøren klarte å etablere en bakdør i et av programmene til SolarWinds.

Bakdøren ble så med i en oppdatering av programmet som SolarWinds selv distribuerte til sine kunder, over 18.000 virksomheter verden over. Disse installerte da en offisiell og tilsynelatende sikker oppdatering fra selskapet, men med en bakdør som kun trusselaktøren visste om og kunne utnytte for videre kompromittering hos kunden.

Noe av alvorlighetsgraden lå i typen program som ble rammet. Det er designet for å utføre nettverksovervåking og vil derfor som regel ha vide tilganger til virksomhetens infrastruktur. Ved å infiltrere dette fikk aktøren et svært gunstig utgangspunkt for å komme seg videre inn i nettverket og omgå sikkerhetsmekanismer.

Sikkerhetsselskaper, SolarWinds og amerikanske myndigheter publiserte mange detaljer rundt programvaren og en rekke tekniske indikatorer. Cybersecurity and Infrastructure Security Agency (CISA) gav kort tid etter at angrepet ble kjent alle myndighetsorganer i USA instruks om å sikre sine data og deretter deaktivere utstyr og programvare fra SolarWinds. Alle private virksomheter ble anbefalt å gjøre samme tiltak.

Amerikanske myndigheter gikk senere ut og pekte på at aktøren bak angrepet sannsynligvis hadde russisk opphav.

Saken hadde omfattende konsekvenser for de som ble rammet, herunder amerikanske myndighetsorganer og store teknologiselskaper som Microsoft. Etter å ha fått tilgang til virksomheter som hadde installert oppdateringen med bakdøren, spisset aktøren sine kapasiteter mot utpekte mål.[5] Det indikerte at aktøren ikke agerte på alle tilganger den har oppnådd, men heller prioriterte enkelte virksomheter som ble utsatt for mer målrettede metoder for videre kompromittering.

NCSC arbeidet tett med nasjonale og internasjonale samarbeidspartnere for å kartlegge omfanget av hendelsen. Vi fulgte anbefalinger fra CISA, FireEye og Microsoft og oppfordret alle virksomheter som brukte programvaren i sin infrastruktur til å sette seg inn tilgjengelig dokumentasjon.

Flere av SolarWinds' kunder i Norge hadde installert en kompromittert versjon av programmet. De store konsekvensene uteble fordi bakdøren ikke ble utnyttet. Denne type leverandørkjedeangrep er noe NSM forventer mer av i tiden fremover, muligens også med betydelige konsekvenser for norske mål.

utilgjengelige. Cyberoperasjonen mot kjøttprodusenten JBS, som ble lagt til Memorial Day-helgen, er et eksempel på at aktører i større grad bruker merkedager til å gjennomføre slike operasjoner. Dette kan være i håp om å forbli uoppdaget lengre i systemene eller for å ramme på verst tenkelige tidspunkt.

Potensialet som ligger i krypteringsvirus gjør metoden attraktiv både for kriminelle grupper og avanserte aktører som stater eller statsstøttede grupper. De potensielle konsekvensene av et krypteringsvirus er store og kan i verste fall sette kritiske samfunnsfunksjoner ut av spill. Løsepengehendelser skaper mye støy og kan potensielt brukes i kombinasjon med annen aktivitet for å ta oppmerksomhet vekk fra en større operasjon, eksempelvis fra en statlig aktør. Internasjonalt har man tidligere sett flere såkalte «false flag» operasjoner, der statlige aktører har gjennomført operasjoner med løsepenger som i realiteten har hatt som formål å sabotere kritisk infrastruktur.

Mange virksomheter som rammes av løsepengevirus er i liten grad forberedt. Veien inn i virksomhetens systemer er ikke nødvendigvis så avansert - et dårlig passord kan være nok. Gjennom dette kan aktøren utløse et potensielt lammende løsepengevirusangrep med enorme kostnader.

Virksomheter som ikke har gjort tilstrekkelig forebyggende tiltak må forvente å kunne bli rammet av krypteringsvirus og løsepengekrav. Dersom man rammes er det viktig å sikre effektiv håndtering av selve hendelsen, men også hindre lekkasje av sensitive data. Gjenoppretting er både tid- og ressurskrevende, og komplisert. Full stans i virksomheten og tap av sensitiv informasjon kan vise seg å bli vesentlig mer kostbart enn å investere i forebyggende sikkerhetsarbeid. Det bør derfor stå høyt på agendaen hos alle å sikre seg mot dette. NCSC har utarbeidet en oppdatert veileder med tiltak for beskyttelse mot skadevare og løsepengevirus.[6]

Hvordan skape sikrere leverandørkjeder?

Økt digitalisering og tjenesteutsetting av samfunnsfunksjoner medfører lengre verdi- og leverandørkjeder. Samtidig medfører tjenesteutsetting nye ledd i leverandør- og verdikjeder, som igjen bidrar til at det blir vanskeligere å ha oversikt over sårbarheter som kan utnyttes av trusselaktører. Verdikjedeangrep mot tilgrensende virksomheter til et egentlig mål forekommer fremdeles i Norge. Programvare- og tjenesteleverandører kan også utnyttes av trusselaktører for å få innpass i systemene til selskapets kunder i såkalte leverandørkjedeangrep. Et eksempel er leverandørkjedeangrepet mot SolarWinds (se tekstboks s. 25).

[6] https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/skadevare/tiltak-mot-skadevare-og-losepengevirus

Programvare- og tjenesteleverandører kan også utnyttes av trusselaktører for å få innpass i systemene til selskapets kunder i såkalte leverandørkjedeangrep.

Leverandørkjedeangrep med bruk av nulldagssårbarhet og løsepengevirus

Tjenesteleverandøren Kaseya ble utsatt for et leverandørkjedeangrep i juli 2021.

Aktøren hadde trolig utnyttet en nulldagssårbarhet i Kaseya VSA, som er en RMM-programvare (Remote Monitoring and Management). Kaseya VSA benyttes av en rekke store tjenesteleverandører globalt, som primært bruker denne for å nå ut til sine kunder. Sårbarheten ble utnyttet for å levere REvil løsepengevirus som berørte en rekke tjenesteleverandører og deres kunder.

Angrepet ble muliggjort ved at en aktør tok seg inn i Kaseya VSA-servere plassert hos tjenesteleverandørene og deretter kjørte en automatisk oppdatering av Kaseya-agenter som befinner seg ute hos tjenesteleverandørenes kunder. Gjennom oppdateringen kjøres et REvil løsepengevirus som legger igjen et løsepengekrav til kundene for gjenoppretting av sine systemer.

Kaseya implementerte en rekke tiltak for å hindre videre spredning av løsepengeviruset og utviklet en sikkerhetsoppdatering til sårbarheten. Videre ble det publisert offisielle verktøy for å avdekke hvorvidt kunder er sårbare for utnyttelse eller berørt av hendelsen.

