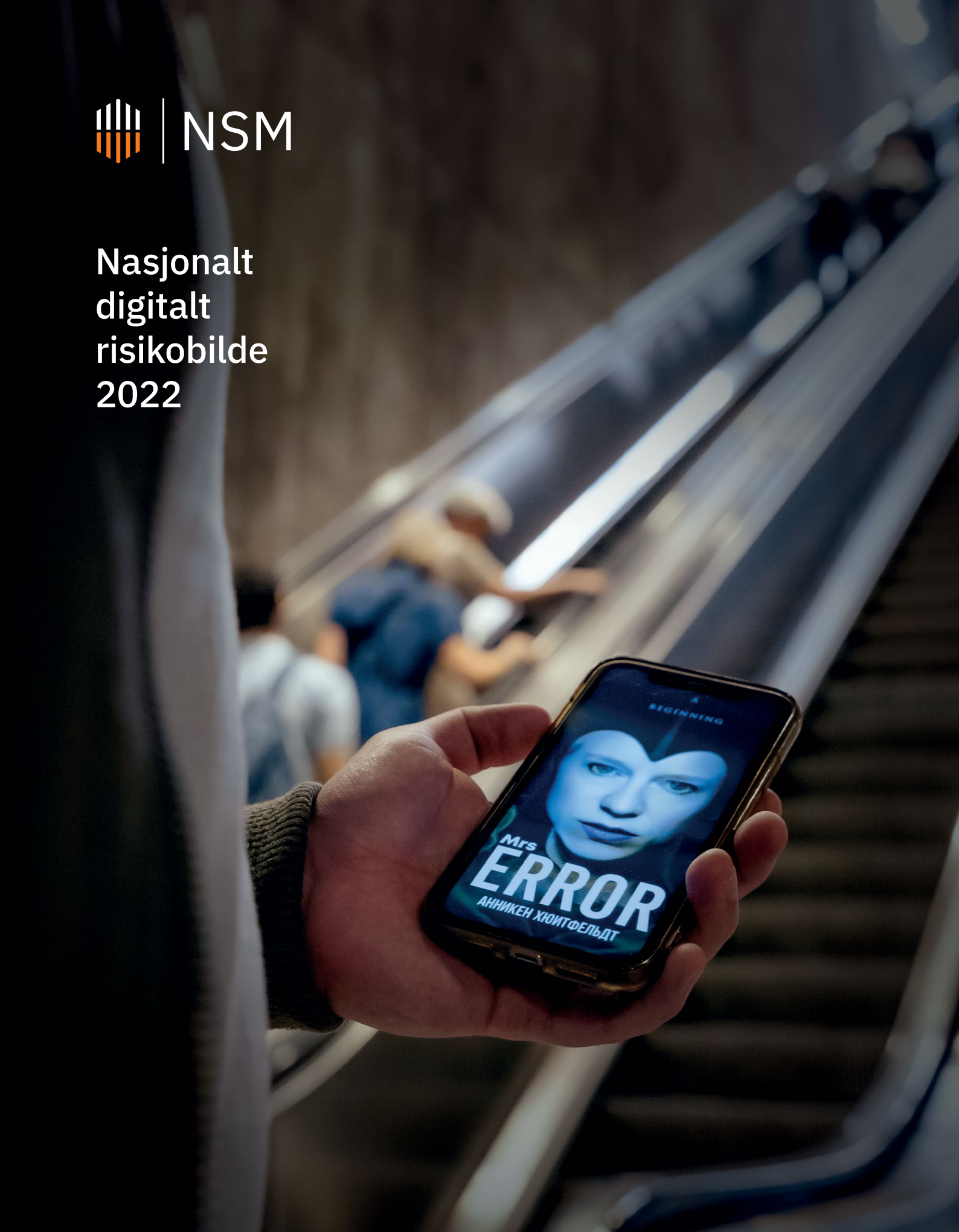
NSM

Nasjonalt digitalt risikobilde 2022



Nasjonalt digitalt risikobilde er NSMs årlige rapport for å øke bevisstheten og motivere til bedre digital sikkerhet i offentlige og private virksomheter. Rapporten henvender seg til ledere og personell med sikkerhetsoppgaver i alle sektorer, og tar opp problemstillinger knyttet til samfunnssikkerhet, statssikkerhet og individsikkerhet innenfor det digitale domenet.

NASJONAL
SIKKERHETSMYNDIGHET

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for nasjonal sikkerhet. Direktoratet gir råd og gjennomfører tilsyn og andre kontrollaktiviteter på sivil og militær side knyttet til sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning. NSM har også et nasjonalt ansvar for å avdekke, varsle og koordinere håndtering av alvorlige cyberangrep.

NSM
NASJONALT
CYBERSIKKERHETSSENTER

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 knyttet til cybersikkerhet og tekniske sikkerhetsløsninger. NCSC yter også bistand ved håndtering av digitale hendelser og vedlikeholder et nasjonalt cybersituasjonsbilde.

Innhold

Det digitale risikobildet 2022 6

Krigen i Ukraina 8

Hvilken rolle har cyberoperasjoner spilt i krigen? 10

Kampen om narrativet 10

Tidslinje: Russlands vedvarende cyberoffensiv mot Ukraina 12

Cybersituasjonsbildet i Norge 14

Tre samfunnsområder rammes spesielt 15

Politisk motiverte tjenestenektangrep 16

Personopplysninger er salgsvare 18

Utnyttelse av programvaresårbarheter utgjør en stor del av aktiviteten vi ser 22

Leverandører fortsetter å være attraktive mål 23

Flere virksomheter rammes digitalt av løsepengevirus og sabotasje i Norge 24

Avdekkede sårbarheter fra NSMs penetrasjonstester 26

Er du forberedt? 30

Det digitale risikobildet 2022

I 2022 har vi gått fra global pandemi til krig i Europa. Den sikkerhetspolitiske situasjonen har endret seg dramatisk i løpet av kort tid. Det digitale risikobildet preges av stadig økende kompleksitet i systemer og teknologier. Sårbarhetene i samfunnet blir mer krevende å oppdage på grunn av stadig mer komplekse digitale verdikjeder.

Oppdukkende hendelser og begivenheter kan raskt endre risikobildet. I en skjerpet situasjon må virksomheten håndtere økt risiko, usikkerhet og et omskiftelig situasjonsbilde. For å redusere denne sårbarhetsflaten bør virksomheter etablere beredskapsplaner og sørge for at disse til enhver tid er gjennomøvde. Risikoforståelse er helt avgjørende for virksomheters sikkerhetsarbeid. Kriser kan oppstå uforutsett, så vær i forkant.

Ukraina har siden begynnelsen av 2000-tallet blitt utsatt for en rekke alvorlige cyberangrep fra Russland, og har frem til krigens utbrudd gjort viktige grep for å styrke cybersikkeheten. I etterkant av invasjonen 24. februar har det blitt avverget flere store cyberangrep mot ukrainske virksomheter. En viktig delforklaring til dette er at en stor del av Ukrainas digitale infrastruktur driftes gjennom private, vestlige leverandører. Ukrainas partnersamarbeid har både skapt kritisk motstandsdyktighet i cyberdomenet, og en synergieffekt ved at unik innsikt i situasjonen deles. Videre har Ukrainas systematiske arbeid med å bedre cybersikkerheten sannsynligvis vært en viktig årsak til at vi ennå ikke har sett de store destruktive cyberoperasjonene i Ukraina etter Russlands invasjon. Dette er viktig lærdom å ta med seg – gode sikringstiltak kan avverge cyberangrep.

