Har vi tid til å vente?

Digital sikkerhet 2024

FOTO: RISTO ARNAUDOV VIA GETTY IMAGES

telenor

Innhold

Tidligere utgaver:

FOTO: ISTOCK.COM / WESTERSOE

Innhold

Innhold: Der det ikke eksplisitt er angitt en ekstern forfatter eller opprinnelse, er de vurderinger, råd og fagkunnskaper 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 og intervjuer:** NewsLab. **Bilder:** Getty Images, iStock, Tore Ellingsen, Anette Ask, Odd Skarbomyr, Anders Martinsen, Harald Pettersen, Ole Jørgen Bratland, Hans A. Rosbach, Harald Spjelkavik, Forsvaret, Equinor, DSB, Nasjonal kommunikasjonsmyndighet, Bertel O. Steen, Telenor. **Trykk:** Aksell.

Digital versjon: *https://www.telenor.no/om/digital-sikkerhet/2024*

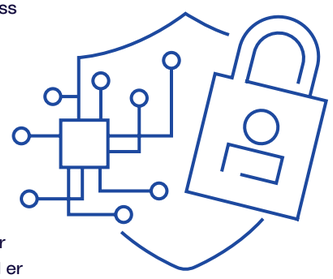
Ønsker du å komme i kontakt med oss? Send e-post til *desken@telenor.no*

Vi må gå fra ord til handling

I en sikkerhetspolitisk situasjon som er mer usikker og farlig enn på flere tiår, må vi som er leverandører av kritisk infrastruktur forberede oss på scenarioer som før var utenkelige. Vi må alle øke innsatsen for å styrke egen motstandsdyktighet.

TRUSSELSITUASJONEN I OG MOT NORGE har endret seg mye i løpet av kort tid. Et angrep mot kommunikasjonstjenester og nettverk vil kunne få betydelige samfunnsmessige konsekvenser. I Telenor øker vi derfor ytterligere vårt fokus på resiliens og motstandskraft. Vi styrker evnen til å beskytte vår digitale grunnmur – og evne til å stå imot angrep. Slik kan vi ivareta forsvarlig sikkerhet for oss selv, våre kunder og samfunnet.

NORDISK SAMARBEID for en mer harmonisert sikkerhetslovgivning og et felles nordisk regime for sikkerhetsklarering har i flere år vært et hovedtema i Telenors sikkerhetsrapport, og vi merker en økende oppslutning om dette i debatten om nasjonal sikkerhet. Mulighetene for samarbeid har aldri vært bedre nå som Sverige og Finland er blitt medlemmer i NATO. Krav til nasjonal autonomi bør operasjonaliseres slik at det gjør det mulig å benytte personell på tvers av landegrensene, samt dele tekniske løsninger og infrastruktur. Vi har ikke tid til å vente.



TILGANG PÅ KRITISK KOMPETANSE er en felles utfordring. Den treffer forsvarssektoren, de viktigste beredskapsaktørene i sivil sektor og næringslivet. En tydeligere felles nordisk tilnærming for å bidra til innovasjon og som i større grad stimulerer de multinasjonale teknologileverandørene til å etablere kompetansemiljøer i Norden, vil kunne bidra til å styrke regionens digitale motstandskraft. Dette vil også kunne bedre nordisk innovasjons- og konkurranseevne. Vi i Norden trenger å samle våre krefter og større miljø for å sikre tilgangen til relevant kompetanse og kapasitet for å levere varer og tjenester i øvre del av krisespekteret.

NORGE TRENGER ET MARKED for beredskaps- og sikkerhetstjenester. Det kan vi få til ved at kunder i privat og offentlig sektor i større grad også etterspør at varer og tjenester skal kunne oppfylle strenge krav til sikkerhet. Beredskap koster og er kun mulig dersom sentrale aktører i offentlig sektor, som stat og kommuner, i større grad stiller krav om nettopp å ivareta langsiktige beredskapshensyn og nasjonale sikkerhetsinteresser i offentlige anskaffelser. Dette må til for å etablere et bredere marked for beredskaps- og sikkerhetstjenester på områder som understøtter kritiske samfunnsfunksjoner. Dette vil også bidra til å øke sikkerheten og vår felles motstandskraft.

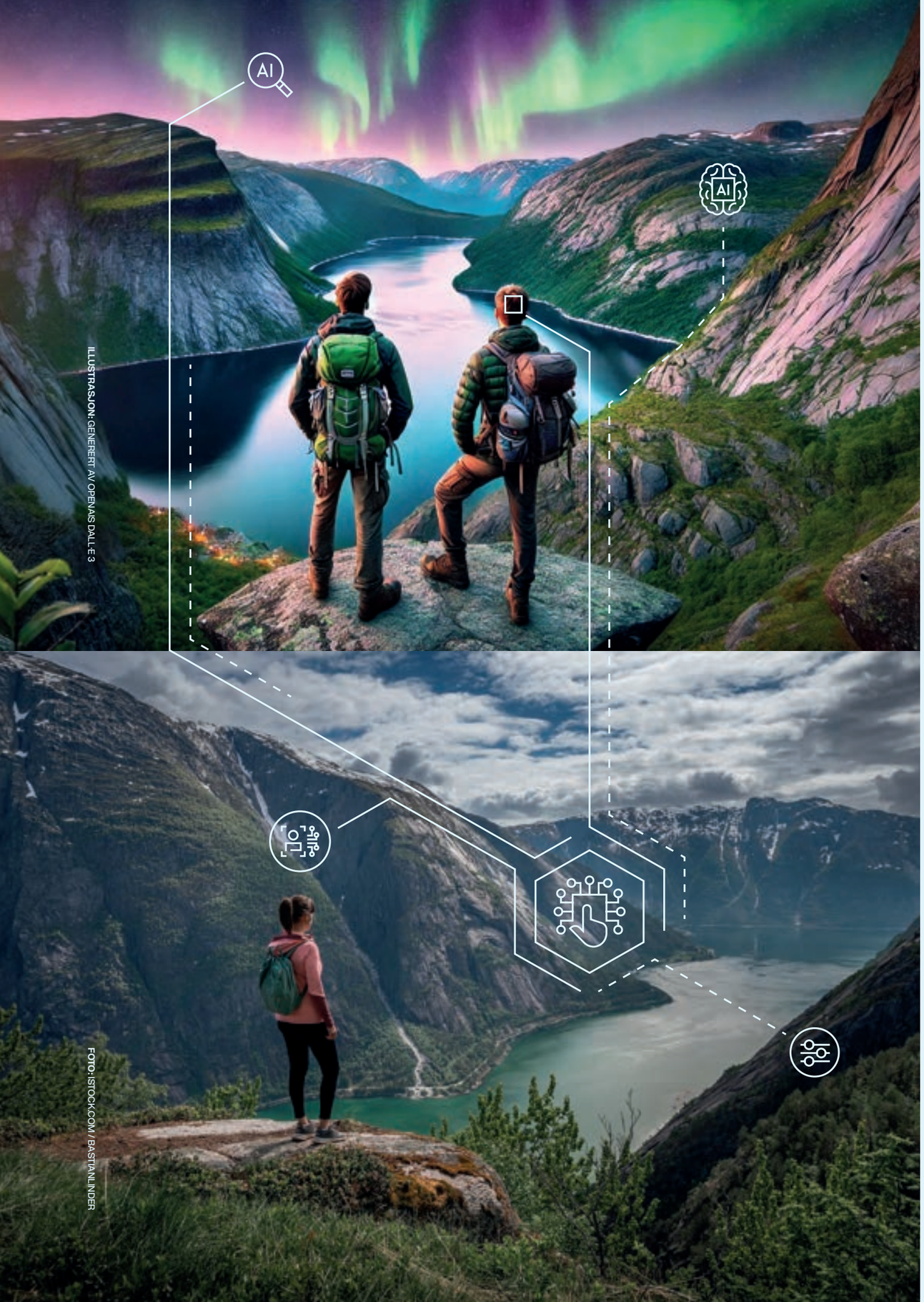
» Integrer de mest sentrale næringslivsaktørene i Kriserådet på fast basis.

