Det blir alvor

Digital sikkerhet 2023

FOTO: GETTY IMAGES

telenor

Tidligere utgaver:

Innhold

FOTO: SØREN SIGFUSSON / NORDEN.ORG

Innhold: Der det ikke eksplisitt er angitt en ekstern forfatter eller opprinnelse, er de vurderinger, råd og fagkunnskap som presenteres i denne rapporten basert på kunnskap Telenor Norge besitter gjennom egne erfaringer og vårt helhetlige sikkerhets- og beredskapsmiljø.

Eksterne kilder: Tekst fra eksterne kilder med kildereferanse er ordrette gjengivelser.

Redaksjon ble avsluttet i august **Design:** Publicis **Bilder:** Søren Sigfusson, Gunnar Ridderström/Unsplash, Yaroslav Krechko, Google maps, ITproX, Telenor, Getty Images, Scanpix **Trykk:** Involve!

Digital versjon: *https://www.telenor.no/om/digital-sikkerhet/2023*

Ønsker du å komme i kontakt med oss? Send e-post til *desken@telenor.com*

Alt må virke hele tiden

Et moderne samfunn forutsetter et solid og sikkert fundament, en digital infrastruktur der sårbarhet er redusert til et minimum. Premisset for den digitale grunnmuren i 2023 er at alt må virke hele tiden.

Det er alvor nå. Den endrede sikkerhetspolitiske situasjonen påvirker våre valg. Telenor har de siste årene bygd et helhetlig sikkerhetsmiljø for å beskytte oss selv, våre kunder og ivareta vårt samfunnsansvar. Vi jobber systematisk innen tre områder; sikkerhet, robusthet og beredskap. Slik bygger, drifter og utvikler vi en så trygg og sikker digital infrastruktur som mulig. Vi tar et ansvar for mer enn bare bedriften. Et utfall i vår infrastruktur og tjenester vil kunne medføre store samfunnsmessige konsekvenser og i en krisesituasjon i verste fall kunne true nasjonale sikkerhetsinteresser.

Digitalisering av industri og operasjonell teknologi stiller økte krav til sikkerhet. I krigen i Ukraina ser vi målrettede fysiske og logiske angrep fra Russland som systematisk søker å bryte ned sivil infrastruktur som strøm, vann, mat, transport, eller bredbånd og mobil. Det er viktig å trekke læring og erfaringer fra telekombransjen i Ukraina. Sikkerhet koster og krever at vi utnytter kompetanse og kapasitet som finnes i industrien for å sikre verdiene til kritiske områder som olje- og gassproduksjon, strømforsyning, kritisk offentlig virksomhet og sykehusdrift. Etablering av nye industrielle partnerskap som tar frem program-

> Det trengs et styrket nordisk samarbeid om sikkerhet, robusthet og beredskap. Flere felles løsninger må utvikles i en nordisk og alliert ramme.

vare og løsninger som kan bidra til å sikre industribedrifter og kritisk infrastruktur er avgjørende. Å utnytte kritisk kompetanse og kapasitet på tvers vil åpne muligheter for innovasjon og verdiskapning innen industriell cybersikkerhet.

Trusselbildet mot Telenor, våre kunder og norske virksomheter og myndigheter, preges av et offensivt Kina og et trolig varig urolig Russland. Vi ser at kritisk infrastruktur blir mer utsatt. NATO utvides og at Arktis blir viktigere. Økt digitalisering innebærer også større spillerom for kriminelle aktører. Dette kan være alt fra svindlere som prøver å lure deg eller virksomheten til profesjonelle cyberkriminelle eller hackere med mer alvorlige motiver.

De åpne trusselvurderingene fra de norske etterretnings- og sikkerhetstjenestene er svært viktige for å forebygge. Deling av informasjon underbygger trusselforståelse som gir grunnlag for systematisk risikostyring. Denne rapporten er Telenors bidrag der vi deler egne erfaringer om trusselbilde og håndtering av sikkerhetshendelser. Og ikke minst setter fokus på områder som er viktige for sikkerhetsarbeid både i virksomheter og i samfunnet for øvrig.

Vi ser et behov for ytterligere å styrke Norges digitale motstandskraft. Det fordrer systematisk samhandling. Og at det etableres bedre løsninger for gradert samhandling og at utvalgte virksomheter gis bedre tilgang til trussel- og sikkerhetsinformasjon.

Kunstig intelligens (KI) debatteres bredt for tiden også knyttet til sikkerhet. Vil denne typen teknologi styrke eller svekke cybersikkerheten? Kunstig intelligens kan anvendes i både cyberangrep og cyberforsvar. Tankeløs bruk av KI kan imidlertid få store negative konsekvenser; så god bruk av kunstig intelligens fordrer menneskelig intelligens.

I en mer urolig verden må norske og nordiske selskaper forberede seg på å møte usikkerhet og større risiko for avbrudd i leveranser og mangel på kritiske komponenter. Et nordisk initiativ

FOTO: TELENOR

for å bedre benytte tekniske løsninger og infrastruktur som fiber og datasentre på tvers av land i Norden vil styrke den nasjonale forsyningssikkerheten med flere ressurser nær Norge. Det vil og styrke motstandskraften i den nordiske regionen totalt sett og stimulere multinasjonale teknologileverandører til å etablere kompetansemiljøer i Norden.

Et samlet Norden i NATO gir derfor muligheter. Det trengs et styrket nordisk samarbeid om sikkerhet, robusthet og beredskap. Flere felles løsninger må utvikles i en nordisk og alliert ramme. Private selskap må være en del av totalberedskapen. En mer harmonisert lovgivning som tillater deling av kompetanse, personell, tekniske løsninger og infrastruktur på tvers av Norden er nødvendig. Det trengs et taktskifte for raskere prosess knyttet til sikkerhetsklarering og bedre bruk av knappe personell-ressurser. Norden kan bygge mer sikkerhet og robusthet om ressursene kan spille bedre sammen på tvers av de nordiske landene. Det krever et sikkerhetspolitisk fundament og vilje til endring.

Sikkerhet er et lederansvar. Det starter med å erkjenne risiko og å sørge for at sikkerhet- og trusselforståelse er integrert i risikostyring og kompetansebygging i hele organisasjonen. Å bygge sikkerhetskultur krever tid og systematisk innsats. Dette er avgjørende for hvor godt vi vil lykkes med å forenkle, forbedre og fornye i egen virksomhet og understøtte digitalisering av samfunnet. Alt henger sammen. Vi må være beredt.

Birgitte Engebretsen,
administrerende direktør i Telenor Norge

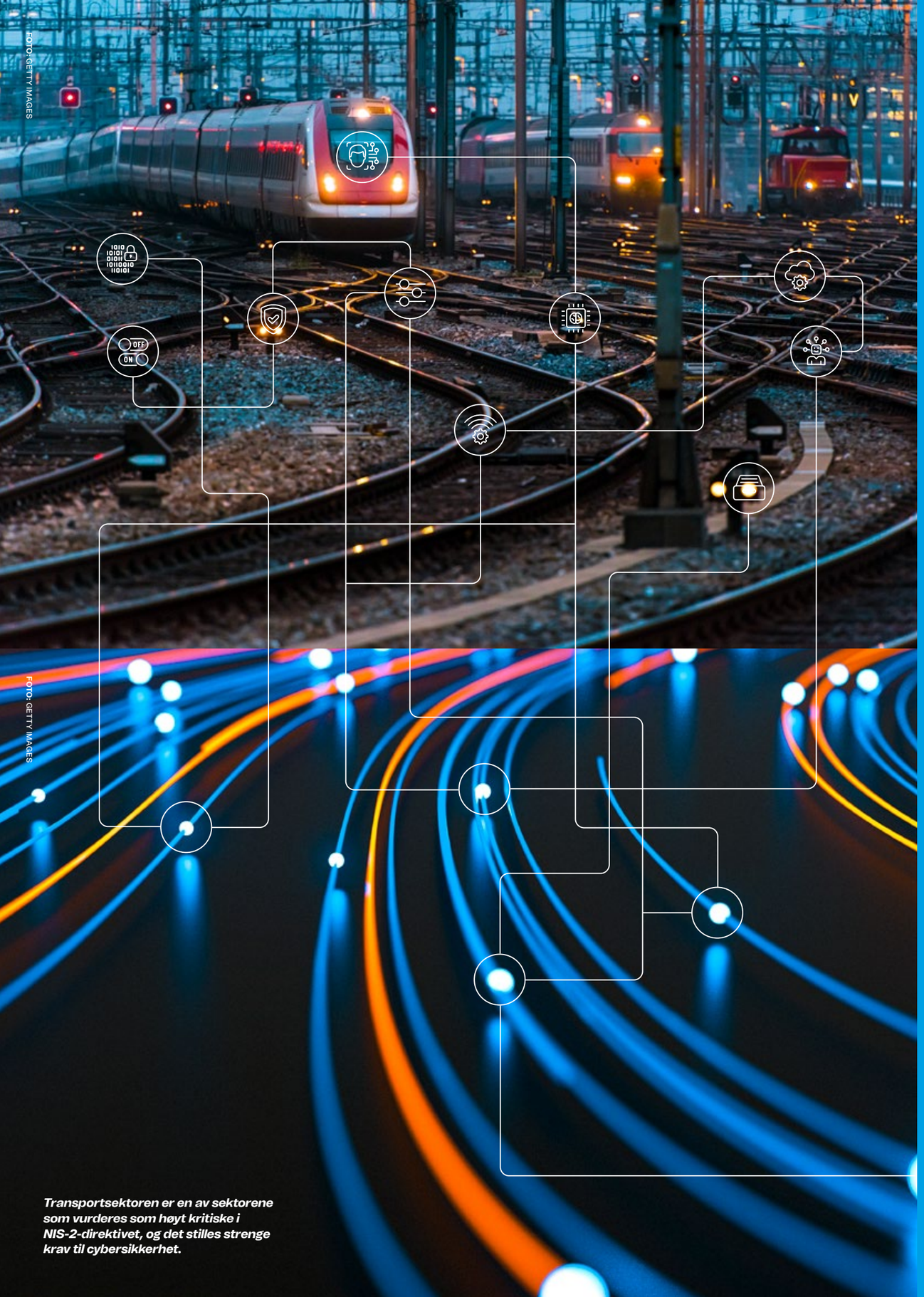


FOTO: GETTY IMAGES

FOTO: GETTY IMAGES

Transportsektoren er en av sektorene som vurderes som høyt kritiske i NIS-2-direktivet, og det stilles strenge krav til cybersikkerhet.

2

Industriell cybersikkerhet – innovasjon og verdiskapning

Digitalisering av operasjonell teknologi (OT) øker teknologi-avhengigheten og eksponerer sårbarheter. Som ved all annen digitalisering innebærer dette også økte krav til sikkerhet. I denne artikkelen belyser forfatterne det unike behovet for cybersikkerhet i IT-OT-integrerte systemer og relaterer dette til etablerte rammeverk og regulering. De tar til orde for å flytte fokus fra kostnadene og heller se på verdiene investeringer i OT-sikkerhet gir.

INFORMASJONSTEKNOLOGI (IT) ER et velkjent begrep som beskriver systemer som håndterer informasjon ved å innhente, behandle, lagre og overføre denne. Operasjonell teknologi (OT) på sin side omfatter enhetene og teknologien som samhandler med den fysiske verden; både de fysiske maskinene i seg selv og systemene som styrer, overvåker og samhandler med dem.

OT byr på unike sikkerhetsutfordringer. Blant annet fordi det er svært høye krav til tilgjengelighet og operasjonell kontinuitet, svært lang livssyklus, et nødvendig hensyn til trygghet (safety) i kombinasjon med sikkerhet, og svak sikkerhet i teknologien i seg selv – gjerne basert på en forutsetning om isolasjon og fysisk sikring.

IT og OT har over tid gradvis smeltet sammen. Ved den digitale transformasjonen i industrien som gjerne omtales som «Industri 4.0», integreres de i kyberfysiske systemer (CPS). Disse systemene har flere egenskaper som skiller dem fra både rene IT- og rene OT-systemer. Dette er intelligente systemer der fysiske, nettverks- og databaserte komponenter samvirker. CPS-er utgjør kjerneelementer i industrielle kontrollsystemer (ICS) som brukes til å styre prosesser i industrien som fabrikasjon, håndtering av produkter, samt produksjon og distribusjon.

OT-cybersikkerhet – en investering i muligheter

Diskusjoner om OT-cybersikkerhet tar ofte utgangspunkt i de potensielle tapene man risikerer ved ikke å investere i dette. Man viser gjerne til tidligere hendelser og utgifter som følge av dem, tapte timeverk på grunn av nedetid, og lignende måledata. Dessverre er dette en av hovedgrunnene til at virksomheter vanligvis betrakter cybersikkerhet som en nødvendig kostnad fremfor en investering og mulighet. Dette er også en av grunnene til at det ofte stilles spørsmål ved behovet for å tildele ressurser til cybersikkerhet, særlig når man ikke er underlagt bransjespesifikke markedstiltak eller regulatoriske krav.

Fremme av OT-cybersikkerhet bør ikke lenger baseres på frykt for uønskede hendelser. Det er på tide å

TEKST:

Sokratis Katsikas, Centre Director, NORCICS

Vasileios Gkioulos, Work Package Leader, NORCICS

Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS) er et av NTNUs sentre for forskningsbasert innovasjon.

Les mer om NORCICs her: https://www.ntnu.edu/norcics

Denne artikkelen er oversatt fra originalspråket og redaksjonelt tilpasset for publisering i Digital Sikkerhet 2023.

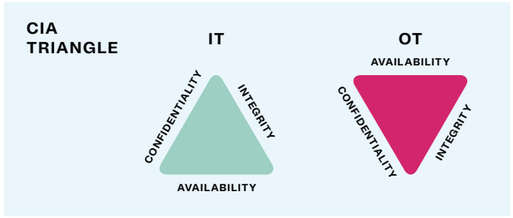
fokusere på mulighetene og fordelene ved å investere i OT-cybersikkerhet. Diskusjonen bør handle om hvordan dette kan muliggjøre innovasjon, digital transformasjon og verdiskapning. OT-cybersikkerhet handler om mer enn bare å beskytte data og systemer mot ondsinnede handlinger. Det handler også om nye tilnærminger til å drive virksomhet, skape verdi og levere tjenester i den digitale tidsalderen. Cybersikkerhet kan hjelpe organisasjoner til å:

- **Styrke omdømme, tillit og lojalitet** blant kunder, samarbeidspartnere og interessenter ved å sikre personvern og sikkerhet.
- **Ta i bruk nye teknologiløsninger raskere, effektivt og sikkert.** Dette øker driftseffektiviteten og produktiviteten, samtidig som organisasjonen er godt rustet til å innovere og tilpasse seg skiftende markedsbehov og kundeforventninger.
- **Fremme innovasjon og kreativitet** ved å muliggjøre sikker eksperimentering, samarbeid, produktutvikling og deling av informasjon.
- **Oppnå konkurransefortrinn** og markedsandel ved å tilby differensierte og sikre produkter og tjenester.
- **Overholde regulatoriske krav** og bransjestandarder ved å ta i bruk beste praksis og rammeverk.

Cybersikkerhet – mer enn bare teknologi

I tillegg til teknologiske endringer, fører iT-OT-integrasjon også til organisatoriske og atferdsmessige endringer som påvirker cybersikkerhet. Det kreves nye mekanismer for å etablere tillit mellom maskiner og mennesker. I tillegg bør man fokusere på motstandsdyktighet for å begrense risikoer i den digitale verdikjeden. Videre krever kompleksiteten ikke bare innovative løsninger, men også innovative perspektiver. Alt dette betyr at det ikke er en enkel anvendelse av cybersikkerhetsteknologier og tiltak som er utviklet for rene IT-systemer, på IT-OT-integrerte systemer. Det er også nødvendig å utvide cybersikkerhetsegenskapene

Det kreves nye mekanismer for å etablere tillit mellom maskiner og mennesker.



utover den konvensjonelle CIA-trekanten (Confidentiality, Integrity and Availability) til å inkludere egenskaper som kontrollerbarhet, observerbarhet og operabilitet. Utfordringene med å håndtere cybersikkerhet for IT-OT-integrerte systemer krever derfor en helhetlig, systematisk tilnærming til både teknologi, mennesker og prosesser som adresserer cybersikkerhet i alle faser av livssyklusen til et produkt eller en tjeneste. En slik tilnærming er kartlagt av NIST Cybersecurity Framework (CSF).

Rammeverk og standarder

NIST utga sitt Cybersecurity Framework (CSF) første gang i 2014 og oppdaterte det i april 2018. Neste oppdatering forventes å bli tilgjengelig i løpet av 2023. Dette er et frivillig rammeverk av standarder, retningslinjer og praksis. Rammeverket består av tre hovedkomponenter: *kjerne, implementeringsnivåer og profiler*. Kjernekomponenten gir en samling av ønskede cybersikkerhetsaktiviteter og resultater organisert i fem kjernefunksjoner, nemlig *identifisere*, *beskytte*, *oppdage*, *respondere* og *gjenopprette*.

1. **Identifisere**-funksjonen har som mål å identifisere de ressursene som trenger beskyttelse
2. **Beskytte**-funksjonen har som mål å fastslå de beskyttende tiltakene som skal settes i verk
3. **Oppdage**-funksjonen har som mål å fastslå tiltakene som skal brukes for å oppdage angrep
4. **Respondere**-funksjonen har som mål å fastslå tiltakene som vil kunne begrense et angrep dersom det oppstår
5. **Gjenopprette**-funksjonen har som mål å fastslå tiltakene som vil tillate rask gjenoppretting hvis et angrep lykkes

Implementeringsnivåene i rammeverket hjelper virksomheter ved å gi kontekst for hvordan en ser på håndtering av cybersikkerhetsrisiko. Profilene er organisasjonens unike tilpasning av krav og mål, risikoappetitt og ressurser mot de ønskede resultatene fra Kjernekomponenten.

Utover rammeverk og anbefalinger gir standarder verdifull veiledning i forhold til cybersikkerhetsutfordringer. Flere standarder omhandler cybersikkerhet for ICSer helt eller delvis, men to utmerker seg som allment aksepterte og sektoruavhengige: NIST SP 800-82r2-guiden og ISA/IEC 62443-serien med standarder. Disse standardene etablerer beste praksis for sikkerhet og gir en måte å vurdere sikkerhetsnivået på. Begge har en helhetlig tilnærming til cybersikkerhetsutfordringen på tvers av drift og informasjonsteknologi, og favner om både trygghet i prosesser

«Svært kritiske» sektorer i NIS-2

- Energi: Elektrisitet, Fjernvarme og -kjøling, Olje, Gass, Hydrogen
- Transport: Luft, Jernbane, Vann, Veier
- Bank
- Finansielle markedssystemer
- Helse
- Drikkevann
- Avløpsvann
- Digital infrastruktur
- ICT-tjenestehåndtering (B2B)
- Offentlig administrasjon
- Rom

«Kritiske» sektorer i NIS-2:

- Post- og kurertjenester
- Avfallshåndtering
- Tilvirkning og distribusjon av kjemikalier
- Produksjon, prosessering og distribusjon av mat
- Produksjon
- Digitale tjenesteleverandører
- Forskning

OT-cybersikkerhet er ikke en engangsinvestering eller en statisk tilstand der noe er «sikkert» eller ikke. Det handler om å være tilstrekkelig sikker.

og cybersikkerhet. ISA/IEC-standardene relaterer seg til alle bransjesektorer som bruker ICSer. Implementeringen av retningslinjene som gis av disse standardene er imidlertid verken enkel eller rett frem.

Regulering

En annen betydelig faktor som påvirker implementeringen av OT-cybersikkerhetsløsninger er regulatorisk samsvar med for eksempel krav i EU-direktivet NIS-2 som utvider og moderniserer det opprinnelige NIS-direktivet. Begge direktivene stiller krav til sikkerhet i nettverks- og informasjonssystemer. I NIS-2 er nye sektorer inkludert, en klar størrelsesgrense innføres og bøter og andre straffereaksjoner økes. NIS-2 har fått et utvidet sektorrettet fokus, der flere sektorer enn tidligere blir omfattet og fastsetter en rekke fokusområder som alle inkluderte organisasjoner må innføre tiltak for.

Et felles ansvar

OT-cybersikkerhet er ikke en engangsinvestering eller en statisk tilstand der noe er «sikkert» eller ikke. Det handler om å være tilstrekkelig sikker. Dette er en prosess som krever kontinuerlig overvåking, oppdatering og forbedring. Det er også et felles ansvar som involverer alle interessenter, fra toppledelsen til ansatte, kunder og samarbeidspartnere. OT-cybersikkerhet er en strategisk ressurs som kan støtte virksomheter i å nå sine mål og visjoner i den digitale tidsalderen.

Ved å investere i cybersikkerhet kan virksomheter ikke bare beskytte sine eiendeler og omdømme, men også åpne opp for nye muligheter og potensial for vekst og transformasjon. Istedenfor å betrakte OT-cybersikkerhet som en utgift, bør virksomheter derfor heller anerkjenne mulighetene for verdiskapning og innovasjon dette gir. //

Tiltaksområder fastsatt i NIS-2:

a. sikkerhetspolicyer og informasjonssystemers sikkerhet;

b. håndtering av hendelser (forebygging, oppdagelse, respons, gjenoppretting);

c. forretningskontinuitet gjennom katastrofeberedskap og krisehåndtering;

d. sikkerhet i forsyningskjeden, inkludert sikkerhetsrelaterte aspekter vedrørende forholdet mellom hver enhet og dens direkte leverandører eller tjenesteleverandører;

e. sikkerhet ved anskaffelse, utvikling og vedlikehold av nettverks- og informasjonssystemer, inkludert sårbarhetshåndtering og offentliggjøring;

f. retningslinjer og prosedyrer for å vurdere effektiviteten av tiltak for cybersikkerhetsrisikostyring;

g. grunnleggende praksis for cybersikkerhetshygiene og opplæring i cybersikkerhet;

h. retningslinjer og prosedyrer for bruk av kryptografi og, når det er hensiktsmessig, kryptering;

i. sikkerhet for menneskelige ressurser, adgangskontrollpolicyer og eiendelsforvaltning;

j. bruk av multifaktorautentisering eller kontinuerlige autentiseringssystemer, sikrede tale-, video- og tekstmeldingskommunikasjon og sikrede kommunikasjonssystemer for nødsituasjoner innenfor enheten, når det er hensiktsmessig.

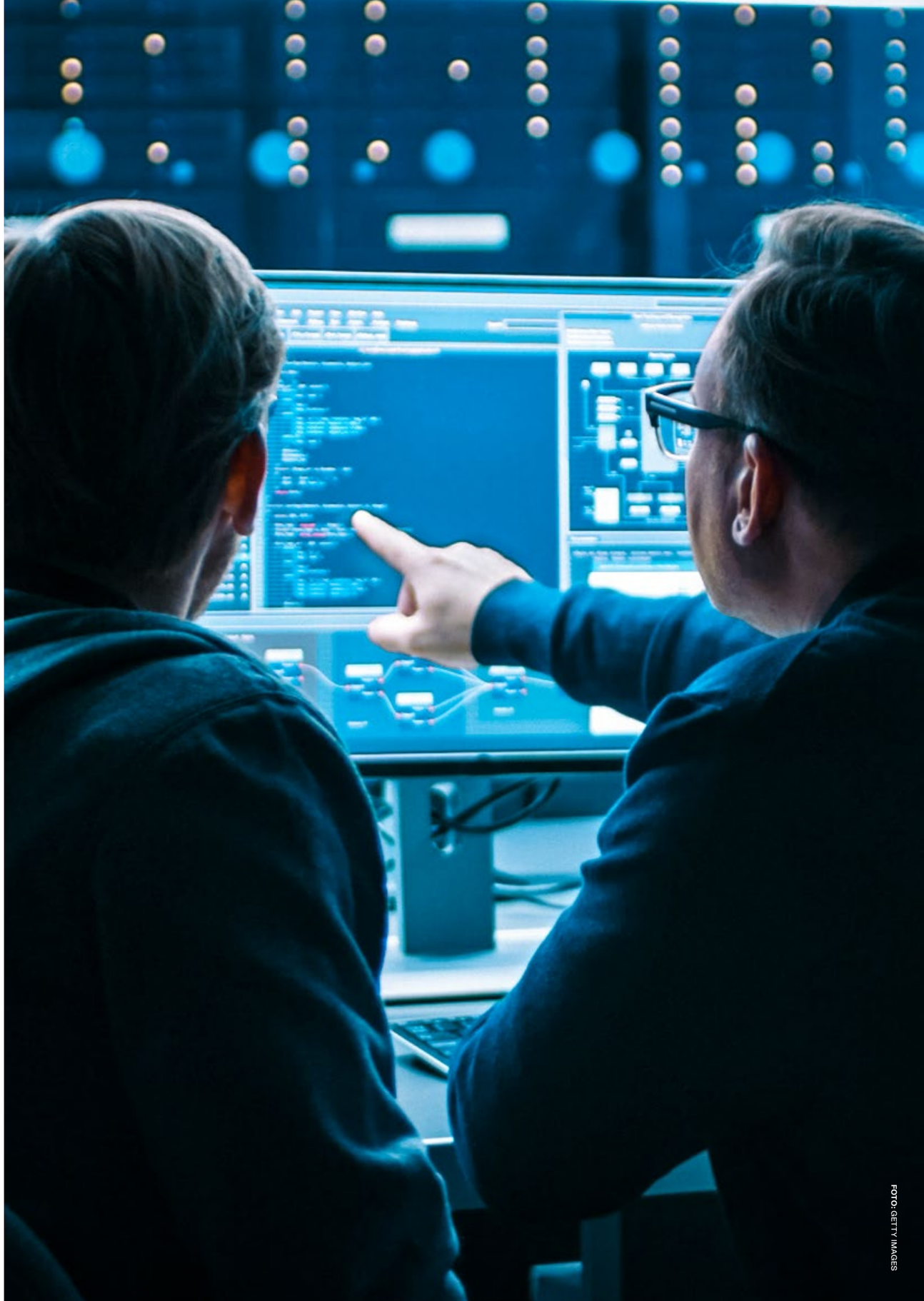


FOTO: GETTY IMAGES

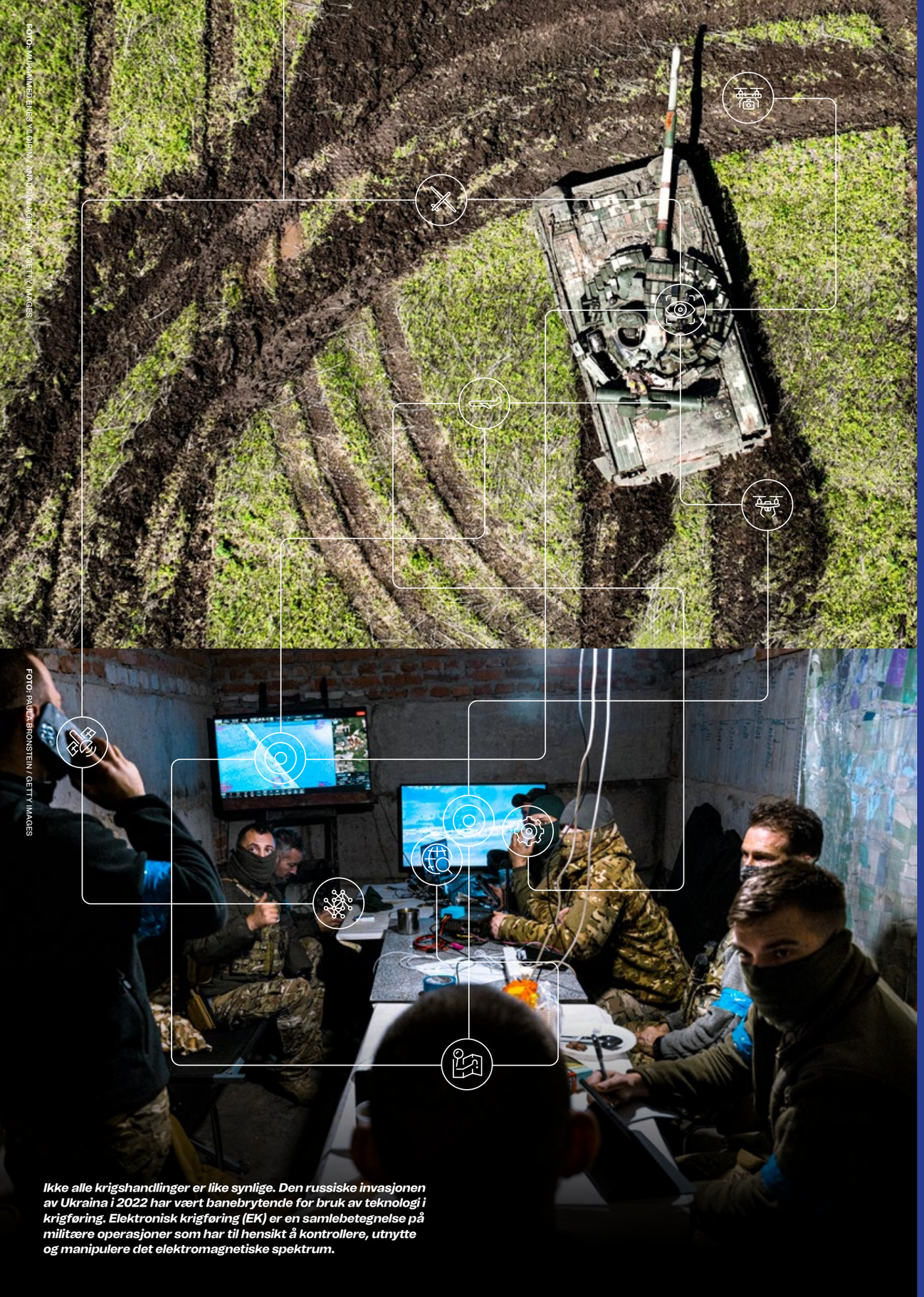


FOTO: MUHAMMED ELMAS YILDIRIM / ANADOLU AGENCY VIA GETTY IMAGES

FOTO: PAULA BRONSTEIN / GETTY IMAGES

Ikke alle krigshandlinger er like synlige. Den russiske invasjonen av Ukraina i 2022 har vært banebrytende for bruk av teknologi i krigføring. Elektronisk krigføring (EK) er en samlebetegnelse på militære operasjoner som har til hensikt å kontrollere, utnytte og manipulere det elektromagnetiske spektrum.

3

Elektronisk kommunikasjon i konflikt og krig

Vi er inne i det andre året med krig i Europa. Elektronisk kommunikasjon er avgjørende for både militære systemers og sivilsamfunnets evne til å fungere. Ikke overraskende er derfor elektronisk kommunikasjon og kommunikasjonsinfrastruktur mål for disruptive og destruktive handlinger, med både cyber-, elektromagnetiske og kinetiske angrep.

I DETTE KAPITLET vil vi først se nærmere på kamphandlinger i det elektromagnetiske spektrum. Deretter oppsummerer Cathal McDaid, CTO i ENEA AdaptiveMobile, viktige erfaringer fra telekombransjen i Ukraina – for innsikt og til ettertanke for beredskapsarbeid i andre land.

Kamphandlinger i det elektromagnetiske spektrum
Til tross for mye hemmelighold har elektronisk krigføring – manipulering av signaler i det elektromagnetiske spektrum – vært en faktor som vi i alle fall delvis har kunnet observere under krigen i Ukraina. Denne artikkelen ser nærmere på de offensive aspektene av elektronisk krigføring, spesielt jamming (se egen tekstboks for terminologi). Noen typer elektronisk krigføring (EK) har vært tydelig observerbare, som jammingen av GPS-signaler, mens andre typer er preget av mye hemmelighold og kan kun forstås basert på indisier.

Å si at 3G, 4G og 5G mobilkommunikasjon er avhengig av radiosignaler er å forklare det åpenbare. Et ikke så godt kjent faktum er at med hver ny generasjon mobilkommunikasjon øker frekvensen mobilsystemene operer på. Konsekvensen er at a) kommunikasjonen blir mer avhengig av frekvenser som ligger nærmere enkelte typer radarer og b) mer avhengig av nøyaktig tidssynkronisering med presise tidssignaler fra navigasjons-satellitter. Elektronisk krigføring rettet mot høyere frekvenser brukt til militær taktisk kommunikasjon og frekvenser for en del typer radarer, er nær aktuelle frekvensbånd for telekommunikasjon. Elektronisk krigføring kan også rettes direkte mot radiosegmentet i mobiltelefonsystemer og kan påvirke telekommunikasjon direkte. Siste nytt er at russiske styrker muligens utvikler systemer for elektronisk krigføring mot kommunikasjonssatellitter som operer i lav jordbane (LEO). Med utgangspunkt i forholdene beskrevet over er det derfor hensiktsmessig for telekomoperatører å se nærmere på den elektroniske krigføringen i Ukraina.