Lærdommen fra Ukraina har understreket målene i vår egen nasjonale strategi for digital sikkerhet[1]: Et godt forebyggende arbeid med digital sikkerhet og en systematisk tilnærming til håndtering av risiko, vil redusere muligheten for at uønskede digitale hendelser får konsekvenser for egen og andres virksomhet, for den enkelte privatperson og for samfunnet i stort.

Beredskap og totalforsvar er ord som blir brukt stadig oftere i norsk offentlig forvaltning og i samfunnet for øvrig. Flere allierte ser med fornyet interesse på det norske totalforsvarskonseptet, som bygger på gjensidig støtte og samarbeid mellom Forsvaret og sivilsamfunnet gjennom hele krisespennet. Komplekse systemer, avhengigheter mellom virksomheter og eierforhold skaper nye sårbarheter og aktualiserer behovet for samarbeid om sikkerhet i totalforsvaret.

Den teknologiske utviklingen gir store muligheter, men også klare sikkerhetsutfordringer. Stadig mer informasjon er tilgjengelig på mobiltelefoner og andre bærbare enheter, muliggjort av raske mobilnett som 5G og økende bruk av skybaserte tjenester. Denne trenden er forventet å fortsette i uforminsket styrke og vil bre om seg etter hvert som digitaliseringen fortsetter.

Digitaliseringen skjer raskt og satsningen på sikkerhet må prioriteres fra start. Myndighetene skal legge til rette for at virksomheter kan beskytte seg mot uønskede digitale hendelser, men å ivareta digital sikkerhet er først og fremst et virksomhetsansvar. Virksomheter må starte med å lukke sine egne sårbarheter, dette bidrar å øke vår kollektive robusthet.

1 Nasjonal strategi for digital sikkerhet (2019): https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/

Krigen i Ukraina

Bare én time før russiske militære enheter krysset grensen inn i Ukraina 24. februar ble satellittnettverket KA-SAT (Viasat) rammet av et cyberangrep – trolig for å påvirke ukrainsk militær kommunikasjonsevne.

KA-SAT tilbyr internett over satellitt i Europa og rundt Middelhavet. Privatpersoner og virksomheter over hele Europa, og spesielt i Ukraina, mistet internettilgang. I Norge mistet meteorologer på Hopen (Svalbard) og Bjørnøya internett, telefon, radio og TV i to uker som følge av cyberangrepet.

Hittil i krigen har cyberangrepet på KA-SAT vært det mest alvorlige med tanke på utilsiktet spredning til andre land. De mindre avanserte operasjonene har spredt seg regionalt – blant annet er det ved ett tilfelle avdekket destruktiv skadevare på systemer til baltiske underleverandører til ukrainske myndigheter.

Russlands angrep på Ukraina innebærer et paradigmeskifte i europeisk sikkerhetspolitikk.

I Norge har mange virksomheter vært urolige, særlig for sin digitale infrastruktur. Informasjonsbehovet har vært stort. Det samme gjelder behovet for veiledning om sikkerhetstiltak. Vi har opplevd at virksomheter har hatt lavere terskel for å varsle NSM om mulige sikkerhetstruende hendelser. Dette vitner om økt årvåkenhet i norske sikkerhetsmiljøer.

Sikkerhetssituasjonen har også tvunget frem en økt bevissthet rundt de utfordringer digitale leverandørkjeder bringer med seg. Problemstillingene har blitt forsterket og tydeliggjort for flere. Trusselaktører hopper over gjerdet der det er lavest. Ofte er dette i de digitale leverandørkjedene. Risikoen for at noe skal ramme oss er større i den situasjonen som Europa står i nå. NSM har derfor hatt høy beredskap for å kunne holde situasjonsbildet oppdatert i en svært omskiftelig situasjon.

NSMs rolle har vært å formidle situasjonsbildet, vurdere risiko for nasjonale sikkerhetsinteresser og å anbefale tiltak. Flere av tiltakene vi har formidlet har dreid seg om beredskapsplaner og tiltak som mange av oss anså å tilhøre en svunnen tid. Plutselig har en skjerpet sikkerhetssituasjon gjort at vi må børste støv av gamle planer og samordningsmekanismer. Totalforsvaret er tilbake.

Overfor norske virksomheter har vår vurdering så langt vært at den umiddelbare risikoen i forbindelse med krigen i Ukraina hovedsakelig ligger hos virksomheter med tilknytning til en eller flere av de stridende partene. Nasjonalt senter for informasjonssikkerhet i kommunesektoren, Kommune CSIRT, skriver i rapporten «Digitalt situasjonsbilde» at kommuner bør være ekstra oppmerksomme på kontaktflakter opp mot russiske og ukrainske selskaper, institusjoner, leverandører og annet samarbeid, fordi disse kanalene kan misbrukes. NSM mener at denne vurderingen er overførbar for offentlige institusjoner og virksomheter for øvrig.

Hvilken rolle har cyber-operasjoner spilt i krigen?

Da Russlands militære angrep på Ukraina startet, hadde mange eksperter sett for seg en innledende fase med cyberangrep som skulle berede grunnen for en intensiv og hurtig invasjon; omfattende strømutfall, bortfall av teknologiske styringssystemer for transport, kritisk industri eller finansstrukturer.

Før krigen og i krigens første fase uteble massive cyberangrep som ødela kritisk infrastruktur og samfunnsfunksjoner. Likevel er bildet mer komplekst.

For det første er cyberoperasjoner et svært bredt begrep, som omfatter alt fra kartlegging og rekognosering, til skjult informasjonsinnhenting og destruktive angrep på kritisk infrastruktur. Cyberoperasjoner som har til hensikt å hente inn informasjon i etterretningsøyemed, vil aktøren ønske å holde skjult. At slike operasjoner ikke har vært kjent, trenger naturligvis ikke bety at de ikke skjer – operasjonene kan tvert imot være svært vellykkede nettopp gjennom at den forblir skjult.

For det andre har flere store cyberangrep mot ukrainske virksomheter faktisk blitt avverget. Ukraina har kraftig forbedret sikkerheten i sin digitale infrastruktur de siste årene. Angrepene mot strømnettet i 2015 og 2016 tok strømmen til flere hundre tusen sivile innbyggere. Et tilsvarende forsøk ble stoppet i april 2022. Ukrainas omfattende arbeid for å sikre seg i cyberdomenet har dermed hatt stor skadebegrensende effekt.