EN TETTERE INTEGRERING AV NÆRINGSLIVET i Totalforsvaret er ett av områdene hvor vi ikke har kommet langt nok. Vi ser at mange større virksomheter som utgjør en naturlig del av Totalforsvaret, fortsatt ikke er fast inkludert i relevante fora. Dette er en alvorlig svakhet for vår samlede nasjonale motstandsdyktighet og gir grunn til bekymring. Relevante myndigheter bør derfor sørge for at utvalgte og sentrale virksomheter systematisk integreres i Totalforsvaret. Vårt viktigste budskap i årets sikkerhetsrapport er at vi trenger et taktskifte for bedre å integrere næringslivet i de nasjonale beredskapsstrukturene.

INVESTERING I DEN DIGITALE GRUNNMUREN som holder samfunn og tjenester oppe, er god forebygging når trusselnivået øker. Det viktigste vi kan gjøre i fellesskap, basert på de mange gode anbefalingene som har kommet fra Forsvars- og Totalberedskapskommisjonene de siste årene, er å gå fra ord til handling. Vi må øve og trene mer på realistiske scenarioer på tvers av sektorer. Vi må integrere næringslivet tettere i de nasjonale beredskapsstrukturene, og vi må samarbeide tettere i Norden og med våre allierte i NATO.

Birgitte Engebretsen,
administrerende direktør i Telenor Norge

FOTO: TELENOR



ILLUSTRASJON: GENERERT AV OPENAIS DALL·E 3

FOTO: ISTOCK.COM / BASTIANLINDER

2

AI og sikkerhet – utfordringer og muligheter

ChatGPT, Bard, DALL-E og GitHub Copilot. Utviklingen innen kunstig intelligens går i et rasende tempo, og fordelene er mange – men klarer egentlig sikkerhetsmekanismene å henge med på utviklingen?

Til venstre: Falske AI-genererte bilder lurte sommeren 2024 turister til å tro at Norge er enda mer spektakulært enn det er. For ordens skyld, her er det øverste bildet falskt, mens det nederste er ekte.

Denne artikkelen er basert på Telenors rapport «Fremveksten av kunstig intelligens: Nye trusler, nye reguleringer og nye løsninger». For å lese rapporten, vennligst besøk telenor.com.

Kunstig intelligens (AI) er en fremvoksende teknologi som representerer et paradigmeskifte som vil endre næringslivet og samfunnet forøvrig. Vi har bare såvidt begynt å se konturene av hva slags virkning denne teknologien kan ha og hvilke fordeler både enkeltpersoner, organisasjoner og bransjer kan dra nytte av. AI er ikke et futuristisk teknologisk konsept – som generative AI-verktøy som ChatGPT, Bard, DALL-E og GitHub Copilot har vist, er teknologien allerede godt integrert i hverdagen vår, og spiller også en viktig rolle på tvers av ulike industrier.

Samtidig er vi helt i startgropen når det gjelder sikker implementering og bruk av kunstig intelligens – både i et cybersikkerhetsperspektiv og i et bredere sikkerhets- og trygghetsperspektiv.

Også AI har sikkerhetsutfordringer

Det store gjennombruddet som offentlig tilgjengelige generative AI-verktøy for tekst, bilder, lyd og video har hatt, har sørget for at et langt bredere publikum har fått øynene opp for teknologien. Imidlertid har de fleste av oss – om ikke alle – allerede benyttet seg av AI-funksjoner i årevis. Maskinlæring og AI-modeller for kategorisering og prediksjon er allerede mye brukt i tjenester, som for eksempel når vi får personlige anbefalinger på Netflix, når vi snakker med en taleassistent eller når vi får hjelp av en kundeservice-chatbot.

Vi har allerede sett flere eksempler på hvordan velment bruk av prediktiv kunstig intelligens kan ha alvorlige, uforutsette negative konsekvenser – som for eksempel å bidra til diskriminering, sementere fordommer og subtilt gi uttrykk for uønskede verdier og preferanser som finnes i treningsdatasettene. Etter hvert som generativ AI er blitt mer fremtredende, har vi også sett hvordan ubetenksom anvendelse kan føre til at «hallusinasjoner» (altså oppdiktede fakta) blir tatt for god fisk, og for eksempel lagt fram som referansedommer i rettssaker. Mer bekymringsfullt er måten trusselaktører med kriminelle eller enda mer alvorlige hensikter utnytter teknologien for å oppnå sine mål.

Sikker bruk av språkmodeller som genererer tekst, som for eksempel en vanlig chatbot, har allerede vist seg å kunne gi utilsiktede konsekvenser. Dette skjedde nylig med et kanadisk flyselskap, der en chatbot ga et altfor godt tilbud til en kunde. Flyselskapets forsøk på å argumentere for at chatboten var en egen juridisk person, hvis handlinger de ikke kunne holdes ansvarlige for, ble ikke godtatt av den kanadiske domstolen.