Satellittnavigasjonssystemer
Den første anvendelsen av EK, som det også finnes en rekke bekreftelser på, er jamming og noen ganger spoofing av signaler fra satellittnavigasjonssystemer. Det mest kjente systemet er det amerikansk-opererte Global Positioning System (GPS), men det eksisterer to andre systemer med global dekning, det russisk-opererte GLONASS og det EU-opererte Galileo. Alle tre systemene er basert på signaler fra et sett av satellitter som sender signaler fra om lag 20 000 km høyde over jordoverflaten. Siden radiosignalene fra disse satellittene sendes fra en slik avstand, er signalene svake når de når mottakeren på jord-overflaten. De er derfor relativt enkle å jamme. En bakkebasert jammer kan dekke et betydelig område, som stort sett kun er begrenset av jordkrumningen. Den russiske kapasiteten til å jamme GPS var godt kjent før invasjonen av Ukraina i 2022. Man hadde sett hendelser i østre Ukraina allerede i 2014 og i grenseområdene mot Norge i 2017.

Etter den russiske invasjonen i februar 2022 ble det registrert flere GPS-utfall, sannsynligvis utført for å støtte de russiske angrepskolonnene. GPS-utfall har også blitt registrert langs store deler av frontlinjen gjennom østre og sørlige Ukraina. Det er tydelige indikasjoner på at også ukrainske styrker etter hvert som krigen utviklet seg har begynt å gjennomføre jamme-operasjoner, og at disse blant annet rettes mot satellitt-navigasjonssystemer. Det er nærliggende å anta at de aktivt jammer frekvenser i det Russiske GLONASS- systemet.

Etter hvert som Ukrainske styrker begynte motangrep med langt-rekkende artilleri og missiler mot flyplasser og forsyningsområder forekom det russisk GPS-jamming i flere områder langt inne i Russland. Mest sannsynlig er dette jamming iverksatt av Russland for å hindre GPS presisjonsstyring av granater og missiler, samt styring av ukrainske ubemannede luftfartøyer (UAVer).

Nær stridsområdene – taktiske kommunikasjonssystemer, radarer og mobiltelfoner
Den andre anvendelsen av jamming som er meldt observert, og referert til i åpne kilder en rekke ganger, er jamming av taktiske kommunikasjonssystemer nær områder hvor det foregår bakkekamper. Jammingen har vært rettet mot frekvensbånd brukt til militær radiokommunikasjon, som VHF og UHF båndene. I de samme områdene er sannsynligvis mobiltelefonsystemer også utsatt for jamming. I den første raske fremrykningen i februar – mars 2022 var denne jamningen ikke så effektiv, mulig på grunn av de hurtige forflytningene og det uoversiktlige strids-feltet. Senere når frontlinjen ble mer låst øst og sør i Ukraina fra høsten 2022 ble lokal jamming mot ukrainske mål mer effektiv. Det foreligger ikke så mye informasjon om ukrainsk jamming rettet mot russiske styrker, men det er klart at ukrainske styrker utfører jamming. Mange av områdene langs frontlinjen i øst og sør, er mest sannsynlig utsatt for omfattende jamming. Dette påvirker ukrainske styrkers evne til å kommunisere, manøvrere, finne mål og bekjempe mål.

> Every day it becomes clearer how well Ukraine has used electronic warfare to degrade enemy radio signals and radars and to disable drones and missiles. Electronic warfare capabilities, including but not limited to cyber, are increasingly relevant.
>
> **Josep Borrell**, High Representative of the European Union for Foreign Affairs and Security Policy
> in *Lessons from the war in Ukraine for the future of EU defence*

Observasjonene av russisk jamming støttes av reelle tap på slag-marken. Onyx, den nederlandsk-baserte analysegruppen som teller tapene på slagmarken, har identifisert 36 skadede eller ødelagte russiske EK –systemer. Disse forskjellige jamme-systemene kan fungere mot bakkebasert og luftbasert taktisk kommunikasjon, mobiltelefoner, satellittnavigasjon, høyhastighets datalenker og en rekke frekvensbånd for radarer. I Onyxs data er det lite informasjon om tap av Ukrainsk EK-utstyr utover identifisering av to systemer.

Jammes det mot kryssermissiler?
Herfra går vi inn i en mer indirekte og noe mer usikker identifisering av bruken av jamming. Til tross for betydelig overlegenhet har ikke det russiske luftforsvaret klart å etablere luftherredømme over østre og sentrale deler av Ukraina. Russiske styrker har derfor vært avhengig av å utføre missilangrep mot mål inne på ukrainskkontrollert territorium. Til dette har de brukt forskjellige typer lavtflygende kryssermissiler. Gjennom hele den russiske kampanjen har missilenes presisjon og evne til å trenge igjennom luftrom vært overraskende dårlig. Umiddelbart er det lett å tilskrive dette til effektiv taktikk fra de ukrainske luftvern-avdelingene. En annen sannsynlig faktor er bruken av EK mot missilene. De russiske kryssermissilene bruker GLONASS for å korrigere kurs, samt radar for å justere høyde og til slutt treffe mål. Jamming mot disse missilene kan rettes både mot de tre frekvensene GLONASS opererer på og de høyere frekvensene for målsøkerradarene. Siden ukrainske styrker ikke kan vite eksakt hvilken type missiler som er på vei inn, så vil jamming av et relativt bredt spekter av frekvenser være nødvendig.

Siste utvikling – mulig utvikler Russland kapasitet til å jamme kommunikasjonssatellitter i lav jordbane
Ifølge en artikkel publisert i Washington Post i april 2023, som var basert på et dokument fra de såkalte «Discord leaks», skal russiske romstyrker ha brukt et bakkebasert system i et forsøk på å jamme Starlink kommunikasjonssatellitter når de passerer »

FOTO: YAROSLAV KRECHKO VIA FACEBOOK

En russisk R-330ZH Zhitel i Donbas.

There are entire segments of the front where [Ukrainian drone operators] can't fly their drones since they are getting jammed by the Russian EW forces.

Samuel Bendett, an analyst and expert in unmanned and robotic military systems at the Center for Naval Analysis

over Ukraina. Man mente opprinnelig at dette skal ha skjedd i en periode på 25 dager, men senere anslag tyder på at jammingen har foregått i et noe lengre tidsrom. Washington Post skriver at dette er et stort system som virker fra faste installasjoner plassert langt utenfor Ukraina. Dette er unikt. Den normale måten å jamme signaler for satellittkommunikasjon er å benytte bakkebaserte jammere nær sendere/mottakere på bakken. Jordkrumningen og geografiske forhold vil da gi begrensninger og man får dekning i et visst operasjonsområde avhengig av hvor store jammerressurser man anvender. Det unike med det russiske systemet Washington Post beskriver er at det jammer fra bakken og opp mot satellittene ved bruk av store retningsbestemte parabolantenner. Disse virker inn mot Starlink-satellittene fra to eller tre lokasjoner utenfor Ukraina.

Starlink generasjon 1 kommunikasjonssatellitter operer i lav jordbane (Eng: Low Earth Orbit – LEO) i en høyde av 340-360 km og beveger seg raskt sett relativt til jordoverflaten. Lignende forhold gjelder for andre operative sivile kommunikasjonssystemer i lav jordbane, for eksempel Iridium-systemet. I tillegg til disse kommer satellitter for militær kommunikasjon.

Metoden Washington Post beskriver er plausibel forutsatt, at parabolantennene kan synkroniseres nøyaktig nok til å følge satellitter på en del hundre kilometers avstand. Det vil kreve betydelig elektromagnetisk energi og i utgangspunktet vil det være ønskelig med størst mulig parabolantenner for å konsentrere radiosignalene. Nærmere undersøkelser av opplysningene gjengitt i Washington Post viser at flere av de beskrevne lokasjonene er tydelig identifiserbare og har nybygd infrastruktur. På noen lokasjoner ser man større bevegelige parabolantenner samt unik kommunikasjonsinfrastruktur. Ytterligere informasjon tilsier at det ble gitt en utviklingskontrakt i 2012 for et system med slike kapasiteter. Det foreligger også informasjon om byggeoppdrag på noen av lokasjonene i senere år, og at systemet har navnet «Tobol».

Parabolantenne er betydelig større enn det som normalt brukes for høyhastighetskommunikasjon til og fra satellitter. Dette gjelder også når man sammenligner med moderne utstyr for kommunikasjon til og fra satellitter i geostasjonære jordbane, 36000 km fra jordoverflaten. Det er også unikt at så store parabolantenner har styring og motorer for å følge bevegelige satellitter (for eksempel satellitter i lav eller middels jordbane). Parabolantenner av denne størrelsen brukes normalt mot geostasjonære satellitter i høy jordbane. Disse satellittene har fast posisjon i forhold til jordoverflaten og antennene står dermed stille under bruk. De har ikke behov for noen stor motor for å bevege parabolantennen raskt.

Av andre typer store bevegelige parabolantenner er det to kategorier som har vært i bruk og brukes i henholdsvis det sovjetiske og det russiske romprogrammet. Eldre systemer fra tidlig i det sovjetiske romprogrammet har mindre presis styring og signalgang, og benytter derfor store parabolantenner. I tillegg har Sovjet og Russland hatt et program for det dypere verdensrom, som omfatter svært store bevegelige parabolantenner for kommunikasjon med romfartøyer utenfor høy jordbane og for radioteleskopisk lytting av det dype rom. Disse har en vesentlig annerledes utforming enn parabolantenne på de angitte lokasjonene. Mye av den eldre strukturen er ute av bruk og ikke vedlikeholdt, mens en del systemer fortsatt er i drift. Ingenting tyder på at parabolantennene som har blitt observert nylig brukes i slike romprogram. De er dessuten installert på andre lokasjoner.

Angivelig skal utviklingsprosjektet også ha inkludert en enhet bestående av mobile kjøretøy utrustet med stor parabolantenne. Det foreligger bilder av en prototyp, men informasjonen er usikker. Videre er det også usikkert om det i det hele tatt har blitt laget et slikt kjøretøy.

Samlet sett er informasjonen om Tobol-systemet, funksjonalitet og operative tester av systemet relativt usikker. Det foreligger ingen tilgjengelig informasjon om satellittkommunikasjonen faktisk ble effektivt jammet. Metoden er likevel unik, plausibel og kan representere en ny kategori trussel mot satellittkommunikasjon i lav jordbane. Lokasjonene skiller seg fra andre bakkestasjoner som brukes av det russiske romprogrammet, kommersielle aktører og det russiske forsvaret, inkludert etterretnings- og sikkerhetstjenestene. Dersom Tobol faktisk eksisterer vil bruken av dette systemet utgjøre en ny og unik trussel. Blant annet vil dette kunne påvirke bruken av satellittsystemer som reservekommunikasjon ved utfall av fiberoptisk kommunikasjon. Vi velger derfor å inkludere dette i vurderingen, på tross av begrenset informasjonsgrunnlag.

Starlink has resisted Russian cyberwar jamming & hacking attempts so far, but they're ramping up their efforts.

Elon Musk on Twitter May 11, 2022

FOTO: GOOGLE MAPS 2023

Konklusjon for telekommunikasjonsindustrien

I krigssituasjoner eller svært tilspissede konflikter vil telekomoperasjoner måtte gjennomføres i et signalmiljø der aktiv elektronisk krigføring (EK) er en betydelig faktor. Radiobølger sprer seg i uhindret i luft, og man vil kunne bli påvirket av begge parters EK-aktiviteter. EK vil sannsynligvis forekomme i spesifikke geografiske områder, på spesifikke frekvenser og vil kunne skifte raskt. Områder nær er kamphandlinger vil sannsynligvis bli kraftig påvirket. Defensiv jamming, for å kontre trusselen fra luftangrep, samt jamming fra mobile plattformer i luftrommet og til havs, kan virke i områder som ligger lengre unna kamphandlingene.

Det er elleve bestemte frekvensområder for GLONASS, Galileo og GPS. Disse og nærliggende frekvenser vil svært sannsynlig blir jammet. De elleve frekvensområdene er spredt ut mellom 1176 Mhz og 1602 Mhz, ingen av disse ligger veldig tett på frekvensbånd som brukes til mobiltelefoni. Jamming av disse frekvensene vil påvirke tilgjengeligheten av satellittbasert signal for tidsstyring, noe som potensielt har omfattende følgekonsekvenser.

Jamming av frekvensen til kryssermissilers målsøkeradarer i X-båndet og Ku-båndet treffer mellom de vanligste og aller høyeste frekvensbåndene for 5G. Dersom det gjennomføres bredspektret jamming mot slike missilradarer kan det, avhengig av detaljerte forhold, potensielt påvirke kommunikasjon mellom basestasjon og terminal (mobiltelefon og andre bruker-enheter).

Jamming rettet mot bakkebaserte radarer for luftromsovervåkning, luftvernsystemer, flyradarer, luftbårne overvåkningsradarer, artillerilokaliseringsradarer og skipsradarer (overvåkning, navigasjon og målfatningsradarer) vil ramme en lang rekke frekvenser spredt over flere frekvensbånd. Hvor man vil bruke slik jamming vil variere med den taktiske situasjonen, og vil skifte fort, både med hensyn til dekningsområde og frekvenser. Jamming her vil kunne komme fra både bakkebaserte systemer som kun flyttes med jevne mellomrom, men også fra mobile luft og sjøplattformer.

Mulig russisk oppbygging av bakkebasert kapabilitet for jamming mot kommunikasjonssatellitter i lav jordbane (LEO) skaper noe usikkerhet om bruk av LEO-kommunikasjonssatellitter som reservekapasitet for å dekke opp brudd i kommunikasjon over fiberforbindelser. Det foreligger foreløpig lite og usikker informasjon om dette. Derfor er det tidlig å trekke konklusjoner om utvikling, omfang, virkeområde og effekt av et slikt sammensatt system. //

Elektronisk krigføring (EK)

Elektronisk krigføring (EK) er en samlebetegnelse på militære operasjoner som har til hensikt å kontrollere, utnytte og manipulere det elektromagnetiske spektrum, hvor blant annet forskjellige radiofrekvenser inngår. Angrep gjennom digitale nettverk regnes ikke som EK. Dette kalles cyberkrigføring eller cyberoperasjoner og skiller seg fra EK. EK kan deles opp i tre typer operasjoner: offensive, støttende og beskyttende. I dette kapittelet har vi fokusert på offensive operasjoner.

Om offensiv elektronisk krigføring (EK)

Prinsipielt er det tre måter å gjøre offensive EK-operasjoner på, jamming, spoofing og decoying. Jamming går ut på å blokkere signaler, vanligvis ved å sende mer effekt mot mottakeren enn det opprinnelige signalet. Med moderne signalering er det også mulig å bruke teknikker som blokker ut bestemte styringssignaler eller bestemte sekvenser av et signal. For eksempel kan blokkering av signalet som styrer at mottakeren åpnes, i praksis føre til samme resultat uten å bruke ekstraordinært høy effekt.

Spoofing er å etterligne et signal og få det til å fremstå som det legitime. Den mest typiske formen for spoofing er å imitere kallesignalet til en annen sender. Med moderne digital signaleringsteknikk er det mulig å imitere en rekke signaler. Decoying er å sende ut sterkere signaler for å få en mottaker til å låse seg til en falsk utsending. Dette blir vanligvis brukt i den delen av EK som handler om å avlede radarer. Bruk av falsk basestasjon i et mobilnettverk er i prinsippet en form for decoying. Brukt mot en radar vil et decoying-signal fremstå som et reelt ekko for radaroperatøren, mens det i virkeligheten er en sender som gir et sterkere signal enn radarekkoet fra et fly eller fartøy.

Moderne EK-utstyr kan dekke et stort spenn av frekvenser i det elektromagnetiske spektrum, treffe frekvensen med høy presisjon og skifte frekvens i løpet av millisekunder. Retningen på signaler kan også styres ved bruk av forskjellige retnings bestemte antenner. Moderne EKutstyr kan være store sammensatte systemer som krever flere lastebiler å flytte, men kan også lages så lite og kompakt at det lett får plass i fly, på fartøy eller kan pakkes inn i en liten bærbar ryggsekk. EK-utrustning er kostbart og antall systemer som er tilgjengelig for krigførende parter er som regel begrenset.

FOTO: AP PHOTO / SERGEI GRITS / NTB

Ukraina: Telekom i krig

Den russiske invasjonen av Ukraina i 2022 har vært banebrytende innenfor teknologi på mange måter. En av de minst kjente, men potensielt viktigste aspektene, har vært krigens bruk av telekommunikasjonsnettverk, og spesielt mobiltelefonnettverk. Dette ble oversett før krigen, da de fleste analytikere (feilaktig) antok at cyberkrigføring skulle spille en stor rolle i konflikten. Mobilnettverk har imidlertid vist seg å ha hatt en massiv innvirkning på krigens gang.

Dette vises på tre forskjellige måter:

For det første: Effekten på moralen og den internasjonale responsen. Fungerende og sikre ukrainske mobilnettverk gjorde at tidlige ukrainske seiere – som nedkjempede russiske styrker og ødelagte russiske stridsvogner i de første dagene av invasjonen – ble synlig for det ukrainske folket. Et annet eksempel var da president Zelensky sendte en video fra telefonen sin i Kyiv morgenen etter invasjonen, noe som ikke ville vært mulig uten fungerende ukrainske mobilnettverk. Mulig enda viktigere på lang sikt, var muligheten til å formidle disse suksessene til den vestlige offentligheten og beslutningstakere over hele verden, noe som akselererte støtte fra disse landene.

For det andre: Virkningen på de russiske invasjonsstyrkene. Ukraina klarte å stenge russiske telefoner ute fra sine mobilnett. Når de russiske styrkene fikk kommunikasjonsvansker med militære radiosystemer, ble de derfor tvunget til å bruke de ukrainske mobilnettene og ukrainske telefoner som et reservesystem. Slik kunne disse russiske styrkene lokaliseres, avlyttes og rammes av andre former for angrep, og det er rapportert at det førte til dødsfall blant flere høytstående russiske offiserer.

For det tredje: Krigens gjennomføring. Denne krigen har vist en ny bruk av mobilnettverkene i form av crowd-sourcing av etterretning. Sivile rapporterer nå om forskjellige aktiviteter, som f.eks. fiendtlige troppers bevegelser, droneangrep og kampskader. Det gjøres ved hjelp av ulike metoder, fra enkle tekstmeldinger og meldingsapper, til Telegram-kanaler og dedikerte mobilapper som rapporterer retningen og lyden av droner og kryssermissiler for å samle informasjon som korreleres til posisjon for avskjæring.

TEKST:

Cathal McDaid, CTO i ENEA AdaptiveMobile

Denne artikkelen er oversatt fra originalspråket og redaksjonelt tilpasset for publisering i Digital Sikkerhet 2023.

Disse suksessene skyldes ikke tilfeldigheter. I begynnelsen av krigen slet noen analytikere med å forstå hvorfor Russland tillot mobilnettverkene å fortsette å operere, gitt de åpenbare fordelene det ga Ukraina i forsvarskampen. Disse analytikerne hadde en tendens til å fullstendig overse det faktum at Ukraina i stor grad kunne bestemme hvordan det forsvarte seg selv og sin infrastruktur. Ukrainske mobiloperatører som Kyivstar beskrev hvordan de forberedte seg på konflikten flere måneder i forveien ved å ta beslutninger som:

- Etablering av ekstra nettverkskontrollsentre
- Etablering av «bunker» basestasjoner i kritiske bygninger
- Flytting av kritisk utstyr bort fra eksponerte/sårbare områder
- Flere tilkoblingspunkter mot resten av verden
- Gjennomføring av grundige sikkerhetsanalyser av mulige sårbarheter.

Alle disse tiltakene ble gjennomført før invasjonen. Betydningen av gode forberedelser må ikke undervurderes. For eksempel, allerede natten etter invasjonen, mindre enn 24 timer etter at invasjonen startet, blokkerte alle de tre ukrainske mobiloperatørene – Vodafone Ukraine, Lifecell og Kyivstar – SIM-kort fra Russland og Belarus som forsøkte å registrere seg på deres nettverk. Som nevnt tidligere, hadde dette stor innvirkning på de russiske styrkene, da de dermed var henvist til å bruke ukrainske numre/SIM-kort, som lettere kunne spores og avlyttes. Dette er helt unikt; ingen land i verden har noen gang deaktivert en eksisterende roaming-avtale med ikke bare én, men to av sine naboland, og (i Ukrainas tilfelle) noen av sine største markeder. Det at et slikt tiltak ble gjennomført koordinert av alle de tre ukrainske mobiloperatørene så raskt etter invasjonen, tyder på at det må ha vært planlagt på forhånd som ett av trolig flere tiltak som den ukrainske regjeringen kunne be den ukrainske mobilbransjen om å iverksette. Tiltaket hadde også en beskyttende effekt ved å redusere angrepsflaten mot ukrainske nett og telefoner over inter-operatør telekom-signalering – et område Russland utnyttet i Ukraina i 2014. Dette var bare ett av en hel rekke tiltak som den ukrainske mobilbransjen gjennomførte. Andre tiltak omfattet tildeling av ekstra frekvensbånd til mobiloperatørene for økt kapasitet og robusthet, stans i deaktivering av kontoer ved manglende kreditt og selektiv håndtering av utgående telefonsamtaler til Russland/Belarus, der noen ble blokkert mens andre ble avlyttet og registrert.

Også et annet tiltak som det ukrainske telekomfellesskapet gjennomførte etter krigsutbruddet hadde en enorm innvirkning på krigens forløp, og har aldri tidligere blitt gjennomført i samme omfang noe sted i verden. Den 7. mars 2022 implementerte de tre største ukrainske mobiloperatørene nød-roaming mellom hverandre i deler av de sørlige og østlige regionene, før det noe etter ble utvidet til andre. Dette gjorde det mulig for en mobiltelefon fra ett nettverk å bruke et annet ukrainsk nettverk når eget nett er utilgjengelig. Dette tiltaket ga betydelig økt robusthet og tilgjengelighet til mobilkommunikasjon i hele Ukraina, spesielt i konfliktsonene, og ble brukt for å sikre kommunikasjon til steder som Mariupol og kjernekraftverket i Zaporizhzhia mens de var under angrep. Selv om nød-roaming hadde vært diskutert i andre land og blitt implementert i liten skala i land som Nederland og USA, hadde ingen land noensinne implementert det i samme skala og suksess som Ukraina gjorde. Utforderingene med implementeringen av nød-roaming for mobiloperatørene var ikke teknologien, men logistikken - særlig i forhold til betaling og kapasitetsplanlegging. Vanligvis forekommer ikke fakturering mellom forskjellige mobiloperatører innenfor ett land, og det var ingen estimater på nettverksbelastningen som hver operatør kunne bli påført hvis folk kunne flytte seg mellom operatører og nett på denne måten. Det ble likevel tatt beslutning om å implementere nød-roaming på grunn av fordelene det hadde, og håndtere eventuelle negative konsekvenser senere.

De ukrainske mobiloperatørenes handlemåte hadde en klar innvirkning på krigen, men Ukraina har ikke vært alene om å utnytte mobilnettene til sin fordel. Etter krigen i Donbass i 2014 begynte Russland å tilpasse seg. To uregistrerte mobiloperatører kalt Phoenix og Lugacom dukket opp i de russisk-støttede separatistområdene Donetsk og Luhansk. Disse ble opprettet av separatistgruppene i Donbass for å kontrollere kommunikasjonen i området, ved å bruke erobret mobilutstyr fra de eksisterende ukrainske mobiloperatørene i området. Noen uker etter invasjonen av Ukraina i 2022, begynte Russland raskt å utvide Phoenix og Lugacom videre til de nyokkuperte regionene i Sør- og Øst-Ukraina. Samtidig dukket det opp to nye uregistrerte mobiloperatører i de okkuperte delene av Ukraina – kalt +7 Telecom og Mir Telecom, slik at det totalt var fire aktive russisk-kontrollerte uregistrerte mobiloperatører i det okkuperte Ukraina sommeren 2022. Når Russland investerte ressurser for å sørge for at ikke bare én, men fire mobiloperatører ble etablert og aktive i løpet av noen få måneder, midt i en aktiv krigssone, viser hvor viktig mobilkommunikasjon – og kontroll på den – var. Til sammenligning tok det flere år for okkuperte Krim å få et tilsvarende antall uregistrerte operatører, selv uten pågående krigshandlinger. Hastigheten og antallet mobiloperatører som ble etablert, og det faktum at de har blitt etablert for å gi dekning i områder som til tider mangler annen sivil infrastruktur som vann eller elektrisitet, indikerer at disse russiske uregistrerte nettene har både militære og sivile formål. De utgjør en alternativ kommunikasjon for russiske styrker og lar en sivil okkupasjonsregjering kommunisere og fungere. I likhet med Ukraina har også Russland pålagt at nød-roaming skal implementeres mellom de uregistrerte russiske mobiloperatørene, for å forbedre motstandsdyktigheten ved å dra nytte av fordelene med overlappende dekning.

> Mens krigen fortsetter, fortsetter vi også å lære av erfaringene. En av de nyere lærdommene i krigen har vært betydningen av energi.

Mens krigen fortsetter, fortsetter vi også å lære av erfaringene. En av de nyere lærdommene i krigen har vært betydningen av energi. Vinteren 2022 hadde omfattende russiske drone- og missilangrep mot den ukrainske energiinfrastrukturen en sekundær virkning på mobilnettene. I den verste perioden – rundt november/desember 2022 – ble omtrent 40 prosent av det ukrainske strømnettet påvirket, noe som gjorde mobilnettene sårbare. Dette førte til at de ukrainske mobiloperatørene både introduserte flere generatorer selv, men også appellerte til crowdsharing for få koble til andre generatorer, noe som til slutt ga strøm til over 600 basestasjoner som manglet ordinær forsyning. Etter hvert, med økt luftforsvar, en reduksjon i dronebruk og forbedret energisikkerhet, var de ukrainske mobilnettene i stand til å håndtere strømbruddene relativt godt.

En annen lærdom har vært bruken av satellittkommunikasjon. Bruken av Starlink blant militære enheter ved fronten har vært godt kjent, men satellittkommunikasjon via Starlink har også blitt brukt for kommunikasjon mellom basestasjoner og kjernenett der fiberforbindelsen har vært brutt. Det har også vært testing av satellitt-til-mobil-kommunikasjon. Selv om krigen har akselerert implementeringen av sikkerhets- og motstandsdyktighetsteknologier og –praksis har den også åpenbare effekter på bransjen – utover ødeleggelse av utstyr og infrastruktur. Rundt 4 millioner brukere har forlatt landet, noe som har gitt en reduksjon på rundt 12 prosent i aktive SIM-kort. Videre er utrullingen av 4G bremset opp, og det er lite fremgang på 5G. Tapet av betalende abonnenter og krigsskader på infrastrukturen vil fortsette å påvirke de ukrainske mobiloperatørene når krigen er over. Dette er imidlertid et problem for fremtiden.

Telekommunikasjonsnettene har hatt en betydelig innvirkning på krigens gang i Ukraina, og nye bruksområder for mobilnett vil fortsette å dukke opp. De mange dyrekjøpte læringspunktene fra den ukrainske telekombransjens erfaringer og tiltak, bør studeres og forstås av alle som er involvert i forberedelser for nasjonale nød- eller sikkerhetshendelser. //

FOTO: GETTY IMAGES

Fokus på sikkerhet rundt vår egen infrastruktur har økt, og myndighetene har flere ganger det siste året beskrevet en økt trussel rettet mot olje- og gassinfrastruktur. Dette gjelder all kritisk infrastruktur, og spesielt infrastruktur tilknyttet eksport av energi til Europa. Undersjøisk infrastruktur som rørledninger som frakter olje, gass, samt fiberkabler er også sårbare.

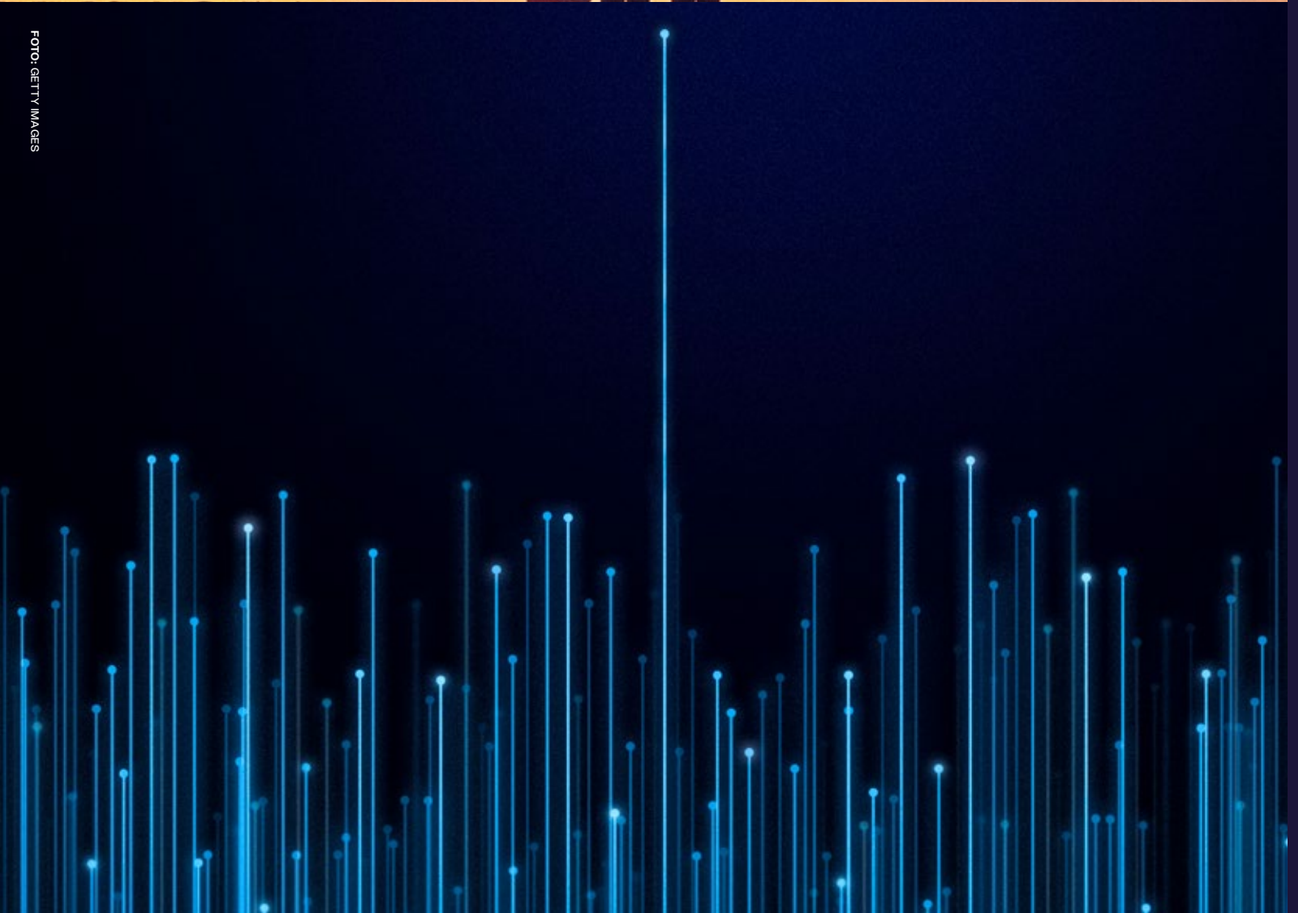


FOTO: GETTY IMAGES

4

Trusselbildet mot Telenor og våre kunder

Dette kapittelet inneholder oppdaterte vurderinger av sikkerhetstrusler som er relevante for Telenor Norge og våre kunder. Beskrivelsen av trusselbildet er utarbeidet på tvers av Telenor Norges ulike fagmiljøer som jobber med å forebygge, avverge og håndtere sikkerhetstrusler mot Telenor Norge. Trusselvurderingen tar for seg både strategiske og mer tekniske aspekter ved trusselbildet som berører nasjonen. Telenors kundegruppe omfatter mange virksomheter av ulik størrelse med ulike verdikjeder og samfunnsroller. Virksomheter må vektlegge forskjellige aspekter av trusselbildet avhengig av sine verdier, funksjoner og roller. Avslutningsvis har vi inkludert betraktninger om trusler mot noen utvalgte kundegrupper.