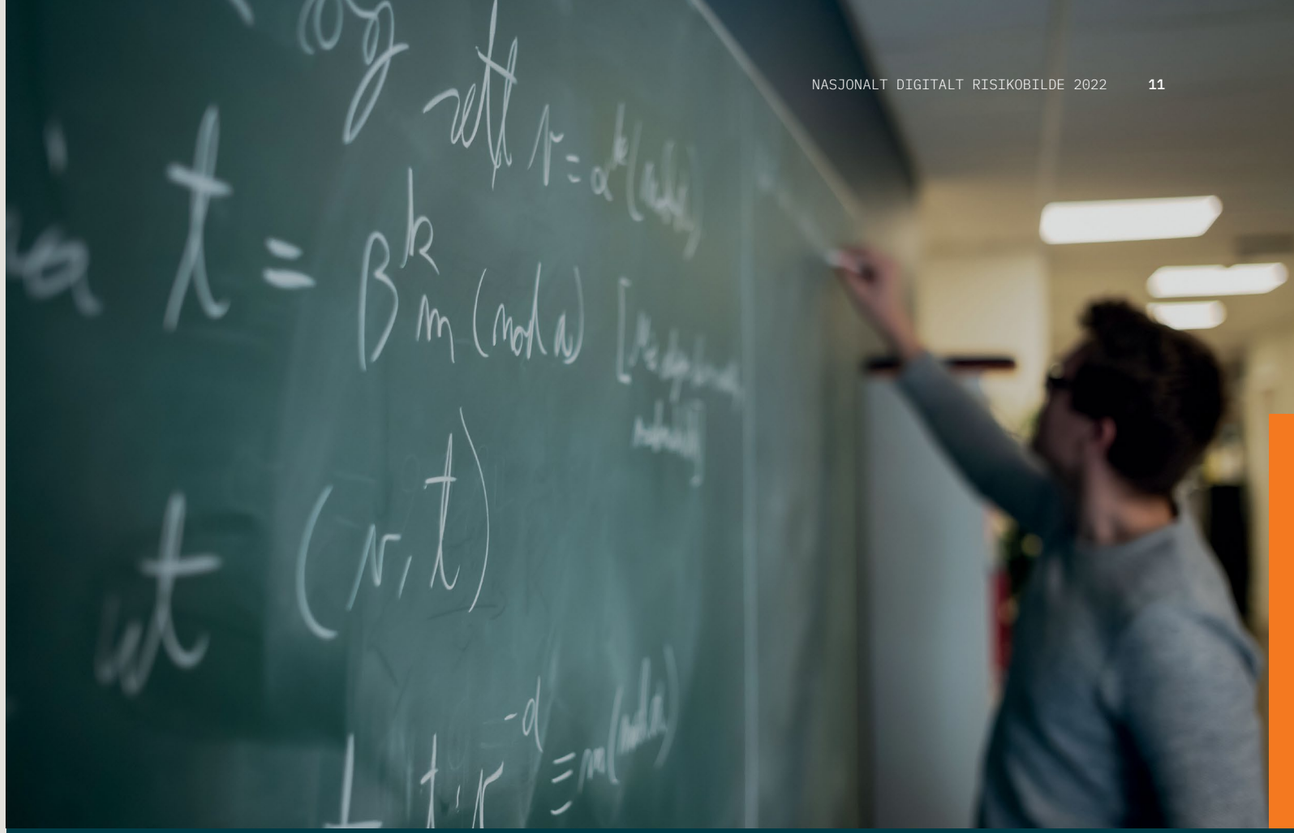
Et tredje poeng er at det faktisk har vært en rekke cyberangrep mot ukrainske virksomheter og infrastruktur. (Se tidslinje s. 11)

Kampen om narrativet

Informasjon benyttes som militærstrategisk virkemiddel av flere stater. Cyberdomenet er en viktig arena for disse aktivitetene. Gjennom krigen er det sett en rekke forsøk på spredning av desinformasjon og påvirkning av det rådende narrativet, både i Ukraina og i Russland.

USA startet allerede i opptrappingen til krigen å offentliggjøre etterretningsvurderinger – som vanligvis holdes strengt hemmelig – rundt Putins mest sannsynlige handlemåter i Ukraina. Dette kan ha vært en bevisst strategi som skulle gjøre det vanskeligere for Kreml å bygge et falskt narrativ og spre desinformasjon om invasjonen og de faktiske forholdene på bakken.

Distribuerte tjenestenektangrep (DDoS) og såkalt «wiper»-skadevare – som permanent sletter filer fra infiserte systemer – er blant angrepstypene som har vært hyppig observert mot ukrainske myndigheter og virksomheter. Befolkningen i Ukraina, så vel som i Russland, har opplevd forstyrrelser i offentlige og private tjenester relatert til betaling, transport og elektrisitet. Departementers nettsider har fått innholdet endret (såkalt defacement). Slike hendelser trenger ikke være teknisk avanserte, men allikevel skaper det stor oppmerksomhet. Dette kan føre til usikkerhet i befolkningen, og over tid kan tilliten til myndighetene svekkes. Øvrige deler av Europa har heller ikke vært skånet fra slike hendelser.



Etablering av et kryptosenter i NSM i 2023

Kryptografiske løsninger er en viktig del av sikkerhet i digitale løsninger og er avgjørende for beskyttelsen av sikkerhetsgradert informasjon og kommunikasjon. For at de kryptografiske løsningene skal gi nødvendig sikkerhet, kreves kontinuerlig analyse og utvikling. Det fordrer opprettholdelse og videreutvikling av kompetanse, utvikling innen kryptologiske algoritmer og kunnskap om den generelle teknologiutviklingen. NSM etablerer et nasjonalt senter for kryptologi som skal bidra til at utviklingen og implementeringen av nye løsninger holder tritt med tiden. Senteret skal bidra til mer effektivt samarbeid mellom allerede eksisterende sterke fagmiljøer hos myndigheter, akademia og kryptoindustri.

Russlands vedvarende cyberoffensiv mot Ukraina

Ukraina har vært gjentagende offer for offensive cyberoperasjoner fra Russland – og kanskje spesielt etter annekteringen av Krim. Angrepene har fått store lokale og globale konsekvenser. NotPetya-angrepet fra 2017 var opprinnelig rettet mot Ukraina, men fikk utilsiktet spredning til over 65 land. Angrepet anses som det mest ødeleggende i historien. Destruktive cyberoperasjoner under krigen i Ukraina har ødelagt data og systemer, forstyrret kritisk infrastruktur og tjenester, kontrollert informasjonen og hentet ut betydelige mengder data. Under følger en tidslinje over større cyberoperasjoner mot Ukraina som i åpne kilder er attribuert til Russland. Listen er ikke komplett, men tar for seg hendelser av alvorlig karakter.