Internasjonalt rapporterte Kaseya om 60 kunder som var kompromittert direkte. NCSC er kjent med at et fåtall norske tjenesteleverandører har hatt kunder som kunne motta løsepengeviruset gjennom det skisserte hendelsesforløpet. Eventuelle forsøk mot disse har i stor grad enten vært stoppet i sikkerhetsløsninger eller involvert kunder som allerede har fulgt Kaseyas anbefalinger, og deaktivert berørte systemer. NCSC er ikke kjent med hendelser av større omfang eller med betydelig konsekvens i Norge.

Trusselaktører kan skjule skadevare i programvare som leverandøren selger videre til sine kunder. På denne måten kan en trusselaktør enkelt etablere brohoder hos mange nye virksomheter. Skadevaren kommer inn i nye virksomheters systemer i form av en ordinær anskaffelse eller oppgradering, og slike sårbarheter kan være vanskelig å oppdage.

Beskyttelse mot leverandørkjedeangrep krever at angrepskjeden brytes. Dette krever god segmentering av nettet, brannmurregler og ikke minst god kontroll på hva som er eksponert mot internett. På denne måten reduseres muligheten for at en aktør får tilgang til systemet.

Dersom bakdøren likevel blir installert vil god sikring og kontroll på hva som eksponeres mot internett hindre denne i å kommunisere tilbake til aktøren, og deretter forhindre ytterligere handlinger mot målet. Kartlegging av egne digitale avhengigheter og verdikjeder, samt å stille krav til tjenesteleverandørenes IT-sikkerhet er helt essensielt for en virksomhet for å redusere konsekvensene av en cyberoperasjon mot tjenesteleverandøren. Virksomheter kan beskytte sine IT-systemer og digitale infrastruktur mot angrep som kan komme via leverandører eller samarbeidspartnere ved å ta i bruk «Zero Trust». Det tar utgangspunkt i at tilliten til de enkelte komponentene i vår egen infrastruktur er like lav som den tilliten vi har til selve internett.

«Zero Trust» er ikke en ny teknisk løsning, men en tilnærming som har utviklet seg over flere år og som nå er tilstrekkelig moden til å kalles en arkitektur. Den favner tidligere anbefalinger om digital sikkerhet fra NSM, og vektlegger behovet for å etablere like sterke sikkerhetstiltak mellom systemene i virksomhetens interne nett som for de systemene som er eksponert for det offentlige internettet. Det er en tilnærming som kan brukes både for tradisjonelle IT-systemer og for skytjenester.

Kritiske samfunnsfunksjoner kan rammes

Den siste tidens hendelser innen leverandørkjedeangrep har ført til at systemer innen operasjonell teknologi og industrielle kontrollsystemer (OT) har blitt indirekte påvirket av digitale hendelser i de administrative IT systemene. Dette er en effekt av økt avhengighet og sammenkobling av nettverk mellom administrative systemer og industrielle systemer. Dette introduserer flere sårbarhetsflater og vil medføre et potensial for risikovandring mellom sårbare OT-systemer og administrative systemer. Her kan kompromitteringer forekomme ved utnyttelse av digitale tjenester, som fjernaksessløsninger, eller innføring av «tingenes internett» (IoT) som i stor grad vil føre til økt nettverkstilkobling. Kompromittering og uønskede hendelser i OT-systemer kan få alvorlige konsekvenser og kan føre til bortfall av kritiske samfunnsfunksjoner.

[7] https://www.telenor.no/binaries/om/digital-sikkerhet/digitalsikkerhet2021.pdf

[8] www.nsm.no/grunnprinsipper-ikt

Ved å ta i bruk «Zero Trust» kan virksomheter beskytte sine IT-systemer og digitale infrastruktur mot angrep via leverandører og samarbeidspartnere

Telenors rapport «*Digital sikkerhet* 2021»[7] fremhever også digitale trusler og sårbarheter i OT- systemer og sårbarheten disse har ved økt tilkobling mot IT-systemer og innføring av IoT. Denne utviklingen fører til økt eksponering av OT-systemer som igjen øker risikoen for at trusselaktører kan gjennomføre digitale operasjoner mot slike systemer.

Sikkerhetsbevisste virksomheter?

NCSC erfarer fortsatt at alle digitale hendelser kunne vært unngått eller skaden begrenset dersom virksomheter i større grad hadde implementert «NSM *Grunnprinsipper for IKT-sikkerhet*».[8] I møte med virksomheter som har vært utsatt for cyberoperasjoner er det fremdeles mange som ikke har grunnleggende sikringstiltak på plass. Virksomheter må forholde seg til teknologisk utvikling, regulatoriske krav, kontraktmessige forpliktelser, og et komplekst trussel- og risikobilde i stadig endring. Å være rustet til å motstå uønskede digitale hendelser beror ikke på å implementere tekniske tiltak alene, men

OPERASJONELL TEKNOLOGI OG INDUSTRIELLE KONTROLLSYSTEMER

Operasjonell teknologi og industrielle kontrollsystemer (OT) brukes i flere sektorer hvor slike systemer styrer eller overvåker viktige fysiske prosesser eller funksjoner i sin verdikjede. Disse systemene har både ulik størrelse og kompleksitet alt etter hvilke fysiske prosesser de overvåker og styrer. Slike systemer finnes blant annet innen petroleum, kraft og energi, luftfart, sjøfart, samferdsel eller annen infrastruktur.

En av utviklingstrendene for OT-systemer er økt bruk av tradisjonelt IT-utstyr i kombinasjon med OT-systemenes rolle og funksjon. Økt bruk av IT-utstyr i slike systemer er en følge av den pågående digitaliseringen og automatiseringen i industrien som kan kalles «industri 4.0».

Dette medfører at det blir flere integrerte og komplekse systemer hvor de tradisjonelt mindre systemene blir erstattet eller integrert inn i et større system. Digitalisering og effektivisering av systemer og prosesser vil i økende grad føre til integrasjon av sensorteknologi, 5G og IoT for å kunne dele og eksportere mer sanntidsdata og informasjon fra OT-systemene.

TRUSSELVURDERING FRA KRAFTCERT/INFRACERT

KraftCERT/InfraCERT ser en stor økning i både antall og type digitale hendelser de siste 18 månedene. Trusselaktørene som opererer mot sektorene er mange og har varierende kompetanse og kapasitet. KraftCERT erfarer variasjon i både angrepsmål og angrepsteknikker som viser at aktørene har evne til å tilpasse seg ulike mål. En av de største truslene er krypteringsvirus (utpressingsskadevare). Det er flere tredjepartsangrep, hvor angrepene skjer gjennom kunder, leverandører eller partnere. Sårbare tillitsforhold mellom kunder og leverandør blir oftere mål for trusselaktører.

Med tanke på trusselaktørenes utvikling, utveksling av tjenester mellom disse og utvikling i skadevare, er det sannsynlig at man vil se ytterligere økning i antall hendelser, spesielt mot systemer og teknologier med stor utbredelse. Kontroll-systemer er fortsatt til dels foreldet teknologi og kan ofte kompromitteres med enkle teknikker, derfor er all direkte internettilgang til/fra slike systemer svært risikabelt. Nyere teknologi åpner muligheter for større grad av kontroll og deteksjon, men åpner også nye sårbarhetsflater.