> ***«Ved et angrep på Norge og NATO vil ødeleggelse av kritisk infrastruktur få prioritet tidlig, og varslingstiden vil være svært kort».***
>
> FOKUS 2023, Etterretningstjenesten

Sikkerhetspolitisk utvikling og overordnet trusselbilde
Urolighetene i Europa etter Russlands invasjon av Ukraina i 2022 fortsetter å prege Norge, og vil å prege vår sikkerhet i lang tid fremover. Etter at Norge høsten 2022 ble Europas største energileverandør har fokus på sikkerhet rundt vår egen infrastruktur økt og fått en mer markant sikkerhetspolitisk dimensjon.

Norske myndigheter har ved flere anledninger presisert at Russland ønsker å sette europeisk energisikkerhet under press. Dette gjør at fokuset mot Norge øker og innebærer skjerpede sikkerhetsmessige implikasjoner for deler av Norge som har tilknytning til kritisk infrastruktur. Kritisk infrastruktur og andre samfunnsviktige funksjoner er i stor grad avhengige av hverandre og krever trygg og sikker kommunikasjon for å fungere.

Telenor vurderer at situasjonen vi nå opplever vil kunne vare over lang tid. Det er også mulighet for at den raskt kan forverres. En forverring vil kunne få svært store konsekvenser for viktig infrastruktur i Norge, inkludert den som Telenor eier og drifter. Evnen til å kommunisere trygt og fritt under forverrede forhold vil være viktigere enn noen gang.

Det er å forvente at kriminelle trusselaktører som opererer i det digitale rom vil benytte ny teknologi som for eksempel kunstig intelligens for å øke muligheten for rask profitt. Kombinert med økonomiske nedgangstider på verdensbasis, vil dette kunne gi et større omfang av kriminelle trusler. Økt innovasjon og kompleksitet innen ransomware gjør dette til en av de farligste truslene Telenor står ovenfor.

Endring i sikkerhetspolitisk bakteppe
Fem eksterne faktorer ved den sikkerhetspolitiske situasjonen vil påvirke sikkerhetsbildet for Telenor Norge og vårt arbeid med sikkerhet fremover.

1 Kritisk infrastruktur blir mer utsatt
Norske og utenlandske myndigheter, deriblant NATO, har fremhevet hvor viktig norske energileveranser og kritisk infrastruktur knyttet til dette vil være for hele Europa i tiden fremover. Myndighetene har flere ganger det siste året beskrevet en økt trussel rettet mot olje- og gassinfrastruktur. Dette gjelder all kritisk infrastruktur, og spesielt infrastruktur tilknyttet eksport av energi til Europa. Kritisk infrastruktur i Norge er knyttet tett sammen og har mange gjensidige avhengigheter, noe som Telenor Norge også må ta innover seg. Telenor Norge er en viktig leverandør til annen kritisk infrastruktur som krever digital kommunikasjon for å fungere.

Virksomheter må regne med at installasjoner, eller tjenester som kan knyttes opp mot annen kritisk infrastruktur, vil kunne være særlig utsatt for etterretningsvirksomhet. For eksempel kan de bli utsatt for forsøk på både fysisk og logisk rekognosering.

> ***«Russland søker å svekke vestlig samhold og vilje til å støtte Ukraina ved å legge press på Europas energisektor. Kreml regner det europeiske eksportmarkedet som tapt, og vil fortsette å ramme europeisk økonomi ved å strupe gasseksporten. Etter hvert som Russlands virkemidler uttømmes, øker muligheten for at Russland vil søke å ramme energileveranser fra andre land.»***
>
> FOKUS 2023, Etterretningstjenesten

2 NATO utvides
PST vurderer at Russland vil ha et økt behov for å forstå konsekvensene av NATOs ekspansjon. Etterretningsinnsamling i Norden vil derfor trolig ha høyere prioritet.

Offentlig forvaltning, andre institusjoner og forskningsinstitusjoner som arbeider med utforming av sikkerhetspolitikk og norskarktisk politikk vil peke seg ut som naturlige mål. Også virksomheter innen bestemte typer teknologiutvikling vil være sannsynlige mål. For Telenor Norge vil dette også innebære at vi må forvente et høyere etterretningstrykk.

Selv om NATOs ekspansjon medfører økt sikkerhet for nordiske land, vil dette også kunne medføre økt misnøye og oppmerksomhet fra russisk side. Ett av verktøyene som benyttes for å uttrykke misnøye er DDoS-angrep mot mål av symbolsk verdi (mer om DDoS-angrep lenger ned).

> ***«I inneværende år forventer vi også at russiske etterretningstjenester vil ha nye politiske og militære informasjonsbehov knyttet til konsekvensene av en NATO-utvidelse i Norden. Svensk og finsk NATO-medlemskap kan øke den samlede betydningen av Norden for russiske etterretningstjenester, og gjøre at de i større grad enn tidligere prioriterer etterretning mot Norden som helhet.»***
>
> PST Nasjonal Trusselvurdering (NTV) 2023

DDoS og annen bruk av virkemidler for å signalere misnøye eller påvirke offentlig diskurs blir ofte benyttet av statsstøttede aktører eller «hacktivister». DDoS i seg selv er vanligvis ikke et virkemiddel som innebærer store konsekvenser for de som blir angrepet. Like fullt er dette en angrepsform som ofte brukes mot symboltunge mål, inkludert private bedrifter. Telenor Norge er, som en stor og kjent norsk bedrift, et sannsynlig mål for DDoS-angrep. Av de samme grunnene som beskrevet ovenfor vil en god del av våre kunder være mulige mål for DDoS-angrep. Spesielt gjelder dette virksomheter som fremmer synspunkter eller tiltak som faller negativt ut for russiske interesser.

3 Arktis blir viktigere
Både Russland og Kina har uttalte interesser i arktiske strøk, og etterretningsaktivitet må dermed forventes. PST forventer i sin vurdering NTV 2023 at russiske etterretningstjenester vil være interessert i informasjon om aktører som er involvert i norsk forvaltning av Svalbard.

For noen statlige aktører, spesielt Russland og Kina, vil Telenors posisjon i nordområdene og Arktis være av særlig interesse. NTV 2023 (PST) peker også på en høyere risikovilje innen etterretningsaktivitet, hos spesielt Russland, grunnet den sikkerhetspolitiske situasjonen. Det er all grunn til å tro at dette vil vedvare. Per i dag har russiske sivile fartøy fremdeles mulighet til å benytte havnelligge i Kirkenes, Båtsfjord og Tromsø. De kan også bedrive regulær aktivitet (primært fiskeri) i områder hvor det er sjøfiberkabler, andre installasjoner eller aktiviteter som kan være av interesse for russisk etterretning.

Høyere aktivitet i nordområdene fra flere stater, kombinert med sikkerhetspolitiske spenninger vil også kunne sette Svalbard i et særlig søkelys. For Telenor Norge blir behovet for redundans og høyere sikkerhetstiltak for tjenester i Nord-Norge og på Svalbard viktigere enn noensinne.

4 Et varig urolig Russland
I Etterretningstjenestens vurdering av Russland i et tiårsperspektiv i FOKUS 2023, er vurderingen den at Russland vil forbli en urolig og ustabil nabo, som i ytterste konsekvens kan oppleve regimekollaps eller borgerkrig. Videre skrives det at *«svært lite tyder på at et grunnleggende mer demokratisk Russland vil vokse frem det neste tiåret, eller at landets interesser i større grad blir forenelige med Vestens»*. Russlands brudd med Vesten blir med andre ord varig, og forholdet mellom Norge og Russland vil trolig fortsette å påvirkes av dette.

For Telenor Norge vil dette si at vi må planlegge og være forberedt på en vedvarende høy etterretningsaktivitet fra Russland i overskuelig fremtid. Vi må også være forberedt på å stå i en situasjon som plutselig kan forverres og vare over tid. Telenor må, med andre ord, planlegge for en lengre periode med usikkerhet når det gjelder den det sikkerhetspolitiske situasjonen og være forberedt på at denne raskt kan forverres.

5 Et offensivt Kina
Kinas utenrikspolitikk er mer utadrettet enn tidligere, og spenningen mellom Kina og Taiwan har økt. Dette er en konflikt som potensielt sett kan ha svært alvorlige følger for mange bedrifter verden over. Konflikten kan bidra til å påvirke leverandørkjeder innen teknologi og begrense tilgang på spesialisert teknologi som halvledere/mikrobrikker fra Taiwan.

Kinesisk teknologi er mer integrert i verden enn tidligere, samtidig som norske myndigheter advarer mot leverandøravhengighet knyttet mot Kina.

Kinas økende interesse i arktiske strøk, både i form av investeringer, oppkjøp og sivil tilstedeværelse, vil også øke deres behov for kunnskap om andre bedrifter som opererer her. Dette vil også kunne være en driver for industrispionasje.

> ***«PST forventer ingen store endringer i etterretningstrusselen fra Kina i Norge. Kina vil fremdeles utgjøre en betydelig etterretningstrussel mot norske interesser i inneværende år. Kinesisk etterretning vil bruke et bredt spekter av virkemidler for å tilegne seg avansert teknologi, kunnskap og sensitiv informasjon fra norske virksomheter og institusjoner. Kina vil også være interessert i informasjon om norsk politikkutforming, særlig knyttet til internasjonalt samarbeid og nordområdene.»***
>
> PST Nasjonal Trusselvurdering (NTV) 2023

Trusselvurderinger fra norske myndigheter har i en årrekke påpekt at både russiske og kinesiske myndigheter vil forsøke å anskaffe avansert teknologi som de i dag ikke er i stand til å produsere selv. Dette skjer gjennom utenlandsinvesteringer, fellesforetak, forskningssamarbeid og industrispionasje.

»»»

Fysiske sikkerhetstrusler mot Telenor Norge

En god del av Telenors kunder er eiere av samfunnskritisk infrastruktur med stor geografisk spredning. Disse kundene står overfor mye av det samme trusselbildet og mange av problemstillingene knyttet til sikring av infrastruktur som oss.

Kritisk infrastruktur regnes som særlig viktig i en konflikt. Man må regne med at infrastrukturen er nøye kartlagt i forkant. Politiets Sikkerhetstjeneste bekreftet høsten 2022 i media at de vurderte at norsk kritisk infrastruktur allerede var kartlagt. Telenor Norge bør dermed regne med at egen infrastruktur er kartlagt, og forvente forsøk på kartlegging av vår infrastruktur også i fremtiden.

Infrastruktur fornyes, og trusselaktører vil ha behov for oppdatert informasjon. Mye fysisk infrastruktur vil kunne kartlegges over internett, men enkelte installasjoner vil likevel være utsatt for fysisk kartlegging. Slik kartlegging kan også gjøres mot våre underleverandører.

Det er sannsynlig at god elektronisk sikring gjennom moderne systemer for fysisk adgangskontroll, perimetersikring og kameraovervåkning vil være effektive forsinkende tiltak. Dette vil i noen grad også være tiltak som har avskrekkende effekt mot avanserte aktører. Slike sikringstiltak alene vil imidlertid ikke kunne stanse avanserte aktører som har vilje, intensjon og kapasitet til å ta seg inn på kritiske lokasjoner.

Sjøfiberkabler og sabotasjetrusselen

Ifølge Forsvarskommisjonen bæres om lag 90 prosent av den transatlantiske internettrafikken, inkludert militær kommunikasjon, av undersjøiske, fiberoptiske kabler som inngår i en sivil elektronisk kommunikasjonsinfrastruktur. Dette gjør sjøfiberkabler til et attraktivt mål. Undersjøisk infrastruktur inkludert rørledninger som frakter olje, gass, samt fiberkabler fremheves også som særlig viktig og sårbart av NATO. NATO har også uttalt at de nå ser mer russisk aktivitet rundt denne type infrastruktur enn på lenge. Telenor Norge er kjent med at russiske militære og sivile fartøy har hatt uregelmessig og gjentatt avvikende aktivitet over steder hvor sjøfiberkabler befinner seg.

Ettersom den sikkerhetspolitiske situasjonen er spent, og kan endres raskt, bør Telenor Norge være forberedt på at sabotasjehandlinger er en sannsynlig del av verktøykassen til russiske trusselaktører. Sabotasje mot sjøfiberkabler kan gjennomføres på en slik måte at den kan forveksles med kriminell aktivitet. Sabotasje eller annen fordekt aktivitet mot sjøfiberkabler i internasjonalt farvann er vanskeligere å tilskrive én aktør. Sabotasje mot sjøfiberkabler kan også i noen sammenhenger lett forveksles med skade utført ved legitim aktivitet som bunntråling eller lignende.

Dersom Russland skulle gå til sabotasjehandlinger på norsk territorium vil det medføre større sannsynlighet for å utløse krig med NATO, sammenlignet med sabotasje i internasjonalt farvann. Så lenge Russland ikke er i direkte konflikt med NATO, eller ønsker å eskalere konfliktnivået, fremstår det mer sannsynlig med fordekt sabotasje rettet mot infrastruktur i internasjonalt farvann.

Digitale trusler mot Telenor Norge og våre kunder

I det digitale domenet vil forskjellige typer trusselaktører, med ulik motivasjon og kompetanse, utgjøre ulike typer trusler mot både Telenor og våre kunder. Vi kan grovt sett inndele trusselaktørene i henholdsvis statlige aktører som oftest har langsiktige mål og kriminelle med mål om økonomisk fortjeneste. Statsaktørers langsiktige mål kan være å kartlegge infrastruktur for å kunne bruke det ved et senere angrep eller hente ut annen informasjon de mener er viktig.

Statlige aktører

Nettverksoperasjoner fra statlige aktører har gjerne lang varighet. Angriperne har som mål å operere i det skjulte over lengre tid for enten å kunne innhente informasjon eller for å kartlegge strukturer for senere benyttelse. Disse operasjonene etablerer tilgang via nøye planlagte metoder. Gjennom langsiktig og varsom kartlegging og bevegelse i nettverket henter man ut informasjon. Det brukes mye kryptering og det er ofte godt skjult i mange ledd hvem som styrer støtteinfrastrukturen på utsiden som brukes til inntrengning og eksport av data. Det finnes nylige eksempler på mer aggressiv tilnærming, men den langsiktige metoden er den mest utbredte. En annen tilnærming brukt av statsaktører kan være leveransekjedeangrep (se lenger ned). Stor sett vil synlige operasjoner som drives av statlige aktører kunne være av mer umiddelbar karakter, som for eksempel DDoS-angrep. Her vil formålet kunne være å uttrykke misnøye. Slike DDoS-angrep av politisk karakter er det ofte ikke statlige, men statsstøttede trusselaktører som står bak. Dette for å gjøre det vanskeligere å avdekke direkte bånd til opphavsstaten.

» Kritisk infrastruktur regnes som særlig viktig i en konflikt. Man må regne med at infrastrukturen er nøye kartlagt i forkant.

FOTO: GETTY IMAGES

Distributed Denial of Service (DDoS)

er en type angrep hvor et høyt antall PC-er, servere eller IoT-enheter styres til å foreta spørringer mot en web-server, som regel en server som driver nettsider. I slike angrep brukes som regel et nettverk av maskiner/enheter som er hacket og organisert i et skjult såkalt botnet. DDoS-angrep er egnet for hacktivist-grupper fordi det normalt ikke krever høy spesialisert kompetanse og effekten kan økes ved at flere deltar. Hacktivister kan også kjøpe seg effekt ved å leie seg inn på botnet styrt av kriminelle, noe som er relativt lett tilgjengelig og billig. DDoS-angrep brukes også av kriminelle grupper som blant annet verktøy for utpressing og for å dekke over enkelte typer inntrenging.

Samtidig med Russlands invasjon av Ukraina i slutten av februar 2022, gjennomførte russiske hemmelige tjenester en serie digitale angrep mot Ukrainsk It-infrastruktur. Mange av disse angrepene var relativt godt synlige og hadde åpenbart til hensikt å ødelegge It-infrastruktur med eksempelvis wiper-skadevare. Det ble også forsøkt angrep med spesialisert skadevare mot OT-systemer (les mer om dette lenger ned). Skulle staten Norge komme i en eskalert konflikt med Russland vil det være sannsynlig at slike virkemidler kan brukes mot både Telenor og kunder av oss.

Statlige, så vel som kriminelle aktører, må uansett gå via It- og telekomleverandørers infrastruktur dersom de ønsker å ramme It/teleleverandører, kunder, eller andre deler av samfunnet.
I noen tilfeller vil et cyberangrep utilsiktet kunne ramme It/teleleverandører dersom det egentlige målet er en av våre kunder. Etterretningstjenesten har grunn til å tro at Russland vil intensivere bruken av nettverksoperasjoner i det digitale rom. Russiske aktører forsøker ofte å angripe og å få tilgang til målet via internetteksponerte nettverksenheter- og tjenester Særlig gjelder dette enheter og tjenester som støtter tilkobling til virtuelle private nettverk (VPN). Slike angrepsforsøk kan i høy grad skjules, samtidig som det kan gi omfattende tilgang dersom det lykkes. En betydelig del av slik aktivitet har vært rettet mot gamle sårbarheter og de er dermed avhengig av manglende pathching/herding for å lykkes. De siste årene har de i økende grad spesialisert seg på å gjøre tilsvarende i Office 365 skyløsninger.

Logisk infrastruktur kan angripes for å sette tjenester ut av spill, og for å ramme sårbare regioner hvor Telenor drifter infrastruktur. Kommunikasjon er nødvendig for å kunne drive krisehåndtering og vil ved en sikkerhetspolitisk krise være svært kritisk å opprettholde.

Kinesiske etterretnings- og sikkerhetstjenester og andre grupperinger med støtte fra kinesiske myndigheter er svært aktive i det digitale rom, hvor aktørene disponerer avanserte verktøy og metoder. De gjennomfører i utstrakt grad nettverksoperasjoner for etterretningsformål, og har sannsynligvis også kapabilitet til å gjennomføre operasjoner for sabotasje og avskrekking. Større kunder av Telenor som forvalter kritisk infrastruktur eller driver grunnleggende nasjonale funksjoner (GNF) kan på tilsvarende måte bli gjenstand for angrep via sine leverandørkjeder. Vi i Telenor Norge erkjenner at vi spiller en viktig rolle i en lang rekke virksomheters leveransekjeder.

Kriminalitet

Ransomware, initial access brokers og annen utpressing
Siden 2018 har vi sett en sterk fremvekst av ransomware-angrep, hvor angriperen lykkes med å komme inn i It-systemene med såkalt krypteringsvirus og kryptere data. Denne type IT-kriminalitet har utviklet seg til et eget lite økosystem og en industri. Kriminelle jobber i virtuelle team organisert med spesialistkompetanse med ansvarsdeling mellom personer og grupper på lik måte som mindre It-virksomheter. Økningen i omfang og spesialiseringen har også gitt fremvekst av egne grupper som spesialiserer seg på å gjøre de første inntrengningene og etablere fotfeste hos de som angripes, såkalte Initial Access Brokers (IAB). Etter å ha etablert tilgang selger de denne over det mørke nettet til andre grupper som utløser skadevaren og gjennomfører selve utpressingen. Det er også grupper som kun utvikler skadevare for både inntrengning og kryptering som selges med brukervennlig grensesnitt og hjelpetjenester.

Ved såkalt dobbelt ransomware-angrep henter angriperne ut data før kryptering. Mange av ransomware-operatørene har egne «lekkasje-nettsteder» der de legger ut data fra sine ofre offentlig. For å øke presset trues ofrene med lekkasje av enda mer informasjon dersom de ikke betaler. Enkelte kriminelle har også gjort rene utpressinger kun basert på trussel om å offentliggjøre uthentet informasjon, uten at data har blitt forsøkt kryptert.

Vi har også observert et utpressingsfenomen som det i en del år var stille om, DDoS-angrep med utpressing. De fleste DDoS-angrepene er drevet av annen motivasjon en utpressing for penger. Det siste året har det vært virksomheter i Norge som har blitt utsatt for DDoS-angrep med krav om penger.

Det er stort overlapp i ransomware-aktørers bruk av taktikker, teknikker og prosedyrer (TTP-er). Tilgang oppnås ofte via gyldige innloggingsdetaljer til eksterne tjenester eller gjennom mail-spam-kampanjer som leverer skadelig programvare, eller ved å utnytte et begrenset spekter av sårbarheter. Aktører er fortsatt svært avhengige av offentlig tilgjengelige verktøy, som AdFind, Mimikatz og PowerSploit, og penetrasjons-testing verktøyet Cobalt Strike. Selv om det ikke regnes som en ny TTP, observerte CrowdStrike i 2022 en betydelig økning i antall ransomware-

aktører som bruker legitime Remote Access Tools (RAT-er) og fjernovervåkingsprogramvare inkludert AnyDesk, Atera Remote Monitoring and Management og SplashTop. Tidlig i 2023 meldte Microsoft sammen med Forta (utvikleren av CobaltStrike), at de har iverksatt en aksjon for å stanse domener og IP-adresser koblet til såkalte «crackede» versjoner av Cobalt Strike. Sikkerhetsleverandøren BAE Systems har meldt at mottiltak mot ulovlig bruk av Cobalt Strike har ført til gradvis nedgang. Til tross for tiltakene er Cobalt Strike fremdeles det mest brukte C2 (kommando og kontroll) verktøyet både blant statlige og kriminelle aktører.

I senere tid nevnes ofte LockBit 3.0, ALPHV (Blackcat), Play, Clop og Black Basta som de mest aktive ransomware-aktørene.
I andre kvartal 2023 ble LockBit og ALPVH ansett for å holde høyest tempo. Begge aktørene opererer etter «Ransomware-as-a-service» modellen, der de tar en prosentvis andel av utbyttet dersom målet for angrepet betaler løsepenger.

Samtidig dukker det stadig opp nye ransomware-aktører. Dette skjer både gjennom at nye kriminelle aktører entrer markedet, og medlemmer bytter grupper. I januar 2023 ble aktøren Hive satt ut av spill som følge av en koordinert internasjonal aksjon. De kriminelle som tilhører denne gruppen er fremdeles på frifot og det antas at de vil søke mot andre grupper, eller gjenoppstå med et nytt navn.

De mest avanserte ransomware og IAB-gruppene har tilhold i en del forskjellige land. Eksempelvis ble en gruppe som sto bak angrepet mot Norsk Hydro i 2019 i fjor arrestert i Ukraina. Flertallet av disse gruppene antas imidlertid å ha tilhold i Russland. Det er usikkert om aktørene i Russland vil bruke sin kompetanse til angrep på vegne av statlige aktører. Motivasjonen til å utføre slike angrep kan også skyldes patriotisk overbevisning, eller de kan være motytelse for ikke å bli arrestert, eller rett og slett betalte oppdrag. Ransomware-angrep ventes å fortsette på det høye nivået som er etablert eller å øke. Fremveksten av IAB, salg av lett tilgjengelig skadevare og et konglomerat av ransomware-grupper gjør det vanskelig å slå fast med sikkerhet hvem eller hvilken gruppe som står bak hvert utpressingsforsøk.

Vinningskriminalitet utover ransomware-aktører
Blant ikke-statlige trusselaktører finner vi hovedsakelig vinningskriminelle som benytter alt fra de enkleste til de mest avanserte metoder. Denne gruppen kriminelle fokuserer primært på å svindle personer og virksomheter, og utgjør en betydelig trussel mot Telenor Norges virksomhet og våre kunder. Rapporter fra finansnæringen og Politiet viser en kraftig økning i antall digitale svindelforsøk. Dette sammenfaller med Telenors erfaringer. Direkte kontakt er fortsatt en viktig del av svindlernes metoder og telefonen er fortsatt et viktig virkemiddel. Vi ser også en økning i bruk av meldingstjenester over sosiale medier. Det benyttes et titalls forskjellige svindelformer. Flere av disse kan brukes mot virksomheter. Det er spesielt to former som utmerker seg:

- **Fakturasvindel** – Å sende falske fakturaer er en gammel og velkjent svindelmetode, som fortsatt er aktuell. Fakturasvindel utføres ved at de kriminelle sender falske fakturaer eller endrer utbetalingsdetaljer på ellers legitime fakturaer.

- **Direktørsvindel** (BEC) er et nyere fenomen, som forutsetter at svindleren har skaffet seg adgang til virksomhetens e-post-system. De som utfører svindelen, har enten fått tilgang på brukernavn og passord eller har på annen måte lykkes med å trenge inn i virksomhetens IT-system. Svindlerne utgir seg deretter for å være for eksempel en daglig leder i en bedrift, for så å lure en ansatt (gjerne med økonomiansvar) til å gjennomføre en transaksjon som ofte «haster». Ved å automatisere de første stegene av svindelen kan de kriminelle lykkes i å øke antall svindelforsøk betraktelig. Automatisering muliggjør for eksempel masseutsendelse av meldinger og e-post. På den måten er det mulig å gjennomføre langt flere svindelforsøk.

Utvikling av AI har mange positive sider, men teknologien kan også utnyttes til kriminelle formål. AI-manipulert stemme over telefon ble første gang benyttet i svindel-sammenheng 2019. Tilsvarende ble det første svindelforsøket med AI-manipulering av videobilde og lyd utført i 2021. Vi har kun sett starten på bruk av denne teknologien i svindelsammenheng. Dette forventes å øke de neste årene.

Det finnes ytterligere utdyping om svindeltrender i Kapittel 5, Slik angriper de.

De som utfører «Direktørsvindelen», har enten fått tilgang på brukernavn og passord eller har på annen måte lykkes med å trenge inn i virksomhetens IT-system.

Leverandørkjedene kan ha sårbarheter hos mennesker, i teknologi og prosesser. Avanserte trusselaktører ser etter slike svakheter.

Trusselaktørers økte tempo i utnyttelse av sårbarheter
Softwareselskaper har et system hvor de gir belønning til hackere som tester softwaren deres og finner sårbarheter, såkalte Bug-Bounty programmer. Avhengig av hva de finner varsler selskapene sine kunder og tilbyr samtidig som regel en «patch» for å rette opp svakheten. (En patch er en korreksjon til programvare som retter en feil; i denne sammenheng en sårbarhet.) Deretter begynner et kappløp mellom trusselaktører og virksomheter som er nødt til å oppdatere systemene sine og patche eller endre prosesser. Sikkerhetsselskaper har lenge overvåket hvor lang tid det tar fra en ny sårbarhet blir gjort kjent til den blir utnyttet i et angrep. Denne tiden minsker stadig. I fjor offentliggjorde sikkerhetsselskapet Rapid7 en undersøkelse som viste at gjennomsnittlig tid fra sårbarheten ble offentliggjort til slike angrep kunne observeres, hadde blitt redusert til 12 dager mot tidligere 42 dager. Rapid7 rapporterte gjennomsnittstid, noen sårbarheter ble utnyttet langt raskere. Selv om antallet identifiserte sårbarheter som ble utnyttet i 2022 sank noe, så gikk også tiden mellom offentliggjøring og utnyttelse ytterligere ned. Mer enn halvparten av sårbarhetene ble utnyttet av trusselaktører i løpet av en uke.

Trusselaktører, ikke bare statlige, men kanskje spesielt Initial Access Brokers /ransomwareaktører, vil bli dyktigere. I tiden fremover må vi forvente at tiden fra sårbarheter blir offentlig kjent til de blir utnyttet vil fortsette å synke.

Utnyttelse av 0-dags sårbarheter

I løpet av 2022 identifiserte sikkerhetsselskapet Mandiant (en del av Google-gruppen) 55 nye ikke-identifiserte sårbarheter, såkalte 0-dags sårbarheter. Utnyttelse av 0-dags sårbarheter forutsetter enten ny og tidligere ikke kjent skadevare eller utnyttelse av en ny angrepsvektor. Selv om tallet gikk noe ned sammenlignet med rekordantallet (81) i 2021, er likevel nivået av ny skadevare/nye angrepsvektorer om lag tre ganger mer enn det var for fem-seks år siden. Mandiant har identifisert hva slags type aktør som står bak i et mindretall av de nye TTP-ene. Om lag tre fjerdedeler er utviklet av statsaktører, mens om lag en fjerdedel er utviklet av ransomware-aktører. Merk at dette er nyutviklet skadevare og/eller angrepsvektorer som krever høy spesialisert kompetanse å utvikle. Den langt vanligste angrepsformen, med stor margin, er bruk av allerede kjent skadevare og angrepsvektor mot IT-system som ikke er patchet.

Living off the land-attacks

I de fleste angrep mot IT-systemer brukes det fortsatt skadevare og den vanligste måten er fortsatt ulike former for phishing. Til tross for at IT-systemene generelt blir sikrere, ser vi likevel en økende tendens til at trusselaktører angriper uten å plassere skadevare. Eller at de etter først å ha brutt seg inn i systemet, lar være å installere ytterligere skadevare. Trusselaktørene arbeider deretter på forskjellige måter for å få tak i lovlige tilganger i systemet. Når angriperen har skaffet seg nødvendige tilganger, arbeider man så videre ved å misbruke forskjellige verktøy som allerede er lovlig installert i systemet. Dette er som regel forskjellige verktøy for systemadministrasjon. Det kan også være annen software. Muligheten for at tradisjonell sikkerhetsovervåkning oppdager angrepet reduseres ved at angriperen utnytter verktøy som er lovlig installert i systemet. Denne typen angrep kalles «living off the land-attacks». Slike angrep må ventes å fortsette og muligens øke i tiden fremover.

Trussel mot leverandørkjeder
Leverandørkjeder fortsetter å være et område som krever ekstra fokus. Enkelte globale forhold som økonomiske uroligheter, politisk ustabilitet og konflikt kan øke risikoen for at deler av leverandørkjeder går konkurs eller ikke lenger kan levere tjenester og produkter som avtalt. Dette kan skape uforutsette utfordringer i leverandørkjeder, og føre til behov for hurtig bytte av leverandører og underleverandører. Ved raske endringer i en lang leverandørkjede, øker også sannsynligheten for at uønskede leverandører kan få innpass.

Leverandørkjedene kan ha sårbarheter hos mennesker, i teknologi og prosesser. Avanserte trusselaktører ser etter svakheter i leverandørkjeder som de kan utnytte. IKT-systemer knyttet sammen gjennom forskjellige selskaper i mange land medfører en økt risiko. Dette gjelder særlig når selskaper med generelt lavere sikkerhetsnivå enn det vi har i Norge kobles sammen med norske systemer.

Både økonomisk motiverte aktører og statlige eller statstilknyttede aktører benytter ulike former for angrep gjennom leveransekjeder. Man har flere eksempler der ondsinnet kode finner veien til et stort antall virksomheter, gjennom et angrep mot morselskapet. Den ondsinnede koden blir kun utnyttet til aktive angrep mot noen få av de mange virksomhetene den er spredt til. Software-leveranser og tilgangsrettigheter gitt til tredjeparter er dominerende angrepsvektorer.

På grunn av Telenor Norges rolle i samfunnet og som leverandør til kunder med betydelig samfunnsansvar vil både Telenor Norge

og våre leverandører fortsette å være mål for trusselaktører som ønsker å gjennomføre leveransekjedeoperasjoner. Avanserte trusselaktører ønsker å ta og beholde kontroll over utstyr, nett og infrastruktur for å kunne utnytte dette til å oppnå egne mål. For våre kunder, spesielt de med særlig store verdier og samfunnskritisk infrastruktur eller oppgaver, eksisterer det en viss fare for å bli utsatt for skadevare distribuert i leveransekjeden.

Mobiltelefoner: misbruk av svakheter i SS7
Nylig avslørte journalister fra Haaretz, Lighthouse Reports, SPIEGEL, Tages-Anzeiger og Mediapart at en sveitsisk teleoperatør, Fink Telecom Services, tilbyr tjenester som muliggjør sporing av andres mobiltelefoner. De gir også tilgang til SMS-meldinger, avlytting av telefonsamtaler og lignende aktiviteter. Fink er ikke den eneste aktøren som tilbyr slike tjenester. Israelske NSO Group, selskapet som står bak blant annet spionprogramvaren Pegasus, har lenge vært kjent for å drive med lignende virksomhet.