MAI 2014

Bølge av cyberangrep mot presidentvalget i Ukraina

ANTATT GRUPPERING
PRO-RUSSISK HACKTIVIST-GRUPPE CYBERBERKUT (OMSTRIDT)

- Kompromittering av valgsystemets nettverk og sletting av filer i den hensikt å ødelegge stemmetellingen
- Skadevare på valgkommisjonens enheter forsøkte å fremstille høyreradikal som vinner av valget
- Forsinkelser i valgresultatet
- Forsøk på å diskreditere valget

23. DESEMBER 2015

Cyberangrep mot strømforsyningen i Vest-Ukraina

ANTATT GRUPPERING
RUSSLAND/GRU (IFØLGE USA)

- Samtidig DDoS mot kundeservice-callsenter
- Første vellykkede angrep på strømnett noensinne
- Om lag 230.000 ukrainere mistet strøm i 1–6 timer
- Forsøk på å skade tilliten til strømtilbydere

17. DESEMBER 2016

Nytt cyberangrep mot strømforsyningen i Kyiv

ANTATT GRUPPERING
RUSSLAND/GRU (IFØLGE USA)

- Skadevare i stand til å automatisere store strømavbrudd
- Angrepet ble knyttet til 2015-angrepet, samt angrep mot jernbane, departementer m. fl i Ukraina.
- Strømavbrudd i om lag én time
- Om lag 20 prosent av Kyivs strømforbruk falt bort

27. JULI 2017

NotPetya-angrepet

ANTATT GRUPPERING
RUSSLAND/GRU (IFØLGE USA)

- Kvelden før Ukrainas nasjonaldag rammet private og offentlige virksomheter inkl. finans-, energisektoren, myndighetsorganer
- Skadevaren slettet harddisker og spredte seg raskt – også globalt
- Kjent som det mest ødeleggende cyberangrepet i historien
- Strålemålingssystem ved Tsjernobyl gikk offline
- Store økonomiske tap; estimert til over 10 mrd. USD globalt
- Traff om lag 49.000 systemer i 65 land

11. JULI 2018

Cyberangrep mot klor-stasjon

ANTATT GRUPPERING
RUSSLAND (IFØLGE UKRAINA)

- Forsøk på cyberangrep mot klor-stasjon knyttet til vannforsyning for Ukraina, Moldova og Belarus
- Ble avverget, men hadde potensiale til å forårsake en mulig katastrofe

JANUAR 2022

«Defacement» av en rekke myndigheters nettsider

ANTATT GRUPPERING
BELARUS (IFØLGE UKRAINA)

- Innhold ble endret til pro-russisk propaganda på over 70 ukrainske offentlige nettsteder i opptakten til invasjonsforsøket 24. februar
- Forsøk på å spre frykt i befolkningen

JANUAR–APRIL 2022

En rekke cyberangrep ved bruk av «wiper»-skadevare

ANTATT GRUPPERING BÅDE RUSSISKE OG BELARUSSISKE AKTØRER ATTRIBUERES

- En lang rekke cyberangrep ved bruk av såkalt «wiper»-skadevare som sletter harddisker mot private og offentlige virksomheter bl.a. grensestasjon mot Romania
- Forsinket flyktningetransitt fra Ukraina

FEBRUAR 2022

En rekke distribuerte tjenestenektangrep mot Ukraina

ANTATT GRUPPERING RUSSLAND/GRU (IFØLGE NCSC UK)

- En rekke distribuerte tjenestenektangrep mot bl.a. ukrainske banker, nyhetsnettsteder og departementer som forsvarsdepartementet.
- Bortfall av tjenester i begrenset tidsperiode

24. FEBRUAR 2022

«Wiper»-skadevare mot Viasat satellittkommunikasjon

ANTATT GRUPPERING
RUSSLAND (IFØLGE USA)

- Cyberoperasjonen ble iverksatt én time før det militære konvensjonelle invasjonsforsøket startet 24. februar
- Forstyrret satellittkommunikasjon i Ukraina – men også i mange andre europeiske land
- Over 5800 tyske vindturbiner ble påvirket
- Tusenvis av internettkunder i hele Europa mistet internett-tilgang, noen i opptil 2 uker

08. APRIL 2022

Forsøk på cyberangrep mot strømleverandør

ANTATT GRUPPERING
RUSSLAND (IFØLGE UKRAINA, ESET)

- Blant skadevaretypene brukt var «Industroyer 2», som ligner den brukt i angrepet som tok strømtilførselen i 2016
- Ble avverget takket være rettidig varsling, rask respons og omfattende cybersikkerhetsstøtte til CERT-UA. Hadde potensiale til å ta strømtilførselen til 2 mill. mennesker

DESTRUKTIVE, MÅLRETTEDE CYBER-OPERASJONER MOT UKRAINA

HERMETICWIPER
HERMETICRANSOM
ACIDRAIN
ISAACWIPER
CADDYWIPER
DOUBLEZERO
CADDYWIPER
INDUSTROYER2
SOLOSHRED
AWFUL SHRED

2014 2015 2016 2017 2018 2019 2020 2021 **2022** Februar Mars April Mai

Cybersituasjonsbildet i Norge

Aktørene som står bak cyberoperasjonene mot Norge det siste året, har brukt et bredt spekter av angrepsmetoder som rangerer fra enkle til svært avanserte. De mest avanserte metodene skreddersys til målet. De enkleste angrepene utnytter sårbarheter til å utløse et løsepengevirus eller oversvømmer nettsider med trafikk gjennom tjenestenektangrep.

En rekke ulike indikatorer, fremgangsmåter og informasjon fra partnere, gjør at NSM kjenner igjen forskjellige avanserte trusselaktører i cyberoperasjonene vi ser mot Norge. Likevel vet vi at vi ikke har et fullgodt situasjonsbilde. Det foregår daglig aktivitet i cyberdomenet som er så avansert at vi ikke registrerer den, og fordekt aktivitet kan holde seg skjult hos norske virksomheter i flere år. Cybersituasjonsbildet vi formidler, er basert på aktiviteten vi ser og aktiviteten vi kan formidle offentlig.

Felles cyberkoordineringssenter (FCKS[2]) vurderer at aktørene i det digitale rom spenner fra opportunister og småkriminelle til organiserte kriminelle og statlige aktører. Det gir derfor et komplekst digitalt risikobilde der aktiviteten fordeles mellom flere ulike aktører, trolig med svært ulike oppdrag.

Tre samfunnsområder rammes spesielt

NSM har de siste årene observert en økning i ondsinnet aktivitet mot norske virksomheter. Imidlertid er bildet noe endret det siste året. I den første halvdelen av 2022 har vi registrert en økning i antallet forsøk på kompromitteringer, mens antallet faktiske kompromitteringer er lavere enn i samme periode i 2021.

Årsakene til endringen i observert aktivitet kan være sammensatte, og sannsynligvis er forklaringen en kombinasjon av en rekke faktorer.

For det første omfatter cyberoperasjoner en rekke forskjellige angrep. Enkelte former for cyberangrep tar vesentlig lengre tid å oppdage enn andre. Nettopp derfor er det viktig å huske at fravær av bevis ikke er bevis på fravær.

For det andre har de seneste årenes økte risiko i cyberdomenet gjort at sikkerhetsarbeidet har stått høyt på agendaen hos mange. Fokus på gode tiltak kan være en faktor i forklaringen på hvorfor vi har sett flere forsøk på kompromitteringer enn tidligere.

Samlet statistikk fra alle hendelser som er registrert av NSM, viser at særlig tre samfunnsområder har vært utsatt for ulike typer cyberangrep det siste året:

- Teknologibedrifter
- Forskning og utvikling
- Offentlige forvaltningsorganer

Dette samsvarer med utviklingen vi har sett de siste årene, og understreker viktigheten av at virksomheter i disse sektorene er særlig årvåkne. Bildet vi ser samsvarer også med trusselbildet som PST og Etterretningstjenesten peker på i sine åpne trusselvurderinger.