Alle digitale hendelser kan unngås eller begrenses ved å ta i bruk «NSMs *grunnprinsipper for IKT-sikkerhet*».

innebærer en rekke faktorer – tekniske, menneskelige og prosessuelle - som til sammen reduserer risiko. Digital sikkerhet er et lederansvar som i større grad må prioriteres av eiere og styret. Ledelsen bør måles på sikkerhetsarbeidet i virksomheten.

NSM oppfordrer alle virksomheter til å regelmessig gjøre risikovurderinger, og oppdatere disse ved endringer, eller ved tilkobling av nye løsninger og funksjoner i virksomhetens digitale infrastruktur. Formålet med risikostyring er å sikre at virksomheten når sine mål og prioriterer de aktiviteter som er mest kritiske for å nå målene. «NSM *risikovurdering av IKT-systemer*»[9] sammen med «NSM *grunnprinsipper for IKT-sikkerhet*» vil hjelpe virksomheten å komme i gang med risikovurderinger. Disse produktene erstatter ikke allerede etablerte metoder eller konsepter innen risikovurdering, men er avgrenset til risikovurdering for digitale systemer med utgangspunkt i tekniske og organisatoriske tiltak. Risikovurderingen bygger på forholdet mellom verdi, trussel og sårbarhet. Virksomheten og ledelsen har alltid ansvaret for sikring av egne verdier. Risikovurdering og risikohåndtering er helt nødvendig for å oppnå et forsvarlig sikkerhetsnivå i egen virksomhet.

Varsling og erfaringsutvekslinger er vesentlig

NSM er avhengig av rapportering fra virksomheter som utsettes for uønskede digitale hendelser. NCSCs nasjonale partnere, sektorvise responsmiljøer og internasjonale partnere er også viktige for å avdekke hendelser mot norske mål. Denne informasjonen danner del av

[9] https://nsm.no/getfile.php/136603-1625054089/Demo/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf

[10] https://nsm.no/fagomrader/sikkerhetsstyring/leverandorforhold/kvalitetsordning-for-leverandorer-som-handterer-ikt-hendelser

[11] https://nsm.no/getfile.php/133853-1593022504/Demo/Dokumenter/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

[12] https://www.dnb.no/portalfront/nedlast/no/om-oss/samfunnsansvar/2021/DNB_rlig_Trusselvurdering_2021_Final_Lowres.pdf

[13] https://nsm.no/tjenester/allvis-nor/

1 PLANLEGGING

Involver og planlegg

- Sørg for å få ledelsesaksept.
- Avgrens og sett et mål for arbeidet.
- Identifisere hvilke relevante ressurser som er nødvendig.
- Lag en plan for risikovurderingen med estimater.

2 RISIKOVURDERING

Identifiser, analyser og evaluer

- Identifiser hvilke IKT-systemer som skal vurderes.
- Indentifisere sårbarheter og eventuelle trusler.
- Identifisere eksistiserende sikkerhetsmekanismer.
- Identifisere konsekvenser ved brudd på tilgjengelighet, integritet og konfidensialitet

3 RISIKOHÅNDTERING

Effekter og videre oppfølging

- Lag en plan for oppfølging av risikoreduserende tiltak.
- Vurder effekten av sikkerhetstiltak ved bruk av styringsparameter (KPI).
- Vurder restrisikoaksept.
- Ledelsesinvolvering og beslutning om videre oppfølging av risikotiltak.

Trestegs-prosessen som gjengitt i *«NSM risikovurdering av IKT-systemer»* består av planlegging, risikovurdering og risikohåndtering. Hvert steg inneholder flere aktiviteter og delleveranser.

grunnlaget for våre vurderinger av endringer i det digitale risikobilde i Norge. Medlemmer i kvalitetsordningen for hendelseshåndtering[10] bistår mange norske virksomheter som utsettes for cyberoperasjoner, og informasjon fra disse bidrar også til å belyse det digitale risikobildet. Også de sektorvise responsmiljøene er viktige i hendelseshåndtering av cyberoperasjoner som rammer mål i sine sektorer.

I 2017 vedtok Justis- og beredskapsdepartementet og Forsvarsdepartementet et rammeverk for håndtering av IKT-sikkerhetshendelser.[11] NSM arbeider i år med en revidering av rammeverket med særlig fokus på forenkling og tydelig ansvarsfordeling.

Varsling er også viktig. I 2020 og 2021 har våre varsler omhandlet alt fra informasjon om trender, sikkerhetsoppdateringer og sårbarheter, samt rådgivning og tiltak. Et eksempel er i forbindelse med sårbarhetene i Microsoft Exchange hvor NCSC sendte ut over 1000 varsler til virksomheter og partnere.

Åpenhet rundt hendelser og informasjonsdeling er viktig og fører til en økt bevisstgjøring generelt i samfunnet. Vi opplever at virksomheter i økende grad er åpne om at de har vært utsatt for uønskede digitale hendelser og deler sine erfaringer. ■

ERFARINGER FRA FINANSBRANSJEN

Nordic Financial CERT peker på at flere alvorlige hendelser og trusler både i verden og i Norge det siste året er en stadig påminnelse om viktigheten av kontinuerlig godt sikkerhetsarbeid – slik det bl.a. er beskrevet i *«NSMs grunnprinsipper for IKT-sikkerhet»*. Nordic Financial CERT rapporterer at godt sikkerhetsarbeid fungerer, og at mangelen på større hendelser i finansnæringen kan sees på som et eksempel på dette.

Nordic Financial CERT rapporterer videre at hendelser som har vært nærmest finansbransjen det siste året er løsepengehendelsene hos Sopra Steria og Qualys, i tillegg til utnyttelse av sårbarhetene i Exchange on-premise instanser samt leverandørkjedehendelsen med SolarWinds. Også NCSCs samarbeidspartner DNB fremhever leverandørkjedeangrepet mot SolarWinds i sin trusselvurdering for 2021[12].

Nordic Financial CERT har sett at finansnæringen har godt fokus og mange gode tiltak på plass, noe som reduserer mulighetene for større hendelser - samt reduserer konsekvensene dersom en uønsket hendelse skulle inntreffe.

OM ALLVIS NOR[13]

Allvis NOR er NSMs automatiserte sårbarhetskartlegger. Dette er en gratis tjeneste som tilbys til virksomheter underlagt sikkerhetsloven og virksomheter som eier eller forvalter samfunnsviktig infrastruktur eller tjenester. Les mer på NSMs hjemmesider.

Bedriften Norsk Vaksine AS (Norvaks AS) blir utsatt for et dataangrep – et typisk hendelsesforløp

Bedrift Norsk Vaksine AS (Norvaks AS) jobber med å utvikle en norsk koronavaksine. Bedriften har i løpet av kort tid vokst fra å være ca 50 ansatte til å bli over 200 ansatte.

De har en egen IT-avdeling og drifter alle IT-systemer selv. De består i all hovedsak av forskere og er vant til å dele mye informasjon seg imellom. Alle ansatte har hatt tilgang til all data virksomheten produserer og de ansatte har tradisjonelt hatt store tilganger i systemene. Norvaks har aldri vært utsatt for dataangrep og ser ikke på seg selv som et særlig attraktivt mål for hackere.