Sikring av AI-modeller og deres bruksområder i et teknisk sikkerhetsperspektiv viser seg også, ifølge sikkerhetsforskere, å være i en tidlig fase. Blant annet har de dokumentert hvordan «prompt injection», altså oppfinnsom og kreativ innmating av tekst til en tekstgenererende AI, kan gi overraskende resultater med tanke på at slike systemer er designet for å analysere vilkårlige input-data. Enkelte tester har til og med ført til kompromittering av datamaskinen som kjører modellen.

AI-drevne assistenter er på vei inn på arbeidsplassene våre, med varierende grad av kontroll. Virksomheter begynner å innse at både hva vi mater inn og hva vi får ut fra AI åpner et helt nytt område innen datasikkerhet. Dette inkluderer både hva som blir presentert av informasjon til brukerne, og all data som deles fra virksomheten som en del av AI-prosessering eller -trening – noe som er mindre åpenbart for mange. Alt dette må sikres.

Det er liten tvil om at ulike typer AI-teknologier vil bli brukt for å oppnå betydelige effektivitetsgevinster i utallige forretningsprosesser og -systemer. AI gjør det også mulig for oss å håndtere, og dermed ta i bruk, prosesser og systemer med økende kompleksitet. Når AI-baserte beslutninger kobles med automatisering, er det imidlertid viktig å ha en tilstrekkelig forståelse av risikoene. Ofte kan det være nødvendig å ha et menneske involvert i beslutninger knyttet til høy risiko.

» Vi har allerede sett flere eksempler på hvordan velment bruk av prediktiv kunstig intelligens kan ha alvorlige, uforutsette negative konsekvenser.

AI og sikkerhet – utfordringer og muligheter

» Akkurat som at vi forventer at AI vil føre til gjennomgripende endringer både i virksomheter og samfunnet, vil det sannsynligvis også bli et allestedsnærværende verktøy for trusselaktører.

Ikke bare «AI i det godes tjeneste»

Den relativt ferske tilgjengeliggjøringen av gratis eller svært rimelige generative AI-tjenester for tekst, bilder, lyd og video er noe også cyberkriminelle raskt har tatt i bruk. Teknologien brukes direkte til svindel, men også som et støtteverktøy for sosial manipulering og i mer komplekse kriminelle aktiviteter. Muligheten til å skrive feilfritt på et fremmed språk, etterligne en virksomhets eller en gruppes tone of voice, endre stemmer for å utgi seg for å være en annen person – eller til og med endre et utseende live i videosamtaler – er åpenbart anvendelige verktøy for kriminelle.

Alle disse eksemplene på kriminell bruk har allerede ført til store tap for både selskaper og enkeltindivider. Et nylig eksempel er et angrep rettet mot en ansatt i et Hongkong-basert selskap. Den ansatte var i utgangspunktet skeptisk og motvillig til å etterkomme en mistenkelig forespørsel om å gjennomføre pengeoverføringer. Men da han ble invitert til en videokonferanse med det som tilsynelatende var flere i selskapets ledelse – men som i virkeligheten var såkalte «deepfake»-endrede videostrømmer – ble han overbevist om at forespørselen om å overføre penger var ekte. Like etter utbetalte han rundt 20 millioner amerikanske dollar til de kriminelle bakmennene.

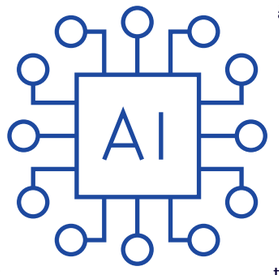
Selv om dette eksempelet har fått mye oppmerksomhet, er det langt fra det eneste tilfellet av ondsinnet bruk av AI-teknologi. Akkurat som at vi forventer at AI vil føre til gjennomgripende endringer både i virksomheter og samfunnet, vil det sannsynligvis også bli et allestedsnærværende verktøy for trusselaktører. Andre ondsinnede bruksområder inkluderer effektiv, automatisert og skalert utforskning av sårbarheter og gjennomføring av angrep, unnvikelse av adferdsbasert deteksjon, forbedret og automatisert «mutasjon» (polymorfisme) av skadelig programvare for å unngå oppdagelse – samt angrep på maskinlæringssystemene i seg selv.

FOTO: ISTOCK.COM / GORODENKOFF

Å kjempe tilbake med AI

Heldigvis kan AI-teknologi også brukes i selve forsvars- og sikkerhetsarbeidet.

Tidligere ble gjerne mange virksomheter som forsøkte å innføre verktøy for forebygging av datatap (Data Loss Prevention) overveldet av innsatsen som kreves for å fininnstille og vedlikeholde disse verktøyene. De ga enten opp i forsøket, eller måtte begrense verktøyene til et relativt smalt sett av lett identifiserbare sensitive datatyper. Med kunstig intelligens er det nå mulig å effektivt analysere svært komplekse sett med ustrukturerte data – noe som gir nytt liv til slike viktige sikkerhetsfunksjoner. Bruken av AI er heller ikke forbeholdt trusselaktører som driver med phishing og sosial manipulasjon – teknologien brukes også i sikkerhetsfunksjoner utviklet for å identifisere slike tekster (eller AI-genererte tekster generelt). Dermed er noe så grunnleggende som e-postfiltrering nå i realiteten blitt en arena der én AI kjemper mot en annen.



Innen cybersikkerhetsovervåking og -deteksjon (når man beveger seg utover deteksjon av det som er «kjent ondsinnet») brukes anomalideteksjon for å identifisere interessante hendelser som er verdt nærmere undersøkelse og som potensielt kan være symptomer på en sikkerhetshendelse. Dette er tradisjonelt en utfordrende disiplin med kontinuerlig forbedring og finjustering av regelsett og terskler. Her må man finne en balanse med tanke på hvor unormal en hendelse eller sekvens av hendelser må være før man bruker ressurser på menneskelig drevet undersøkelse. Selv om effektivitet selvfølgelig kan oppnås gjennom enkel automatisering av noen steg i analyseprosessen, for eksempel ved automatisert berikelse av data før eksponering til analytikere, har anvendelsen av kunstig intelligens på anomalideteksjon potensial til å drastisk endre balansepunktet og radikalt forbedre «signal-til-støy-forholdet» – altså forekomsten av falske positiver. På samme måte ser vi nå at AI-drevne produkter som kommer på markedet adresserer den nåværende arbeidskrevende normaliseringen av data fra heterogene kilder, for å gjøre dem egnet for deteksjon og analyse.