2 Felles cyberkoordineringssenter er et fagmiljø for felles koordinering av cyberangrep som ledes av NSM og består av representanter fra NSM, Etterretningstjenesten, Politiets sikkerhetstjeneste og Kripos

Politisk motiverte tjenestenektangrep

I etterkant av Russlands invasjon av Ukraina har tjenestenektangrep vært en mye brukt angrepsmetode fra pro-russiske aktører mot en rekke NATO-land. NSM gikk i mai ut og ba virksomheter påse at de var i stand til å motstå denne typen cyberangrep.

Norge utsatt for tjenestenektangrep

Morgenen 29. juni ble NSM kontaktet av flere virksomheter som opplevde driftsforstyrrelser på nettsidene sine, som følge av det som viste seg å være et stort koordinert tjenestenektangrep. Parallelt med dette sirkulerte meldinger på plattformen Telegram om at flere norske virksomheter var utpekt som mål for tjenestenektangrep fra en kriminell hacker-gruppe kjent som Killnet.

En av Telegram-kanalene som distribuerte mållisten publiserte også det som fremstår som en begrunnelse for angrepene, som oversatt til norsk hevder at «norske myndigheter har avslått Russlands søknad om passasje av varer til russiske bosettinger på Svalbard gjennom det eneste sjekkpunktet på den russisk-norske grensen ved Storskog».

Den påfølgende uken opplevde et stort antall norske virksomheter nedetid på sine nettsider. NSMs nettsider var også av de som ble indirekte rammet, og var sporadisk utilgjengelige gjennom en kort periode. NSMs tjenester var ikke påvirket av angrepet, det var kun nettsidene som var nede. Nedetid på nettsider kan være alvorlig dersom det bidrar til å spre mistillit om myndigheters evne til å beskytte befolkningen mot cyberoperasjoner.

Mangel på kompetanse om ulike cyberangrep skaper unødvendig uro og forstyrrelser, og det gjør at effekten av et metodisk enkelt tjenestenektangrep blir uforholdsmessig stor. Når angrepene begrunnes som «straff» for en politisk beslutning, kan dette skape en oppfatning om at det er noe våre politiske ledere har skyld i. På denne måten kan tjenestenektangrep benyttes som ledd i en påvirkningsoperasjon. Ifølge Etterretningstjenesten gjennomføres påvirkningsoperasjoner for å endre det offentlige ordskiftet, holdninger, beslutninger eller utfall[3]. PST peker på at cyberoperasjoner er en metode som blir mer relevant når konfliktnivået gjør det vanskeligere å operere på andre måter[4].

3 https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus

4 https://www.pst.no/alle-artikler/pressemeldinger/oppdatert-trussel-vurdering-pst-ser-en-okt-etterretnings-trussel-fra-russland-i-norge/

Hva er et tjenestenektangrep?

Et tjenestenektangrep rammer kun tilgjengeligheten til tjenesten, systemet eller de infrastrukturkomponenter som blir angrepet. Dette kan gjøres ved å overbelaste en eller flere ressurser (nettverksbåndbredde, CPU, minne, disk) hos målet for angrepet, eller utnytte svakheter i nettverks- eller applikasjonsprotokoller som brukes av målet for angrepet.

Selv om målene for distribuerte tjenestenektangrep vanligvis ikke blir kompromittert, er kildene som genererer trafikk gjerne kompromitterte systemer. NSM sender ut varsler dersom vi registrerer norske IP-adresser som deltar i ondsinnet aktivitet, blant annet tjenestenektangrep.

Hva er formålet med et tjenestenektangrep?

Tjenestenektangrep brukes av flere typer trusselaktører og kan ha forskjellige formål:

1. Påvirkningsoperasjon
2. Sabotasje
3. Element i et hybrid angrep
4. Politisk aktivisme
5. Vinningskriminalitet hvor trusselaktør bruker tjenestenektangrep i forbindelse med løsepengevirus
6. Hærverk, som kan ha forskjellig motiv eller opptakt

Tiltak mot tjenestenektangrep

I NSMs grunnprinsipper for IKT-sikkerhet[5] er utfordringen med tjenestenektangrep omtalt i tiltak 2.2.7 «Etabler en robust og motstandsdyktig IKT-arkitektur».

5 NSMs grunnprinsipper for IKT-sikkerhet: http://nsm.no/gp-ikt

Personopplysninger er salgsvare

Cyberdomenet er på mange måter en personlig arena. Vi lagrer konfidensiell informasjon digitalt, enten privat eller om virksomheten. Cyberoperasjoner kan ramme konfidensialiteten til enkeltpersoner og virksomheter gjennom at personsensitiv informasjon kommer på avveie eller at bedriftssensitiv informasjon lekkes. De fleste privatpersoner oppgir frivillig personsensitiv informasjon på sosiale medier og i apper. Frivillig oppgitt personsensitiv informasjon og personopplysninger aggregeres av store og små selskaper verden over, og selges videre til andre selskaper som skreddersyr reklame. Den samme informasjonen kan brukes av trusselaktører for å planlegge sine operasjoner, enten det er påvirkning, rekruttering av innsidere eller å forberede cyberoperasjoner.

NSM har gjennom flere år sett eksempler på kartleggingsaktivitet mot enkeltindivider som vurderes som interessante for fremmede stater. Høyre-politikeren Michael Tetzschner gikk ut i media i september i 2021 og delte at han var fratstjålet over 4000 e-poster fra sin Stortings-e-post.

Persondata om 3,3 millioner nordmenn på avveie

I mai ble det kjent at en database hos karttjenesten Norkart, som henter data fra Statens kartverk, var kompromittert og lastet ned av en ukjent aktør. Persondata som navn, adresser, fødselsnummer og informasjon om hva man eier kom på avveie.

Hendelsen skal ha blitt muliggjort gjennom en feil i brannmuren til søketjenesten som ga uvedkommende tilgang til en kopi av Norges offisielle eiendomsregister.

På kort sikt kan denne typen informasjon for eksempel utnyttes i svindelforsøk.

Selv om vi foreløpig ikke har sett datalekkasjene misbrukt, er det særlig bekymringsfullt om denne type datasett blir satt i sammenheng med annen tilgjengelig informasjon. Dette vil kunne føre til utnyttelser eller eksponering av enkeltpersoner eller virksomheter som på en eller annen måte er sårbare. Generelt bør virksomheter påse at data er forsvarlig sikret. Sikkerheten skal være like god gjennom hele livsløpet til en tjeneste, både under utvikling og test som under normal drift.

Personlige innloggingsdetaljer som brukernavn og passord blir omsatt i storskala på ulovlige markedsplasser på det mørke nettet. NSM har sett eksempler på at aktører nyttiggjør seg av innloggingsdetaljer som er hentet ut i en kompromittering, til cyberoperasjoner flere år senere. Vi ser at legitime brukeropplysninger er en hyppig benyttet inngangsmetode inn i virksomhetens systemer. Dette viser at informasjon som innhentes i kartleggingsøyemed av ondsinnede aktører faktisk omsettes og utnyttes. Aktivitet der brukeropplysninger blir utnyttet kan dermed både være et resultat av og en del av en kartleggingskampanje mot en virksomhet.