Disse aktørene utnytter seg av svakheter i SS7 (Signalling System 7), en gruppe protokoller som brukes internasjonalt i telefoninettet for å håndtere telefonsamtaler, sende og motta SMS-meldinger og andre tjenester.

Disse sikkerhetshullene er svakheter som blant annet gjør det mulig å unngå å betale for telekomtjenester. Man kan også fange opp SMS-meldinger som sendes, og dermed få tilgang til for eksempel engangskoder dersom SMS brukes for tofaktor-autentisering. Det er også mulig å avlytte andres telefonsamtaler og man kan lokalisere mobiltelefoner til et begrenset geografisk område.

Salg av denne typen ulovlige overvåkningstjenester er sannsynligvis noe som ikke kommer til å avta med det første.

Fink har også rekruttert eller forsøkt å rekruttere folk som jobber med SS7-nett for å få tilgang til nettene. Denne tilgangen kan brukes til å tilegne seg informasjon uten at det er synlig at det er Fink som står bak. Det vil se ut som det er leverandøren der den rekrutterte personen jobber som har hentet ut informasjon.

Media har flere ganger skrevet om hvordan svakheter i SS7 kan misbrukes av for eksempel kriminelle eller statlige aktører. I enkelte tilfeller spekuleres det i at informasjon innhentet på denne måten har blitt brukt for å spore opp personer som senere har blitt drept. For eksempel kan dette ha skjedd i forbindelse med drapene på de meksikanske journalistene Cecilio Pineda Birto og Fredid Román.

De siste årene har Telenor observert aktivitet fra den sveitsiske aktøren rettet mot vårt nett. Selv om disse forsøkene har blitt stoppet, er det er sannsynlig at Telenor vil se mer aktivitet som forsøker å utnytte svakhetene i SS7 i tiden som kommer.

Innsidetrussel
Innsidetrussel, det vil si rekruttering av ansatte eller personer som er gitt tilgang til informasjon, anlegg eller systemer, representerer en betydelig trussel. Erfaring fra de nordiske land i de senere år tilsier at personer på innsiden av offentlig forvaltning og private foretak har blitt rekruttert og medvirket i kriminelle handlinger til skade for virksomheten. Vanligvis handler det om å frigi sensitiv informasjon, som kan brukes i svindelforsøk mot virksomheten. Det kan også være snakk om inngripen eller støtte til forretningsprosesser ved anbud eller oppkjøp.

Både statlige aktører og vinningskriminelle har stått bak slike handlinger. Motivasjonen er ofte økonomisk, men ansatte har også blitt manipulert til å bli innsidere av andre årsaker. Politi og sikkerhetsmyndigheter i de nordiske landene advarer unisont mot innsidetrussel. De nevner også flyktningspionasje og deltakelse i større kriminelle nettverk som viktige faktorer. En person som PST anser for å være en plantet illegalist, har nylig blitt siktet i Norge. Denne personen har infiltrert utenlandsk etterretning i lang tid gjennom bosetting i flere land.

Telenor har også tidligere erfaring med at kriminelle forsøker å rekruttere ansatte (se Digital Sikkerhet 2022). Vi har videre observert at ansatte innen bank og finans sammen har utført svindelforsøk mot egen virksomhet. Vi legger til grunn at ganske mye av kriminell innsideaktivitet ikke blir rapportert, og at det derfor eksisterer betydelige mørketall.

» Erfaring fra de nordiske land i de senere år tilsier at personer på innsiden av offentlig forvaltning og private foretak har blitt rekruttert og medvirket i kriminelle handlinger til skade for virksomheten.

» Regimer i ikke-demokratiske land har et annet syn når det gjelder å utnytte eller presse personer til å utføre oppgaver.

Verving kan foregå over tid. Trusselaktører kan tilby ansatte fordeler i gråsonen mellom det som er lovlig kundepleie og korrupsjon. Gaver og andre materielle gjenstander, eller ikke-økonomiske fordeler tilbys ansatte. Hensikten er ofte å kunne be om en senere gjenytelse, uten at dette nevnes i tilnærmingsfasen. Ansatte, innleide eller leverandørers handlinger som utføres på vegne av en trusselaktør kan i verste fall medføre at konfidensiell informasjon blir kompromittert eller at en trusselaktør får tilgang til viktige systemer, anlegg eller verdier virksomheten har. Dette kan føre til betydelig skade for virksomheten og i ytterste konsekvens true rikets sikkerhet.

Mange kriminelle nettverk har forgreninger internasjonalt. Regimer i andre ikke-demokratiske land har også et annet syn når det gjelder å utnytte eller presse personer til å utføre oppgaver. Bakgrunnskunnskap, åpenhet og kjennskap til personer bidrar til å beskytte. Samarbeid mellom sikkerhets- og politietater på tvers av landegrenser vil redusere muligheten for verving eller plassering av innsidere i viktige virksomheter. Mennesker med sterk tilknytning til land Norge ikke har et sikkerhetssamarbeid med har større sjanse for å bli satt under press. Det er også vanskelig å få gjennomført god bakgrunnskontroll når man ansetter personell fra slike land.

Høyere usikkerhet og en forverret sikkerhetssituasjon gir større behov for innsamling av etterretning fra blant annet Russland og Kina. Rekruttering av nøkkelpersonell er mest sannsynlig fortsatt et mål for russiske og kinesiske etterretningstjenester. På grunn av dagens sikkerhetspolitiske situasjon må Telenor Norge ta høyde for at dette også vil gjelde andre land som inngår i en militærallianse eller som har annet tett samarbeid med Russland eller Kina.

Verving av innsidere utført av kriminelle nettverk må også forventes å fortsette. Telenor støtter seg her også på nordiske politimyndigheter som advarer mot kriminelle gruppers innpass i offentlige og private virksomheter.

Trusselen mot Operasjonell Teknologi (OT)
Når man snakker om OT-teknologi så handler det om systemer som brukes til å styre fysiske prosesser og funksjoner. Dette kan være innenfor en rekke områder som produksjonsmaskineri, maskineri for kjemisk prosessering, elkraft, overføring av gass og vesker, styring av bygninger med mer.

OT-nettverk har lenge vært sett på som atskilt fra IT-nettverk og teknologi. Systemene integreres ofte ved bruk av IT-nettverk for overføring av data, programvareoppdateringer og for å gi brukergrensesnitt over nettverk enklere styring og bedre tilgang. Sammenkobling mot internett kan fort gjøre nettverket sårbart for angrepsmetoder mot konvensjonelle IT-nettverk. I denne delen av trusselvurderingen skal vi likevel holde et spesielt fokus på angrep mot industrielle kontrollsystemer (på engelsk forkortet til: ICS eller SCADA). Sentralt for disse systemene er programmerbare logiske styringer (PLS-er) som brukes til å styre aktuatorer, ventiler, rotasjonshastigheter og mye mer. PLS-er finnes normalt ikke i tradisjonelle IT-nettverk.

Første offentlige kjente angrep mot OT-teknologi med PLS-er var Stuxnet-angrepet i 2010, et svært spesialisert angrep mot klynger av sentrifuge for anrikning av uran i Irans kjernefysiske program. Angrepet var mot et i utgangspunktet lukket anlegg. Skadevaren skal angivelig ha blitt fysisk installert av en rekruttert person ved anlegget. En eller to ressurssterke etterretningsorganisasjoner står trolig bak.

I desember 2015 gjennomførte, det som høyst sannsynlig er en underavdeling av den russiske militære etterretningstjenesten, GRU et angrep mot distribusjonsnettverket i to ukrainske kraftregioner. Dette angrepet rettet seg ikke mot PLS-er eller OT-funksjoner, men IT-nettverket og brukergrensesnittet som ble brukt til å styre. Angrepet ble gjennomført med overtakelse av kontroll, feilstilling av parameter og sletting med wiper-skadevare. Wipere er en velkjent metode for å angripe IT-nettverk.

I et nytt angrep i desember 2016 var målet en transformator som koblet sentral til regional kraftforsyning i Kyiv, Ukraina. I dette angrepet ble PLS fra Siemens manipulert med en spesielt utviklet skadevare kalt Industroyer 1. Angrepet er verdens første kjente angrep mot PLS innen elkraft. Resultatet av angrepet var at strømleveransen ble koblet ut i omtrent en time. I likhet med angrepet i 2015 var angrepsvektoren i dette tilfellet at de kom inn via virksomhetens IT-nettverk. Et spesielt trekk ved skadevaren som ble brukt mot selve kontrollsystemet er at den er modulær og protokoller som virker mot PLSer fra Siemens kan erstattes med protokoller som virker mot andre produsenters styringsenheter. Også her mistenker man at det er en underenhet i den russiske etterretningstjenesten GRU som står bak.

FOTO: KENNY HOLSTON FOR THE NEW YORK TIMES / NTB

FOTO: AP PHOTO / DAVID J. PHILLIP / NTB

I april 2023 advarte USAs president Joe Biden om at FBI og sikkerhetsselskaper hadde identifisert aktivitet som truet USAs energiinfrastruktur.

I 2017 ble et ikke-identifisert raffineringsanlegg i Saudi-Arabia gjenstand for et cyberangrep. Her benyttet man en spesifikk skadevare kalt Triton (noen steder: Trisis) med kapasitet til å virke mot Schneider-styringer. Iranske aktører er mistenkt for å ha stått bak dette angrepet.

I februar 2022 ble en skadevare kalt Industroyer 2 forsøkt brukt mot en elkraftenhet i Ukraina. Angrepet, som anses å ha feilet, kom som en del av Russlands invasjon av Ukraina. Det er derfor nærliggende å anta at det var russisk etterretning som stod bak.

I april 2023 advarte USAs president Joe Biden om at FBI og sikkerhetsselskaper hadde identifisert aktivitet som truet USAs energiinfrastruktur. I oktober 2022 advarte sikkerhetsselskapet Dragos om en hackergruppe som arbeidet for en underenhet av den russiske etterretningstjenesten GRU. Siden 2017 hadde denne gruppen lykkes med å etablere fotfeste i OT-nettverk for strømstyring hos flere elkraft-leverandører og distribuører sine kraftnett i USA. Angrepet er todelt, og består av en gruppe som etablerer tilgang og en annen som står for videre manipulering inne i nettverket. Angrepet gjøres ved bruk av spearphishing, inntrenging i VPN-tjeneste og bruteforce-angrep mot blant annet skytjenester for å skaffe brukeridentiteter. Når tilgang er etablert bruker den andre enheten en avansert modulær skadevare tilpasset OT-protokoller og systemer kalt Pipedream.

Dragos beskriver at samme angriper i 2017-2018 lyktes med å trenge inn i tilsvarende OT- infrastruktur i Tyskland og i minst to andre vest-europeiske land. Dette har ikke vært offentlig kjent tidligere. Sikkerhetsselskapet identifiserte ytterligere to grupper med kapabilitet til å angripe OT-systemer, hvorav en var en kinesisk statlig aktør.

Samlet sett kan skadevarene Industroyer 1 og 2, samt Pipedream nå virke mot flere PLS-er fra Siemens, Schneider, Omron og serversystemer fra OPC-UA, samt Windows-baserte styrings-systemer av OT. Skadevarene er modulære og det er grunn til å tro at de vil bli videreutviklet til å virke mot andre firmaers OT-teknologi. Angrep kan støttes av en egen gruppe som behersker flere avanserte inntrengningsmetoder.

Trusselaktører med kapabilitet til å angripe OT-systemer er så langt identifisert primært som statlige. Erfaring fra andre områder indikerer imidlertid at kriminelle i løpet av noen år vil tilegne seg samme kompetanse som statlige aktører har. Man må også forvente at antall aktører som er kapable til å bryte seg inn og manipulere OT-systemer vil øke de neste årene.

Spesielt om trusselen mot noen av våre kundegrupper
I dette avsnittet forsøker vi å trekke frem trusler som er mer spesifikke for enkelte av Telenor Norges kundegrupper. Vi har brukt begrepet «viktige kundegrupper» fordi disse kunde-gruppene spiller særskilt viktige roller i samfunnet. Flere av de største virksomhetene i disse gruppene utarbeider egne trussel-vurderinger. Derfor ønsker vi her spesielt å støtte mindre kunder som ikke har ressurser til å utarbeide slike. Det understrekes at dette er trusler som kommer i tillegg til det samlede trusselbildet som er beskrevet over.

Olje- og gassindustri, elkraft og produksjonsindustri
Trussel mot OT-systemer
Den avansert skadevaren Pipedream (se avsnittet om OT-sikkerhet) var rettet mot elkraftsystemer. En enhet, høyst sannsynlig tilknyttet Russlands hemmelige etterretningstjeneste GRU, har også i 2015,

Industroyer 1 og Industroyer 2

- Sikkerhetsselskapet ESET har gitt skadevaren navnene Industroyer 1 og Industroyer 2. Andre sikkerhets-selskaper bruker navnet CrashOverride om Industroyer 1
- Mange sikkerhetsselskaper bruker kodenavnet Sand-worm om enheten/gruppen som står bak Industroyer 1 og 2 angrepene. Enkelte sikkerhetskilder navngir enhet 74455 i den russiske etterretningstjenesten GRU.
- Kodenavnet Pipedream på skadevaren er gitt av Dragos. Sikkerhetsselskapet Mandiant kaller den Incontroller.

2016 og i 2022 angrepet Ukrainsk kraftforsyning. De to siste angrepene var rettet mot OT-systemer. Vi ser at metodene russiske statsaktører benytter til å nå inn i OT-systemer blir mer og mer avanserte over tid. Basert på åpen tilgjengelig informasjon har aktører som jobber for statene Iran og Kina også brutt seg inn og gjort skade mot OT-infrastruktur. Disse aktørene ligger imidlertid etter Russland i utvikling av verktøy og TTP-er.

Kriminelle aktører har så langt ikke gjennomført angrep rettet mot selve OT-teknologien. Erfaringsmessig tilegner kriminelle seg tilsvarende avanserte metoder som statsaktører benytter seg av, men de ligger noen år bak.

Flertallet av angrepene mot OT-systemer har vært rettet mot elkraft. Vi har også sett angrep rettet mot raffineri.

Satellittkommunikasjon
Geografisk distribuerte produksjonsenheter kan være avhengige av sårbar satellittkommunikasjon. Samtidig med invasjonen av Ukraina 24. februar 2022, tok det som man antar å være russiske hemmelige tjenester ned KA-SAT. Dette er et system for satellittkommunikasjon over en geostasjonær satellitt. Angrepet ble gjennomført med skadevare som ødela funksjonen til brukerterminalene. En konsekvens av dette var at et stort antall vindmøller langt utenfor Ukraina mistet kommunikasjonen. Slik tap av kommunikasjon kan medføre tap av styring over OT-system.

Bank og finans

Utpressing, svindel og tyverier av digitaliserte penger
Bank- og finanssektoren er utsatt for mange av de samme truslene som andre virksomheter. Mye informasjon kan ha stor verdi, men verdien av informasjonen som forvaltes i bank og finansforetak har mer direkte verdi, idet den omfatter digitalisert representasjon av penger. I tillegg til å forårsake skade for bank og finansvirksomheten vil konsekvensene for annen kommersiell virksomhet være stor hvis det oppstår driftsavbrudd. En ransomware-aktør med ønske om å presse målet for penger vil ha en gunstig posisjon dersom de skulle lykkes i å nå inn i sentrale deler av bank og finansforetaks systemer.

Digital svindel har hatt en eksplosiv vekst i senere år og bank og finans vil også være truet av enkelte typer avansert svindel. Det er særlig farlig med svindel der ansatte blir manipulert, imitasjon av kunder som vil ha gjennomført utbetalinger eller IT-angrep med påfølgende manipulasjon av ansatte som har betalingsfullmakt. Det første tilfellet av svindel med AI-generert imitasjon av stemme over telefon ble gjennomført i 2019. Bank og finansinstitusjoner har blant annet begynt å bruke systemer for stemmegjenkjenning for å hindre manipulasjon. En svakhet er imidlertid at slike systemer kan manipuleres ved hjelp av AI-generert stemmesimulering. Det første svindelforsøket med AI-generert videokonferanse ble gjennomført i 2021. På noe sikt kan angrep med AI-generert telefonoppringning eller falsk video kunne ramme personer i norsk eller nordisk finansnæring.

Fram til om lag 2018 ble det gjennomført en rekke digitale banktyverier av til dels av store beløp. Angrep av denne typen gikk mot kontrollsystemet til minibanker. Dette gjorde det mulig for de kriminelle å foreta uautoriserte utbetalinger. Angrepene var også rettet mot systemene som bankene har koblet opp mot det internasjonale transaksjonssystemet, SWIFT. Bankenes systemer ble manipulert til å foreta uhjemlede overføringer over SWIFT.
De mest avanserte trusselaktørene er spesialiserte kriminelle grupper med tilhold øst i Europa, samt den såkalte Lazarus gruppen fra Nordkoreansk etterretning som stjeler penger for regimet. Lazarus-gruppen har de siste årene hentet inn penger ved å angripe kryptobørser og forvaltere av kryptovaluta. De spesialiserte kriminelle gruppene i Øst-Europa er antatt å ha skiftet til ransomware-angrep og svindel, ettersom dette er enklere å utføre og har gitt bedre avkastning. Det er en mulighet for at kriminelle som tidligere har sittet på spesialkunnskap om banksystemer kan gjøre nye forsøk. Sannsynligheten for at dette vil ramme norsk finansnæring er imidlertid svært lav.

Helsesektoren

Operasjonell kontinuitet og personsensitive data
Helsesektoren forvalter personsensitive data om pasienter, samt sine mange ansatte. IT-systemene brukes også på daglig basis til å styre en strøm av pasienter til behandling og overføring til andre enheter. Helseforetak er derfor avhengige av å opprettholde operasjonell drift. Avbrudd i behandlingsstrømmen vil umiddelbart kunne sette pasientenes liv og helse i fare. Forskjellige enheter i helsesektoren vil derfor være svært egnede mål for initial access brokers/ransomware-grupper. Erfaring fra andre

» Mye informasjon kan ha stor verdi, men verdien av informasjonen som forvaltes i bank og finansforetak har mer direkte verdi, idet den omfatter digitalisert representasjon av penger.

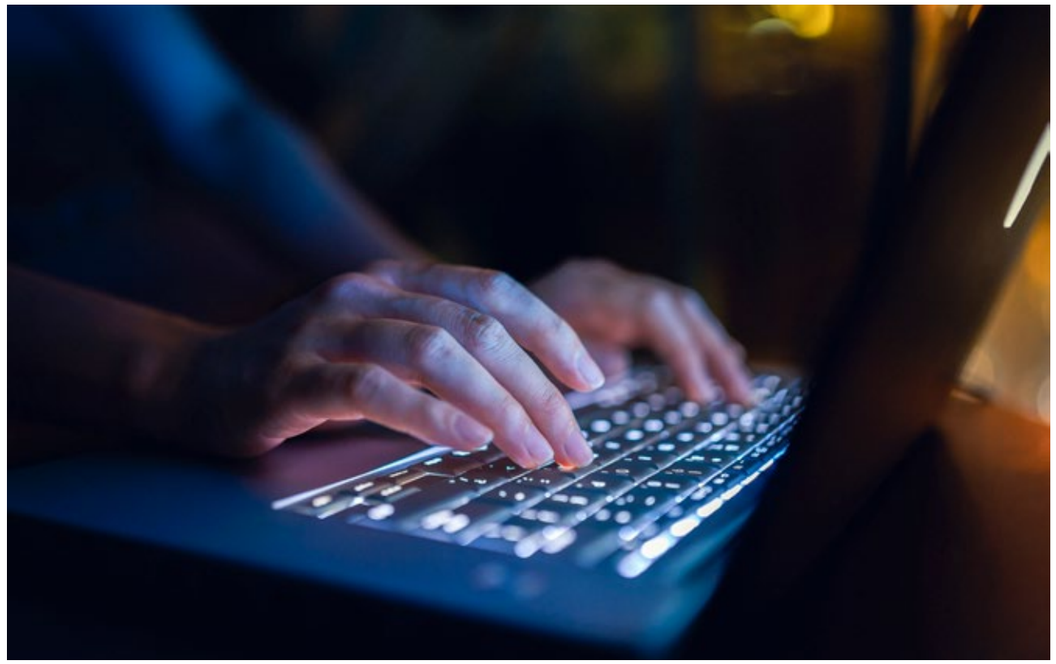


FOTO: GETTY IMAGES

land, hvor det riktignok er flere kommersielle helseforetak, tilsier at virksomheter innenfor helsesektoren kan bli mål for utpressingsangrep.

I likhet med krypterings- og utpressingsangrepene vi har sett i senere år, har vi også i utlandet observert såkalt dobbel utpressing. Dette er ransomware-angrep, hvor angriperne henter ut sensitiv informasjon før krypteringvirus utløses i IT-systemet. Angriperne truer med å offentliggjøre denne informasjonen, og kommer i tillegg med pengekrav for å åpne krypterte data. I noen angrep henter de kriminelle ut kun informasjon og bruker trussel om offentliggjøring alene som utpressingsmiddel. Med en helseinstitusjons personsensitive data, vil en trusselaktør stå relativt sterkt i en utpressingssituasjon.

Trippel utpressing har heldigvis ikke forekommet ofte. Det første kjente tilfellet fant sted i Finland[1] i 2020, og var rettet mot en landsdekkende kjede av psykoteriapiklinikker. I tillegg til å presse foretaket, presset angriperen også pasienter direkte ved å true med å offentliggjøre informasjon de hadde hentet ut. Saken fikk bred medieomtale etter at utpresseren kontaktet selskapet og pasienter i 2020[2]. Den mistenkte utpresseren ble pågrepet i Frankrike og utlevert til Finland i februar 2023, der han avventer rettsak. Tidligere administrerende direktør i selskapet er imidlertid allerede idømt betinget fengsel for straffbart brudd på GDPR.

Dobbel utpressing eller utpressing med store mengder personsensitive data vil sette både virksomheter og pasienter under press og skape høy grad av usikkerhet. Erfaring fra utlandet er at helseforetak har blitt gjenstand for ransomware-angrep. Fra angripers ståsted er helsesektoren et særlig egnet angrepsmål. De forvalter store mengder sensitive data og er avhengige av denne i sin daglige drift. //

1 https://en.wikipedia.org/wiki/Vastaamo_data_breach
2 https://edition.cnn.com/2020/10/27/tech/finland-therapy-patients-blackmailed-data-breach-intl/index.html

FOTO: GETTY IMAGES

Telefonsvindel er et alvorlig samfunnsproblem som rammer stadig flere nordmenn. Det er nå så mange svindelforsøk, at mange vegrer seg for å ta telefonen om det ringer fra et ukjent nummer. Også svindel gjennom bruk av norske telefonnummer øker.

FOTO: GETTY IMAGES

5

Slik angriper de

Uansett hvor vi snur oss i det digitale rom opplever vi et jevnt trykk fra angriperne – fra økonomisk motiverte kriminelle som prøver lure deg og virksomheten til hackere med andre og enda verre motiver. I dette kapittelet ser vi nærmere på angripernes metoder og deler egne erfaringer.

DET ER NÅ så mange svindelforsøk, at mange sier de vegrer seg for å ta telefonen om det ringer fra et ukjent nummer. Dette er med andre ord noe som påvirker mange, selv de som ikke direkte rammes av svindelen.

Uansett hvor vi snur oss i det digitale rom opplever vi et jevnt trykk fra kriminelle som prøver å lure deg. Dette gjør de ved bruk av kanaler som SMS, telefonanrop, sosiale medier, direkte-meldinger, nettsider og konkurranser, samt falske nettannonser som dukker opp på ellers troverdige sider. Er du uoppmerksom, sulten, trøtt eller har dårlig tid, trykker du gjerne på en lenke du ellers ville unngått.

I økonomisk usikre tider ser vi gjerne også et oppsving i svindel-aktivitet. Befinner man seg i en presset situasjon, er det lettere å ta uoverveide valg. Da er det enkelt å falle for tilbud eller muligheter som egentlig er for gode til å være sanne.

I angrep mot bedrifter ser vi at etablerte trender videreføres. Phishing, direktørsvindel og utpressingsangrep preger bildet. I tillegg ser vi tjenestenekt (DDoS) og øvrige angrep som til dels kan relateres til krigen i Ukraina.

Hacking av private sentralbord er en gammel utfordring som dessverre fortsatt er aktuell.

Svindel gjennom fjerntilgang øker

Mange nordmenn opplever å få anrop fra ukjente, norske mobil-numre, der noen utgir seg for å være fra for eksempel «Amazon». Dette er kriminelle som forsøker å ta kontroll over mobilen din via egne programmer for fjerntilgang.

Tar du telefonen, får du som regel høre en forhåndsinnspilt beskjed om at noen har bestilt en iPhone i ditt navn. I beskjeden blir du bedt om å trykke på '1' for å komme i kontakt med en servicemedarbeider. Dersom du faktisk gjør det, blir du viderekoblet til en svindler.

Telenor erfarer at slike phishing-angrep går i bølger. I senere tid har de som ringer utgitt seg for å være fra Amazon, men også Microsoft og andre kjente store virksomheter blir misbrukt til slik svindel.

Fremgangsmåten er i utgangspunktet lik: Du blir oppringt, og du blir forelagt et problem – for eksempel en «feilkjøpt iPhone» eller at de har oppdaget et «virus på maskinen din». Svindlerne sier at de kan hjelpe deg, bare du gjør som de sier. For at de lettere skal kunne «hjelpe deg», blir du bedt om å laste ned en app på mobilen din, og muligens også et program på datamaskinen. Dette blir gjerne beskrevet som en «sikkerhetsapp», men er i virkeligheten et verktøy som gir de kriminelle tilgang til mobilen eller datamaskinen din.

Det er spesielt appen AnyDesk som har vært de kriminelles foretrukne verktøy – men også programmer som TeamViewer har vært misbrukt. Dette er apper som i utgangspunktet er legitime og gratis å laste ned via både AppStore og Play Store. Problemet er bare at de også er svært enkle å misbruke. Alt de kriminelle trenger å gjøre, er å overbevise den som eier mobilen eller datamaskinen om å gi dem tilgang. Dette gjøres til tross for advarsler i appene om svindelfaren.

Appene gjør det mulig for andre både å se hva du gjør på skjermen og å fjernstyre mobilen eller datamaskinen. Dersom du installerer en slik app, og gir uvedkommende tilgang, er det i praksis fritt fram for de kriminelle.

Det du ser på din egen skjerm, kan de også se på sin skjerm. For eksempel kan de be deg om å gå inn på nettbanken, eller få deg til å taste inn bankdetaljer. Dette er informasjon de da får tilgang til og kan misbruke. De kan også fange opp engangskoder du får tilsendt via for eksempel SMS, og bruke disse til å kapre brukerkontoen din. Mulighetene for misbruk er mange når fjerntilgangen først er etablert.

Direktørsvindel – fortsatt en alvorlig trussel

For syvende år på rad anser Telenor direktørsvindel for å være svindelmetoden med størst tapspotensial for seg og sine datterselskaper. Metoden går ut på at svindlerne utgir seg for å være en leder i en bedrift, for så å lure en ansatt (gjerne med økonomiansvar og fullmakter) til å gjennomføre en transaksjon som «haster».

De kriminelle manipulerer ansatte via e-post og skaffer seg informasjon som de bruker til å få ansatte i organisasjonen til å gjennomføre en betaling ved bruk falsk faktura, eller å endre et kontonummer på en eksisterende faktura. Slik endring av betalingsinformasjon er også en mye brukt metode sammen med såkalt «business email compromise», der svindlerne skaffer seg tilgang til en e-postkonto hos virksomheten eller leverandøren.

Hvert år er vi vitne til forsøk på å lure ansatte i Telenor. En salgs-direktør i Telenor Linx ble forsøkt svindlet da han mottok en e-post merket «HASTER» som var signert av administrerende direktør i selskapet.

» Uansett hvor vi snur oss i det digitale rom opplever vi et jevnt trykk fra kriminelle som prøver å lure deg.

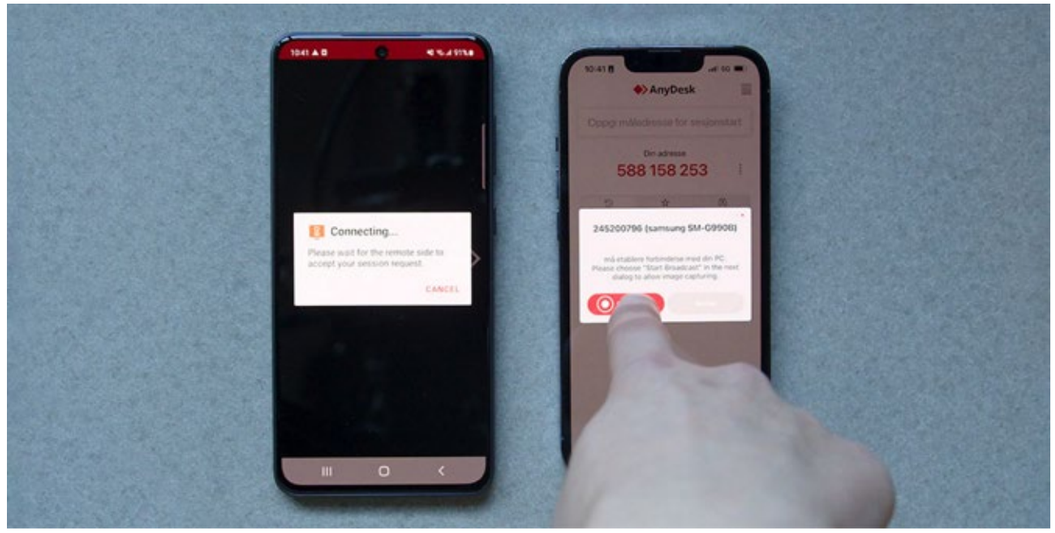


FOTO: TELENOR

BER DEG LASTE NED APP: Som et ledd i svindelen, ber de kriminelle deg gjerne laste ned en app som for eksempel AnyDesk. Gjør du dette, og gir de kriminelle tilgangene de trenger, kan de få innsyn i alt du gjør på mobilen – og i verste fall ta full kontroll over den.

Salgsdirektøren var på dette tidspunktet opptatt med å følge barna sine til skolen, men svarte raskt tilbake at «joda, jeg er tilgjengelig – det er bare å ringe». Like etter kom svaret, igjen signert av sjefen: «Jeg er i et viktig møte akkurat nå, og jeg kan ikke anrop. Jeg trenger at du håndterer en presserende oppgave for meg forsiktig.»

Det er ikke uvanlig med en hverdagslig tone i slike e-poster og at de har enkelte skrivefeil. Salgsdirektøren svarte at han kunne rydde kalenderen frem til 14.30. Igjen kom svaret kontant «Ok bra. Jeg vil at du skal kjøpe gavekort til bestemte kunder. Klarer du det på 25 minutter? Gi meg beskjed slik at jeg kan sende deg navnene på gavekortene og den nøyaktige verdien av hvert. Jeg vil refundere pengene dine umiddelbart etter møtet.»

Først da barna var levert på skolen, fikk salgsdirektøren sett nærmere på e-postene han hadde mottatt, og da blinket alle varsellampene. Han kontaktet assistenten til administrerende direktør, og fikk avklart at dette var et svindelforsøk.

I forbindelse med direktørsvindel benytter de kriminelle seg av den etablerte tilliten, respekten og noen ganger frykten mange ansatte har for autoriteter i virksomheten. Dersom den ansatte tror det faktisk er sjefen som er avsender og ber dem om å gjøre noe, så er sjansen relativt stor for at dette også blir gjort. Det kan starte med noe så ufarlig som kjøp av gavekort, men kan eskalere til større beløp når tillitten og kommunikasjonen er etablert. Her kan det ofte også være snakk om store beløp.

Hva de kriminelle faktisk var ute etter i dette tilfellet, er ikke sikkert, men digitale gavekort, som det her ble bedt om, er kjent for å være et lett omsettelig verdiobjekt på nettet.

Telenor tror organiserte kriminelle de senere årene i større grad benytter åpne kilder som LinkedIn og Facebook til å kartlegge ansatte og bedrifter i forbindelse med direktørsvindel. Denne informasjonen kan deretter brukes sammen med annen informasjon. Når brikkene i puslespillet er lagt, kan de kriminelle med høy presisjon effektivt gjennomføre målrettede direktørsvindelangrep. Vi ser også at svindlerne bruker mer tid på informasjonsinnhenting og forberedelser, slik at de kan konstruere mer komplekse og troverdige historier enn denne nokså typiske og enkle gavekort-svindelen. Da går de også etter langt større verdier.