Å omgjøre trusseletterretning til effektiv deteksjon er fortsatt en relativt arbeidskrevende disiplin for cybersikkerhetsorganisasjoner – fra det relativt enkle basert på atomiske indikatorer, til mer komplekse hendelsesmønstre for deteksjon på spesifikke teknologier. Her kan kombinasjonen av flere AI-kapabiliteter gi radikale effektivitetsgevinster, med langt raskere og bredere implementering av effektive deteksjonsregler. Et tilsvarende potensial finnes for generering av preventive tiltak, som for eksempel blokkeringsregler og dynamiske policies. Der hvor falske positiver viser seg å være ubetydelige, og operasjonell risiko tillater det, vil vi sannsynligvis se en økende grad av automatisering – som til slutt kan gjøre mennesker overflødige i prosessen.

I tillegg til det ovennevnte kan Security Operations Center (SOC) og Incident Response høste store effektivitetsgevinster fra bruk av ulike AI-teknologier. Mye av det såkalte «førstelinjearbeidet» som utføres av analytikere på SOC-en kan automatiseres eller støttes av AI. Dessuten kan deler av innledende analysearbeid og skadevurderinger støttes på en måte som reduserer behovet for tung kompetanse, og til en viss grad også nødvendig erfaring. Dette senker kompetanse- og erfaringskravet for å fylle en slik rolle effektivt, noe som igjen kan bidra til å tette det velkjente og globale kompetansegapet på feltet.

Uten at vi skal forsøke å liste opp alle måtene kunstig intelligens kan bidra til å styrke cybersikkerhet, er bruken av språkmodeller (LLM-er) i SOC og Incident Response også verdt å nevne. Muligheten til å samhandle med verktøy, data og kunnskapsbaser ved bruk av naturlig språk, samt støtten LLM-er kan gi til å skrive tidslinjer, rapporter, presentasjoner og annen kommunikasjon, er eksempler vi på kort sikt vil kunne se.

Det er ikke bare de kriminelle som prøver å lure oss – vi prøver også å lure de kriminelle. Såkalte «deception technologies» har lenge vært brukt i cybersikkerhet. Dette kan for eksempel være ressurser som gir seg ut for å være attraktive, verdifulle og/eller sårbare (som filer, kontoer, datamaskiner eller hele nettverk), men som i realiteten ikke brukes i produksjon. Overvåking av slike ressurser kan gi pålitelige signaler, øke evnen til å studere angriperens TTP-er (taktikker, teknikker og prosedyrer), og avlede angriperen til å fokusere på de falske ressursene i stedet for de ekte. Imidlertid kan angripere som bruker AI over tid få tilstrekkelig informasjon om forsvarssystemene og identifisere slike såkalte «honeypot»-nettverk, for dermed unngå dem i senere angrep. Innføringen av AI-baserte og dynamiske «honeypot»-ressurser kan motvirke dette gjennom automatisk omkonfigurerte feller som håndterer angrep basert på angriperens oppførsel.

Konklusjon

Som vi har sett ovenfor, fører AI-teknologi med seg en rekke nye risikoer og sikkerhetsaspekter. Innenfor cybersikkerhet ser vi at AI har ført til en opptrapping der angrepene blir bedre, og der sikkerhetspersonell bruker den samme teknologiske utviklingen for å holde tritt. Enkelte mener at fordelene ved bruk av AI for å styrke cyberforsvar for en gangs skyld faktisk overgår fordelene AI gir trusselaktørene – men det er fortsatt for tidlig å slå fast.

Som fagfolk innen sikkerhet har vi en tendens til å være litt dystopiske. Når det gjelder utviklingen av AI og den enorme økningen i bruk av teknologien, har ikke akkurat advarslene fra flere kjente teknologer og AI-eksperter om at AI kan utgjøre en eksistensiell trussel mot menneskeheten, hjulpet på dette. Als mange bruksområder innen sikkerhet kan likevel inspirere til noe håp.

Det er nødvendig å forstå risikoen ved bruk av AI og iverksette nødvendige tiltak. Det være seg sikkerhetstiltak for AI-systemer og bruken av dem, hvordan disse systemene brukes i forretningsprosesser, behovet for nye sikkerhetskapabiliteter i virksomheten som følge av dette, graden av menneskelig involvering i beslutningsprosesser – eller til og med tøyle jaget etter stadig mer effektivitet og automatisering. Her har vi alle en jobb å gjøre, og et ledelsesansvar å erkjenne.

ILLUSTRASJON: LINUS ZOLL / GOOGLE DEEPMIND

Et menneskes illustrasjon av tekst-til-bilde-diffusjon. Illustrasjonen er en del av prosjektet «Visualising AI» av Google DeepMind, der kunstere ble invitert til å lage illustrasjoner av forskjellige aspekter ved KI. Denne illustrasjonene er laget av Linus Zoll.

3

Den store sikkerhetstesten

Bertel O. Steen er for de fleste synonymt med bil. Konsernet er imidlertid også en viktig aktør innen både eiendom, forsvarsindustri og energi. De siste årene har de vært gjennom en omlegging av måten de jobber med digital sikkerhet – noe som allerede har betalt seg.

Til venstre: I 2022 ble Bertel O. Steen rammet av et hackerangrep. I kjølvannet rustet de opp den digitale sikkerheten i konsernet.

FOTO: BERTEL O. STEEN

Bilforhandler Bertel O. Steen har de siste årene vært gjennom en stor omorganisering for å sette fart på den digitale utviklingen.

Internt har konsernet vært gjennom en minst like viktig omlegging av måten de jobber med digital sikkerhet. Det har allerede betalt seg.

– Jeg har blitt spurt om hva det verste som kan skje ved et cyberangrep er. Da svarer jeg at det må de som har ansvar for forretningene svare på, for det er der de store konsekvensene ligger, sier Steingrim Soug, leder for IT-sikkerhet i Bertel O. Steen.

I dag har konsernet en tydelig plan for måten de tenker sikkerhet og dybdeforsvar. Det er imidlertid ikke lenge siden kriminelle stod med foten i døråpningen – på full fart inn.

Fikk varsellampene til å blinke

– Fordi vi har leveranser til både forsvar og politi, er vi nok mer aktuelle for enkelte typer angrep. Det er en realitet vi er nødt til å forholde oss til. I tillegg hadde vi en hendelse som gjorde at flere fikk seg en øyeåpner, forteller Soug.

For de fleste er Bertel O. Steen synonymt med bil. Ikke så rart med sin over hundre år lange historie som importør av merker som Mercedes-Benz og Kia, i tillegg til Stellantis-merkene. Familiekonsernet er imidlertid også en viktig aktør innen både eiendom, forsvarsindustri og energi.

Da 30 butikker i bilforhandlerkjeden Mobile ble rammet av et massivt hackerangrep i 2022, holdt mange i konsernet derfor pusten.