Dette understreker viktigheten av identitets- og tilgangshåndtering som blant annet er omtalt under prinsipp 2.6 i NSMs grunnprinsipper for IKT-sikkerhet. Her kan tiltak 2.6.7 «Bruk multifaktor autentisering» bidra til å redusere risikoen for at trusselaktører får tilgang ved bruk av opplysninger som er hentet ut i en kompromittering. Det er imidlertid viktig at virksomhetene også har en sikkerhetskultur som gjør det vanskelig å utnytte slike opplysninger for sosial manipulering som for eksempel ved spearphishing.

Erfaringer fra en virksomhet i NSMs kvalitetsordning

I 2022 viser statistikk fra Netsecurity blant annet følgende trender:

1. De to vanligste angrepsteknikkene i 2022 er innhentede brukerdetaljer og automatisert passordgjetting (<brute force). Aktører kan samle inn brukerdetaljer blant annet gjennom phishing.
2. Mellom februar og mai i 2022 er det registrert en markant økning i angrep, denne økningen har flatet ut mot sommeren.
3. Det er registrert en svakt økende trend i at angrep blir mer avanserte og omgår deteksjon i en tidlig fase.
4. Det er registrert en nedgang i uthenting av data i forbindelse med kompromitteringer. Dette kan tyde på at angrep blir oppdaget og stoppet før aktøren rekker å gjennomføre dette steget.

Netsecurity er en av fem virksomheter i NSMs kvalitetsordning for digital hendelseshåndtering, sammen med Defendable, mnemonic, ATEA og Sopra Steria.

Utnyttelse av programvare-sårbarheter utgjør en stor del av aktiviteten vi ser

I NSMs datagrunnlag ser vi at utnyttelse av programvaresårbarheter har muliggjort en stor del av aktiviteten vi har registrert de siste årene. I 2021 og 2022 har nulldagssårbarheter i Microsoft Exchange, Atlassian Confluence og Apache Log4j muliggjort cyberoperasjoner mot en rekke norske virksomheter, også virksomheter med kritiske funksjoner. Det er også sannsynlig at vi ennå ikke ser alle konsekvensene av utnyttelsen av disse programvaresårbarhetene. Aktører profesjonaliserer tjenestene sine og velger i økende grad målrettet ut sårbare virksomheter når større programvaresårbarheter blir kjent.

Nulldagssårbarheter utnyttes oftere

De siste årene har vi sett et økende antall eksempler på utnyttelse av nulldagssårbarheter. Et av de mest kjente eksemplene på nulldagssårbarheter fra det siste året er «log4shell»-sårbarheten i Apache Log4j.

Den 9. desember 2021 meldte amerikanske sikkerhetseksperter om at «the internet is on fire» grunnet en nyoppdaget, svært alvorlig sårbarhet i loggverktøyet Apache Log4j. Apache Log4j er et av flere programvarebiblioteker som brukes for logging i Java-baserte applikasjoner. Sårbarheten berørte i prinsippet alt som er integrert mot og logges av Log4j, noe som omfatter et svært betydelig antall utbredte tjenester. I tillegg var sårbarheten enkel å utnytte og kunne potensielt gi angripere full kontroll over berørte systemer. Bruken av Log4j er svært utbredt i Norge og et stort antall virksomheter i en rekke sektorer var dermed eksponert for sårbarheten.

NSM ser at det ofte går svært kort tid fra en sårbarhet publiseres til trusselaktører forsøker å utnytte den. Dette gjelder særlig sårbarheter som tillater fjernkjøring av kode fra uautentiserte brukere, og det gjelder spesielt tilfeller hvor utnyttelseskode for sårbarheten er blitt gjort offentlig kjent. Den aktuelle sårbarheten i Log4j er et eksempel på begge deler. I tillegg ligger ansvaret for sikkerhetsoppdatering i flere tilfeller hos tredjepartene som leverer tjenester integrert mot Log4j.

De store konsekvensene av Log4j har tilsynelatende uteblitt for norske virksomheter, men vi kan ikke utelukke at aktører har utført handlinger vi ikke kjenner konsekvensene av ennå.

Leverandører fortsetter å være attraktive mål

De fleste virksomheter benytter en rekke ulike typer programvare og kanskje fra en rekke ulike tjenesteleverandører. Enhver virksomhet bør ta utgangspunkt i at sikkerhetsbrudd vil skje og derfor bygge motstandsdyktighet mot dette. Kompleksitet i tjenester og systemer gjør oss svært sårbare.

To kjente eksempler på leverandørkjedeangrep er Kaseya VSA og SolarWinds[6]. I begge tilfeller ble skadevare spredt gjennom tilsynelatende legitime programvareoppdateringer fra leverandører som kundene hadde tillit til. Slike hendelser kan svekke virksomheters tillit til programvareoppdateringer. Det er problematisk dersom virksomheter oppfatter at risikoen er større ved å implementere en oppdatering raskt, enn det er å vente og se hva som skjer. NSM understreker at sikkerhetsoppdateringer alltid bør installeres så raskt som mulig – og særlig i forbindelse med et nyoppdaget sikkerhetshull.

At ondsinnede aktører målrettet ønsker å ramme tjenesteleverandører, er sannsynligvis fordi skadepotensialet er stort og ringvirkningene massive. En vellykket kompromittering av en leverandør skaper en multiplikatoreffekt, og en virksomhets cybersikkerhet kan påvirkes av svakere sikkerhet andre steder i verdikjeden.

Digitale leverandørkjeder omfatter leveranser av programvare, maskinvare og digitale tjenester. Dette er leverandørkjeder som ofte består av mange ledd og hvor leveransene som regel også omfatter oppdateringer gjennom hele levetiden til produktet eller tjenesten. I sum fører dette til dynamiske og komplekse leverandørkjeder. Det stiller derfor økende krav til kompetanse for anskaffelser, oppfølging av leveransene og risikostyring av virksomheters leverandørkjeder. Dette er tema i NSMs grunnprinsipper for IKT-sikkerhet, prinsipp 2.1 «Ivareta sikkerhet i anskaffelses- og utviklingsprosesser» hvor det er spesielt viktig at virksomhetene vektlegger tiltak 2.1.4, 2.1.9 og 2.1.10.

6 Se Nasjonalt digitalt risikobilde 2021 https://nsm.no/aktuelt/nasjonalt-digitalt-risikobilde-2021

Flere virksomheter rammes av digital utpressing i Norge

I NSMs tallgrunnlag ser vi at løsepengevirus er den typen cyberoperasjon som relativt sett har økt mest de seneste årene. I fjorårets rapport pekte vi på at «ransomware as a service» (RaaS)[7] utgjorde en profesjonalisering av løsepengetrusselen. Dette kan være en del av forklaringen på økningen. En annen delforklaring er at løsepengevirus er en type cyberoperasjon som gjør seg synlig raskt fordi hensikten er å kreve inn penger. Til forskjell fra for eksempel spionasje der aktøren ønsker å forholde seg skjult i systemene i lang tid.