Det interne nettverket bærer preg av stor tillitt og åpenhet. Det er delt inn i noen enkle soner, men data flyter stort sett fritt mellom de ulike sonene. Virksomheten bærer preg av mye manuell drift og mangler en god oversikt over alt som er koblet til nettverket.

Tiltakene under er hentet fra *"NSM grunnsprinsipper for IKT-sikkerhet"*.

1

Aktøren har kartlagt Norvaks AS og forsøker deretter å kompromittere en internetteksponert tjeneste (A) i DMZ-nettverket til virksomheten. Dette forsøket lykkes ikke.

TILTAK:
Her har Novaks fulgt *«NSM Grunnprinsipper for IKT-sikkerhet»* og sikret sine internetteksponerte tjenester på en forsvarlig måte.

2

Aktøren forsøker deretter å kompromittere en server (B) i Norvaks' interne nettverk som er tilgjengelig på internett. Serveren er ikke sikkerhetsoppdatert til nyeste versjon og dårlig sikret. Aktøren lykkes i å kompromittere serveren.

TILTAK:
> Prinsipp 1.2. Kartlegg enheter og programvare med underliggende tiltak.

3

Aktøren beveger seg sideveis i Norvaks' nettverk og kompromitterer en ny server (C) i lukket nett. Kompromitteringen skjer ved å gjette et dårlig passord «Sommer2021» over RDP*. Serveren (C) er en databaseserver.

TILTAK:
> 2.2. Etabler en sikker IKT-arkitektur
> 2.3. Ivareta en sikker konfigurasjon
> 2.5. Kontroller dataflyt
> 2.6. Ha kontroll på identiteter og tilganger

* *Remote Desk Protocol.*

4

Aktøren beveger seg fra databaseserver (C) til server (D) i en sikker sone via en kjent sårbarhet i en fildelingsprotokoll. Denne serveren er ansett så «sikret» og «isolert» at denne ikke er sikkerhetsoppdatert. Serveren inneholder verdifull informasjon for aktøren og er målet til aktør.

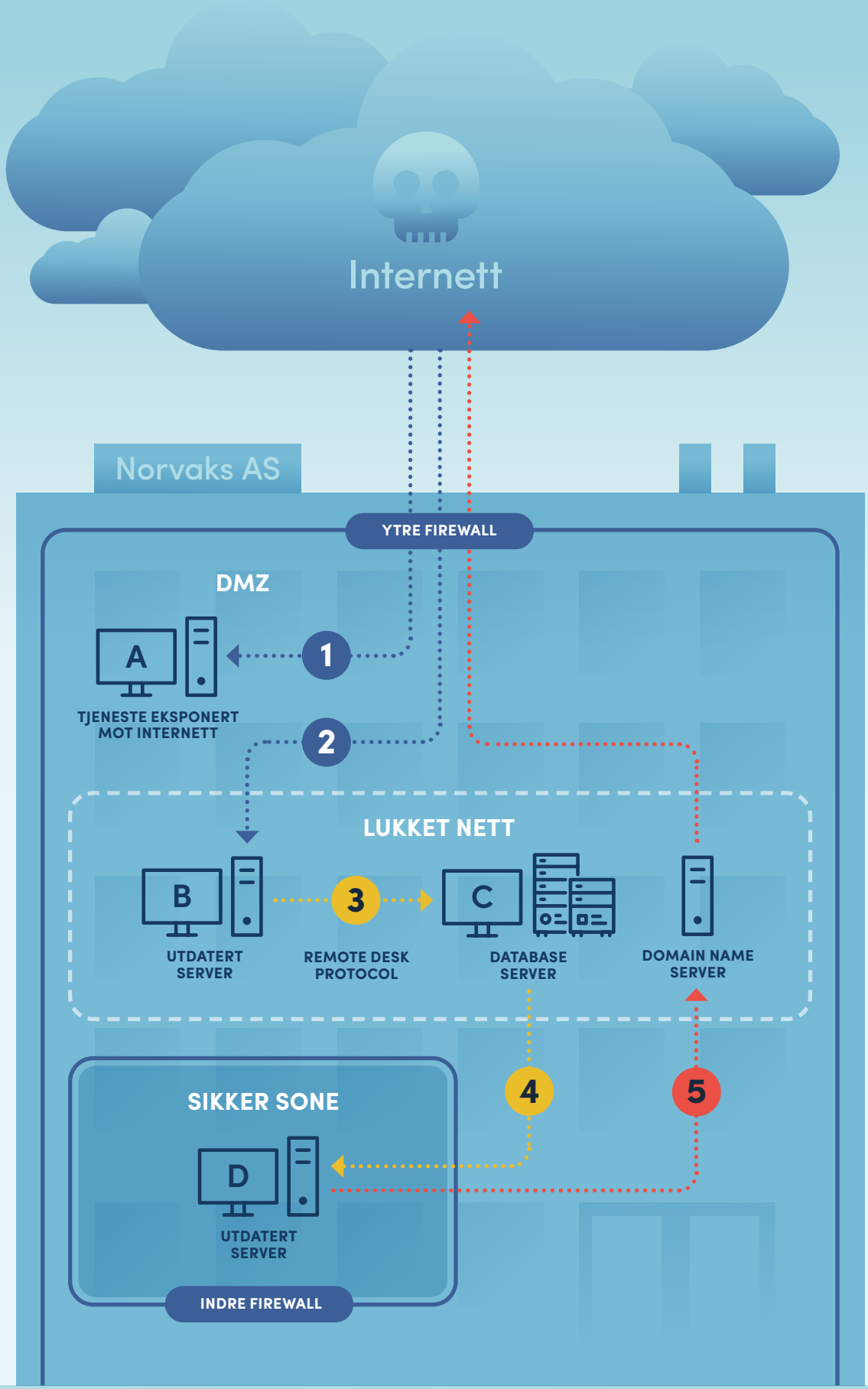
TILTAK:
> 2.3. Ivareta en sikker konfigurasjon
> 2.3.3. Deaktiver unødvendig konfigurasjon
> 2.5. Kontroller dataflyt
> 3.1. Oppdag og fjern kjente sårbarheter og trusler

5

Aktøren henter ut verdifull data fra server (D) og eksfiltrerer denne tilbake til seg selv via DNS** i Norvaks' nettverk over internett.