– Da nyheten sprakk, følte nok flere at hackerne hadde kommet ubehagelig tett på. Mobile er en frittstående forhandler under Bertel O. Steen-konsernet, og sånn sett ikke direkte tilknyttet samme systemer og nettverk. Likevel fikk det konsernledelsen til å reagere.

Like etter det omfattende cyberangrepet ble det utført en modenhetsanalyse og tatt en beslutning om å ruste opp den digitale sikkerheten. Blant annet ble Soug selv ansatt som konsernets CISO (Chief Information Security Officer), med ansvar for IT-sikkerhet internt.

Kanskje kom beslutningen i grevens tid, for det skulle ikke gå lang tid før varsellampene igjen lyste.

FOTO: BERTEL O. STEEN

BERTEL O. STEEN

3000 ÅRSVERK

100 SELSKAPER

6000 BRUKERE

7000 ENDEPUNKTER

Lite motstand innenfor murene

Blant tiltakene Soug iverksatte var å utarbeide retningslinjer for å gjøre konsernets systemer og nettverksløsninger mer motstandsdyktige, dersom et angrep faktisk skulle finne sted.

Bertel O. Steen har i flere år hatt en avtale med Telenor om overvåking av sikkerhetsplattformen. Det vil si at Telenor fungerer som konsernets Security Operation Centre (SOC) og dermed har det daglige ansvaret for konsernets sikkerhetsløsninger mot ytre trusler.

– Vi hadde allerede et godt sikkerhetsskall. Det vil si at det alltid har vært vanskelig å ta seg inn på nettverket vårt. Utfordringen var at om du først kom deg inn, var det litt for mange veier videre som stod åpne, forteller Soug.

Målet ble å få på plass tiltak som skulle minimere skadepotensialet, dersom en hacker slapp gjennom det ytre sikkerhetslaget. For et stort konsern er imidlertid ikke en slik «herding» av systemene gjort i en håndvending.

– Hele konsernstrukturen består av mer enn 3000 årsverk fordelt på mer enn 100 selskaper. I nettverket drifter vi mer enn 6000 ulike brukere, og har mer enn 7000 endepunkter. I tillegg drifter vi flere tusen OT-enheter. Nettverket måtte derfor deles inn i ulike soner, noe som ga oss mulighet til å isolere et eventuelt angrep.

Det samme gjaldt i skyløsningene. Ingenting skulle heller kjøre med annet enn nødvendige konfigurasjoner og tillatelser, og den generelle dybdesikkerheten skulle styrkes.

– For eksempel er krypteringsnøkler nå lagret på ulike steder, slik at det ikke er mulig å låse hele nettverket fra ett enkelt sted i systemet. Det er samme logikk som at du ikke vil ha nøklene til alle bilene hos forhandleren innelåst i én og samme safe, forteller Soug.

» Om du først kom deg inn, var det litt for mange veier videre som stod åpne.

Styrket beredskapen

Det var også behov for en opprusting av beredskapen rundt alt som har med IT-sikkerhet å gjøre. Dette har blant annet blitt ivaretatt ved å utarbeide faste prosedyrer for håndtering av et angrep eller en hendelse.

Bertel O. Steen bruker et ISO-sertifisert styringssystem som gjelder for hele bedriften. Det gjør at de har formelle krav til hvordan ting skal utføres og dokumenteres i alle ledd, også innen IT og sikkerhet.

– Prosedyrene er en del av konsernets overordnede kriseberedskapsplan, som beskriver hvordan ulike typer kriser skal håndteres. Planen har tydelig definerte roller med egne arbeidsoppgaver og ansvarsområder, forklarer Soug.

Sammen med en tydelig presisering av formål og omfang, inneholder prosedyrene en detaljert beskrivelse av CSIRT (Computer Security Incident Response Team) og teamets medlemmer og funksjoner. Prosedyrene beskriver også hvordan innkalling til krisestab og varsling skal foregå, samt hvilke punkter som alltid skal gjennomgås i møtene.

I tillegg har konsernet utviklet tiltakskort som beskriver de ulike rollene i krisestaben og deres oppgaver.

– Tiltakskortene er i praksis en sjekkliste for hva man skal vurdere, hva man må huske å gjøre for å begrense skade, og hvordan man skal jobbe for å komme tilbake til normal drift og avslutte krisen, forklarer Soug.

Alarmen går

Underveis i arbeidet med å implementere de nye tiltakene og beredskapsprosedyrene, går plutselig alarmen hos SOC. Her kan Telenor se mistenkelig aktivitet i en av konsernets innloggingsportaler.

– Vi har en løsning som gir brukere mulighet til å logge seg på en nettside som gir tilgang til ulike applikasjoner. Løsningen er laget slik at brukere kun får opp de applikasjonene de har tilgang til i systemet, sier Soug.

FOTO: BERTEL O. STEEN

» Når man står midt i et angrep, er det lett at det koker litt. Da er styringssystemer og tiltakskort veldig gode å ha.

Ved en feil ble løsningen nedgradert, noe som innebar at den ble sårbar for et sikkerhetshull kalt Citrix Bleed. Det betyr i prinsippet at en hacker kan overta en allerede innlogget bruker, med alle de tilhørende rettighetene.

– Vi så at de hadde hentet ut en liste med brukernavn fra innloggingssystemet og installert et par trojanere, altså skadevare skjult i legitime programmer. Trojanerne ble heldigvis raskt plukket opp av sikkerhetssystemene, slik at disse automatisk ble fjernet.

Hackerne forsøkte deretter å logge seg inn i de ulike applikasjonene i portalen. Her ble de stoppet av krav om tofaktorautentisering.

– Når man står midt i et angrep, er det lett at det koker litt. Da er styringssystemer og tiltakskort veldig gode å ha. Det gir deg mulighet til å gå inn og sjekke hva du skal gjøre i en gitt situasjon.

Både drift og IT hos Bertel O. Steen har i dag hvert sitt incident response-team som håndterer hendelser, som igjen rapporteres til konsernets overordnede beredskapsgruppe.

– I prosedyrene er en av de definerte rollene våre en loggfører. Denne rollen har kun én oppgave, og det er å loggføre alle avgjørelser som blir tatt med begrunnelse. Dette er svært viktig når man evaluerer krisehåndtering i ettertid.

På tiltakskortet for IT-sikkerhetshendelser står det at systemer som er hacket eller infisert, ikke skal restartes, men isoleres. Grunnen til dette er at når et system restartes, kommer det ofte opp i et standardoppsett – og da vil alle logger og programmer som er installert på serveren, bli slettet.

– Dessverre ble det gjort en feil her. Hendelsen ble tolket som en driftsfeil og ikke en sikkerhetsfeil. Da er instruksen å restarte for å komme raskt tilbake. Dette gjorde det vanskelig å finne ut nøyaktig hva som har skjedd, og gjorde håndteringen mer utfordrende.