Telenors sikkerhetsavdeling har det siste året fulgt opp flere henvendelser fra egne ansatte som har mottatt suspekte henvendelser og kontaktforespørsler via LinkedIn. LinkedIn krever ikke verifikasjon for å knytte en brukerkonto til en bedrift, og dette utnytter de kriminelle. De kan for eksempel oppgi at de jobber i Telenor og bruke dette til sin fordel i direktemeldinger til andre Telenor-ansatte på plattformen. »

Over 40 Telenorbutikker angrepet – slik gjennomskuet vi hackeren

En ansatt i en Telenorbutikk i Oslo ble oppringt på jobb og trodde først det var en kollega som tok kontakt. Han skjønte fort at noe ikke stemte. I kulissene jobbet sikkerhetsfolk i Telenor allerede med å spore angrepet.

Den 3. januar i år blir Telenorbutikken på Stovner oppringt fra et svensk telefonnummer.

Stemmen i den andre enden tilhører en ung norsk mann som sier han ringer fra Telenors IT-support. Grunnen til at han tar kontakt, er for å fikse problemer de ansatte har hatt med en printer i butikken.

Omtrent på samme tid blir mer enn 40 Telenorbutikker oppringt fra det samme nummer. Det hele er et systematisk angrep, der målet er å få tilgang til Telenors datasystemer ved hjelp av phishing og sosial manipulasjon.

– Shit! Hva har jeg gjort?!

Angrepet mot Telenorbutikkene føyer seg inn i rekken av phishing-angrep, der gjerningspersonen forsøker å få tak i sensitiv informasjon ved hjelp av en falsk nettside eller en applikasjon som kalles *AnyDesk*.

Denne gangen snakket gjerningspersonen i tillegg flytende norsk.

– Jeg stusset over at personen ringte fra et svensk nummer, siden han åpenbart var norsk. Samtidig virket det logisk at noen fra support tok kontakt, forteller den ansatte som var alene på jobb da telefonen ringte.

Den ansatte hadde selv meldt fra til sjefen om at printeren ved den ene kassa ikke fungerte som den skulle. Han oppfattet derfor dette som en troverdig henvendelse. Ti minutter senere skjønte han imidlertid at han hadde blitt lurt.

– Med en gang tenker man jo selvfølgelig «shit! hva har jeg gjort?!» Jeg har hørt om andre bedrifter som har blitt hacket, men så ikke for meg at gjerningsmennene var så proffe.

Slik foregikk svindelforsøket: Falsk nettside og AnyDesk

Etter å ha presentert seg, forklarer mannen på telefonen at trøbbelet med printeren skyldes en nettverksfeil. For å løse problemet trenger han tilgang til butikkens systemer og ber den ansatte om å åpne en nettside: Billett-Telenor.com

Nettsiden ser identisk ut som en global Telenor-side, men er falsk.

På nettsiden må den ansatte logge inn med brukernavn og passord til Telenors systemer – noe han ikke har ettersom Telenorbutikken kjører sitt eget nettverk uavhengig av Telenor sitt.

Mannen ber derfor den ansatte om å laste ned AnyDesk, så han kan hjelpe til med innloggingen.

– Jeg kjente til AnyDesk fra før, og visste at det er et verktøy som gjør det mulig å fjernstyre en PC fra en annen. Siden dette var en person fra Telenor, tenkte jeg at det var trygt å la ham få tilgang, sier den ansatte.

FOTO: IT PRO X

Så begynner ting å skurre.

Først legger den ansatte merke til at nettleseren varsler om at URL-en han er inne på, er usikker. Så oppdager han at noen har opprettet et nytt skrivebord på PC-en, som ligger skjult bak nettleseren han har oppe.

Det er åpenbart at mannen i den andre enden holder på med noe annet enn det han sier han gjør. Når den ansatte i tillegg blir bedt om å la AnyDesk stå på over natten, skjønner han at butikken kan være under angrep.

– Da det gikk opp for meg hva som skjedde, gikk jeg rett inn og avinstallerte applikasjonen, slettet filen og skrudde av PC-en. Etterpå ringte jeg til driftslederen min og fortalte hva som hadde skjedd. Nå er jeg bare glad for at jeg gjennomskuet ham i tide, forteller den ansatte.


Thorbjørn Busch
FOTO: TELENOR

Visste om angrepet før telefonen ringte

Mens den ansatte pratet med svindleren på telefonen, var Telenor allerede i full gang med å spore angrepene mot Telenorbutikkene. En forhandler i Bergen hadde tidlig varslet om et phishing-forsøk der svindlerne utga seg for å være fra Telenors IT-support.

– Da vi mottok det første tipset, satte vi umiddelbart i gang en gransking for å kartlegge omfanget av saken, sier Thorbjørn Busch, senior sikkerhetsrådgiver i Telenor.

Det svenske telefonnummeret viste seg å være et reelt nummer tilkoblet en Skype-konto.

At det ble brukt et svensk nummer kan være et signal om at aktørene forsøker å gå nye veier, etter at Telenor i 2022 innførte en sperre som forhindrer misbruk av norske fastnettnumre ved hjelp av såkalt spoofing, mener Busch.

– Mange bedrifter har forbindelser til Sverige, så et svensk nummer innbyr ofte til tillit. Men når anropet kommer fra Sverige, betyr det også at man må gå etter de kriminelle i utlandet – noe som gjør det mer utfordrende å granske angrepet.

Etter et omfattende søk i trafikkdata på det svenske nummeret, kunne sikkerhetsteamet raskt se hvilke andre Telenorbutikker som allerede hadde blitt utsatt for phishing-angrepet.

– Etter å ha pratet med noen av forhandlerne, fikk teamet mistanke om at gjerningspersonene forsøkte å få tilgang til Telenors øvrige datasystemer via Telenorbutikkene – noe som heldigvis i kke er mulig, forklarer Busch.

– Her har trolig første mål vært å samle inn brukernavn og passord via den falske nettsiden. Når det ikke lyktes, har steg to vært å få tilgang til bedriftens PC via AnyDesk.

Målet kan ha vært kontroll over mobilnumre

Det er fortsatt usikkert hva det endelige målet med angrepet var – men det er ingen tvil om at de kriminelle kan utnytte en slik tilgang til en rekke formål, der hensikten stort sett er å tjene penger. Et potensielt mål kan ha vært såkalt SIM-swap.

Dette kan i verste fall bli brukt for å skaffe seg tilgang til offerets kontoer – for eksempel til e-post eller kryptolommebøker – ved å nullstille passord eller motta koder for totrinnsverifisering over SMS.

– Dette er ikke bare en trussel for private, men også bedrifter – der full tilgang på telefonsamtaler og SMS-er til en ansatt kan åpne dørene videre for spionasje, direktørsvindel eller andre typer angrep mot en virksomhet, sier Busch.

– En teori er at gjerningspersonen denne gang var på jakt etter kundelister for å få kontroll over mobilnumre på disse listene, sier Busch.

– Åpenhet avgjørende for å avdekke svindel

På Stovner er den ansatte og daglig leder glade for at Telenor var raskt på ballen, og at de tidlig fikk svar på hva som faktisk hadde skjedd.

– Før vi rakk å melde fra til Telenor, tok de kontakt med oss. Da fikk vi vite at de allerede jobbet med å granske det som hadde skjedd. Selv om det føles skremmende å bli utsatt for noe sånt, er det også betryggende å vite at Telenor følger nøye med, sier daglig leder.

Busch forteller at saken ble overlevert til politiet, og han roser de andre ansatte i Telenorbutikkene for rapporteringen og åpenheten rundt svindelforsøket.

– Selv om anmeldelser ikke alltid fører til noen pågripelse, gir det politiet viktige etterretningsopplysninger som kan komme til nytte ved en senere anledning.

– For å kunne granske slike saker, er vi også helt avhengige av at ansatte og ledere sier ifra når de oppdager noe mistenkelig eller frykter at de kan ha blitt lurt. Når vi rekker å gjøre en grundig granskning selv, øker sjansen for at politiet kan foreta en pågripelse.

Men hvordan kunne egentlig svindlerne vite at printeren på Stovner ikke virket?

– Dessverre er nok det en gambling med lav risiko, uansett hvilken bedrift du ringer, sier Busch, og legger til:

– For hvem har vel egentlig ikke en printer det er noe trøbbel med?

Spoofing – mottiltak og tilpasningsdyktige kriminelle
Telefonsvindel er blitt et alvorlig samfunnsproblem som dessverre rammer stadig flere nordmenn. Svindlere som ringer og gir seg ut for å være for eksempel bankansatte eller politi, utnytter tilliten folk har til disse yrkesgruppene for å svindle dem for relativt store summer.

De siste årene har vi sett en sterk økning av tilfeller der kriminelle har misbrukt norske telefonnumre i svindelforsøk. Det som fremstår som anrop fra norske telefonnumre, kan være organiserte kriminelle som opererer fra eller via utlandet. Med relativt enkle grep har de kunnet «gjemme seg» bak norske fastnettnumre. Spoofing innebærer at det originale utenlandske telefonnummeret erstattes med et selvvalgt norsk nummer.

Etter at Telenor i 2021 innførte tiltak mot spoofing av mobilnumre, har vi sett en økning i spoofing av norske fastnettnumre. Fastnettnumre starter med 2, 3, 5, 6 eller 7 – og er numre som angir en stedstilhørighet, for eksempel 21 80 21 80 til Oslo kommune eller 75 55 50 00 til Bodø kommune. Dette er numre det er knyttet stor grad av troverdighet til.

Selv om samtalene kommer via utlandet, har vi i det siste også sett mange svindelanrop utført av norske kriminelle, som gjerne opptrer høflig og imøtekommende. Sjansen for at du tar telefonen øker betraktelig dersom du får opp et norsk nummer i displayet når det ringer, fremfor et utenlandsk eller skjult nummer. Dersom nummeret tilhører et kjent selskap eller en offentlig institusjon, tar folk telefonen. Da er de også i større grad tilbøyelige til å gjøre det de blir bedt om.

I november 2022 gikk flere norske teleoperatører sammen og blokkerte kriminelles mulighet til å spoofe norske fastnettnumre. Initiativet var resultatet av samarbeidet i den ideelle sammenslutningen «ITAKT», som samler norske internett- og teleoperatører for å bekjempe svindel og misbruk av tjenester og infrastruktur. Blokkeringen ble innført i tråd med anbefalinger fra Nasjonal kommunikasjonsmyndighet (NKOM) og retningslinjer satt i ekomforskriften og nummerforskriften.

Med denne blokkeringen vil slik spoofing av norske fastnettnumre fra utlandet ikke lenger være mulig. Dersom et anrop som kommer inn fra utlandet til Norge er satt opp med et norsk fastnettnummer som avsender, vil dette bli blokkert og ikke nå frem til norske forbrukere.

Hva er spoofing?

Spoofing er en svindelteknikk med falsk avsender- eller opprinnelsesinformasjon. De mest brukte kanalene hvor spoofing forekommer er e-post, tekstmeldinger eller telefonsamtaler der kriminelle forfalsker avsenderidentitet for å gjennomføre svindelforsøk. Teknikken er mye brukt som del av et angrep med bredere sosial manipulering, men spoofing av opprinnelsesadresse for IP-trafikk benyttes også i forbindelse med noen typer tjenestenektangrep.

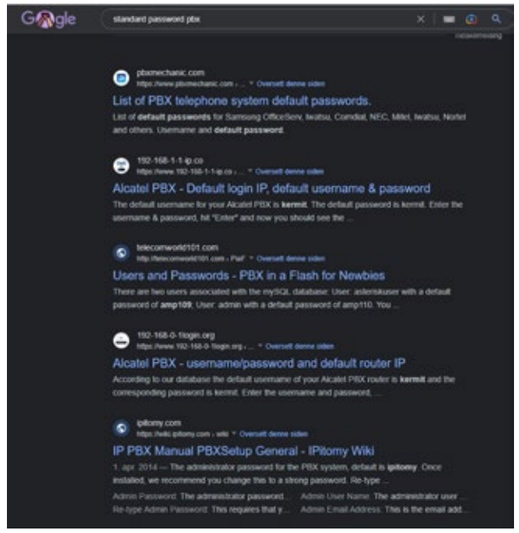
Selv om fastnettnumre er mindre i bruk hos private, brukes de fortsatt gjerne av bedrifter og offentlige institusjoner som NAV, Skatteetaten og Politiet. Dette er etater som opplever å få både sine navn og numre misbrukt i svindel. Blokkeringen gir norske bedrifter og offentlige institusjoner bedre beskyttelse mot misbruk.

Hacking av hussentraler – et vedvarende problem
Telenor ser at virksomheters hussentraler (såkalte PBX-er) fremdeles utsettes for «innbrudd». Ved å utnytte svakheter i hussentralens funksjoner kan kriminelle utføre svindelforsøk. De kan også bruke dette som utgangspunkt for videre cyberangrep, for eksempel ransomware-angrep.

Hussentraler leveres med standard brukernavn og passord og installeres opp mot internett. Hvis ikke brukernavn og passord blir endret og hussentralen sikret ved installasjon, utsetter virksomheten seg for stor risiko. Dette kan sammenlignes med å gå fra eget hus med ulåst dør. Det å endre standard passord og innstillinger er helt grunnleggende sikkerhetshygiene, fordi oversikt over standard brukernavn og passord finnes på internett.

Dersom de kriminelle får kontroll på hussentralen, kan de starte søk etter å finne åpne internasjonale «premium rate» numre (IPRN). Denne typen destinasjoner kalles også «international revenue share numbers». Jo flere minutter med anrop til slike nummer de kriminelle klarer å generere fra hussentralen, jo mer penger tjener de.

> Svindlere som ringer og gir seg ut for å være for eksempel bankansatte eller politi, utnytter tilliten folk har til disse yrkesgruppene for å svindle dem for relativt store summer.



Oversikt over standard brukernavn og passord finnes på nett.

Telenor har iverksatt tiltak for å stenge aksess til IPRN-numre i hele verden. Monitorerings-løsninger har blitt tatt i bruk for å kunne identifisere denne type uønsket trafikk i vårt nett. De kriminelle bruker gjerne et script – omtalt som en «dialer» – for å automatisere søk etter åpne premium rate-numre. De må ofte foreta mer enn 1000 anrop mot ulike land og numre før de finner åpne numre. Ofte kan Telenor se disse forsøkene mens de pågår og starte jobben med å stenge denne trafikken før svindlerne lykkes. Vi stenger dermed for videre misbruk. Telenor erfarer at når svindelen blir politianmeldt, er vi i stand til å stoppe betalingene relatert til slik svindel i over 95% av tilfellene.

Det er derfor viktig å politianmelde dette, selv om Telenor uansett kan begrense den økonomiske skaden ved å stoppe videre trafikk. En anmeldelse vil i tillegg gi politiet en mer helhetlig oversikt over denne formen for kriminalitet.

Premium Rate numre og Wangiri-svindel
Premium Rate numre benyttes også i såkalt wangiri-svindel. Ved å blokkere anrop til og fra Premium Rate-numre som brukes i svindel, avverger vi også wangiri-angrep mot våre kunder.

Vi ser at majoriteten av Premium Rate-numre kommer fra ulike nasjonale nummerserier som ikke skal kunne ringes til. Dette er for eksempel serier som ikke er i allmenn bruk i landet, eller det kan være tekniske serier som er øremerket særskilte formål. I. Dersom du for eksempel mottar et wangiri-anrop fra den britiske atlanterhavsøyen Ascesion og ringer tilbake, er det lite trolig at ditt anrop faktisk blir besvart i Ascesion. Det er langt mer sannsynlig at anropet ditt blir videresendt til en Premium Rate leverandør av en utro tredjepart. Når anropet kobles opp, vil man få avspilt en automatisk talemelding (IVR) som er laget for at man skal holde linjen lengst mulig. «*Please hold the line – your call is important to us*». Dessverre er det også noen få lokaloperatører som lar seg friste til å betale kommisjon til Premium Rate-leverandører for trafikk til numre i deres nett. Her kan det være alt fra enkeltnummer til hele serier. Telenor blokkerer alle slike numre så fort de blir identifisert.

Det finnes flere selskaper som tilbyr tjenester som i praksis tilrettelegger for svindlerne. De tilbyr nødvendige verktøy og tjenester som IVR-server, søkeverktøy og testnumre. De leverer også numre til de kriminelle enten direkte eller via andre selskaper. Telepremium (https://telepremium.net/how-it-works/) er et eksempel på en slik leverandør. Noen av disse selskapene tilbyr også en app man kan laste ned til sin telefon for å sjekke ut hvilke numre som er tilgjengelig hos gjeldende operatør. Kontakt med selskapene er ofte kun mulig via Skype. De opererer sjelden med fysisk adresse eller firmanavn.

Wangiri-svindel og hacking av hussentraler er dessverre kun to eksempler på hvordan svindlere tjener penger på Premium Rate-numre. Alle fremgangsmåter som lurer offeret til å ringe nummeret og holde linjen i noen tid gir svindlerne inntekter. Veiledning og forslag til forskjellige metoder finnes også fritt tilgjengelig på nett.

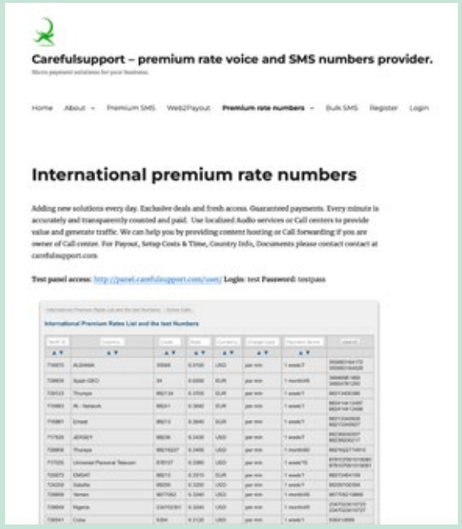
Telenor prioriterer arbeidet med å sikre at trafikk til og fra slike Premium Rate-serier blokkeres og forblir blokkert. Dette er viktig.

Hacktivister utfører målrettede og direkte DDoS-angrep
Det siste året har antallet DDoS-angrep registrert gjennom Telenors systemer holdt seg jevnt, med et snitt på rundt ni registrerte angrep per døgn. De fleste angrepene rammer privatpersoner og er relativt kortvarige.

De aller fleste angrepene går ut på å sende et stort volum datatrafikk for å lamme Internett-forbindelsen til offeret. Mye av denne trafikken blir generert ved å benytte tilfeldige feilkonfigurerte servere på nettet til å reflektere og forsterke trafikk som treffer målet for angrepet. Siden angrepstrafikken kommer fra en feilkonfigurert server, blir også angriperens egentlige IP-adresse effektivt skjult.

Telenor og andre større Internett-tilbydere (ISPer) har systemer som effektivt kan oppdage og stoppe denne type angrep. Systemene overvåker angrepstrafikk på Telenors rutere som grenser mot andre ISPer. Denne trafikken kommer fra «lovlige» tjenester, men i langt større mengder enn det som er normalt. Eksempler på tjenester som gjerne blir misbrukt er NTP (Network Time Protocol), DNS (Domain Name System) og LDAP (Lightweight Directory Access Protocol).

Søk etter premium rate-numre

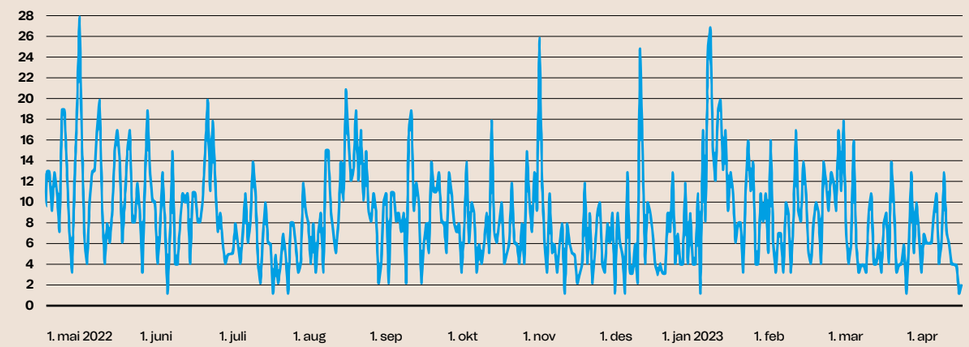


Carefulsupport.com; Et eksempel på selskap som tilbyr dedikert testpanel.

Utdrag av instruksjoner for installasjon og bruk av mobilapp fra Carefulsupport.com

Angrep per dag

DDoS-angrep pr. dag gjennom siste år (april 2022 – april 2023)



Etter Russlands invasjon av Ukraina har det vokst fram mange hacktivist-grupper, både på russisk og ukrainsk side. På russisk side har spesielt KillNet og NoName057 vært aktive. Disse gruppene har også vært omtalt i norske medier i forbindelse med DDoS-angrep. I løpet av det siste året har blant annet Arbeidstilsynet, BankID, Altinn, NRK, Schibsted, NAV og NSM blitt rammet. Gruppene skifter stadig hvilke land og mål som angripes, alt etter hva som rapporteres av media. Noname057 angrep for eksempel norske mål den 2. mars, etter at norske myndigheter kunngjorde en avtale om økonomisk støtte til Ukraina verdt flere milliarder kroner.

Både Killnet og Noname057 koordinerer aksjonene sine og diskuterer aktuelle mål for angrep i chattegrupper på meldingstjenesten Telegram. Sistnevnte benytter et DDoS-verktøy skrevet i Python kalt DDosia, som er tilgjengelig for nedlasting via lenker delt i Telegram-grupper. Medlemmene registrerer seg via en Telegram-bot, og får utdelt en unik ID som de legger inn i verktøyet. Verktøyet installeres på medlemmenes egne maskiner, på hackede servere eller på leide virtuelle maskiner i skyen. De som bidrar mest til angrepene kan høste både berømmelse og i noen tilfeller mindre mengder kryptovaluta overført til sin konto som takk for innsatsen.

I de fleste tilfeller angripes nettsidene direkte, med fullt oppkoblede TCP-forbindelser. Dette gjør at forbindelsene blir kryptert, og det blir vanskelig å se ut fra nettverkstrafikken hva som skjer og hva angrepstrafikken består av. Før angrepene starter, sjekker hacktivist-gruppene målene sine nøye og finner funksjoner på nettsidene hos hvert enkelt mål som typisk belaster web-serveren og bakenforliggende systemer mest mulig. Dette kombineres gjerne med sesjoner som aldri kobles ned igjen, såkalte Slowloris-angrep. Når angrepet retter seg mot applikasjonslaget, kan serveren som angripes blir overbelastet uten at nettverksforbindelsen fylles med trafikk.

Angrepstrafikken består av tilsynelatende vanlige oppkoblinger fra vanlige brukere. Ved hjelp av vanlig trafikkanalyse er det derfor vanskelig å oppdage når bedriften er under angrep. Denne typen angrep oppdages ofte først ved at web-servere som er under angrep ikke svarer eller svarer svært tregt. Noen ganger kan en ikke en gang se en tydelig økning i trafikken ved å analysere trafikkgrafer mot webserveren, men angrepet kan kjennes igjen ved å se på antall spørringer eller hvilke ressurser som blir etterspurt.

Siden det er vanskelig å skille angrepstrafikk fra nyttetrafikk i nettverkslaget, stoppes denne typen angrep gjerne ved hjelp av geografiske IP-filtre. Dersom et norsk nettsted er under angrep, kan en for eksempel blokkere alle innkommende forbindelser som kommer fra utenfor Norden. Denne typen blokkering er naturligvis mindre egnet dersom brukerne av nettstedet er svært geografisk spredt.

For å kunne blokkere DDoS-angrep av denne typen er det best å ha tilgang til de faktiske spørringene som gjøres mot webserveren. Etter å ha analysert disse har man mulighet til å blokkere uønskede spørringer. Dette kan gjøres direkte på webserveren, eller helst via et system før serveren, som en proxy eller WAF (Web Application Firewall). Gjennom logger og statistikk kan man kartlegge hvilke ressurser på serveren som misbrukes under angrepet og sperre disse. Systemer som tar imot trafikk fra vanlige brukere bør også konfigureres for å hindre Slowloris-angrep. Dette kan gjøres ved for eksempel å begrense antall åpne nettverksforbindelser per klient, hvor lenge de skal kunne holdes åpne osv.

Det er viktig å ha en avtale på plass med sin ISP, før angrepet faktisk inntreffer for å kunne stoppe DDoS-angrep. Sørg også for å ha gått nøye igjennom webserverens arkitektur, samt at det er lett å få tilgang til logger og sperre forespørsler som brukes i angrep.

Phishing – teknikker og tiltak

Phishing-eposter har i mange år vært en av de mest brukte fremgangsmåtene for å få ulovlig innpass på innsiden av en organisasjon. Har man tilgang til brukernavn og passord til en eller flere ansatte i en bedrift, er det mange tjenester som kan misbrukes, inkludert skybaserte tjenester bedriften benytter seg av. Ifølge organisasjonen Anti Phishing Work Group (APWG) var 2022 et rekordår for phishing med mer enn 4,7 millioner angrepskampanjer verden over. Siden 2019 har antall angrep av denne typen steget med over 150% per år.

Mange bedrifter trener sine ansatte i å kjenne igjen phishing-forsøk og ikke trykke på «mistenkelige» lenker i e-poster. Men det å skille ekte lenker fra phishing viser seg å være vanskelig. Flere firmaer bruker eksterne leverandører for mange av sine interne tjenester. Dette betyr at ansatte ofte må trykke på lenker til sider som ligger utenfor organisasjonens interne domener. Dette gjør det vanskeligere for ansatte å skille på legitime og illegitime lenker. Det er ofte vanskelig selv for eksperter på datasikkerhet å avgjøre hva som er en legitim epost eller svindel. Dersom man gjennomfører en phishing-test mot et større firma, vil alltid minst én ansatt bli lurt til å gi fra seg sensitiv informasjon som brukernavn og passord. Angriperne har dermed oppnådd det de ville.

For å unngå angrep har flere organisasjoner de siste årene innført forskjellige former for multifaktor autentisering; i tillegg til det faste passordet må brukerne skrive inn en engangskode for å logge inn. Angripere omgår i stadig større grad denne typen ekstra sikkerhet ved også å spørre om engangskoden. Koden kan skrives inn manuelt på tjenesten som etterlignes, eller det kan settes opp en proxy som gjør det mulig for angriperne å logge seg inn. På denne måten kan uvedkommende få tilgang til offerets sesjonsnøkkel og dermed fremstå som rettmessig eier av kontoen.

Et eksempel på en kommersielt tilgjengelig tjeneste (PaaS - Phishing as a Service) som tilbyr denne funksjonaliteten er «Greatness», som Cisco Talos rapporterte om i mai 2023. Her tilbys en komplett phishing-pakke med ferdiglagde e-poster, phishing-side, proxy-funksjonalitet og kontrollpanel klart for bruk mot tjenester som for eksempel Microsoft 365. For å sikre seg mot avanserte angrep som dette, må man bruke autentiserings-mekanismer som er motstandsdyktige mot phishing.

Fysiske sikkerhetsnøkler, som Yubikeys, er et eksempel på en autentiseringsform som ikke er utsatt for phishing. En fysisk nøkkel blir knyttet til brukerens konto. Denne kommuniserer ved hjelp av USB eller Bluetooth med enheten det logges inn fra. Nøkkelen må fysisk stjeles for å kunne brukes av uvedkommende til å logge inn. Google innførte denne typen sikkerhet for sine ansatte i 2017 og har siden ikke vært utsatt for vellykkede phishing-angrep. Barrieren for å ta i bruk sikkerhetsnøkler er imidlertid stor. De må distribueres til brukerne og registreres. De er også lettere å miste, noe som vil sperre brukeren ute til vedkommende får en ny nøkkel.

En ny teknologi tas nå i bruk som skal gi brukerne nesten like god sikkerhet som fysiske sikkerhetsnøkler, uten ulempene de fører med seg. Teknologien kalles passnøkler (passkeys) og baserer seg på samme standard som fysiske sikkerhetsnøkler kalt «WebAuthn», utarbeidet av sikkerhetsalliansen Fast Identity Online (FIDO). Både Microsoft, Apple og Google tilbyr nå passnøkler for innlogging. Passnøkler fra disse leverandørene vil igjen også kunne brukes til å autentisere brukeren videre mot andre tjenesteleverandører.

En passnøkkel består av henholdsvis en privat og en offentlig nøkkel som genereres lokalt av operativsystemet på enheten brukeren benytter. Den offentlige nøkkelen deles med tjenesten brukeren skal logge inn på. Ved innlogging låses den private nøkkelen opp lokalt på maskinen. Dette gjøres for eksempel ved at brukeren autentiserer seg med ansiktsgjenkjenning, fingeravtrykk eller en PIN-kode. Biometrisk informasjon deles ikke med tjenesten det logges inn på. Dersom man skal ta i bruk en ny enhet, kan en ny nøkkel genereres på den nye enheten ved å autentisere seg via eksisterende enhet, som for eksempel en mobiltelefon. Mobiltelefonen vil kontakte den nye enheten via Bluetooth eller NFC (Near Field Communication) for å verifisere at brukeren har fysisk kontroll over den nye enheten. Leverandører kan også velge å synkronisere passnøkler mellom enheter brukeren er logget inn på, slik Apple for eksempel gjør via Keychain.

Passnøkler gjør phishing-angrep umulig å gjennomføre. Adressen til nettsiden som brukeren prøver å logge inn på, blir utvekslet kryptert med tjenesteleverandøren som en del av innloggingsprosessen. Ved et forsøk på phishing vil denne adressen være feil, og innloggingen vil bli avvist. I motsetning til passord, er også passnøkler umulig å gjette seg fram til og består av en lang rekke med tilfeldige data, i kontrast til klassikere som «Passord123!».

Fremover vil passnøkler bli mer og mer vanlig for innlogging. En av de største utfordringene med løsningen er autentisering dersom brukeren ikke får logget inn, som for eksempel når man har mistet mobiltelefonen sin. Da må brukeren autentisere seg på en alternativ måte, for eksempel via en annen innlogget enhet, engangskoder skrevet ut på papir, en fysisk sikkerhetsnøkkel, forhåndsbestemte kontakter som kan bekrefte brukerens identitet, en SMS-melding eller ved å kontakte kundeservice. Slike backup-løsninger må utformes for å minimere risikoen for at brukerne blir stengt varig ute, samtidig som at man sikrer at uvedkommende ikke får tilgang til kontoer ved å utgi seg for å være eieren.

Kanskje kan drømmen om en passordfri hverdag uten phishing-angrep eller gjenbruk av passord gå i oppfyllelse om noen år. //

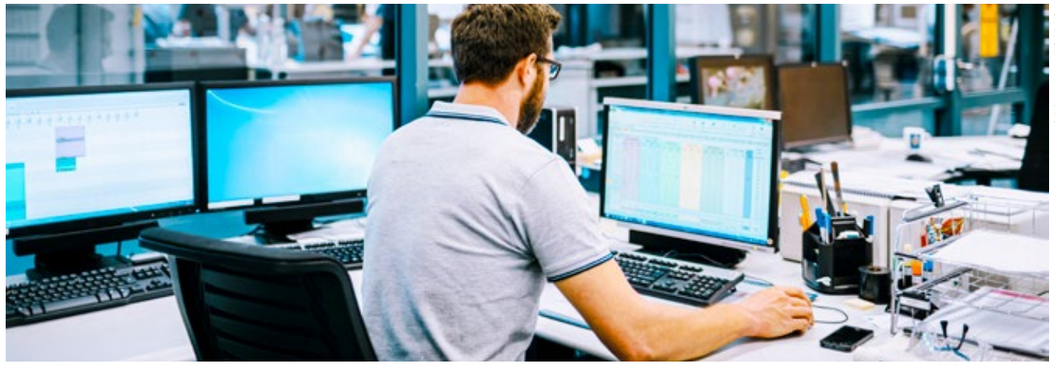


FOTO: GETTY IMAGES

Kanskje kan drømmen om en passordfri hverdag uten phishing-angrep eller gjenbruk av passord gå i oppfyllelse om noen år.

KraftCERT: Sett fra kraftsektoren

KraftCERT er sektorvis responsmiljø for kraftsektoren og jobber med å forebygge, oppdage og håndtere hendelser i sektoren.