TILTAK:
> 2.3. Ivareta en sikker konfigurasjon
> 2.5. Kontroller dataflyt
> 3.2. Etabler sikkerhetsovervåkning
> 3.3. Analyser data fra sikkerhetsovervåkning

** *Domain Name Server.*

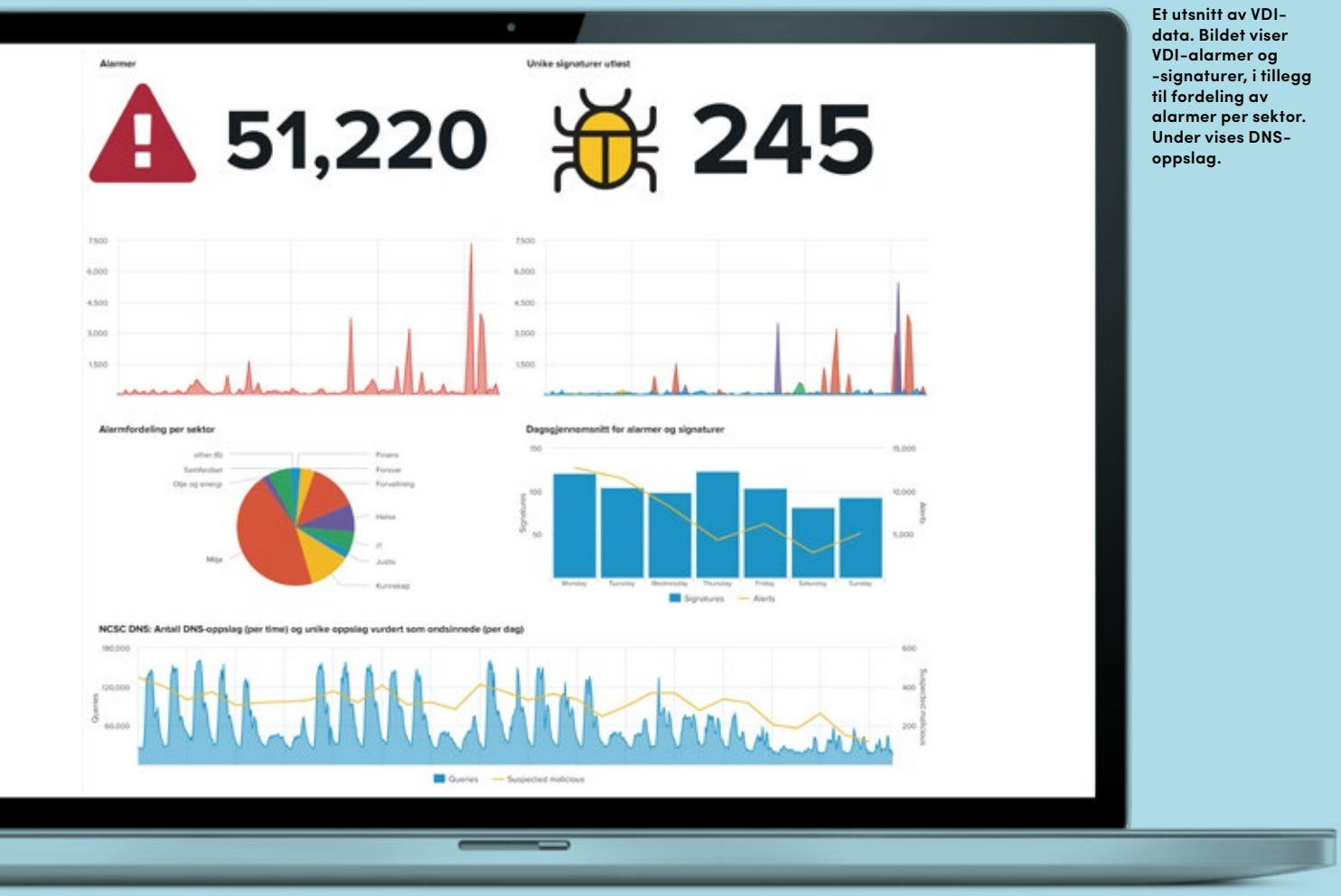

Internett
Norvaks AS
YTRE FIREWALL
DMZ
A
TJENESTE EKSPONERT MOT INTERNETT
1
2
LUKKET NETT
B
UTDATERT SERVER
3
REMOTE DESK PROTOCOL
C
DATABASE SERVER
DOMAIN NAME SERVER
SIKKER SONE
4
5
D
UTDATERT SERVER
INDRE FIREWALL

Slik beskytter NSM Norge mot cyberoperasjoner – varslingssystem for digital infrastruktur (VDI) utgjør et aktivt cyberforsvar

NSMs mandat er å oppdage de avanserte aktørene og designe tiltak ut ifra deres verktøybruk og operasjonsmetode. VDI er et sensornettverk som er under kontinuerlig utvikling som bidrar til et aktivt cyberforsvar. VDI skal kunne oppdage og varsle om cyberoperasjoner som treffer kritisk infrastruktur eller kritiske funksjoner i Norge.

Frem mot 2023 gjøres en betydelig videreutvikling av VDI. Arbeidet med å bygge et aktivt cyberforsvar blir vi ikke ferdige med – dette må kontinuerlig utvikles for å kunne forebygge, oppbygge og håndtere digitale operasjoner. Les mer på NSMs hjemmesider.[14]

[14] https://nsm.no/tjenester/varslingssystem-vdi/



Et utsnitt av VDI-data. Bildet viser VDI-alarmer og -signaturer, i tillegg til fordeling av alarmer per sektor. Under vises DNS-oppslag.

ERFARINGER FRA NSMS INNTRENGINGSTESTING 2020 - 2021

Inntrengingstesting i regi av NSM innebærer en evaluering av utvalgte servere, klienter og infrastruktur. Inntrengningstesting beskriver et øyeblikksbilde av sikkerheten til en virksomhet, og er basert på stikkprøver mot utvalgte komponenter og vil således ikke gi en komplett oversikt over et systems sårbarheter. Tester og oppfølgende råd og anbefalinger er basert på en antakelse om at aktuelle trusselaktører både er ressurssterke og særdeles kompetente. Ved å benytte offentlig tilgjengelige og egenutviklede angrepsteknikker har NSM tatt kontroll over systemene til en rekke samfunnskritiske virksomheter.

Bruk av offentlig tilgjengelige sårbarheter har ved flere anledninger gitt fulle tilganger til ulike tjenester og systemer. Med slik tilgang kan en angriper få uautorisert tilgang til virksomhetens verdier og kommunisere tilbake til egen infrastruktur. I teorien kan dette innebære alt fra fjernstyring av kontrollsystemer til å få tilgang til eller mulighet for å endre eller slette informasjon.

Ved å kompromittere en internett-eksponert tjeneste, eksempelvis en nettside, kan man slette, endre og/eller publisere egne dokumenter. Dersom dette gjøres mot en nettside som offentligheten har stor tillitt til kan endring av innhold på nettsiden få konsekvenser i form av feilaktig informasjon til offentligheten.

Vi erfarer fremdeles at dårlige passord i de fleste tilfeller er den enkleste veien inn i virksomheters systemer. Korte passord på under tolv tegn er sårbare for både regelbaserte- og uttømmende angrep. Flere brukere har så svake passord at det er mulig å gjette seg frem til dem, og det er følgelig enkelt å få tilgang til dataene deres. NSM har sett bruk av passordene «Sommer2020», «Sommerferie2021» og «September2020» i sine inntrengingstester. Det er funnet flere gamle systemkontoer som tilsynelatende ikke lenger var i bruk. Flere av disse hadde også gamle, eller svært gamle passord. Ett passord var sist endret i 1999.

Vi erfarer fortsatt at nettverkssikkerheten hos svært mange virksomheter er svak. I mange tilfeller er nettverkssikkerhet så godt som fraværende, og selv i virksomheter som har implementert segmentering har NSM ved flere anledninger klart å utnytte svakt sikrede servere med koblinger i ulike sikkerhetssoner. Dette gjør det mulig å angripe ellers godt isolerte tjenester og soner.