Hadde Bertel O. Steen i stedet isolert portalen, som de hadde mulighet til gjennom soneinndelingen av nettverket, ville alle digitale spor vært tilgjengelig etter hendelsen.

Uten sikkerhet i flere lag, kunne imidlertid hackerne enkelt ha kommet seg langt innover i nettverket. Potensielt kunne de her ha slettet eller lastet ned alle kundedataene til konsernet, eller kryptert alle systemer. Det kunne fått enorme konsekvenser, mener Soug.

Nødt til å tenke helhetlig

– De neste ukene hadde vi flere tusen forsøk på innlogginger fra blant annet Russland og Bulgaria. Stort sett var dette heldigvis blind gjetting på passord, og etter hvert så vi at de begynte å gi opp.

– Det er lett å lage retningslinjer, men det tar tid å få dem implementert. Man er avhengig av en strukturert tilnærming. Vi har nå en sikkerhetsstrategi med klart definerte mål om hvor vi skal de neste to årene. Dette omfatter både tekniske og organisatoriske mål.

Soug mener det ikke lenger er mulig å tenke at man skal løse ett problem eller én utfordring innen sikkerhet.

– Du er nødt til å tenke helhetlig. Det betyr at retningslinjene må inneholde alt fra herding – det vil si å gjøre enheter og tjenester sikrere ved å endre konfigurasjonen eller fjerne funksjonalitet – til opplæring av brukere og å tegne cyberforsikring.

– IT-sikkerhet handler til syvende og sist om forretningsdrift. Blir systemene rammet, kan det få direkte innvirkning på både inntjening og kundeforhold. Stanser systemene helt opp, snakker vi om milliontap hver time.

– Stanser de lenge nok, kan det bety at vi mister våre viktigste kunder, avslutter Soug.

» IT-sikkerhet handler til syvende og sist om forretningsdrift. Blir systemene rammet, kan det få direkte innvirkning på både inntjening og kundeforhold.

FOTO: BERTEL O. STEEN

FOTO: TELENOR

4

Beskyttelse av kritisk infrastruktur – med innebygd sikkerhet mot nye risikoer

Hva har sikkerhet å si for beskyttelse av mobilnett og kritisk infrastruktur? I denne artikkelen får du et innblikk i flere aspekter knyttet til kritisk infrastruktur og dens evolusjon innen telekom-sektoren. Det vil si alt fra 5G, telekomnettverkenes rolle i å støtte kritiske operasjoner, fremveksten av nye teknologier som confidential computing, til betydningen av regulatorisk etterlevelse.

Tekstbidrag fra:
Kaël Haddar,
Customer Security Director,
Ericsson

Denne artikkelen er oversatt fra originalspråket og redaksjonelt tilpasset for publisering i Digital Sikkerhet 2024.

Telekommunikasjon har utviklet seg til å bli en helt essensiell del av tiden vi lever i, og kobler sammen mennesker på kryss og tvers av landegrenser over hele verden.

Telekommunikasjon har også direkte innvirkning på både økonomisk utvikling, industrielle fremskritt og global konnektivitet. Tjenesteavbrudd kan få store konsekvenser for både samfunnsfunksjoner, økonomisk stabilitet og statlig styring.

Som en avgjørende del av dagens kritiske infrastruktur, stilles det også strengere myndighetskrav til mobile nettverk, inkludert revisjoner og verifisering av sikkerhet. Etterhvert som mobilteknologien brukes på nye måter i industrielle og virksomheters nettverk, betyr det også at man må ta nye hensyn med tanke på både sikkerhet og trygghet.

Alt dette er med på å forme sikkerhetsaspektene innen fremtidig testing, utvikling og operasjonell drift.

I denne artikkelen ser vi nærmere på den avgjørende rollen sikkerhet spiller i å beskytte kritisk infrastruktur innen telekommunikasjon. Teksten omfatter ulike sider, som viktigheten av 5G, telekomnettverkenes rolle i å støtte kritiske operasjoner, fremveksten av nye teknologier som confidential computing, og betydningen av regulatorisk etterlevelse.

FOTO: EYESFOTO VIA GETTYIMAGES

Kritisk infrastruktur avhenger av 5G, sikkerhet og resiliens

Både myndigheter og næringsliv er raskt ute med å implementere avanserte 5G-drevne teknologier, både for å sikre mer stabil drift og å styrke sikkerheten i kritiske operasjoner.

Den viktigste funksjonen et robust 5G-system har, er evnen til å levere uavbrutt tilgjengelighet, stabilitet og responsivitet – selv ved forstyrrelser eller angrep. Pålitelighet, tilgjengelighet, robusthet og sikkerhet er ikke bare egenskaper som bidrar til å ivareta personvernet, men sørger også for kontinuitet i tjenestene.

Parallelt med at stadig flere kritiske funksjoner blir digitalisert, har telenettverkene utviklet seg til å bli avgjørende bærebjelker for eksisterende operasjoner – samtidig som de åpner for nye og innovative bruksområder. For eksempel krever den stadige økningen av fjernstyring av utstyr og maskineri lynrask kommunikasjon, noe som igjen senker responstiden i møte med potensielle trusler.

Kritisk infrastruktur utvikler seg raskt – med intelligente nettverksplattformer som tilbyr et bredt spekter av viktige funksjoner, som sikkerhet, personvern, stabilitet og robusthet, tilpasset ulike bruksområder. Etter hvert som vi nå går fra 5G til 6G, blir det stadig viktigere å styrke disse nettverkene med avanserte komponenter for å sikre ytterligere robusthet og effektivitet.

Konfidensiell databehandling (confidential computing) har utviklet seg til en sentral teknologi som styrker sikkerheten i virtualiserte systemer. Ved å beskytte data under behandling og lagring, bidrar konfidensiell databehandling til økt tillit blant både brukere og myndigheter. At dette integreres i nettverksarkitekturen legger grunnlaget for sikker identitetsstyring og gjør det mulig å automatisere tillitsvurdering på tvers av alle nettverkselementer.

Sikre identiteter og protokoller utgjør en annen hjørnestein innen nettverkssikkerhet, og er essensielt for å beskytte kommunikasjonskanaler på tvers av ulike sektorer. Nye teknologier som pålitelige identiteter, rammeverk for autentisering og tilgangsstyring gir sikker kommunikasjon på alle nivåer, og fremmer enhetlig identitetsstyring og automatisert datastyring.