Aktører vil jobbe kontinuerlig for å utvikle evne til destruktive/disruptive angrep
Lekkasjen fra det russiske selskapet NTC Vulkan, som blant annet er leverandør til russiske myndigheter, viser tydelig at russiske aktører har prosesser for å vedlikeholde verktøy-kassen for cyberangrep. Mot vederlag kan den benyttes av trusselaktører, primært statlige eller oppdragsstyrte. Verktøykassene omfatter også verktøy for disruptive/ destruktive angrep.

Verktøyene som NTC Vulkan har utviklet til angrepsformål er godt planlagte, flere av dem er modulære, og noen er også demonstrert som fungerende. Det kan være flere grunner til at en trusselaktør ønskes å demonstrere en kapabilitet eller et verktøy, enten for å vise frem verktøy til potensielle kunder, eller å understøtte statlige aktørers påstander om kapabiliteter. Det er likevel slik at selv om visse kapabiliteter demonstreres, vil alle aktører, statlige eller kommersielle, ikke ønske å vise full kapabilitet. De ønsker derimot at alle skal vite at dette ikke er deres fulle kapabilitet.

Informasjonen fra NTC Vulkan og koden til angrepsverktøy som PIPEDREAM er eksempler på lekkasjer som er svært uønsket for trusselaktører da de i for stor grad viser deres ekte kapabiliteter. Trusselaktørene ønsker ikke at noen skal få tid til å utvikle mottiltak. På den annen side ønsker alle potensielle angrepsmål tilgang til slik informasjon for å kunne forberede mottiltak.

De siste lekkasjene viser at trusselaktører i stor grad er undervurdert, og er langt mer modne og profesjonelle i skadevareutvikling enn det tidligere analyser har vist.

Langsiktig strategisk planlegging av angrep mot OT
Det er komplisert å angripe kontrollsystemer, og det krever mer planlegging enn angrep på konvensjonelle IT-systemer. Angrep som Stuxnet og Trisis har vist at det likevel er fullt mulig. Selv om planleggingen av slike angrep tar tid, så er ikke endringsraten i OT så høy at dette nødvendigvis er så stor hindring for trusselaktørene.

I forbindelse med Russlands angrep på Ukraina i 2022, ble det benyttet en skadevare som man har gitt navnet «Industroyer2». Det hersker liten tvil om at angriper her satt på en betydelig mengde informasjon om angrepsmålet før angrepet fant sted. Det at planlegging tar tid og at det må være spesialsydd for angrepsmålet gjør at OT-rettede angrep er kostbare.

Andre faktorer som gjør angrep kostbare er om angrepsmålene er godt beskyttet, slik som de som beskytter store verdier eller de som har strenge regulatoriske krav. De angrepsmålene som er vanskeligere tilgjengelig vil være mest interessante for avanserte aktører som har høy kompetanse, god tid og er villig til å betale mer for tilganger og nulldagssårbarheter.

Trusselaktører vil i slike tilfelle ikke gå ut på det åpne markedet for å skaffe seg tilganger, men direkte kontakte leverandører som de stoler på. Disse tilgangene som omsettes i en-til-en fora vil ikke dukke opp på lister over kjente informasjons-lekkasjer, og vil for angrepsmålet være skjult.

For å kunne utføre vellykkede angrep på kontrollsystemer er det behov for detaljert informasjon om disse, inkludert plassering. Verdien av denne type informasjon blir ofte undervurdert av informasjonseierne, og informasjon som ikke er dokumentert som spesielt sensitive i seg selv blir beskyttet for dårlig. Dette er også relevant for leverandører, noe som ble klart både i hendelsen hos Sargent & Lundy som hadde dokumentasjon om 900 kraftstasjoner og Black & McDonald som hadde militær, kraft- og transportdokumentasjon.

HelseCERT: Sett fra helsesektoren

HelseCERT er helse- og omsorgssektorens nasjonale senter for cybersikkerhet. Senteret skal øke sektorens evne til å oppdage, forebygge og håndtere alvorlige cyberangrep.

Angrep i helsesektoren
Den sikkerhetspolitiske situasjonen har endret seg kraftig i løpet av de siste årene. Vi ser økt etterretningstrussel, kraftig økt aktivitet fra hacktivister og en stadig større avstand til Russland.

Det som i mindre grad har endret seg er hvordan trussel-aktører angriper. Vi har lenge sett at kjente sårbarheter, svake passord og manglende flerfaktorautentisering brukes aktivt for å angripe virksomheter. Angripere begynner raskt å lete etter sårbare systemer etter at informasjon om sårbarheter blir offentlig kjent. Vi ser kontinuerlig forsøk på å gjette brukernavn og passord, og at passord på avveie benyttes for å gjennomføre angrep. Her illustrerer vi dette ved tre ulike datainnbrudd som har skjedd i helsesektoren i 2023.

Datainnbrudd 1 – sårbar server på nett
Et system med en sårbar tjeneste ble kompromittert av minst to ulike trusselaktører, hvor begge har knytninger til løse-pengeangrep. Systemet var eksponert på Internett og hadde en offentlig kjent sårbarhet. Den første angriperen ble stoppet av anti-virus, og ga opp. Den andre ble ikke stoppet og klarte å få administratortilgang og beveget seg videre til en rekke servere, inkludert domenekontroller, filserver, database-servere, med flere. Sårbarheten ble utnyttet kort tid etter at den ble offentlig kjent. Angrepet ble oppdaget etter ca. tre uker. Virksomhetens IKT-systemer ble tatt offline i ca to døgn da angrepet ble oppdaget og mye tid og ressurser er brukt på analyse og opprydding i etterkant.

Datainnbrudd 2 – uautorisert tilgang til VPN-løsning:
Svakt passord på en VPN-løsning gjorde at angriper lyktes med å logge inn i et lab-miljø gjennom å gjette brukernavn og passord. Angriper koblet opp en VPN-tunell over en periode på ca. fem minutter. Via denne tunellen kunne de nå flere systemer videre inn i virksomheten. Analyse av loggdata tyder ikke på at angriper har gjort mer enn å bekrefte tilgang. Vi antar at angriper planla å komme tilbake på et senere tidspunkt.

Datainnbrudd 3 – passordgjetting og sårbar server
Det vi antar er en løsepengevirus-gruppe står bak dette datainnbruddet. Angriper starter med bruteforce-aktivitet (passordgjetting) mot en server. De benytter om lag 400 generiske brukernavn og ulike passord i forsøkene på å gjette riktig brukernavn og passord. De gjør mellom 50-500 påloggingsforsøk hver dag over flere uker før de treffer en gyldig kombinasjon av brukernavn og passord og får logget inn på systemet. Etter å ha logget inn med brukernavn og passord som de har gjettet seg fram til, utnytter de en kjent sårbarhet, hvor patch ikke er installert for, til å installere et program som gir dem mulighet til å fjernkontrollere serveren. Angrepet blir oppdaget av en tredjepart som oppdager mistenkelig trafikk fra den kompromitterte serveren. Hendelseshåndtering starter, og angrepet blir stoppet uten større konsekvenser.

» Angriper gjør mellom 50-500 påloggingsforsøk hver dag over flere uker før de treffer en gyldig kombinasjon av brukernavn og passord og får logget inn på systemet.

FOTO: GETTY IMAGES

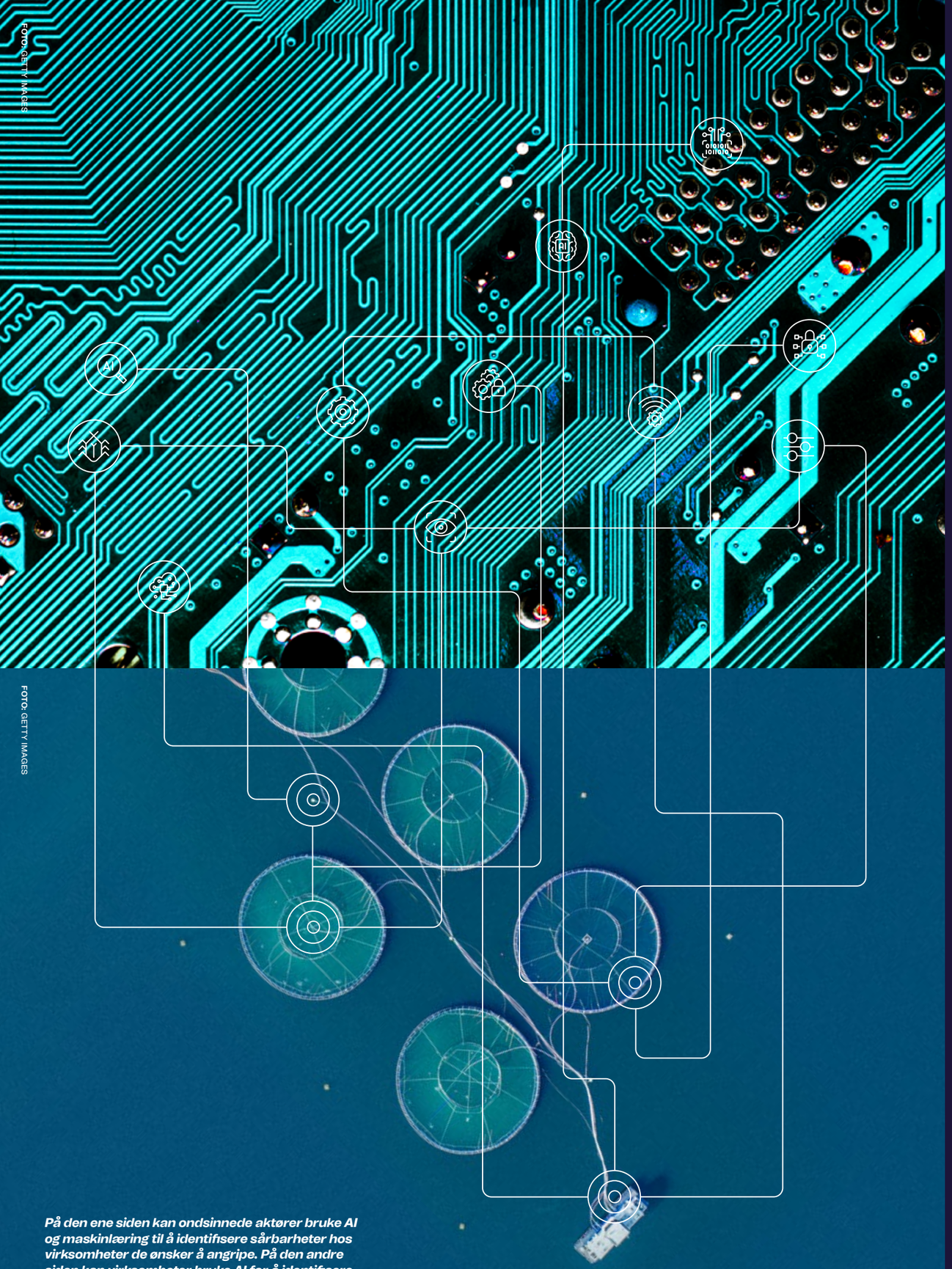


FOTO: GETTY IMAGES

På den ene siden kan ondsinnede aktører bruke AI og maskinlæring til å identifisere sårbarheter hos virksomheter de ønsker å angripe. På den andre siden kan virksomheter bruke AI for å identifisere potensielle trusler og avverge cyberangrep.

6

Vil kunstig intelligens styrke eller svekke cybersikkerheten?

I denne artikkelen ser forfatterne på hvordan AI kan brukes i cyberangrep og cybersikkerhetsforsvar. Forfatterene peker på at menneskelige overveielser vil være kritisk for god og ansvarlig bruk av AI. Samtidig kan velment bruk av AI også få negative konsekvenser for samfunnet.

De tilkoblede enhetenes tidsalder
5G tilbyr et bredt spekter av konnektivitetsmuligheter og støtter ulike enheter – fra datakrevende smarttelefoner til primitive sensorer og presisjonsenheter som krever forbindelser med høy pålitelighet og lav forsinkelse (ultra-reliable low-latency). Med innføringen av 5G ser vi en massiv økning i antallet tilkoblede enheter. Ifølge Statista[3] «forventes antallet tingenes internett (IoT)-enheter globalt å nesten tredobles fra 9,7 milliarder i 2020 til over 29 milliarder IoT-enheter i 2030.» Disse enhetene vil gi nyttige og nyvinnende applikasjoner og tjenester som beriker folks liv, men bringer også med seg nye cybersikkerhetstrusler.

Trusselbildet innen cybersikkerhet har endret seg dramatisk på grunn av den store og raskt voksende angrepsflaten med milliarder av tilkoblede enheter og de enorme datamengdene de genererer. Tradisjonelle cybersikkerhetsmekanismer og filtrering av innkommende data for potensielle trusler ved nettverksperimeteret er ikke lenger tilstrekkelig. Dette krever nye tiltak innen cybersikkerhet, og bruk av kunstig intelligens (AI) er et naturlig førstevalg. Desverre er ikke AI kun forbeholdt aktører med gode intensjoner; ondsinnede aktører og fiendtlige nasjoner har allerede tatt i bruk AI for å gjennomføre flere ødeleggende cyberangrep samtidig som de omgår tradisjonelt cybersikkerhetsforsvar. La oss først se på hvordan AI kan brukes i cyberangrep, og deretter utforske hvordan det kan benyttes innen cybersikkerhetsforsvar.

AI i feil hender – bruk av kunstig intelligens i cyberangrep

Identifisere sårbarhetene i offerets systemer

Ondsinnede aktører kan samle store mengder data fra cybersikkerhet, digitale medier, og andre relevante informasjonskilder, og deretter bruke AI/ML til å identifisere sårbarheter hos den virksomheten de har til hensikt å angripe. Angripere kan utføre automatisert ekstern skanning av et bredt spekter av vilkårlige nettverk for å identifisere svakheter i nettverksstrukturer og konfigurasjoner.

Unngå deteksjon

Angripere kan bruke AI/ML for å sikre at skanningen deres er under «radarnivået» og unngår å skape anomalier som kan oppdages av sikkerhetssystemet til offeret. Skadelig programvare kan utvikles slik at den dynamisk endrer adferd, og slik unngår å bli oppdaget av sikkerhetssystemer, ved hjelp av Generative Adversarial Networks (GANs)[4] eller forsterkende læring.

GANs er en form for generativ modellering som består av et par nevrale lærende nett; ett generatornett og ett diskriminatornett. Genereratornettet lærer å generere stadig bedre resultater ved å gjentatte ganger prøve å lure diskriminatornettet til å tro at de genererte resultatene er ekte eller, ved generering av skadevare, harmløse.

Bedrageribrev og målrettet phishing (Spearphishing)

Phishing-angrep har som mål å lure enkeltpersoner til å avsløre sensitiv informasjon eller utføre skadelige handlinger ved hjelp av svindelteknikker. AI kan utnyttes av trusselaktører til å lage svært overbevisende og personlig tilpassede svindelbrev. Ved å bruke naturlig språkbehandling (NLP) og ML- algoritmer, kan AI bidra til å generere meldinger som er svært gode etterligninger av ekte kommunikasjon. Dette gjør det svært vanskelig for mennesker å skille mellom ekte og falske meldinger.

Deepfake-angrep

Deepfakes[5], som er en kombinasjon av «deep learning» og «fake», er data som er fabrikkert og digitalt manipulert for å erstatte én persons tilstedeværelse, i tekst, lyd eller bilde, med en annens på en overbevisende måte. Ved å kombinere deepfake-videoer med GPT (Generative Pre-trained Transformer), en type stor språkmodell (LLM) som for eksempel ChatGPT[6], kan «virtuelle personer» opprettes med noen få klikk.

Deepfake-angrep kan generere kompromitterende eller misvisende innhold, utgi seg for å være kjente personer eller spre desinformasjon, noe som kan føre til omdømmetap, økonomisk tap eller sosial uro.

Angrep mot maskinlæringssystemer

Adversarial Machine Learning Attacks, også kjent som angrep mot maskinlæringssystemer, har som mål å lure eller forvirre et maskinlæringssystem, noe som resulterer i feilaktige prediksjoner og beslutninger. Slike angrep deles gjerne i hovedkategoriene feilklassifisering av inndata eller angrep gjennom uriktige inndata

TEKST:

Thanh van Do, Telenor/Oslo Metropolitan University

Bruno Dzogovic, Telenor/Oslo Metropolitan University

Denne artikkelen er oversatt fra originalspråket og redaksjonelt tilpasset for publisering i Digital Sikkerhet 2023.

3 https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

4 Goodfellow, Ian; Pouget-Abadie, Jean; Mirza, Mehdi; Xu, Bing; Warde-Farley, David; Ozair, Sherjil; Courville, Aaron; Bengio, Yoshua (2014). Generative Adversarial Nets (PDF). Proceedings of the International Conference on Neural Information Processing Systems (NIPS 2014). pp. 2672–2680.

5 Kietzmann, J.; Lee, L. W.; McCarthy, I. P.; Kietzmann, T. C. (2020). "Deepfakes: Trick or treat?" (PDF). Business Horizons. 63 (2): 135–146. doi:10.1016/j.bushor.2019.11.006. S2CID 213818098.

6 Douglas, Will (March 3, 2023). «The inside story of how ChatGPT was built from the people who made it». MIT Technology Review

> Deepfake-angrep kan generere kompromitterende eller misvisende innhold, utgi seg for å være kjente personer eller spre desinformasjon.

(«data poisoning»). Feilklassifisering av inndata er den vanligste varianten, der angripere skjuler ondsinnet innhold i filtrene til en maskinlæringsalgoritme, med mål om å føre til feilklassifisering av et bestemt datasett. Angrep gjennom uriktige inndata går ut på å endre maskinlæringsprosessen ved å legge inn uriktige data i et datasett, noe som gjør utdataene mindre nøyaktige eller feilaktige.

AI i cybersikkerhet

Anomalideteksjon

En lovende og aktuell anvendelse av kunstig intelligens- og maskinlæringsmetoder innen cybersikkerhet, er deteksjon av atferdsmønstre og anomalier relatert til IoT-enheter. Med sine spesifikke egenskaper og instruksjoner, kan en IoT-enhet som er koblet til et nettverk forventes å ha et unikt, men identifiserbart mønster når den sender data; enten gjennom en fast datamengde, gjennom en fast overføringsfrekvens (for eksempel et begrenset antall ganger den kobler til nettverket for å sende data) eller ved annen gjenkjennelig atferd knyttet til enhetstypen. En «forstyrrelse» i dette gjenkjennelige mønsteret kan oppfattes som en anomali og kan indikere en mulig trussel ikke bare for enheten det gjelder, men også for teleoperatøren den er koblet til.

Telenor Research[7] har i samarbeid med OsloMet (Oslo Metropolitan University)[8], arbeidet for å bedre forstå

TEKST:

Bernardo Flores, Oslo Metropolitan University

Van Thuan Do, Oslo Metropolitan University

Boning Feng, Oslo Metropolitan University

denne typen trafikkdata-drevne mønstre og gjenkjenning av anomalier i 5G-nettverk[9]. Dette arbeidet har som mål å utvikle retningslinjer for å identifisere potensielle trusler ved bruk av IoT-enheter, for eksempel flomming eller DDoS-angrep[10], ved å analysere kontroll- og dataplanene og forstå atferden til tilkoblede IoT-enheter for å etablere det som kan kalles en enhetsprofil. Denne profileringen består av en rekke unike kjennetegn ved en spesifikk IoT-enhet, basert på dens historiske atferd når den er koblet til et mobilnettverk, slik at det er mulig å skille, for eksempel i en IoT-smarthus-kontekst, mellom et overvåkingskamera og en temperatursensor. AI/ML-plattformer bruker disse enhetsprofilene som terskler når de analyserer trafikk i et mobilnettverk. Hvis noe ligger innenfor et enhetsmønsterspekter, men ikke passer til den spesifiserte terskelen, vil det bli betraktet som en anomali, og det krever videre undersøkelse fra teleoperatørens cybersikkerhetsteam.

Generere IOC-er (Indicators of Compromise)

Dersom en potensiell trussel faktisk blir identifisert basert på de registrerte anomaliene, kan AI/ML-baserte indikatorer for kompromittering (IoCs)[11] ekstraheres og deles med samarbeidspartnere innenfor cybersikkerhetsmiljøet gjennom trusselutvekslingsplattformer, forutsatt at en passende modelleringsramme brukes. Rammer som CMTMF[12], som er designet for telekomindustrien, bidrar til å forstå den fulle effekten av et angrep som har brukt tilkoblede IoT-enheter som medium. Slike verktøy kan bidra til å styrke inntrengings- eller anomalioppdagelsessystemer (*Intrusion or Anomaly Detection Systems*, I/A DS) idet virkningsgraden ved slik deteksjon er tett relatert til deling av data fra tidligere angrep.

AI-baserte I/A DS som er designet med fokus på enhetsdrevne atferdsprinsipper, men også med andre verktøy for å gjenkjenne andre angrepstyper, understøtter i noen grad avverging og begrensning av cyberangrep. Imidlertid blir angripere som ønsker å utnytte IoT-løsninger mer kjent med hvordan disse systemene fungerer og har funnet vellykkede og uoppdagede måter å utføre angrepene sine på. »»

7 https://www.telenor.com/innovation/research/

8 https://www.oslomet.no/

9 B. Santos, B. Dzogovic, B. Feng, N. Jacot, V. T. Do og T. V. Do, «Improving Cellular IoT Security with Identity Federation and Anomaly Detection», 2020 5th International Conference on Computer and Communication Systems (ICCCS), 2020, pp. 776-780, doi: 10.1109/ICCCS49078.2020.9118438

10 Gupta, B.B., Chaudhary, P., Chang, X. & Nedjah, N. (2022). «Smart Defense Against Distributed Denial of Service Attacks in IoT Networks Using Supervised Learning Classifiers.» Computers & Electrical Engineering, 98 (March 2021), 107726. https://doi.org/10.1016/j.compeleceng.2022.

11 https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise

12 107726B. Santos, L. Barriga, B. Dzogovic, I. Hassan, B. Feng, N. Jacot, V. T. Do and T. V. Do, «Threat Modelling for 5G networks», 2022 International Wireless Communications and Mobile Computing (IWCMC), 2022, pp. 611-616, doi: 10.1109/IWCMC55113.2022.9825149.

» Et område der det er arbeidet med bruk av AI og maskinlæring innenfor cybersikkerhet, er design av dynamiske honeypots – «feller» designet for å lokke ondsinnede aktører og isolere skadelig aktivitet fra viktig infrastruktur.

» Dette kan være tilfelle med et Adversarial Attack[13], der angriperne ved å manipulere IoT-enheter på en isolert måte gjennom kortvarige datastrømmer, kan få systemer for innbruddsdeteksjon (IDS-systemer) til å betrakte hver isolerte hendelse som en ren anomali. Det blir da for sent å forhindre når alle de infiserte enhetene brukes koordinert.

Cybersikkerhetsteamene hos teleoperatører og andre eiere av kritisk infrastruktur blir også mer bevisste på denne angrepsformen og optimaliserer IDS-systemene og AI-modellene sine for å være mer motstandsdyktige[14]. I de fleste tilfeller har det vært forbedringer. Men selv om AI vil være et verktøy for å øke effektiviteten innen cybersikkerhet, særlig ved håndtering av rutinearbeid og mindre truende angrep, vil det fortsatt være behov for dedikerte cybersikkerhetsteam for å støtte mer kritiske og komplekse beslutninger. Dette er blant annet fordi verktøyene og modellene lærer av tidligere erfaringer og trening fra nettopp disse fagfolkene. Dessuten vil ikke alle etablerte handlemåter for å begrense skade fortsette å være like effektive etter hvert som angrep (og angripere) videreutvikler sine metoder.

Dynamiske honeypots

Et annet område med fokus på bruk av AI og maskinlæring innenfor cybersikkerhet, er design av dynamiske honeypots. En honeypot er en «felle» designet for å lokke ondsinnede aktører og isolere skadelig aktivitet fra viktig infrastruktur. Honeypots kan være reelle og simulerte datamaskiner, tjenester, nettverk, brukerkontoer og dataobjekter – gjerne også kombinert på en måte som etterligner en hel infrastruktur. Imidlertid kan angripere som bruker AI for Adversarial Attacks over tid få tilstrekkelig informasjon om forsvarssystemene og identifisere honeypot-nettverk, og dermed prøve å unngå dem i påfølgende angrep. Innføringen av AI-baserte dynamiske honeypots har som mål å kontre dette gjennom automatiske omkonfigurerbare feller for å håndtere AI-drevne Adversarial Attack angrep, basert på angriperens atferd.

Samfunnseffekter av kunstig intelligens (AI)

Trusler mot personvernet

Med fremveksten av milliarder av tilkoblede enheter som kontinuerlig overvåker menneskers aktiviteter overalt, genereres og samles det inn enorme mengder data. Imidlertid utgjør ikke disse dataene i seg selv en trussel mot personvernet uten den enorme databehandlingskraften til AI/ML.

AI/ML-algoritmer, inkludert ansiktsgjenkjenning, kan identifisere, analysere og forutsi en persons bevegelser ved å syntetisere data fra en rekke kilder, som sosiale medieinnlegg, geotaggede bilder, videoer fra overvåkningskameraer og lignende. Denne evnen til AI/ML kan misbrukes blant annet av ærlige aktører, kriminelle organisasjoner og diktatoriske myndigheter for å overvåke borgerne, og utgjør dermed en trussel mot personvernet, retten til anonymitet og personlig frihet.

Sosial manipulasjon gjennom AI-algoritmer

En av de største farene med AI/ML er sosial manipulasjon, da bedrifter, politikere og offentlig personer benytter seg av sosiale medier for å fremme sine strategier og politiske synspunkter, for å oppnå popularitet eller sanke stemmer. Sosiale nettverk oversvømmes av innhold basert på AI-algoritmer valgt av dem selv, og mislykkes ofte i å beskytte brukerne mot skadelig og misvisende medieinnhold. Situasjonen forverres med fremveksten av deepfakes, som gjør det mulig å spre falske nyheter og propaganda. Ingen vet lenger hva som er sant eller falskt.

Diskriminering og urettferdige utfall

Gjennom analyser basert på komplekse modeller og en enorm mengde data kommer prediktiv AI/ML til konklusjoner som kanskje ikke kan forklares for mennesker. Konklusjonene er samtidig heller ikke alltid 100% korrekte, og dette kan være fatalt innen områder som helsevesenet og andre områder der større transparens er nødvendig. Videre kan skjevhet (bias) oppstå fra AI/ML-algoritmer, der resultatene som produseres er fordomsfulle på grunn av feilaktige antakelser, ufullstendige datasett eller datasett fra menneskelige avgjørelser som gjenspeiler menneskers fordommer. Dette kan for eksempel føre til diskriminering basert på rase, kjønn, alder, religion, med mer.

Håndtere risikoen ved AI/ML

AI/ML er et tveegget sverd som kan tilføre samfunnet både stor verdi og alvorlig skade. Derfor er det først nødvendig å forstå både muligheter og begrensninger i AI/ML. Mer forskning er nødvendig, og det er avgjørende å fokusere på personvern, frihet, rettferdighet og etiske spørsmål. Til slutt bør det være myndigheter som kan regulere bruken av AI/ML og sikre rettferdig bruk av ML/AI. Dette er akkurat det både EU og USA arbeider med; å definere regulering for å forhindre misbruk av AI/ML samtidig som den muliggjør det potensielt enorme bidraget til samfunnet.

Konklusjon

Intensjonen og målet med AI er å gagne menneskeheten, men hvis den velger å oppnå målet på en destruktiv (men effektiv) måte, vil det ha negative konsekvenser for samfunnet. AI-algoritmer må bygges for å være i tråd med menneskers overordnede mål.

AI-algoritmer drives av data. Når stadig mer data samles inn om hvert eneste minutt av hver persons dag, setter det personvernet vårt i fare. Hvis virksomheter og myndigheter bestemmer seg for å ta beslutninger basert på informasjonen de samler inn om deg, slik Kina gjør med sitt sosiale kredittsystem, kan det utvikle seg til sosial undertrykkelse.

Én ting er sikkert: Fremtiden vil definitivt være med AI. Om den er på vår side eller ikke, avhenger nå av oss! Bruk vår egen «naturlige intelligens» nå! //

FOTO: GETTY IMAGES

13 Anthi, E., Williams, L., Rhode, M., Burnap, P., & Wedgbury, A. (2021). Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems. Journal of Information Security and Applications, 58(February), 102717. https://doi.org/10.1016/j.jisa.2020.102717

14 Anthi, E., Williams, L., Javed, A., & Burnap, P. (2021). Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks. Computers & Security, 108, 102352. https://doi.org/10.1016/j.cose.2021.102352

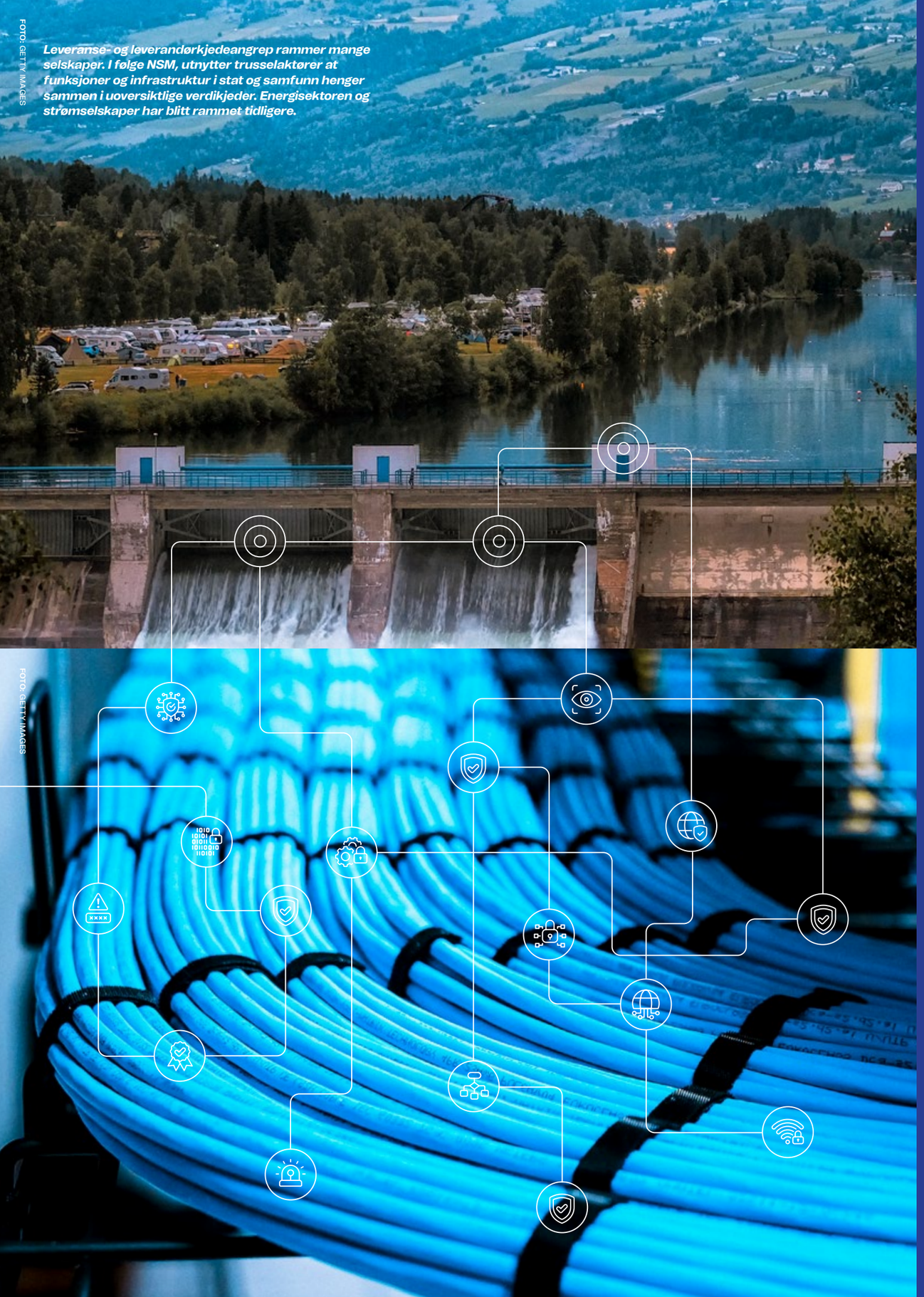


FOTO: GETTY IMAGES

Leveranse- og leverandørkjedeangrep rammer mange selskaper. I følge NSM, utnytter trusselaktører at funksjoner og infrastruktur i stat og samfunn henger sammen i uoversiktlige verdikjeder. Energisektoren og strømselskaper har blitt rammet tidligere.