NSM har også sett eksempler på god nettverkssikkerhet. Dette innebærer blant annet mikrosegmentering, hvor klientene har vært forhindret fra å kommunisere direkte med hverandre. Det er også eksempler på effektiv filtrering som i stor grad bidrar til å beskytte systemet gjennom å hindre unødvendig trafikkflyt mellom servere. Dette gjør angrepsflaten vesentlig mindre, og bidrar dermed til å forhindre mange potensielle kompromitteringer. Videre er det tilfeller hvor virksomheten har installert beskyttelsesmekanismer mot å koble eget utstyr i systemet, noe som bidrar til å styrke sikkerheten.

Implementering av risikoreduserende tiltak, som «*NSMs Grunnprinsipper for IKT-sikkerhet*», kan bidra sterkt til å øke virksomhetens motstandskraft ved angrep mot systemets tilgjengelighet, integritet eller konfidensialitetsbeskyttelse. Resultatet vil totalt sett være redusert risiko for tap av virksomhetens verdier, tillit eller omdømme.

3. Strategier og utfordringer: status i sikkerhetsarbeidet

Samfunnet har blitt mer digitalisert. Ny teknologi endrer måten vi jobber på og hvordan vi behandler data. Det oppstår flere og større avhengigheter mellom ulike digitale systemer og dette skaper sårbarheter. Det er bekymringsverdig at stadig flere samfunnsverdier flyttes over i det digitale domenet, uten at det først er gjennomført tilstrekkelig verdi- og risikovurderinger. Når en risikovurdering foreligger med risikoer identifisert og evaluert, må beslutningstaker håndtere risikoen på en god måte.[15]

En trygg digitaliseringsprosess krever innebygd sikkerhet. Dette må planlegges og bygges inn som en del av løsningen fra starten og kan ikke komme som et tillegg når produkter og løsninger er ferdig og skal tas i bruk. Sikkerhet må være et gjennomgående tema for løsningsvalg, design, systemarkitektur og kultur i virksomhetene. Tekniske sikkerhetstiltak alene vil ikke stoppe trusselaktører, det er nødvendig med gode prosesser i virksomheten og god sikkerhetskultur hos brukere av system og virksomhetens ansatte. Dette øker robusthet, men også bevissthet og forståelse for sikkerhet hos den enkelte.

Nasjonal satsing på digital sikkerhet

Nasjonal strategi for digital sikkerhet med tilhørende tiltak ble lansert i 2019. Strategien har bidratt til å synliggjøre de overordnede nasjonale målene for digital sikkerhet og viktige nasjonale tiltak i en helhetlig tilnærming for bedre digital sikkerhet. NSM arbeider selv med å iverksette en rekke av tiltakene i strategien, og ser at den digitale risikoen er stadig mer krevende. Derfor er det viktig med fortsatt målrettet, systematisk forebyggende digitalt sikkerhetsarbeid langs mange akser. Den nasjonale strategien er derfor et viktig verktøy også fremover.

Grunnleggende nasjonale funksjoner (GNF-er) er funksjoner som har betydning for statens evne til å ivareta de nasjonale sikkerhetsinteressene. Det er det enkelte departement som er ansvarlig for å identifisere og holde oversikt over GNF-er innen sine ansvarsområder. Arbeidet med å identifisere, konkretisere og avgrense GNF har pågått siden lov om nasjonal sikkerhet trådde i kraft 1. januar 2019. Våren 2021 publiserte NSM på våre hjemmesider en samlet oversikt over identifiserte GNF-er.[16] Det er i dag identifisert over 40 GNF-er. Arbeidet med identifisering av GNF er en kontinuerlig prosess, og prosessen påvirkes av den teknologiske utviklingen, endringer i trusselbildet, og den generelle samfunnsutviklingen. Over tid vil det derfor være endringer i hvilke funksjoner som anses som GNF, og hvordan disse funksjonene er avgrenset og konkretisert. De identifiserte GNF-ene synliggjør bredden i arbeidet med nasjonal sikkerhet. Noen funksjoner ivaretas i hovedsak av offentlige etater, med avhengighetsforhold til private virksomheter. Andre funksjoner ivaretas imidlertid primært av private virksomheter.

Virksomhetenes arbeid med å kartlegge avhengighetsforhold til andre virksomheter er en pågående og løpende prosess. Kartlegging, vurdering og rapportering av avhengigheter mellom virksomheter er avgjørende for å kunne danne seg et helhetlig bilde av hvilke innsatsfaktorer som er av betydning for grunnleggende nasjonale funksjoner. Dette arbeidet vil føre til at flere virksomheter blir omfattet av sikkerhetsloven.

[15] *Les mer i temarapport «Risikovurdering av IKT-systemer», https://nsm.no/getfile.php/136603-1625054089/Demo/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf*

[16] *https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-nasjonale-funksjoner-gnf/*

Digital sikkerhet er i økende grad på dagsorden både hos statsledere og i internasjonalt diplomati.

STORTINGS- OG SAMETINGSVALGET 2021

Åpenhet og tillit er grunnleggende i demokratiet vårt. De siste årene har vi sett forsøk på å påvirke valg i flere land. NSM vurderte at det kunne være en risiko for at valgprosessen og/eller valggjennomføringen i 2021 kunne bli utsatt for cyber- eller påvirkningsoperasjoner. Erfaringsmessig vil særlig utenlandske etterretningstjenester ha et vedvarende fokus på politiske mål, uavhengig av valgår. Vi vet at flere aktører har både evne og vilje til å gjennomføre både cyber- og påvirkningsoperasjoner mot mål i Norge.

En av NSMs viktigste oppgaver i år har derfor vært å bidra til en sikker gjennomføring av valget. Dette innebar både å bidra til en teknisk sikker valggjennomføring, men også til å forhindre urettmessig og fordekt påvirkning av befolkningen.

Regjeringen Solberg lanserte 1. juni i år 13 tiltak for å hindre uønsket påvirkning i valget.[17] Disse tiltakene skulle styrke motstandsdyktigheten mot uønsket påvirkning før, under og etter høstens Stortings- og sametingsvalg. NSM har i samarbeid med PST, Etterretningstjenesten, Kripos og andre myndighetsorganer bidratt til flere av disse tiltakene.

NSM har arbeidet tett med Valgdirektoratet for å gjøre den tekniske valggjennomføringen så sikker som mulig – både for å herde systemene, men også for å kunne avdekke forsøk på ondsinnet aktivitet. NSM har også hatt utstrakt rådgivningsaktivitet og vært i tett dialog både med de politiske partiene som er representert på Stortinget, og andre aktører med betydning for valggjennomføringen.

Kjernen i NSMs forebygging av påvirkningsoperasjoner opp mot valget er en beredskapsordning for sosiale medier. NSM har hatt tett kontakt med de store plattformleverandørene og kunne videreformidle informasjon til disse dersom vi fikk informasjon om kompromitterte eller falske kontoer i sosiale medier.