I tillegg er sikkerhetsgarantier og forsvarsmekanismer nødvendige i både utviklings-, distribusjons- og driftsfasen. Mens nåværende metodikk primært fokuserer på produktsikkerhet, vil fremtidige løsninger inneholde innebygde mekanismer som sikrer etterlevelse av sikkerhetsstandarder og forskrifter, som GDPR.

Det regulatoriske landskapet spiller i det hele tatt en viktig rolle i utformingen av sikkerhets- og personvernstandarder innen kritisk infrastruktur. At man overholder strenge regulatoriske krav fremmer tillit blant alle involverte og sikrer samsvar med sikkerhetsspesifikasjoner og standarder i stadig utvikling.

» Den viktigste funksjonen et robust 5G-system har, er evnen til å levere uavbrutt tilgjengelighet, stabilitet og responsivitet.

Veien mot motstandsdyktige nettverk

Når vi beveger oss mot motstandsdyktige og sikre nettverksinfrastrukturer, vil samarbeid, innovasjon og etterlevelse av regulatoriske krav være avgjørende for å kunne beskytte kritiske verdier og sikre bærekraftig vekst i de ulike næringene.

For å møte utviklingen i trusselbildet på en effektiv måte, er tre utviklingskomponenter helt avgjørende for å oppnå pålitelige systemer. Disse komponentene driver innovasjon og robusthet, og gir 5G-nettverk muligheten til å tilpasse seg og virkelig komme til sin rett i møte med stadig skiftende omgivelser.

Pålitelighet

Påliteligheten til den trådløse infrastrukturen bygges på bruk av internasjonale standarder, sterke sikkerhetsløsninger og tydelig definerte prosesser – kombinert med god trusseletterretning, som er aktivt og kontinuerlig oppdatert på aktuelle sikkerhetstrusler.

Skalert sikkerhet

Skalert sikkerhet innebærer blant annet å kunne beskytte store mengder enheter og data som har en rekke ulike bruksområder. For å oppnå dette, forsker Ericsson på tilpasningsdyktige, skalerbare og automatiserte sikkerhetsløsninger for fremtidige nettverk og tilkoblede enheter.

Policybasert automatisering

Policybasert automatisering, i tråd med bransjestandardene, sammen med regelbasert analyse (for kjente trusler) og AI-basert analyse (for avvik og ukjente trusler) gjør det mulig med holistisk og kostnadseffektiv tilnærming til sikkerhet for fremtidige bruksområder.

Ericssons tilnærming til telekom-sikkerhet bygger på fire sentrale pilarer: **standardisering**, **produktutvikling**, **implementering** og **drift**. Disse fire områdene bidrar til å skape en sikker plattform som gir et ideelt grunnlag for utvikling av store, sikkerhetssensitive systemer.

Ericsson har en lang historie med å systematisk innarbeide sikkerhets- og personvernhensyn i alle relevante aspekter og faser av verdistrømmene til våre produkter.

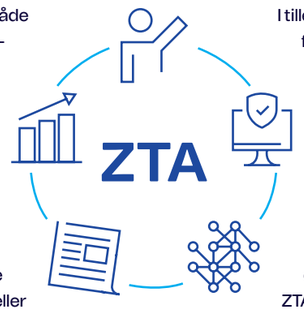
Vi har et veletablert rammeverk for internkontroll, Security Reliability Model (SRM), med en kontrollert, risikobasert tilnærming til sikkerhets- og personvernhåndtering, der kravene er tilpasset målgruppens omgivelser og behov. Denne tilnærmingen gjør det enklere for oss å møte interessenters forventninger og følge den raske teknologiutviklingen og de stadige regulatoriske endringene globalt.

ZTA innebærer strenge tilgangskontroller, kontinuerlig autentisering og sanntidsovervåking for å redusere risikoer og forhindre uautorisert tilgang.

Veien til Zero Trust Architecture for kritisk infrastruktur

I møte med de mange utfordringene knyttet til kritisk infrastruktur, fokuseres det mer og mer på operasjonell resiliens. Evnen til å ivareta operasjonell resiliens i en tid preget av stadig flere cybertrusler, naturkatastrofer og nye arbeidsformer, utgjør et vedvarende dilemma for mange virksomheter. Disse utfordringene krever en omfattende tilnærming til sikkerhet og resiliens, som inkluderer robuste protokoller, avanserte teknologier og proaktive strategier for risikohåndtering.

Parallelt med at truslene har utviklet seg, har både mobilnettverksoperatører (MNO-er) og myndigheter aktivt omfavnet konseptet Zero Trust Architecture (ZTA) som et ledd i å beskytte kritisk infrastruktur.



ZTA representerer et paradigmeskifte innen cybersikkerhet, der vi beveger oss fra den tradisjonelle perimeterbaserte sikkerhetsmodell til en langt mer granulær og dynamisk tilnærming. ZTA legger til grunn at ingen uten videre er til å stole på – uavhengig av om de er på ut- eller innsiden av en barriere. ZTA innebærer strenge tilgangskontroller, kontinuerlig autentisering og sanntidsovervåking for å redusere risikoer og forhindre uautorisert tilgang.

Det å oppnå en Zero Trust Architecture innebærer imidlertid mer enn bare å følge bransjestandarder.

Telekombransjens 3GPP-standarder (The 3rd Generation Partnership Project) er en sammeslutning av syv nasjonale og regionale standard-organisasjoner innen telekom, som blant annet har utviklet spesifikasjonene for 2G, 3G, 4G og 5G mobilnett. Selv om disse standardene gir et grunnleggende rammeverk for å implementere zero trust i nettverksfunksjoner (NF-er) og grensesnitt, omfatter operasjonell sikkerhet langt mer enn det som er mulig å standardisere.

Operasjonell sikkerhet omfatter et bredt spekter av praksiser og prosedyrer, der målet er å beskytte nettverksinfrastruktur, data og ressurser mot interne og eksterne trusler. Dette inkluderer – men er ikke begrenset til – regelmessige sikkerhetsrevisjoner, sårbarhetsvurderinger, beredskapsplanlegging og så videre.

I tillegg krever en vellykket implementering av ZTA god forståelse av den enkelte nettverkskonteksten og de operasjonelle kravene til hver MNO. Det er viktig å skreddersy utrulling og konfigurasjon av ZTA, slik at arkitekturen er tilpasset de spesifikke utfordringene og rammebetingelsene virksomheten står overfor. Dette innebærer, men er ikke begrenset til, grundige risikovurderinger, identifisering av kritiske punkter og avhengigheter, og å etablere klare retningslinjer og prosedyrer for å implementere og administrere ZTA-kontroller.