Økning i digital utpressing

I desember 2021 så vi en økning i løsepengeangrep i Norge. Hotellkjeden Nordic Choice ble utsatt for løsepengevirus i begynnelsen av desember, og på hotellene måtte bookingsystemet erstattes med tavle og gjester måtte følges til rommet av ansatte for å bli låst inn fordi nøkkelkortsystemet var nede. NSM valgte å gå ut med en advarsel og en oppfordring til virksomheter om å ha ekstra bemanning gjennom fridagene. Dessverre ble flere virksomheter likevel rammet gjennom høytiden. Mediene meldte om løsepengevirus mot Nortura, Nordland fylkeskommune og Amedia. Konsekvensene av løsepengevirus fortsetter å gå sterkt utover forbrukere og kunder, i tillegg til virksomheten selv. Gjennom angrepet mot Amedia ble produksjonen av papiraviser midlertidig stoppet. Angrepet mot Nortura førte til stans i slakting, noe som både gikk utover varetilgang i butikker og bønder som ikke fikk levert inn dyr til slakt. Videregående skoler i Nordland måtte gjennomføre undervisning uten bruk av de digitale systemene, som skoler nå benytter i det daglige.

NSM har opprettet en egen temaside om hvordan virksomheter kan sikre seg mot løsepengevirus på nsm.no[7].

Fem effektive tiltak mot dataangrep

NSM har i flere tiår utviklet sikkerhetstiltak for beskyttelse av IKT-systemer. Ut fra disse erfaringene ser vi at virksomheter kan stanse de fleste dataangrep med følgende tiltak:

1. Installer sikkerhetsoppdateringer så fort som mulig, og mest mulig automatisk
2. Ikke tildel administrator-rettigheter til sluttbrukere
3. Ikke tillat bruk av svake passord, og bruk multifaktorautentisering der det er mulig
4. Fas ut eldre IKT-produkter
5. Tillat kun programvare som er godkjent av virksomheten eller enhetsleverandøren

«Fem effektive tiltak mot dataangrep» er publisert på nsm.no/5tiltak med utfyllende informasjon til hvert punkt.

7 Se https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/digital-utpressing/

NSM er bekymret for at små og mellomstore virksomheter i økende grad blir offer for løsepengevirus og sabotasje, fordi de ikke alltid har økonomisk mulighet til å investere i tilstrekkelig god digital sikkerhet. Større internasjonale tilfeller av løsepengevirus som de som rammet Colonial Pipeline eller Kaseya[7] har gjort at store virksomheter – også nasjonalt – har investert mer i digital sikkerhet og gjort det vanskeligere for aktørene å ramme dem.

Internasjonalt fremhever sikkerhetseksperter[8] at frem til høsten 2021 har 80–90 prosent av løsepengevirushendelser brukt fjernpålogging med innhentede brukerdetaljer som metode for å sikre veien inn. Utfordringen er at det er en svak tendens til at disse angrepene benytter mer avanserte metoder for å komme inn i systemene. Det er viktig at sikkerhetstiltak og evne til å avdekke angrep forbedres. For å få størst effekt av et løsepengevirus vil mange av angrepene forsøke å bevege seg fra maskin til maskin i virksomhetens nettverk for å spre seg til flest mulig maskiner. Et effektivt sikkerhetstiltak mot dette er at virksomheten deler inn sitt eget nett i mindre soner og etablerer tilstrekkelige sikkerhetsmekanismer mellom disse[9].

Varslingssystem for digital infrastruktur (VDI)

NSM drifter og organiserer et nasjonalt sensornettverk på internett, som står utplassert hos virksomheter som anses som en del av kritisk infrastruktur. VDI skal kunne detektere og varsle om cyberoperasjoner som treffer kritisk infrastruktur eller kritiske funksjoner i Norge.

Data fra nettverkssensorer er en kilde for å oppdage cyberoperasjoner. En utfordring er at mesteparten av nettverkstrafikken i dag er kryptert og krypteringsgraden øker. Jevnt over ser vi at om lag 80 prosent av trafikken i VDI er kryptert.

I tillegg flyttes flere tjenester til skyløsninger. Dette gjør at synligheten i sensornettverket blir dårligere. De siste årene har NSM arbeidet med en betydelig oppgradering av VDI for å bedre imøtekomme fremtidens utfordringer.

Trusselaktører er flinke til å skjule sporene sine. Det vi leter etter kan være små avvik som er vanskelig å oppdage når vi arbeider med store mengder data. NSM bidrar derfor i forskning på hvordan maskinlæring kan brukes til anomalideteksjon for scenarier som er relevante i cyberdomenet.

Arbeidet med å bygge et aktivt cyberforsvar blir vi ikke ferdige med. Vi må kontinuerlig utvikle oss for å kunne forhindre, avdekke og håndtere angrep.

8 Coveware Quarterly report : Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022 (coveware.com)

9 Se tiltak 2.2.3 «Del opp virksomhetens nettverk etter virksomhetens risikoprofil» i NSMs grunnprinsipper for IKT-sikkerhet.)

Avdekkede sårbarheter fra NSMs penetrasjonstester

I 2021 gjennomførte NSM et titalls inntrengingstester i norske virksomheters datasystemer. Testingen er nøye avtaleregulert mellom NSM og virksomhetene det gjelder, og er forbeholdt virksomheter underlagt sikkerhetsloven[10].

En inntrengingstest søker å avdekke fysiske, logiske, tekniske, menneskelige og administrative sårbarheter i et informasjonssystem eller ved virksomhetens fysiske lokasjon.

Under følger en rangert liste over de vanligste sårbarhetene vi ser, og hvordan disse kunne vært unngått med bruk av NSMs grunnprinsipper for IKT-sikkerhet (GP-IKT).

Dårlige passord

Mange brukere av systemet velger dårlige passord som det er lett for NSM å gjette/knekke. En trusselaktør trenger kun å knekke ett av hundre- eller tusenvis av passord for å få tilgang, avhengig av virksomhetens størrelse.

Anbefalt tiltak: Bruk et sentralt verktøy til å kontrollere passordkvaliteten opp mot virksomhetens sikkerhetskrav (GP-IKT 2.6.3 e)). Bruk multi-faktor autentisering, om mulig (2.6.7 e)).

Lagrede passord

Mange virksomheter lagrer passord i filer som alle har tilgang til. Grunnen til dette er blant annet at flere ansatte bruker samme spesialbrukere – som de ikke husker passordet til.

Anbefalt tiltak: Etabler retningslinjer for tilgangskontroll. Alle kontoer bør kunne spores til en ansvarlig bruker. Ansvarliggjør brukere mht. at passord er personlige og hemmelige, og aldri skal deles med noen. (GP-IKT 2.6.1 c) og g)) Minimer rettigheter til sluttbrukere og spesialbrukere (GP-IKT 2.6.4).

Programvare med feil

Virksomheten bruker programvare som inneholder feil (bugs). Ofte vil det finnes sikkerhetsoppdateringer til programvaren, men virksomheten har ikke installert denne ennå. En trusselaktør kan utnytte feilene til å skaffe seg flere rettigheter eller få tilgang til nye maskiner.

Anbefalt tiltak: Etabler et sentralt styrt regime for sikkerhetsoppdatering. Installer sikkerhetsoppdateringer så fort som mulig (GP-IKT 2.3.1).

Passordgjetting mot passord-database

Virksomhetens systemer er konfigurert slik at det er praktisk mulig å gjette passord mot alle brukerne i virksomhetens passorddatabase. Selv om antallet gjetninger per time vil være lavt, vil man ofte klare å gjette dårlige passord.