Når denne rapporten publiseres er det noen uker siden vi gjennomførte Stortings- og sametingsvalg i Norge. NSM har ikke har sett aktivitet som tyder på koordinert innsats for å påvirke valget i 2021. Det betyr ikke at tiltakene som ble iverksatt har vært overflødige – tvert imot. Det betyr bare at vi kan si dette med større grad av sikkerhet.

Internasjonale utviklingstrekk

Digital sikkerhet er i økende grad på dagsorden både hos statsledere og i internasjonalt diplomati. Formålet er å klargjøre grensene for ansvarlig statlig opptreden i det digitale domenet. Dette gjøres både bilateralt og multilateralt. Et bilateralt eksempel var da presidentene i USA og Russland møttes i juni. Her tydeliggjorde president Biden at han anser digitale angrep på kritisk infrastruktur, herunder energi, helse, transport og finansiell infrastruktur, som uakseptabelt. Dette gjaldt uavhengig av om det er statlige aktører eller kriminelle grupperinger som står bak slike handlinger.

[17] https://www.regjeringen.no/no/aktuelt/tiltak-for-a-hindre-uonsket-pavirkning-i-valget/id2854721/

FOTO: NTB SCANPIX / ESPEN BRATLIE / SAMFOTO

En av NSMs viktigste oppgaver i år har vært å bidra til sikker gjennomføring av valget.

Også multilateralt gjøres det mye arbeid for å tydeliggjøre rammene for akseptabel adferd i det digitale domenet. FN har siden 2010 oppnevnt seks ekspertgrupper for å belyse hvilke konsekvenser digital utvikling har for internasjonal sikkerhet. Ekspertgruppene har levert til sammen tre rapporter som har klargjort både hvordan internasjonal rett kommer til anvendelse i det digitale domenet og hvilke normer som bør gjelde for å ansvarlig statlig adferd. Dette er et svært viktig bidrag i rettsutviklingen på feltet.

EU som premissleverandør for digital sikkerhet

EU tar en stadig større rolle som pådriver innenfor digital sikkerhet. I desember 2020 lanserte EU kommisjonen både en ny strategi for digital sikkerhet og forslag til et revidert direktiv om sikkerhet i nettverk- og informasjonssystemer (NIS2).

I 2018 sendte regjeringen Solberg utkast til «lov om sikkerhet i nettverk og informasjonssystemer» på høring, som skulle implementere NIS-direktivet i norsk rett. I 2020 samarbeidet NSM og ulike sektormyndigheter med å identifisere hvilke virksomheter som skulle omfattes av regelverket. Etter planen skal loven legges frem i løpet av 2021, og forskrift til loven sendes på høring samtidig. Det reviderte direktivet omfatter flere sektorer og stiller flere

Amerikansk presidentordre stiller nye krav til digital sikkerhet

Den 12. mai 2021 utstedte USAs president Joseph R. Biden en 'Executive Order on Improving the Nation's Cybersecurity'.

Ordren kom på bakgrunn av statlige og ikke-statlige trusselaktørers stadig mer sofistikerte og ondsinnede cyberoperasjoner mot offentlig og privat sektor i USA. Sikkerhetstiltakene skulle iverksettes innen 60 – 180 dager.

Cyberoperasjonene mot SolarWinds og Colonial Pipeline, samt utnyttelse av sårbarheter i Microsoft Exchange er eksempler på dette og noe av årsaken til at tiltakene i Bidens presidentordre dekker både leverandørkjedeangrep og løsepengeangrep.

Et fellestrekk ved disse hendelsene er, ifølge ordren, synliggjøringen av behovet for omfattende endringer og investeringer i cybersikkerhetsarbeidet. Ordrens formål er å bidra til økt beskyttelse mot ondsinnede aktører gjennom blant annet;

- Et tettere offentlig-privat cybersikkerhets-samarbeid
- Mistenkelig trusselaktivitet skal informeres om umiddelbart til myndigheter med ansvar for cybersikkerhet
- Anvendelse av moderne skytjenester med høyt sikkerhetsnivå skal fremskyndes
- Implementering av risikobasert sikkerhets-arkitektur med utgangspunkt i «Zero Trust»
- Myndighetene skal tilstrebe mest mulig standardisering for systemer som ikke behandler gradert informasjon
- Informasjon som ikke er formelt gradert skal likevel verdivurderes og beskyttes etter skadepotensial

Alle tiltakene er kjente og flere av dem er allerede anbefalt fra NSM for norske forhold. Den forebyggende delen av presidentordren overlapper med anbefalinger og veiledninger vi har i Norge, blant annet «*NSMs grunnprinsipper for IKT-sikkerhet*». Ordren har også mange viktige tiltak for hva som skal skje etter en uønsket cyberhendelse, en tilnærming vi i mindre grad har i Norge.