FOTO: GETTY IMAGES

7

Når nettene blir lange – del III

I dette kapittelet tar vi opp tråden fra Digital Sikkerhet 2020 og 2021, og ser nærmere på leveransekjederisiko i forhold til programvare, samt kontinuitetsrisiko i leveranser.

I *DIGITAL SIKKERHET 2020*[15] tok vi i artikkelen *Når nettene blir lange* for første gang tak i leveransekjederisiko, og satte fokus på sikkerhet i leverandørgrensesnittet, kravstilling og hvordan skape insentiver og samhandling for sikkerhet i både leveranser, leverandørorganisasjonen og bakover i leveransekjeden. I *Digital Sikkerhet 2021*[16] dykket vi ned i software supply chain risiko. Alle kunne selvsagt ønske seg at temaet sikkerhet i leveransekjeder nå var løst, men vi må konstatere at det fortsatt er høyaktuelt. Vi ser i år nok en gang risiko relatert til leveransekjeder for programvare og hvordan SBOM bidrar til håndteringen, men ikke er nok. Vi retter også søkelys mot kontinuitetsrisiko i leveransekjeder, et forhold som også er belyst av henholdsvis Forsvars- og Totalberedskapskommisjonen.

Software supply chain

Til tross for et års opphold i temaet leveranse- og leverandørkjedeangrep i *Digital sikkerhet*, har disse indirekte angrepsvektorene slett ikke dalt i popularitet blant trusselaktørene. Innenfor software supply chain angrep rapporterer flere kilder om til dels dramatisk økning; f.eks. rapporterer Sonatype i siste utgave av sin *«State of the Software Supply Chain»* om 633% økning over det siste året. Noe av forklaringen kan ligge i forholdet Veracode belyser i sin State of Software Security rapport, basert på sine observasjoner; «79% of the time, once a library is included, it never gets updated».

Utvalgte angrep fra perioden

Blant større angrep fra den siste perioden kan vi særlig legge merke til, og høste lærdom fra;

Okta

Identitets- og autorisasjonstjenesten Okta Inc. var i skuddlinjen for ikke mindre enn tre leveransekjede-angrep i 2022.

I januar ble en underleverandør av callcenter og kundebetjeningstjenester, Sitel, kompromittert av utpressingsgruppen Lapsu$, som demonstrerte sin tilgang ved å vise skjermbilder av Oktas interne systemer. Undersøkelser viste at kundedata tilhørende 366 virksomheter, ca 2,5 prosent av Oktas kunder, ble kompromittert. Inngangen var gjennom et tredje selskap, Sykes, som nylig var kjøpt opp av Sitel.

I august ble IP-telefoniselskapet Twilio kompromittert – en tjeneste Okta benyttet for utsending av engangskoder til sine kunder. Et «mindre antall» telefonnummer og engangskoder ble berørt. Disse to første hendelsene peker i retning av krav til, og verifikasjon av, sikkerhet hos leverandører. Det belyser også behovet for sikkerhetsgjennomgang som del av due dilligence ved oppkjøp.

Til sist, i desember, ble deler av Oktas kildekode eksponert for uvedkommende, ved at GitHub kontoen deres ble kompromittert. Om dette siste egentlig er et leveransekjedeangrep er ikke definitivt avklart – det er spekulert i at tilgangen var muliggjort gjennom en av de to foregående hendelsene. Oktas uttalelse om at *«Okta does not rely on the confidentiality of its source code for the security of its services.»* får vi håpe stemmer – det er slik det skal være. Likevel vil tilgang til kildekode ofte bidra til å lette arbeidet for de som leter etter utnyttbare sårbarheter.

GitHub

I april ble GitHub rammet av en type angrep som har fått betydelig oppsving de siste par årene; tyveri av forskjellige former for «tokens» for autentisering og tilgang. Det kan dreie seg om informasjon i cookies og aksess-tokens med begrenset levetid, eller mer langlivede nøkler og sesjons-IDer. I den aktuelle saken lyktes angriper i å tilegne seg OAuth tokens – en form for identifiserende token som benyttes for å kunne gi tilgang over et konfigurerbart tidsrom uten å kreve re-autentisering – utstedt til tredjeparts-integratorene *Heroku* og *TravisCI*. Med de stjålne OAuth-tokenene fikk angriperne så tilgang til organisasjoner som bruker *Heroku Dashboard* og *TravisCI* produktene.

GitHubs undersøkelser avdekket at angriperne systematisk søkte i nedlastet innhold de fikk tak i, etter ytterligere nøkler og tokens som kunne gi enda flere tilganger. Slik fikk angriperne blant annet tak i en AWS API-nøkkel, som igjen ga dem tilgang til GitHubs *Node Package Manager (npm)* produksjonsmiljø, men heldigvis uten at de kunne endre på *npm*-pakker – kun laste ned kode.

Det er flere momenter å legge merke til her. Tyveri av API-nøkler og tilsvarende tokens, skyldes ofte mangelfull applikasjonssikkerhet eller svak håndtering av «secrets» (tokens, nøkler, m.v.) i applikasjoner, utviklings-, bygg- og testmiljøer. Et annet punkt som gjerne er oversett – både i profesjonell applikasjonsutvikling og – bruk, så vel som når vi som enkeltpersoner autoriserer tredjepartstjenester og apper for tilgang til våre konti på f.eks. sosiale medier – er opprydning og fjerning av gamle tillatelser som ikke lengre er i bruk. Det er rimelig å anta at enkelte virksomheter der *Heroku* og *TravisCI* verktøyene var autorisert for tilgang, ikke lenger brukte disse produktene aktivt.

Håndtering og tiltak har også vært gode fra alle involverte parter. GitHub har – uavhengig av hendelsen – utviklet en tjeneste som skanner kode for secrets før den lastes opp til distribusjonskanaler. I et leveransekjede-perspektiv er det imidlertid grunn til å fremheve varsling og handling. GitHub var tidlig ute med å varsle alle berørte brukere, og både *Heroku* og *TravisCI* varslet sine kunder samt iverksatte revokering og ny-utstedelse av tokens og

15 Telenor Digital Sikkerhet 2020: https://www.telenor.no/binaries/om/digital-sikkerhet/Telenor_Digital_Sikkerhet_2020_1.pdf
16 Telenor Digital Sikkerhet 2021: https://www.telenor.no/binaries/om/digital-sikkerhet/digitalsikkerhet2021.pdf

» Tyveri av API-nøkler og tilsvarende tokens, skyldes ofte mangelfull applikasjonssikkerhet eller svak håndtering av *secrets* i applikasjoner, utviklings-, bygg- og testmiljøer.

nøkler for sine tjenester. Det sistnevnte er ingen enkel beslutning, da det påvirker tjenestene og kundene, men likevel den rette for å minimere skade og sikkerhetsrisiko.

Fishpig

Du har kanskje ikke hørt om Fishpig før, men denne programvaren for integrasjon mellom den ekstremt populære publiseringsplattformen *Wordpress* og den svært utbredte netthandelsprogramvaren *Magento*, er i bruk i over 200.000 nettbutikker. Angriperne kompromitterte Fishpig sine distribusjonsservere, dvs. serverne som kundene henter programvare og oppdateringer fra. De lastet opp modifiserte versjoner av programvaren som infiserte kundenes systemer med *Rekoob* trojaneren – som gir angriperne en bakdør inn i kundenes systemer. Skadepotensialet er betydelig, da dette er nettbutikker med betalingsfunksjoner, og *Magento*-baserte nettbutikker har vært et yndet mål for økonomisk motiverte trusselaktører i en årrekke – til dels med store tap.

Det kan være grunn til å stille spørsmål ved sikkerhetsovervåkningen hos Fishpig, da angriperne var inne i om lag 12 uker før det pågående leveransekjedeangrepet ble avdekket (og ikke det faktum at angripere var inne i Fishpig sine systemer). For de teknisk interesserte, finnes flere gode analyser av de mange inkarnasjonene av Linux-trojaneren *Rekoob* siden den ble observert i sin første versjon i 2015, samt de forskjellige rootkitene og teknikkene som er i bruk for å deployere og skjule den.

Fra et leveransekjedeperspektiv er denne type angrep utfordrende å håndtere for kundene, da angriperne lyktes i å få sin kode inkludert i tilsynelatende autentisk programvare. Mekanismer for automatisk oppdatering – som generelt er å anbefale fra et sikkerhetsståsted – begrenser også i noen grad mulighetene til tiltak som f.eks. kjøring i sikkerhetsinstrumenterte test- og sandkassemiljøer før installasjon i produksjon; tiltak som også vil være for ressurskrevende for mange av de aktuelle kundene. *Rekoob* er på den annen side en kjent skadevarefamilie, og *Endpoint Detection and Response* (EDR) verktøy på Linux- serverne vil kunne ha effekt. Det er også viktig å abonnere på, og respondere på, varsler fra sine leverandører. Etter hendelsen har Fishpig utgitt forbilledlig veiledning til berørte kunder – endog verktøy som lar kunder med begrenset kompetanse rydde opp i en kompromittert nettbutikk.

3CX

I mars ble det kjent at programvare fra IP-telefoniselskapet 3CX var kompromittert, og det er uklart over hvor lang tid, men de første rapportene om avvik hos brukerne – først antatt å være falske positivier – kom ut 22. mars 2023. 3CX sin legitime programvare, i bruk hos over 600.000 selskaper og mer enn 12 millioner daglige sluttbrukere, viste seg å ha fått tilskudd av ondsinnet kode for DLL *sideloading*. Litt forenklet forklart, er det instruksjoner i installasjonsrutinen, om å hente ekstra kodebibliotek (DLL) fra en ekstern kilde. Det finnes igjen flere svært omfattende, lærerike og detaljerte tekniske analyser av både skadevaren og angriperens teknikker, som vi ikke skal gjengi her.

3CX-angrepet gir assosiasjoner til Solarwinds-angrepet, og strengt tatt helt tilbake til «APT 1» sine angrep mot *managed service providers* (MSP-er). Felles for APT1, Solarwinds og en portefølje av mellomliggende kampanjer, er evne og vilje til å bruke leveransekjedeangrep som rammer svært bredt, og dermed også nødvendigvis blir ganske synlige, for å i realiteten kun gå etter noen få utvalgte mål. Det er modus som – sammen med fraværet av økonomisk vinning – peker i retning av etterretningsmotiverte aktører.

Fra et leveransekjedeperspektiv merker vi oss at 3CX-angrepet faktisk var muliggjort gjennom et annet *software supply-chain* angrep, på selskapet Trading Technologies og deres programvare for handel med verdipapirer (såkalte futures), *X_Trader*. Flere analyseselskaper og medier omtaler dette som første gang ett programvare-leveransekjedeangrep har ført til et annet. Den infiserte versjonen av *X_Trader* ble ganske enkelt lastet ned og installert av en ansatt hos 3CX. Det er bred konsensus blant analyseselskaper når *X_Trader* kampanjen og det påfølgende angrepet gjennom 3CX' programvare knyttes til Nord-Koreanske *Lazarus Group*. *X_Trader* kampanjen rammet flere andre selskaper, inkludert minst to strømselskaper i hhv. USA og Europa. Den bredt anlagte sekundære kampanjen gjennom 3CX, mål i energisektoren og kompromittering av programvare for verdipapirhandel, åpner for spørsmål om angripers motivasjon primært er økonomisk eller geopolitisk. Selv med sterk attribusjon kan det være vanskelig å konkludere, da *Lazarus Group* operer ut fra begge motiver.

Recursive dependencies – en vedvarende utfordring

Vi ser også at organiseringen av økosystemene av åpen kildekode byr på sikkerhetsmessige utfordringer og mulighetsrom for angripere, blant annet gjennom måten utvikling forholder seg til avhengigheter (*dependencies*), det vil si kode eller en programvaremodul som en annen kode er avhengig av, og derfor henter inn og inkluderer. Slike *dependencies* kan i noen økosystemer, som f.eks. *npm*, være gjentakende i mange lag nedover.

Flere angrepstilnærminger drar nytte av dette, og andre forhold rundt måten utvikling og distribusjon av åpen kildekode er organisert:

Ondsinnede avhengigheter – Event-stream hendelsen[17], 2018
I august 2018 publiserte utvikleren «Antonio Macias» parser-biblioteket *flatmap-stream* på *npm*, og kontaktet ansvarlig utvikler av det mye brukte parser-biblioteket *event-stream* med forslag om å inkludere førstnevnte som en avhengighet (*dependency*) til sistnevnte. I september slippes neste versjon av *event-stream*, der *flatmap-stream* koden er inkludert. I oktober oppdateres kodebasen til *flatmap-stream* med ondsinnet kode. Fra dette tidspunktet inneholder også all ny henting av *event-stream* automatisk denne koden.

Event-stream er en populær pakke, og er selv en *dependency* i minst 3.931 andre pakker. Det reelle målet for angrepet er imidlertid kun ett; den svært populære bitcoin-lommeboken *Copay*. Koden som ble introdusert i *flatmap-stream* er kun virksom som del av *Copay*, der den muliggjør tyveri av bitcoins og private nøkler.

Dependency Confusion – Alex Birsan, 2021
Vi omtalte i Digital Sikkerhet 2021, hvordan sikkerhetsforsker Alex Birsan tidlig dette året demonstrerte «dependency confusion» angrep[18]:

«En ytterligere faktor, som bidrar til å redusere tid og kost, er dynamisk bruk av tredjeparts-biblioteker som Node, JQuery og Chartbeat. Med dynamisk menes at bibliotekene enten lastes ned når applikasjonen bygges eller når den kjører i en nettleser. På den ene siden medvirker ofte slike biblioteker til sikrere kode, ettersom de ofte hjelper programmerere å «gjøre ting riktig», mens de på den andre siden øker risikoen for å bli kompromittert gjennom leverandørkjeden. Dette ble behørig demonstrert i februar da en sikkerhetsforsker beskrev hvordan han hadde utnyttet denne typen dynamisk nedlastning ved å publisere pakker med konseptuell «skadevare» til forskjellige offentlige rammeverk (npm, RubyGems og PyPI) med samme, eller nesten samme, navn som det flere større teknologiselskaper selv benyttet på sine interne moduler.»

Konsekvensen ble at automatiske bygg-verktøy hos de aktuelle virksomhetene, lastet inn Birsan's offentlig publiserte programvarekomponenter med samme navn, i stedet for komponenter fra selskapets private kodebase.

Npm Manifest Confusion attack[19], 2022
Npm pakker har en såkalt «manifest-fil», som inneholder metadata om kodepakken og lister avhengigheter til andre pakker. Den tidligere GitHub-ansatte Darcy Clarke har avdekket at det ikke finnes noen mekanismer som sammenligner den publiserte manifest-filen med den som er inkludert i den *tar*-komprimerte nedlastbare kodepakken. Mange sikkerhetsverktøy, så vel som menneskelig inspeksjon, vil legge informasjonen i den frittstående manifest-filen til grunn, mens det er den inkluderte som faktisk styrer byggprosessen og hvilke *dependencies* som faktisk trekkes inn. Dette gir mulighet for at en utgiver eller angriper kan inkludere ondsinnet eller kjent sårbar kode i den inkluderte manifest-filen, mens den frittstående publiserte manifest-filen ikke trenger nevne det.

Repojacking, 2023
Sikkerhetsselskapet Aqua Security publiserte sommeren 2023 informasjon[20] fra en studie av 1,25 millioner kodeprosjekter på GitHub, der de fant at nær 37.000 av dem var sårbare for såkalt repojacking. Teknikken er enkel, og går ut på at trusselaktører registrerer kodeprosjekter med prosjekt- eller brukernavn som ikke lengre er i bruk. Det kan skyldes at brukerkontoen er kansellert, eller at prosjektet bytter navn – uten at alle andre prosjekter som forsøker å hente inn prosjektets kode blir tilsvarende oppdatert. Dette gir mulighet for trusselaktører, som ved å registrere det gamle navnet får mulighet til å publisere kode som andre automatisk henter inn og bruker i sine prosjekter. Aqua Security har bare scannet et lite utvalg, og uttaler at det den reelle angrepsflaten sannsynlig er flere millioner kodeprosjekter – ikke bare de nær 37.000 identifiserte.

Hva sier norske myndigheter?

Norske myndigheter, gjennom rapporter fra PST, NSM og Etterretningstjenesten, har omtalt forskjellige former for trusler og angrep gjennom leveransekjeder. Vi merker oss særlig nedenstående.

PST: Nasjonal trusselvurdering 2023
«I januar 2022 ble Litauen utsatt for en omfattende og sammensatt reaksjon fra kinesiske myndigheter da landet lot Taiwan få åpne et representasjonskontor i Vilnius. Litauen ble etter hendelsen utsatt for en påvirkningskampanje og flere digitale nettverksoperasjoner. I tillegg ble landet utsatt for omfattende leverandørkjedepress, tjenestestans og andre formelle og uformelle sanksjoner. Samtidig hadde selskaper i Litauen problemer med å få tak i kinesiske deler og komponenter. Kinesiske myndigheter la også press på virksomheter i andre europeiske land for å få dem til å begrense sin handel med selskaper fra Litauen.»

«Det siste året har PST sett at flere statlige etterretningstjenester, eller trusselaktører som opererer på vegne av disse, har gjennomført såkalte verdikjedeangrep. Dette er nettverksoperasjoner rettet mot svake og mer perifere punkt i en virksomhets verdikjede, for eksempel hos underleverandører. Virksomheter med solide datasikkerhetssystemer og -rutiner er sårbare dersom deres underleverandører ikke har tilsvarende sikringstiltak. PST forventer flere nettverksoperasjoner av denne typen i 2023.»

«Statlige aktører benytter et bredt spekter av metoder for å omgå kontrollmekanismer og sikre seg tilgang til teknologi og kunnskap fra norske virksomheter. [...] Virkemidler som falsk dokumentasjon, kompliserte selskapsstrukturer, strå- og frontselskaper og leverandørkjeder vil også benyttes.»

Etterretningstjenesten: Fokus 2023
«Samhandling skaper også sårbarhet. Avhengigheter i forsyningskjeder blottstilles og åpner for utpressing.»

NSM: Risiko 2023
«Selv om en virksomhet har god fysisk og digital sikkerhet, så kan trusselaktører utnytte underleverandører som er langt dårligere sikret for å få tilgang til sine egentlige mål. Dette gjør at vi også må sikre oss godt på flankene.»

«Sikkerheten vår blir ikke bedre enn det svakeste leddet i leverandørkjeden.»

«Lange og uoversiktlige leverandørkjeder utgjør fortsatt en sårbarhet som trusselaktører vet å utnytte. De siste årene har vi sett mange eksempler på at leverandørkjedeangrep mot leverandører av IKT-tjenester med svært store kundebaser får omfattende konsekvenser. »»

17 https://snyk.io/blog/a-post-mortem-of-the-malicious-event-stream-backdoor/
18 https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610
19 https://www.bleepingcomputer.com/news/security/npm-ecosystem-at-risk-from-manifest-confusion-attacks/
20 https://blog.aquasec.com/github-dataset-research-reveals-millions-potentially-vulnerable-to-repojacking

FOTO: ANDREJ VASILENKO / THE NEW YORK TIMES / NTB

Taiwans representasjonskontor i Vilnius, Litauen.

Flere amerikanske etater og byråer har gjort seg bemerket i fremsnakking av behovet for transparens i programvare-leveranser og -leveransekjede, gjennom bl.a. bruk av SBOM.

Utenfor det digitale rom ser vi også at trusselaktører utnytter leverandørkjeder for å oppnå tilgang til sine egentlige mål. Når målet er å ramme en stor virksomhet krever det mindre ressurser å angripe en mindre sikker underleverandør eller enkeltpersoner.»

NSM: Sikkerhetsfaglig råd
«Trusselaktører utnytter at funksjoner og infrastruktur i stat og samfunn henger sammen i uoversiktlige verdikjeder. Hendelser som tilsynelatende er rettet mot verdier ett sted i en verdikjede, kan i realiteten være konstruert for å ramme et egentlig mål et annet sted i verdikjeden.»

«Mangelfull oversikt over leverandørkjeder og fravær av sikkerhetskrav til leverandører i anskaffelser og prosjekter åpner muligheten for at trusselaktører bruker anskaffelsesprosesser som virkemiddel for å få tilgang til verdier. Trusselaktører kan dermed ramme virksomheten gjennom leverandører og underleverandører.»

Software Bill of Materials

Software Bill of Materials (SBOM) er en spesifikasjon av alle komponenter i en programvarepakke. Dette er nå et begrep på alles lepper, men veien hit har vært lang – og det er fortsatt en vei igjen å gå.

SBOM milepæler
Blant milepæler så langt, kan det være grunn til å fremheve:

- Oktober 2015: SWID Tags standarden fra *NIST* publisert som ISO/IEC 19770-2:2015.
- Mars 2018: Versjon 1.0 av *CycloneDX*, en SBOM-standard fra OWASP.
- Desember 2020: ISO publiserer «The ISO International Standard for open source license compliance» (ISO/IEC 5230:2020 – Information technology — OpenChain Specification), med krav om en prosess for håndtering av SBOM for levert programvare.
- 2020/2021: Amerikanske *National Telecommunications and Information Administration* (NTIA) publiserer betydelig arbeid fra sitt *Software Component Transparency initiativ* relater til SBOM.
- Februar 2021: President Biden signerer *Executive Order 14017* on *America's Supply Chain*, med krav om SBOM ved føderale anskaffelser.
- Mai 2021: President Biden signerer *Executive Order 14028 on Improving the Nation's Cybersecurity* med krav om blant annet sikkerhetstesting og sårbarhetshåndtering, og SBOMs rolle i det.
- Juli 2021: NIST publiserer sine *Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028.*
- August 2021: Det åpne SBOM-rammeverket SPDX, fra *Linux Foundation*, blir publisert som standarden ISO/IEC 5962:2021.
- April 2023: Versjon 1.0 av SLSA (Supply-Chain Levels for Software Artifacts) rammeverket publiseres av Open Source Security Foundation.

Til tross for at flere bidrag har fått forankring gjennom de internasjonale standardorganisasjonene ISO og IEC, preges denne listen av amerikanske innslag, noe det primært er to grunner til; for det første er teknologibransjen og dens aktører – både på ideell og kommersiell side – i stor grad USA-basert. For det andre er det mye markedsmessig «kjøttvekt» i det når føderal sektor i USA begynner å stille krav til alle sine teknologileverandører, som fører til at effektuering og operasjonalisering av bl.a. EO 14017 og 14028 – gjennom en rekke direktiver og sertifiseringer som vi ikke redegjør for i detalj her – har global effekt ved å tvinge aktuelle leverandører til samsvar. Blant annet i forhold til å sikre sine programvare-utviklingsmiljøer, ha oversikt over sine programvare- leveransekjeder, og kunne dokumentere sine programvareleveranser gjennom SBOM.

En tydeligere plass i faglige råd
Flere amerikanske etater og byråer har gjort seg bemerket i fremsnakking av behovet for transparens i programvareleveranser og -leveransekjede, gjennom bl.a. bruk av SBOM. Det finnes omfattende introduksjons- og opplæringsmateriale hos blant annet National Telecommunications and Information Administration (NTIA)[21] og ikke minst det svært produktive Cybersecurity and Infrastructure Security Agency (CISA)[22], der sistnevnte blant annet uttaler:

21 https://ntia.gov/page/software-bill-materials
22 https://www.cisa.gov/sbom

«A «software bill of materials» (SBOM) has emerged as a key building block in software security and software supply chain risk management. A SBOM is a nested inventory, a list of ingredients that make up software components. The SBOM work has advanced since 2018 as a collaborative community effort, driven by National Telecommunications and Information Administration's (NTIA) multistakeholder process.

CISA will advance the SBOM work by facilitating community engagement, development, and progress, with a focus on scaling and operationalization, as well as tools, new technologies, and new use cases. This website will also be a nexus for the broader set of SBOM resources across the digital ecosystem and around the world.

An SBOM-related concept is the Vulnerability Exploitability eXchange (VEX). A VEX document is an attestation, a form of a security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities.»

Også i Europa har SBOM fått økt oppmerksomhet fra myndighetssiden, blant annet fra ENISA, som i sin «Threat Landscape 2022» uttaler:

«It is almost-certain that adversaries will further abuse this lack of visibility into dependencies, as well as the increased complexity and the trust organisations put into their suppliers, to gain a foothold within organisations. We need to highlight initiatives such as the Software Bill of Materials (SBOM) that aim at making such things more transparent and auditable.

Et utvalg aktuelle spesifikasjoner og rammeverk

CSAF: Common Security Advisory Framework[23] (CSAF) er en spesifikasjon fra OASIS for utveksling av strukturerte maskinlesbare sikkerhetsvarsler («Security Advisories»). Overgangen til omforente maskinlesbare strukturer for security advisories, fremfor prosatekst som må utformes og konsumeres av mennesker, er avgjørende for automatisering – både ved generering, men spesielt i forhold til mottak, behandling og videre anvendelse av informasjonen i håndtering av sårbarheter.

VEX: Vulnerability Exploitability eXchange (VEX) er et strukturert format for sårbarhetsinformasjon, mer spesifikt fokusert på å kommunisere hvorvidt en programvare er sårbar for en bestemt sårbarhet, og anbefalinger til håndtering. VEX er en informasjonsprofil i CSAF, men VEX-meldinger kan også være del av andre spesifiserte informasjonsstrukturer, f.eks. CycloneDX.

CycloneDX: OWASP CycloneDX[24] er en omfattende Bill of Materials (BOM) standard som ikke bare spesifiserer en struktur for Software Bill of Materials (SBOM), men også:
- Software-as-a-Service Bill of Materials (SaaSBOM),
- Hardware Bill of Materials (HBOM),
- Operations Bill of Materials (OBOM), og
- Vulnerability Disclosure Reports (VDR).

CycloneDX har også en profil for Vulnerability Exploitability eXchange (VEX)

SPDX: Software Packaged Data Exchange[25] er et en åpen standard for SBOM-format; støttet av et konsortium av aktører fra teknologiindustrien. Den er nå også formelt standardisert som ISO/IEC 5962:2021.

SWID: Software Identification (SWID) Tags er et format for å beskrive et software-objekt, og springer ut av software asset inventory og -management tilbake til 2012, da det først ble spesifisert som en ISO-standard. Siste gjeldende formelle standard er ISO/IEC 19770-2:2015. Formatet er del av spesifikasjonene til bl.a. Trusted Computing Group (TCG) og Internet Engineering Task Force (IETF). En SWID tag kan også være del av en CycloneDX SBOM.

SLSA: Supply-chain Levels for Software Artifacts[26] er et sikkerhetsrammeverk for programvaretilvirkning og -distribusjon. Rammeverket omfatter retningslinjer, sjekklister og controller for å motvirke illegitim påvirkning av primært programvarens integritet, i alle ledd fra produksjon til anvendelse. Der SBOM kan sammenlignes med ingredienslisten på matvarer, kan SLSA sammenlignes med retningslinjer for trygg tilvirkning, distribusjon og oppbevaring av næringsmidler. Vi sier «tilvirkning», og ikke utvikling, da SLSA ikke dekker sikkerhetskvalitet i koden som skrives, men fokuserer på hva som skjer deretter. Rammeverket er til nytte både for produsenter og konsumenter – gjennom å hhv. veilede i og måle god sikkerhetspraksis.

23 https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html
24 https://cyclonedx.org
25 https://spdx.dev
26 https://slsa.dev/

Gaining visibility into the web of third-party relationships and dependencies is a must.»

ENISA understreker tilsvarende i «*Good Practices for Supply Chain Cybersecurity*» (vår utheving), og knytter det – i likhet med CISA – til sårbarhetshåndtering:

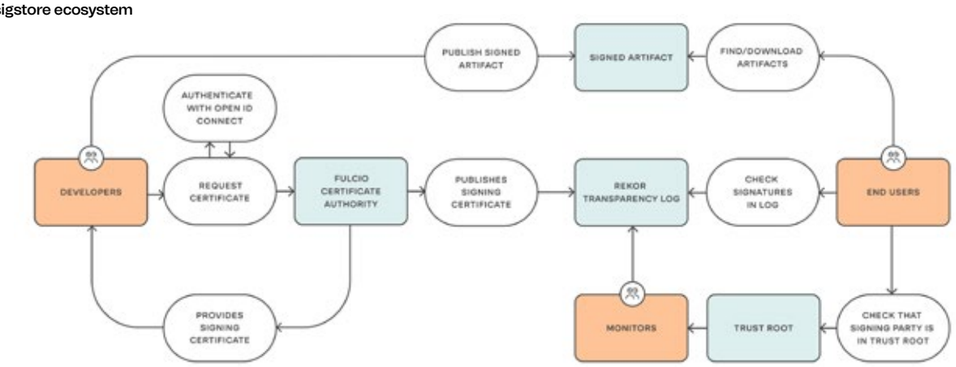
«The handling of vulnerabilities has two aspects; one aspect is the monitoring of vulnerabilities which leads to an analysis on the vulnerabilities identified up to a patch delivered and deployed. The other aspect is the publishing of advisories, i.e. the vulnerability notifications. A vulnerability notification has the objective to warn product users of critical vulnerabilities and might recommend alternative mitigation measures to minimise the likelihood of an exposure. Tools that support the operators as well as the developers towards this direction are the software bill of materials and Vulnerability Exploitability eXchange concepts, and the Common Security Advisory Framework.»

Fortsatt skepsis – Høna og egget

Samtidig som SBOM, sammen med VEX og CSAF, framsnakkes av både sikkerhetsfolk generelt og premissgivende myndigheter spesielt, finner man fortsatt også en del skepsis. Mange kritikere stiller seg tvilende til verdien av SBOM, all den tid mange av mottakerne ikke har prosesser og verktøy på plass for å nyttiggjøre seg informasjonen. Den strukturerte informasjonen må mottas og integreres i virksomhetens prosesser og systemer, blant annet for *asset inventory* og sårbarhetshåndtering, for å kunne gi reell verdi. Overføring og prosessering må også ha en verktøystøtte som tilrettelegger for høy grad av automasjon, da informasjonen er dynamisk og oppdateres hyppig. Det er legitimt å stille spørsmål til verdien av å kreve SBOM for all levert programvare, all den tid svært mange virksomheter har store utfordringer med grunnleggende prosessere og verktøy for å vite hva de har (*inventory*) og håndtere sårbarheter og sårbarhetsinformasjon (*vulnerability management*). Også sårbarhetsinformasjon må produseres, distribueres og konsumeres på maskinlesbare formater som muliggjør automasjon.

Dette er til dels en klassisk «høna og egget» problemstilling; ingen investerer i verktøy for å håndtere informasjon som ikke finnes; og få ser behov for å stille krav om – eller tilby – informasjon som få har kapasiteter til å nyttiggjøre seg. De aller fleste er imidlertid enige om at kontroll på hva du har og hvilke sårbarheter det inneholder, er en forutsetning for tilstrekkelig digital sikkerhet. Ett sted må man da begynne, og som for høna og egget, finnes det faktisk et svar[27]. Også hos programvareprodusentene må det verktøy på plass for å kunne generere SBOM og VEX data på en ressurseffektiv og agil måte – og også denne verktøystøtten kan ta tid å innføre. Det er derfor ingen grunn til å vente med å stille krav – og imøtekomme dem. Uten krav skjer det ingenting, og vi må vente lenge på både høns og egg. Det må først finnes informasjon å behandle – selv om verktøyene og prosessene for å behandle den optimalt og få maksimal verdi av den ennå mangler i mange virksomheter, og tilsvarende gjenstår å innføre hos mange programvareprodusenter. Vi har ikke råd til å bli stående i status quo. Selv om parallellen til utrulling av hydrogen som drivstoff er lett å se – der få vil bygge fyllestasjoner når det er få kunder, og få vil kjøpe hydrogenbiler når det er få fyllestasjoner – er dagens situasjon i håndtering av programvare og programvaresikkerhet mye mer prekær. Dagens praksis virker ikke, og skalerer ikke. Overgangen til høy automasjonsgrad i utveksling og bruk av informasjon, bør heller sammenlignes med å gå fra hest og kjerre til motordrevne kjøretøy.