Anbefalt tiltak: Tiltak for å sette opp og gjennomføre overvåking slik at man kan oppdage og agere på denne type angrep er beskrevet i GP-IKT 3.2 og 3.3.

Utdaterte, ikke-støttede operativsystemer

Virksomheten har datamaskiner hvor operativsystemet er så gammelt at leverandøren ikke lenger produserer sikkerhetsoppdateringer. Dette skjer gjerne fordi maskinene kjører spesialprogramvare og/eller utstyr som kun fungerer på dette, eldre systemet.

Anbefalt tiltak: Kartlegg operativsystemer i virksomhetens nett (GP-IKT 1.2.4 a)). Det vil enten være mulig å oppgradere til et nyere OS (GP-IKT 2.1.2) eller isolere utstyr som ikke kan oppgraderes (GP-IKT 2.5.4)

Gamle systembrukere

Det kan være mange grunner til at systembrukere er inaktive, som at folk slutter, at systemer ikke brukes lenger, at leverandører byttes ut. Ofte henger disse brukerne igjen i systemet, og ofte har de passord som enkelt kan knekkes.

Anbefalt tiltak: Kontoer som ikke benyttes, bør deaktiveres (GP-IKT 2.6.2 b)).

Sårbare tjenester og protokoller

En trusselaktør med tilgang til virksomhetens nett vil ha mulighet til å utnytte sårbare tjenester som kjører i nettet. For eksempel kan det være mulig å avlytte trafikk, overta kommunikasjon, eller forfalske meldinger.

Anbefalt tiltak: Deaktiver unødvendig funksjonalitet, f.eks. eldre eller ubrukte protokoller (GP-IKT 2.3.3).

10 Se nsm.no/pentest for mer informasjon

Konseptvalgutredning om nasjonal sky

Å gjøre lagring, programmer og tjenester tilgjengelig fra store felles datasentre over nettverk fremfor å være avhengig av at det leveres fra lokale servere og maskiner, gir økt smidighet og fleksibilitet, og innebærer ofte også en kostnadsreduksjon. Slike skytjenester er også ofte levert fra en sikker infrastruktur og har profesjonelle sikkerhetsmiljøer. Dette bidrar ofte til å øke sikkerhetsnivået for virksomhetene ettersom de da kan fase ut utdaterte IKT-systemer og kvitte seg med «teknisk gjeld».

NSM er bekymret for den samlede nasjonale avhengigheten til utenlandske skyleverandører og hva denne avhengigheten kan medføre ved potensielle kriser og konflikter. Samtidig ser vi at bruk av utenlandsk sky for eksempel kan bidra med spredning av risiko. Dette er en positiv effekt både i tilspissede situasjoner og i fredstid.

For noen virksomheter bør bruk av skytjenester vurderes opp mot behovet for nasjonal kontroll og nasjonal beredskap. NSM er også bekymret for at samfunnskritiske IKT-tjenester tjenesteutsettes uten tilstrekkelige risikovurderinger og sikringstiltak, og at data flyttes til utlandet uten tilstrekkelige sikkerhetsfaglige vurderinger. Problemstillinger som f.eks. jurisdiksjon og sikkerhetspolitikk, gjør at bruk av skytjenester fra kommersielle, multinasjonale aktører kan innebære risiko for staten.

Problemstillingene rundt bruk av skytjenester har NSM diskutert over flere år og i flere publikasjoner. NSM har fått i oppdrag fra Justis- og beredskapsdepartementet (JD) å gjennomføre en konseptvalgutredning (KVU) for etablering av en nasjonal skytjeneste. Dette inkluderer blant annet å vurdere i hvilke tilfeller staten bør ta eierskap til digital infrastruktur, plattformer, plattformutvikling og standardutvikling. Denne utredningen skal leveres i desember 2022.

Er du forberedt?

Det er krevende for de fleste norske virksomheter å holde tritt med det stadig skiftende risikobildet. Det viktigste en virksomhet kan gjøre er å redusere egne sårbarheter. Alt for ofte ser vi at trivielle og elementære feil og svakheter utnyttes av en trusselaktør. Det kan være kostbart. Det er unødvendig. Ofte kunne det vært forhindret ved følge NSMs grunnprinsipper for IKT-sikkerhet.

I Nasjonal strategi for digital sikkerhet[1] er visjonen at det skal være trygt å bruke digitale tjenester i Norge. Både privatpersoner og virksomheter skal ha tillit til at den nasjonale sikkerheten blir ivaretatt. Det oppnår vi når virksomhetsledere er sitt ansvar bevisst og prioriterer det forebyggende sikkerhetsarbeidet i egen virksomhet. Økt sikkerhetsnivå hos norske virksomheter skaper en økt nasjonal robusthet og motstandsevne for hele det norske samfunn.

Din jobb er å forsøke å forestille deg det uforutsette, å anta at din virksomhet blir rammet av en cyberoperasjon og å øve på hvordan disse scenariene skal håndteres.

I den nye sikkerhetspolitiske situasjonen vi står i, kan ett svakt ledd få konsekvenser for mange andre. Det er spesielt viktig at virksomheter som understøtter grunnleggende nasjonale funksjoner eller som skal bidra inn i totalforsvaret imøtekommer morgendagens risiko i cyberdomenet. Vår oppfordring er klar: rust opp.

Er du forberedt?

Design: Tank
Foto: Ilja Hendel

Utsatt for et dataangrep?

NSMs nasjonale cybersikkerhetssenter (NCSC) ivaretar cyberberedskap og bistår med krisehåndtering. NCSC er knutepunkt for nasjonalt og internasjonalt samarbeid innen deteksjon, håndtering, analyse og rådgivning knyttet til cyberangrep.

Dersom en virksomhet rammes av en alvorlig digital hendelse, kan NCSC gi bistand til hendelseshåndtering. Denne bistanden inkluderer rådgivning og støtte til IKT- og sikkerhetsavdelinger. Rådgivningen kan omhandle alt fra enkle tiltak som endring av sikkerhetsoppdateringsrutiner og innføring av to-faktor, til å informere ledelsen i virksomheten om dagens situasjonsbilde og medieuttalelser. Teknisk analyse kan omhandle alt fra analyse av nettverkslogger og skadevare, til full undersøkelse av berørt infrastruktur og tips til opprydding.

NCSC er en rådgiver under hendelseshåndtering og ønsker derfor å bli kontaktet av rammede virksomheter. Alvorlige digitale hendelser rapporteres inn til NCSCs operasjonssenter på cert@ncsc.no eller telefon 02497 (+47 23 31 07 50). Informer også raskt til relevant sektor-CERT der det finnes.

NSM har opprettet en godkjenningsordning for leverandører som tilbyr tjenester for hendelseshåndtering av cyberangrep. Selskapene i kvalitetsordningen kan bistå virksomheten i håndtering av hendelser.

Se NSMs nettsider for kontaktinformasjon.

NASJONAL
SIKKERHETSMYNDIGHET

Postboks 814,
1306 Sandvika
Tlf. 67 86 40 00

Tlf. 67 86 40 00
nsm.no/NDIG2022
www.nsm.no