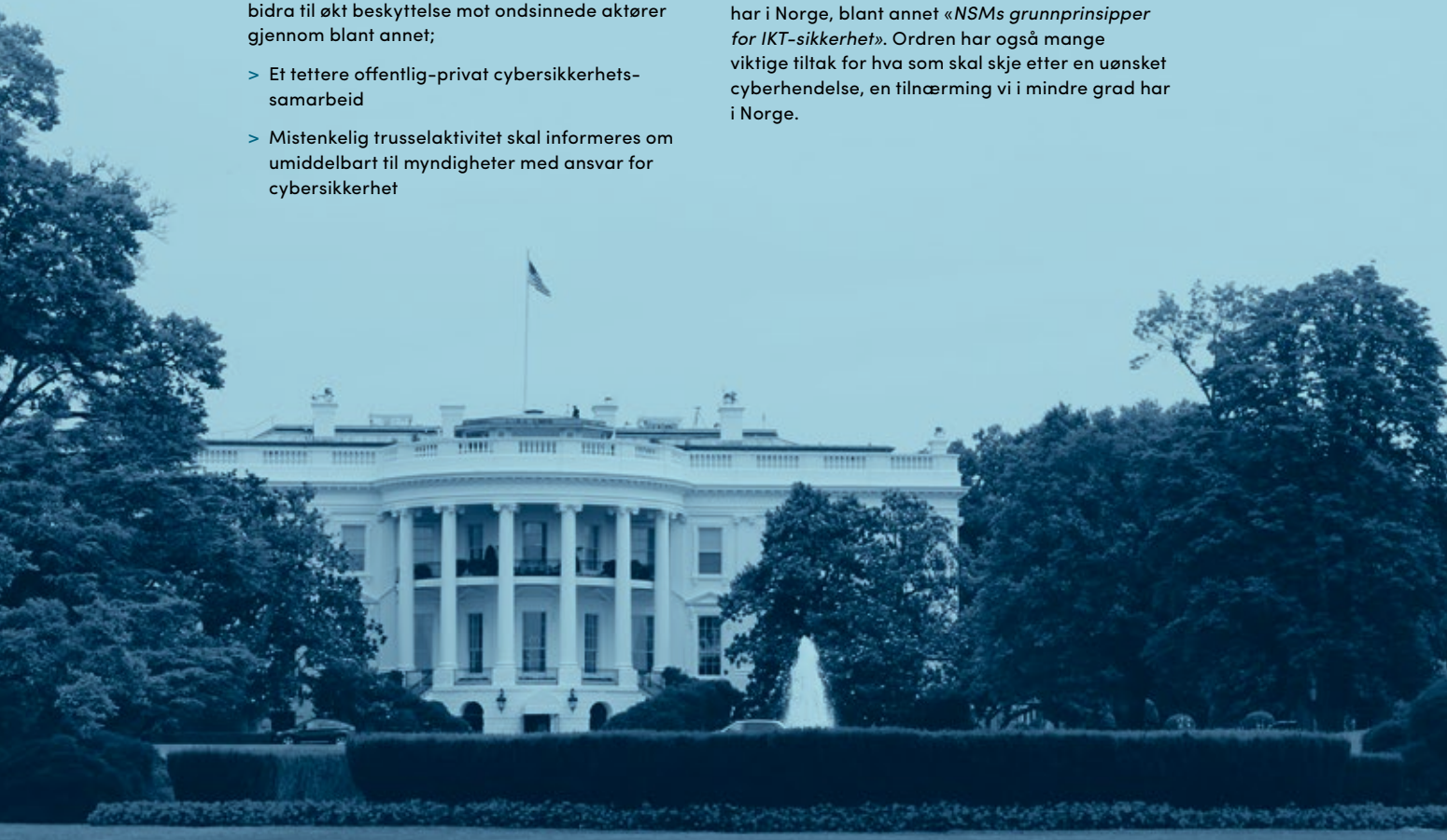


FOTO: DOUG MILLS/THE NEW YORK TIMES

Putin og Biden under bilateralt møte i juni 2021.

nye krav til virksomhetene. Også for EUs medlemsland kommer det flere nye plikter, blant annet skal det utvikles rammeverk for håndtering av alvorlige digitale hendelser, et slik rammeverk[18] har Norge hatt siden 2017.

EU har etablert flere investeringsprogrammer innenfor områder som er relevante for digital sikkerhet. I perioden 2021-2027 vil EU gjennom disse programmene investere opp mot 2 milliarder Euro, i tillegg til investeringer fra det Europeiske forsvarsfondet. Disse investeringene vil også komme Norge til gode.

EUs samlede pakke med rettslig regulering, store investeringer i forskning og utvikling og felleseuropeiske tiltak viser en betydelig satsning på digital sikkerhet i Europa. ■

EUs samlede pakke med rettslig regulering, store investeringer i forskning og utvikling og felleseuropeiske tiltak viser en betydelig satsning på digital sikkerhet i Europa.

[18] https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/

FOTO: CORNELIUS POPPE / NTB

IoT – Tingenes muligheter eller fremtidens sårbarheter?

En teknologitrend med raskt økende utbredelse er «Internet of Things» (IoT) eller tingenes internett. En rekke ulike enheter («ting») kobles til internett gjennom wifi, 4G eller 5G-nettet.

IoT gir muligheter for økt datainnsamling som er nyttig underlag for beslutningsstøtte og kan medføre at kunstig intelligens vil tas i bruk i flere virksomheter og verdikjeder.

Teknologien vil gi en økning innen sammenkobling av nettverk og enheter, samtidig som det medfører økte sårbarhetsflater. Utstrakt bruk av smarte sensorer i fysiske prosesser, lokalsamfunn og fabrikker vil gi økte muligheter, men også økt risiko i form av komplekse digitale verdikjeder: IoT-komponenter kan påvirkes og manipuleres, med potensielt store konsekvenser.

IoT må også sees i sammenheng med innføring av 5G, som vil gi økte muligheter for å etablere betydelig prosesseringskapasitet som en del av mobilnettet (edge computing). Dette innebærer at datalagring, prosessorkraft og enkelte skytjenester flyttes nærmere endeutstyr og sluttbruker. Dette vil kunne gi raskere respons og mer effektiv ressursdeling. Utbredelsen av IoT medfører at det vil bli økt maskin-til-maskin-kommunikasjon (M2M-kommunikasjon) hvor ulike kommunikasjonsbærere benyttes alt etter kapasitet, avstand og behov. Med dette innføres også flere muligheter til bruk av sensorbasert teknologi i ulike sektorer.

Flere kommunikasjonsplattformer vil øke sårbarhetspotensialet slike enheter kan innføre i vår øvrige digitale infrastruktur, og dette utgjør en risiko. Riktige beslutninger om både innkjøp og drift bør bygge på gode verdi- og risikovurderinger. Det offentlige bør vurdere å spesifisere krav til sikring av IoT-enheter som benyttes i samfunnskritisk infrastruktur, og som et minimum benytte anerkjente produktleverandører.

Taktskiftet innenfor det digitale risikobildet må møtes med forebyggende sikkerhetsarbeid

Norge har digitalisert infrastruktur i verdenstoppen, og en befolkning som ligger langt fremme når det gjelder å ta i bruk ny teknologi. Det pågår store digitaliseringsprosjekter innen både sivil og militær sektor hvor blant annet anvendelse av sky og skytjenester står sentralt i flere av prosjektene. Virksomheter som nødetater, Forsvaret med flere, har behov for moderne IT-plattformer med innovative digitale tjenester, som fungerer bra i hele krisespennet og mellom berørte virksomheter. IT-moderniseringen i staten må være helhetlig og enhetlig og målet bør være å opprette en felles digital plattform for samhandling, innovasjon og tjenesteyting.

I arbeidet med digitaliseringen av Norge og de store digitaliseringsprosjektene, må ikke den underliggende digitale grunnmuren glemmes og tas for gitt. Vår kraftforsyning, ekom og datasentre er helt avgjørende for den pågående digitaliseringen. Enkelte digitale tjenester til disse sektorene er kritiske for samfunnet og vil kreve nasjonal digital autonomi. Militær, offentlig og sivil sektor vil i økende grad benytte felles digital infrastruktur da tjenestene vil bli levert fra de samme kommersielle leverandørene av skytjenester. Fundamentet for disse leveransene vil i stor grad være datasentre som dermed står sentralt i vår felles digitale grunnmur. Dette må adresseres på en grundig måte og NSM har derfor valgt å rette oppmerksomhet mot norske datasentre og digital autonomi i en egen temarapport i høst.

For alle norske virksomheter er det forebyggende sikkerhetsarbeidet med på å redusere digital risiko. Det gode sikkerhetsarbeidet vi ser i mange virksomheter må ikke stoppe opp, men fortsatt styrkes og integreres i virksomhetens øvrige leveranser og tjenester. Med det utfordrende risikobildet vi står i, hvor konsekvensene av cyberoperasjoner blir mer alvorlige, haster det mer enn tidligere å implementere risikoreduserende tiltak.

Et robust digitalt samfunn oppnår vi når alle bidrar med å sikre sin egen virksomhet.

Økt digital grunnsikring krever en nasjonal innsats.

Design: HyperRedink
Innhold: NSM

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

Telefon: 67 86 40 00
Epost: post@nsm.no
www.nsm.no

Nasjonalt Cybersikkerhetssenter
Telefon: 02497 (+47 23 31 07 50)
Epost: norcert@cert.no (Hendelser)
post@cert.no (Admin)