The sigstore ecosystem



KILDE: HTTPS://SIGSTORE.DEV/HOW-IT-WORKS

27 https://www.science.org.au/curious/earth-environment/which-came-first-chicken-or-egg

FOTO: AFP PHOTO / SATELLITE IMAGE ©2021 MAXAR TECHNOLOGIES / NTB

Containerskipet Ever Given gikk på grunn i Suezkanalen, våren 2021.

Sikring av autentisitet i åpen kildekode – flere initiativer på trappene

Selv om signering av kode og publisering av sjekksummer som kan kontrolleres ved nedlasting er langt fra nytt, har helhetlige og enhetlige løsninger for skalerbar signering og sporbar autentisitet for åpen kildekode vært mangelvare. Dette har ført til at mye bruk av åpen kildekode komponenter i programvareprosjekter enten skjer gjennom tillit på mangelfullt grunnlag, eller avhenger av retrospektiv kontroll ved bruk av tredjepartsverktøy som leter etter «known bad». Signering og sporbar autentisitet for open source komponenter, biblioteker, avbildninger med videre, har derfor fått økende oppmerksomhet. Ett slikt rammeverk er *Sigstore*[28], med Google, Redhat, Linux Foundation, Chainguard og Purdue University i ryggen.

En annen tilnærming for å komme i forkant, fremfor å lete etter og avdekke ondsinnet påvirkning i etterkant, er tredjeparter som gjør sikkerhetsverifikasjon av populær åpen kildekode og re-publiserer den i egne distribusjonskanaler. En slik tjeneste som har fått mye oppmerksomhet siden lanseringen i 2022 er Google Assured Open Source Software. Mens Sigstore ivaretar verifiserbar og sporbar opprinnelse og autentisitet, går Google Assured Open Source Software betydelig lengre, med blant annet;

- build-prosess og dokumentasjon iht. SLSA-2,
- omfattende SBOM for hver pakke, med supplerende informasjon som f.eks. sårbarhetsinformasjon, i SPDX og VEX formatene
- fuzzing og sårbarhetstesting
- distribusjon fra infrastruktur driftet og sikret av Google.

Kontinuitets- og tilgjengelighetsrisiko i leveransekjedene

Flere hendelser har – til dels sammenfallende – gitt store utfordringer i leveransekontinuitet de siste par årene, og vist en annen type leveransekjederisiko; risikoen for kontinuitets- og tilgjengelighetsbrudd i leveransene. Både samfunnspåvirkningen fra Covid-19-pandemien, ett skip fast i Suez-kanalen[30], økt geopolitisk spenning med konflikt på flere arenaer, inkludert handel, og krigsutbrudd i Europa, har hvert på sitt vis bidratt til å påvirke leveransekontinuitet – og synliggjort hvor avhengige og sårbare vi har blitt.

Jakten på effektivitet

Siden opprinnelsen i Japan på 50- og 60-tallet, har *just-in-time* produksjon bredt om seg som den rette skole for ressurs- og kapitaloptimalisert produksjon. Konseptet, og den nødvendige *just-in-time* logistikken penetrerer nedover i hele verdikjeden,

28 https://www.sigstore.dev/
29 https://cloud.google.com/assured-open-source-software
30 https://en.wikipedia.org/wiki/Ever_Given

og har i løpet av 70- til 90-tallet nådd global utbredelse på tvers av bransjer. Kort sagt; ingenting produseres eller leveres til neste ledd i leveransekjeden før det foreligger, eller er bestilt eller prognostisert å foreligge, et konkret behov. Det er få eller ingen buffere; alle prosesser er optimalisert, og lagerhold er ansett å være «waste» (jf. Lean / Kaizen).

Dette gir et stort koordineringsbehov, stor sårbarhet for følgekonsekvenser ved forstyrrelser i ett ledd i leveransekjeden, og ingen av delene blir noe bedre når leverandørleddene blir mer spesialiserte, leverandørene derfor flere, og leveransekjedene stadig dypere og bredere. Det har drevet frem en helt annen dimensjon av risiko i leveransekjeder; leveransekontinuitetsrisiko. Om vi skal definere dette som del av *sikkerhetsrisiko* kunne sikkert ansporet mang en interessant fag- og semantikkdiskusjon, men det er uansett en risikodimensjon som siden forrige gang vi adresserte leverandør- og leveransekjeder i *Digital Sikkerhet*, både har manifestert seg og fått økt oppmerksomhet. I kontekst av en stadig tilspisset geopolitisk situasjon, er også kontroll på leveranse av kritiske varer og innsatsfaktorer blitt et «våpen».

Leveransekjeden – del av kontinuitet og resiliens
I Digital Sikkerhet 2022[31] tok vi, i stor grad basert på erfaringene med forstyrrelser i leveransekjedene og akutte behov som oppstod i Ukraina i ukene og månedene etter invasjonen, til orde for at vi i Norge bør vurdere å opprette buffer-lagre av standard IKT-komponenter. Dette er imidlertid kun ett forslag innenfor – grovt sett – én bransje, og har til dels adresse til norske myndigheter ut fra en refleksjon om at dette er en form for grunnleggende nasjonal ressurs.

For virksomheter generelt, også aktører i kritiske sektorer med *grunnleggende nasjonale funksjoner*, må imidlertid vurdering av leveransekontinuitetsrisiko, og tiltak for å håndtere den, inngå i den enkelte virksomhets planer for *kontinuitet* og *resiliens*.

Dette åpner en Pandoras eske av informasjonsbehov:
> Har vi oversikt over våre kritiske innsatsfaktorer og vet vi hvem de kritiske leverandørene er?
> Har vi tatt høyde for at også bortfall av innsatsfaktorer som i sin natur fremstår mindre kritiske, likevel kan påføre virksomheten kontinuitetsavbrudd ved bortfall?
> Vet vi hvem de kritiske underleverandørene til leverandørene er, og hvor langt ned i kjeden klarer vi å skaffe oss oversikt?

Det motiverer også nytenkning i forhold til potensielle former for tiltak:
> Gitt påregnelige scenarier i en uforutsigbar verden med tilspisset geopolitikk, kan det være riktig å binde mer kapital i lagerhold av kritiske komponenter?

Fra Telenor Digital Sikkerhet 2022:

Det bør vurderes om det skal opprettes nasjonale beredskapslagre for standard / «Commercial Off-the-Shelf» IKT-komponenter. Prioriterte produktkategorier og produkter vil trenge en nærmere analyse, men både grunnleggende nettverksutstyr, servere og sluttbrukerutstyr vil være relevant. Beredskapslagrene kan fungere som nasjonal buffer, med kontinuerlig gjennomstrømning. Ordningen må være forpliktende for «medlemsvirksomhetene» for å sikre at produktkategoriene ikke holdes på lager i lang tid og blir utdatert. Virksomhetene vi snakker om her er primært offentlige og private eiere av kritisk infrastruktur som understøtter sentrale samfunnsfunksjoner.

- Kan vi samarbeide med noen om det? Kanskje til og med konkurrentene? Kan bransjeorganisasjoner spille en rolle i koordinering av felles tiltak?
- Klarer vi å få til slikt samarbeid mellom konkurrenter uten å gå på kompromiss med konkurranse- og kartellregler?

> Bør vi diversifisere leveransekjeden og spre leveransekontinuitetsrisikoen ved å etablere flere alternative leverandører for samme kritiske innsatsfaktorer?
- Vet vi da at de to primære leverandørene ikke har de samme kritiske innsatsfaktorene / underleverandørene?
- Står den økte sikkerhetsrisikoen som følger av en bredere leveransekjede, der flere leverandører kommer i posisjon som utgangspunkt for leveransekjedeangrep mot oss, i forhold til den reduserte leveransekontinuitetsrisikoen?

Belyst av kommisjonene
Både Forsvarskommisjonen og Totalberedskapskommisjonen legger i sine vurderinger, både generelt og innenfor spesifikke sektorer, stor vekt på beredskap og resiliens. Sårbarheten lange og uoversiktlige leveransekjeder gir i så måte, blir grundig drøftet, med tydelige konklusjoner om behov for styrking og tiltak – primært initiert av, men slett ikke kun i regi av, myndighetsapparatet. Det er også slik at mange kritiske komponenter produseres av svært få geografisk konsentrerte aktører, eller avhengig av innsatsfaktorer (mineraler, m.m.) hvor aktive kilder er geografisk konsentrert. Også sårbarheten som følger av super-effektive just-in-time verdikjeder blir belyst. Blant kommisjonenes tiltak finner vi styrket evne til selvforsyning, buffere og beredskapslagre, leverandørdiversitet for å ha flere ben, og stramme retningslinjer ift. hvilke opprinnelsesland vi skal tørre å eksponere oss mot eller gjøre oss avhengige av leveranser fra.

31 Telenor Digital sikkerhet 2022: https://www.telenor.no/binaries/om/digital-sikkerhet/2022/Digital_sikkerhet_2022.pdf

Fra Totalberedskapskommisjonens rapport (NOU 2023:17) vil vi blant annet fremheve:

«Det er behov for større robusthet med tanke på lagring av kritiske innsatsfaktorer og økt egenberedskap. Vi har bak oss en lang periode med globalisering og stadig mer effektive, men komplekse internasjonale forsyningskjeder. Dette har gitt oss rimelige handelsvarer. Samtidig har våre egne lagre blitt bygget ned, og på enkelte områder har vi gjort oss avhengige av land og regioner vi ikke har interessefellesskap med.»

«Kina fortsetter å utfordre det vestlige fellesskapet på flere måter. Landet søker å kontrollere strategisk infrastruktur, ressurser og verdikjeder.»

«Pandemien og krigen i Ukraina har synliggjort sårbarheter knyttet til tilgang på kompetanse og materiell. Det er ikke gitt at spesialisert kompetanse og reservedeler alltid er tilgjengelige fra utlandet.»

«Samfunnsfunksjoner blir i økende grad avhengige av lange og uoversiktlige digitale verdikjeder, noe som gjør det mer krevende å ha kontroll på alle involverte aktører og underleverandører. Avhengigheter i flere ledd gir økt risiko for at sårbarheter utnyttes, at digitale tjenester blir utilgjengelige, at uvedkommende får tilgang til sensitivt innhold, og at innhold endres slik at det er usikkert hva som er ekte eller falskt.»

«Den tette koblingen mellom digitale systemer og lange digitale verdikjeder med ofte ukjente avhengigheter til et stort antall aktører, kompliserer arbeidet med digital sikkerhet ytterligere.»
«Kommisjonen mener at digitale tjenester er blitt så viktige for å ivareta kritiske samfunnsfunksjoner at myndighetene må ta et større ansvar for sikkerhet gjennom verdikjeder og på tvers av alle samfunnssektorer.»

«For å redusere digitale sårbarheter nasjonalt i kritisk infrastruktur har det samtidig blitt viktigere å avgjøre hvilke land man ikke vil ha materiell fra eller andre former for avhengighet til. Kommisjonen mener at norske myndigheter fremover, i enda større grad, må legge premisser og gi råd med hensyn til hvilke land, teknologier og tjenester som anses å utgjøre en risiko for nasjonal sikkerhet.» //

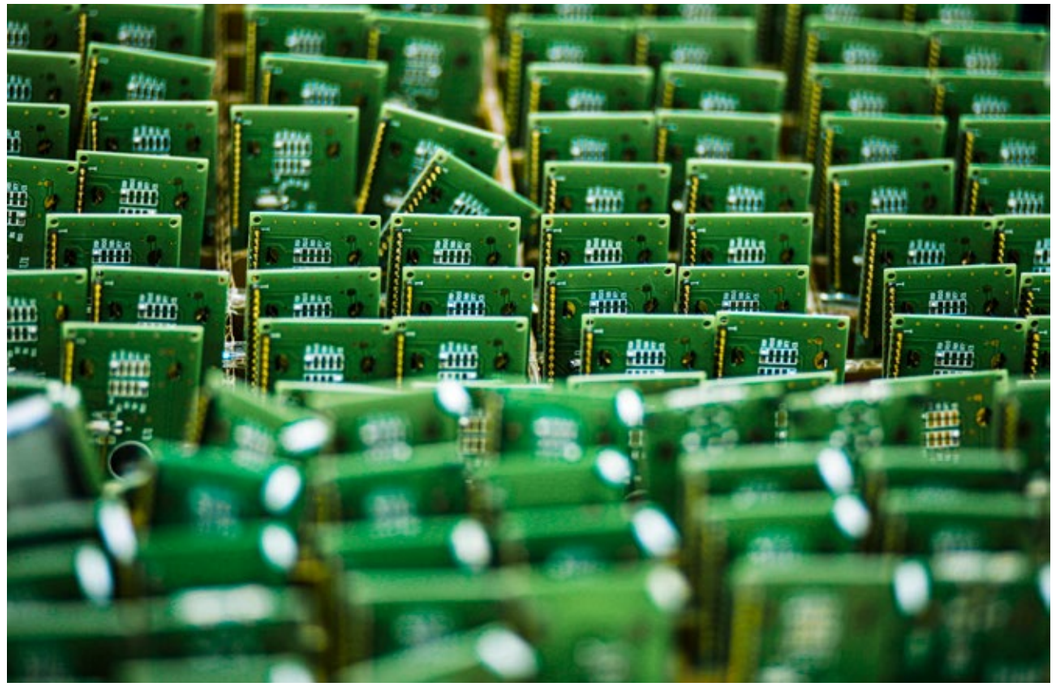


FOTO: GETTY IMAGES

FOTO: GUNNAR RIDDERSTRØM / UNSPLASH

FOTO: GETTY IMAGES

En stor andel av all datatrafikk i Norge går gjennom Telenors tjenester og infrastruktur. Det gir oss et betydelig samfunnsansvar og innebærer at vi må levere stabile og trygge tjenester i fred, konflikt, krise og krig.

8

Et annet alvor

Vi lever i en internasjonal skjebnetid. Russlands invasjon av Ukraina medfører varig endring av den sikkerhetspolitiske situasjonen i våre nærområder. Økt geopolitisk spenning stiller eiere av kritisk infrastruktur overfor et stadig mer komplekst trussel- og risikobilde. Global endringer vil påvirke våre valg. Private selskap må være en del av totalberedskapen. Flere felles løsninger må utvikles i en nordisk og alliert ramme. Vi må være beredt.

Alt må virke
En moderne infrastruktur forutsetter et solid og sikkert fundament, der sårbarhet er redusert til et minimum. Premisset for den digitale grunnmuren i 2023 er at alt må virke hele tiden. Å lykkes med dette vil være avgjørende for hvor godt vi lykkes med å forenkle, forbedre og fornye i egen virksomhet og understøtte digitalisering av samfunnet.

Den endrede sikkerhetspolitiske situasjonen påvirker våre valg. Telenor har over de siste 10-12 årene bygd et helhetlig sikkerhetsmiljø i Telenor i Norge for å beskytte oss selv, våre kunder og ivareta vårt samfunnsansvar. Vi jobber systematisk innen tre områder: Sikkerhet, robusthet og beredskap. For at vi bygger, drifter og utvikler en så trygg og sikker digital infrastruktur som mulig. Vi har økt årvåkenhet både i det digitale og fysiske domenet, lavere terskel for å varsle, og enda tettere samarbeid med myndighetene, som Nasjonal sikkerhetsmyndighet (NSM) og Nasjonal kommunikasjonsmyndighet (Nkom).

Møte det teknologiske og geostrategiske skiftet
Det siste året har vi fått en rekke viktige rapporter som gir grunnlag for et styrket arbeid med sikkerhet og beredskap. Forsvarskommisjonen har anbefalt at det utarbeides en nasjonal sikkerhetsstrategi, at Statsministerens kontor (SMK) får tilført mer stabskraft, samt at kriserådets rolle bør utvides for å styrke evnen til tverrsektoriell situasjonsforståelse og krisehåndtering på tvers av sektorer.

Totalberedskapskommisjonen har foreslått et mer robust beredskapssystem, tilpasset vår tids utfordringer for å kunne håndtere kriser i hele krisespektret. I rapporten beskrives et forbedret beredskapssystem med motstandsdyktighet mot alle former for fare, i hele krisespektret og så lenge situasjonen varer. Kommisjonen oppsummerer sine hovedanbefalinger i ti punkter, der en rekke av disse berører Telenors virksomhet. Særskilt tettere integrering av næringslivet i den nasjonale beredskapsstrukturen, utvidet nordisk beredskapssamarbeid og forsterket arbeid med infrastruktur og digital sikkerhet er av strategisk viktighet for vår virksomhet.

Summen av endringer i globale maktforhold, økt regional ustabilitet, fragmentering av det internasjonale systemet og høyere risikovilje for maktbruk mot andre stater markerer en ny sikkerhetspolitisk situasjon. Europa vil i årene som kommer måtte ta langt større ansvar for egen sikkerhet. Det samme gjelder i høy grad for Norge, som en rik og sårbar liten stat med et åpent demokratisk samfunn, en utadrettet økonomi i et geopolitisk utsatt område.
fra NOU 2023: 14 Forsvarskommisjonen av 2021
- kapittel 17.1 En ny tid

Telenors rolle som beredskapsaktør

Telenor i Norge eier og forvalter samfunnskritisk infrastruktur, og sørger for trygge og stabile leveranser av digitale tjenester på mobil, fastnett og bredbånd. Dette inkluderer å levere tale, data og sms som grunnleggende nasjonale funksjoner (GNFer), som er kritiske for at det norske samfunnet fungerer. En stor andel av all datatrafikk i Norge går gjennom våre tjenester og infrastruktur. Det gir oss et betydelig samfunnsansvar og innebærer at vi må levere stabile og trygge tjenester i fred, konflikt, krise og krig. Vi erkjenner at vi er et mål for avanserte trusselaktører. Vår virksomhet er underlagt sikkerhetsloven.

For private virksomheter som Telenor har det vært viktig å understreke at styring og samarbeid må formaliseres for at vi skal få et mer effektivt totalforsvar innen disse områdene, der også private virksomheter og selskaper mer systematisk trekkes med. Private virksomheter innen olje og gass, kraft, mat, og ekom er betydningsfulle aktører for opprettholdelse av samfunnssikkerhet og statssikkerhet fordi de eier kritisk infrastruktur. De har en naturlig rolle i totalforsvaret for å gi innsikt og kompetanse om funksjonene de opprettholder, og avhengighetene de har til andre. At sikkerhetsloven ikke er fullt ut implementert i alle sektorer er et hinder for dette.

Nye muligheter med hele Norden i NATO
Vi har lange tradisjoner for å samarbeide tett i Norden. Med Sverige og Finland i NATO ligger alt til rette for ytterligere nordisk samarbeid også i det digitale domenet. Et slikt samarbeid er viktig med tanke på stabil og trygg infrastruktur i krise og krig. Erfaringene fra Ukraina, der det internasjonale samfunnet og industripartnere har stilt opp, viser viktigheten av internasjonalt samarbeid for å kunne holde digitale tjenester og infrastruktur oppe. Et slikt samarbeid kan utvikles til å bli viktig i den nordiske regionen.

Det er positivt at *«regjeringen vil kartlegge strategisk viktig infrastruktur for å identifisere hvilke allierte og nære partnere vi er mest avhengig av for å sikre nasjonal kontroll, og etablere et tett, forpliktende og forutsigbart samarbeid med disse»*. Det er samtidig behov for økt grad av samarbeid på tvers av landegrensene. Sikkerhetssituasjonen vi står overfor i dag har et annet alvor enn tidligere. Det krever nye strategier og valg. Et tettere nordisk samarbeid vil kunne bidra til rask effekt dersom nordiske industripartnere kan mobilisere innovasjonskraft innenfor rammeverk som bygger på strategiske samarbeidsavtaler.

Vi har merket oss initiativet om mer forpliktende samarbeid og integrasjon mellom de nordiske landene på forsvarsfeltet, og ser det som naturlig at dette sees i sammenheng med tilsvarende prosesser på sivil side. Det er etter vår oppfatning nå svært viktig for ekombransjen å formalisere muligheten for å dele tekniske løsninger og infrastruktur på tvers i Norden, innenfor rammen av forsvarlig sikkerhet, for økt motstandsdyktighet og utholdenhet.

Flere aktører i den norske ekomsektoren har i innspill til kommisjonen understreket at de definerer hele Norden som sitt hjemmemarked. Innenfor rammene av forsvarlig sikkerhet mener Telenor at autonomi må forstås i en nordisk kontekst. I den endrede sikkerhetspolitiske situasjonen vises det til initiativet om mer forpliktende samarbeid og integrasjon mellom de nordiske landene på forsvarsfeltet. Det ytres i den forbindelse ønske om et nordisk initiativ innen sektoren for å benytte knappe personalressurser mellom nordiske naboland og benytte tekniske løsninger og infrastruktur som fiber og datasentre på tvers av land i Norden. Dette vil styrke den nasjonale forsyningssikkerheten med flere ressurser nær Norge, og det vil styrke den nordiske regionen totalt sett og stimulere de multinasjonale teknologileverandørene til å etablere kompetansemiljøer i Norden.
fra Totalberedskapskommisjonens NOU 2023: 17
- Nå er det alvor

Telenor har spesielt merket seg at Totalberedskapskommisjonen anbefaler at *«Norske myndigheter ved finsk og svensk Nato-medlemskap tar initiativ til samarbeid om digital sikkerhet og økt beredskap i Norden»*. Etter Telenors vurdering trengs et nordisk initiativ for å bedre benytte tekniske løsninger og infrastruktur som fiber og datasentre på tvers av land i Norden og for felles nytte av begrensede personalressurser. Dette vil styrke den nasjonale forsyningssikkerheten med flere ressurser nær Norge, og den nordiske regionen totalt sett og stimulere de multinasjonale teknologileverandørene til å etablere kompetansemiljøer i Norden. Et slikt samarbeid vil kreve endringer og harmonisering av nasjonale regelverk. Dette arbeidet bør iverksettes straks.

Tettere integrering av næringslivet
Det er positivt med en økende erkjennelse av næringslivet som beredskapsaktør og beredskapsressurs. I et beredskapsperspektiv er det helt avgjørende, som blant annet Totalberedskapskommisjonen har understreket at *«næringslivet er tettere knyttet til beredskaps- og krise-håndteringssystemene fra det sentrale nivået til de regionale og lokale nivåene»*.

Telenor opplever å være en anerkjent Totalforsvarsaktør. Det er ikke i departementer eller direktorater at Grunnleggende nasjonale funksjoner (GNF) blir rammet, det vil være i offentlige og private, sivile og militære virksomheter. Slike aktører med samfunnskritisk funksjon må derfor innpasses bedre i Totalforsvaret for å gi innsikt og kompetanse som trengs for å kunne være bedre forberedt på å virke sammen i konflikt, krise og krig. Dette vil kreve formalisering og et betydelig videre arbeid for å få effekt.

Regjering og Storting har, basert på kommisjonenes rapporter, et sjeldent godt grunnlag for å klargjøre rammer, roller og forventninger til samfunnskritiske virksomheter i privat sektor. En slik styrking av beredskapsevnen bør drives av et behov for innovasjon, nytenkning og bærekraftig verdiskapning. En mer strategisk tilnærming til utvikling og beskyttelse av kompetanse og teknologi innen kritisk kommunikasjon bør prioriteres.

Styrke evnen til digital hendelseshåndtering
Telenor merker seg regjeringens ambisjon om at den «nasjonale innsatsen bør kraftsamles» knyttet til nasjonal hendelseshåndtering. Etter Telenors oppfatning er det behov for et styrket tverrsektorielt samarbeid som samler alle domener, og hvor både offentlige og private aktører er med. Etter vår oppfatning kommer sektorprinsippet og tilhørende fragmentert koordinering til kort i denne forbindelse.

Telenor merket seg Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor, jf. Dokument 3:7 (2022–2023). Riksrevisjonen bekrefter at «[s]vak samordning av roller, ansvar og krav gjør arbeidet med digital sikkerhet krevende for virksomhetene», at det ikke er «lagt godt nok til rette for tverssektoriell hendelseshåndtering», og at det er «det er behov for mer øving av tverrsektoriell håndtering av hendelser på nasjonalt nivå». Telenor deler disse vurderingene.

Øve og trene
Telenor har tidligere tatt til orde for øvelser på tvers av sektorer hvor vi får testet samvirke, samhandling, ledelse og koordinering som kan ha relevans for å kunne håndtere faktiske hendelser. I denne sammenhengen må viktigheten av at det øves på reelle scenarier understrekes.

Etter Telenors vurdering vil økt bruk av øvelser kunne bidra til styrket tverrsektorielt samvirke og ledelse på strategisk, operasjonelt og taktisk nivå. God felles situasjonsforståelse, ikke bare informasjonsdeling, vil og sette alle med beredskapsansvar bedre i stand til å forstå hendelser i kontekst og å fange opp helheten i hybride operasjoner. Øvelser er også en god arena »»

Kriserådets rolle bør utvides for å styrke evnen til tverrsektoriell situasjonsforståelse og krisehåndtering på tvers av sektorer. Antall medlemmer bør utvides til en bredt sammensatt embetsgruppe med representanter fra alle sentrale beredskapsaktører, næringslivet og det regionale nivået. Dette vil både styrke analysearbeidet og legge til rette for bedre og bredere beslutningsgrunnlag for regjeringen. Sentralt totalforsvarsforum bør utvikles til et nasjonalt totalforsvars- og beredskapsråd med en styrket myndighet som rådgiver for regjeringen, både med hensyn til forebygging, beredskap og nasjonal krisehåndtering. Dette rådet bør ha et fleksibelt format som kan tilpasses og utvides, og der utvalgte kommersielle virksomheter og partene i arbeidslivet inkluderes.
fra NOU 2023: 14 - kapittel 17.2.2 Nye krav til styring, ledelse og ressursbruk

Øvelse Bukkesprang

Telenor Norge har siden 2017 arrangert «Øvelse Bukkesprang», Norges største og tverrsektorielle «live fire»-øvelse i digital hendelseshåndtering. I samarbeid med Cyberforsvaret og Nasjonal sikkerhetsmyndighet (NSM) samler Telenor Norge deltakere fra sentrale aktører i offentlig sivil, militær og privat sektor på Fornebu, hvor vi øver i dedikert infrastruktur med tekniske spor etter simulerte trusselaktører av høyst realistisk karakter. I løpet av en ukelang øvelse oppnår vi erfaring, kunnskapsutveksling og nettverksbygging på tvers av sektorer. Det overordnede målet med øvelsen er å styrke totalforsvaret av Norge. Øvelsen er unik i norsk sammenheng, og et viktig bidrag til den digitale totalberedskapen.

» for å bygge kjennskap til hverandres kapabiliteter og arbeidsmetodikk, samt utvikle nettverk og relasjoner mellom nøkkelpersoner hos kritiske totalberedskapsaktører.

Informasjonsdeling og plattform for samhandling
Styrket samhandling mellom norske sikkerhetsmyndigheter, Forsvaret, Politiet og andre naturlige samarbeidspartnere i sivil sektor er avgjørende for å oppnå et mer robust og sikkert beredskapssamvirke i Norge. Samarbeidet i dag mangler grunnleggende innsatsfaktorer, er for fragmentert og på enkelte områder fortsatt mer dugnadsorientert enn forpliktende.

Blant annet har ikke virksomheter tilstrekkelig tilgang til oppdatert trussel- og sikkerhetsinformasjon. I tillegg mangler mange virksomheter, som fremhevet i NSMs sikkerhetsfaglige råd, løsninger for sikkerhetsgradert samhandling. Dette er spesielt alvorlig når det gjelder virksomheter som er en del av Totalforsvaret.

En særskilt utfordring er at det per i dag ikke finnes kommersielle datasentre eller offentlige skyplattformer tilrettelagt for virksomheter underlagt sikkerhetsloven. Et stadig økende antall virksomheter vil få et behov for skyplattformer og datasenter til utpekte skjermingsverdige systemer eller behandling av skjermingsverdig informasjon. Det er derfor viktig at myndighetene i ulike relevante prosesser, som konseptvalg for nasjonal skyløsning eller regulering av datasentre, bidrar til at dette kan realiseres.

Datasentre og skytjenester for sensitiv informasjon, funksjoner og infrastruktur av betydning for nasjonale sikkerhetsinteresser bør etableres i Norge. Datakraft må sikres gjennom distribuerte skytjenester i regionale og lokale datasentre i Norge og beredskapsavtaler med nære allierte i tilfelle krise.
fra Sikkehetsfaglig råd – Et motstandsdyktig Norge, Nasjonal Sikkerhetsmyndighet 2023

Harmonisert sikkerhetslovgivning
Telenor merket seg at regjeringen har fremmet forslag til lov om digital sikkerhet, og at sentrale mål med dette er å ansvarliggjøre virksomheter, sikre gjennomføring av nasjonale råd og anbefalinger, samt legge til rette for innføring av EUs NIS-direktiv. Telenors holdning er at jo flere tilbydere av samfunnsviktige tjenester innen sentrale områder som er forpliktet til å gjennomføre sikkerhetstiltak og varsle om alvorlige digitale hendelser, jo mer motstandskraftig blir vårt åpne og digitale samfunn. Dette kan være med på å bidra til en bedre koordinert respons på tvers av sektorer.

Kompetanse og industrisamarbeid
Telenor opplever en økende utfordring med tilgang på kompetanse på teknologi- og sikkerhetsfeltet. Det er et stort underskudd på slik spesialkompetanse i Norge i dag. Ikke minst opplever vi utfordringer i tilgangen på personell med riktig sikkerhetsklarering. Vi mener et tettere nordisk samarbeid rundt dette ville være nødvendig. Tettere samordning vil gi mulighet for mer effektiv utnyttelse av kompetansebasen i offentlig og private virksomheter på tvers av nordiske land. Ut over nasjonale tiltak som økt utdanningskapasitet innen relevante fagretninger, mener Telenor det er behov for å styrke det helhetlige arbeidet med å tilrettelegge for bedre teknologiutnyttelse og industrisamarbeid. Det gir anledning til å trekke på den teknologikunnskapen norsk, nordisk og internasjonal industri og næringsliv har å by på.

Telekom er en internasjonal bransje med multinasjonale leverandører, og fra leverandørsiden vil man generelt prioritere markeder av en viss størrelse. Nordisk samarbeid, med en mest mulig harmonisert sikkerhetslovgivning og klarering, vil kunne bidra til nødvendig skala og dermed i større grad kunne stimulere de multinasjonale teknologileverandørene til å etablere kompetansemiljøer i Norden. Ut over å bidra til regionens digitale motstandskraft, vil dette også kunne styrke nordisk konkurranseevne.

Et sikkerhetspolitisk fundament
Et tett teknisk samarbeid mellom bedrifter og organisasjoner over landegrensene krever et sikkerhetspolitisk fundament. Dette innebærer harmonisering av sikkerhetslovgivning og samarbeid mellom nasjonale regulatører på et helt annet nivå enn det vi ser i dag. Med et økende press på talent og kompetanse, og konsentrasjon av leverandørmarkedet med stadig lengre forsyningskjeder, blir de enkelte land i Norden hver for seg for små. Med et tettere sikkerhetssamarbeid på tvers av den nordiske regionen vil vi kunne virkeliggjøre helt andre forutsetninger for et effektivt, sikkert og robust totalforsvar.

Det trengs et styrket nordisk samarbeid om sikkerhet, robusthet og beredskap. En mer harmonisert lovgivning som tillater deling av tekniske løsninger og infrastruktur på tvers av Norden er nødvendig. Sikkerhet bygges best sammen. //

Telenor vil:

- styrke sikkerhetssamarbeidet om klarering og autorisasjon av nordiske statsborgere med et felles nordisk regime for sikkerhetsklarering, og at krav til nasjonal autonomi operasjonaliseres slik at det muliggjør å benytte personell på tvers samt dele tekniske løsninger og infrastruktur for økt robusthet og motstandsdyktighet
- at det for sentrale aktører i Totalforsvaret raskt etableres bedre løsninger for gradert samhandling og gis bedre tilgang til trussel- og sikkerhetsinformasjon
- at det i større grad stilles krav om å ivareta beredskapshensyn og nasjonale sikkerhetsinteresser i offentlige anskaffelser

Telenor

Snarøyveien 30
N-1360 Fornebu
Norway
Sentralbord: +47 810 77 000

www.telenor.no

Les rapporten digitalt:

https://www.telenor.no/om/digital-sikkerhet/2023