Ericsson-produkter har som mål å tilby de nødvendige egenskapene som trengs for å realisere en ZTA, og vi er aktivt engasjert i ZTA-reisen sammen med MNO-er og bransjeorganisasjoner som O-RAN Alliance, 3GPP og ATIS. Å realisere en ZTA som er i tråd med alle de syv prinsippene for zero trust fra NIST samt CISA ZTMM, krever en høy grad av automatisering og synlighet i mobilnett-sikkerhetsoperasjoner. Derfor tilbyr Ericsson en løsning for sikkerhetsstyring designet for å automatisere og orkestrere sikkerhetsoperasjoner, og slik styrke mobilnettet mot eksterne og interne trusler.

Behov for fortsatt samarbeid på tvers av bransjen

For å oppnå robust sikkerhet i distribuerte nettverk, kreves det en mangefasettert tilnærming som innebærer mer enn bare standardisering. Med sikkerhet og personvern som en stadig viktigere del av kritisk infrastruktur, kombinert med enda flere regulatoriske hensyn, er det avgjørende at bransjens aktører samarbeider effektivt i implementering av cybersikkerhet.

Samhandlingen bør naturligvis prioritere forretningsresultater innen nettverksytelse og -tilgjengelighet, men også omfavne prinsippene for Zero Trust Architecture (ZTA).

Ved å konsolidere sikkerhetskontroller og tilby omfattende anbefalinger, baner initiativer som disse veien for at bransjen kan lykkes med å realisere de fire viktige utviklingskomponentene som er kritiske for å bygge pålitelige systemer og ZTA i 5G-nettverk. I tiden fremover vil fortsatt samarbeid og samsvar med regulatoriske krav være helt essensielt for å sikre motstandsdyktighet og integritet i mobilnettene, i møte med trusler i stadig utvikling.

FOTO: ISTOCK.COM / SANDY BELL

FOTO: DAVID MERRON PHOTOGRAPHY VIA GETTY IMAGES

5

Trusselvurdering

Truslene mot Telenor som leverandør av kritisk infrastruktur har økt de siste årene. Geopolitisk spenning og usikkerhet, større mengder desinformasjon og hybrid krigføring er bare noen av temaene vi må forholde oss til. Her er Telenors åpne trusselvurdering for 2024.

Til venstre: Telenors tilstedeværelse i arktiske strøk innebærer et ekstra behov for å vurdere sikkerhet, beredskap og trusselanalyse.

FOTO: TORE ELLINGSEN / FORSVARET

Norske instruktører fra Heimevernet trener ukrainske soldater i England.

Trusselsituasjonen i og mot Norge har endret seg mye de siste årene. Som et resultat har også trusselen mot Telenor og telekom økt.

Telekom-selskaper er attraktive mål for trusselaktører, ettersom de fleste selskaper som opererer i dette domenet har tilgang på en omfattende mengde sensitiv data. I tillegg er de en digital inngangsport til andre målgrupper og bransjer, og har en større angrepsflate enn i de fleste andre bransjer. Enkelte selskaper innen telekom vil også eie, drifte og sikre nasjonal kritisk infrastruktur som de fleste er avhengige av i dagliglivet.

Telenor er Norges største digitale tjenesteleverandør innenfor innholds-, telekommunikasjon- og datatjenester. Dette øker også trusselen mot Telenor, både gjennom symbolverdien av et angrep og gjennom våre kundeforhold.

Vår åpne trusselvurdering har en helhetlig tilnærming til Telenor Norges sikkerhetsutfordringer. Vi ser på trusselaktørers intensjoner mot Telenors kunder, enten det er privatkunder, bedriftskunder, virksomheter eller nasjonale myndigheter. I dette ligger det også en anerkjennelse av hvor viktig det er å forstå verdiene kundene våre besitter og som Telenor tar del i å beskytte.

Telenor Norge baserer seg i stor grad på vurderinger fra nasjonale myndigheter. Dette gjelder både Norges sikkerhetssituasjon generelt og spesifikke trusler rettet mot telekommunikasjonsbransjen og Telenor Norge.

» Trusselsituasjonen i og mot Norge har endret seg mye de siste årene.

En manglende evne til å lese trusselbildet og iverksette tilstrekkelige sikkerhetstiltak, vil kunne påvirke både Telenor og samfunnet vårt. For Telenor Norge, som eier og drifter kritisk infrastruktur, vil en alvorlig sikkerhetshendelse også kunne gi svært alvorlige konsekvenser for Norge. Vi legger derfor vekt på å kontinuerlig vurdere og oppdatere vår trusselforståelse.

En forverret sikkerhetssituasjon

Økt geopolitisk spenning fortsetter å påvirke dagens situasjon. Trusselbildet vil kunne endre seg raskt og være vanskelig å forutsi – nettopp denne usikkerheten er noe vi må lære å håndtere. Dette krever god beredskap, oppdatert situasjonsforståelse og gjennomtenkte løsninger.

Sikkerhetssituasjonen blir nå beskrevet som farligere enn for kun ett år siden. Først og fremst handler dette om Russland og usikkerheten knyttet til sikkerhetssituasjonen i Europa. Hvorvidt Russland vil øke sin militære oppbygging de neste årene og hvorvidt de vinner krigen i Ukraina, vil være avgjørende for trusselbildet i Norge. Dette påvirker direkte hvordan vi jobber med sikkerhet i Telenor Norge. Sikkerheten i Telenor gjelder ikke bare vår bedrift og våre kunder. At den er ivaretatt er også en forutsetning for at de fleste digitale tjenester i landet fungerer i enhver situasjon. Det er derfor særdeles viktig at dette prioriteres, gitt dagens sikkerhetsbilde.

Norge fortsetter å oppgradere sin nasjonale infrastruktur for å stå imot økte digitale trusler. Telenors innsats for å sikre både privat og offentlig sektor spiller en kritisk rolle i denne sammenhengen. I takt med utviklingen av trusselbildet, styrkes samarbeidet innen nordisk forsvar og sikkerhet. Dette gjøres også innen privat næringsliv. Målet er å kunne bidra med robuste kommunikasjonsnettverk tilpasset dagens situasjon. Den skjerpede trusselen mot kritisk infrastruktur kan påvirke oss både direkte og indirekte. De gjensidige avhengighetene i kritisk infrastruktur i Norge er store. Utfall hos Telenor vil direkte påvirke svært mange andre samfunnskritiske tjenester og funksjoner. På samme måte vil større utfall hos andre leverandører av kritisk infrastruktur, for eksempel innen kraftbransjen, ha påvirkning for vår drift. Vår robusthet er viktigere enn noensinne – ikke bare for Telenor, men for hele samfunnet.

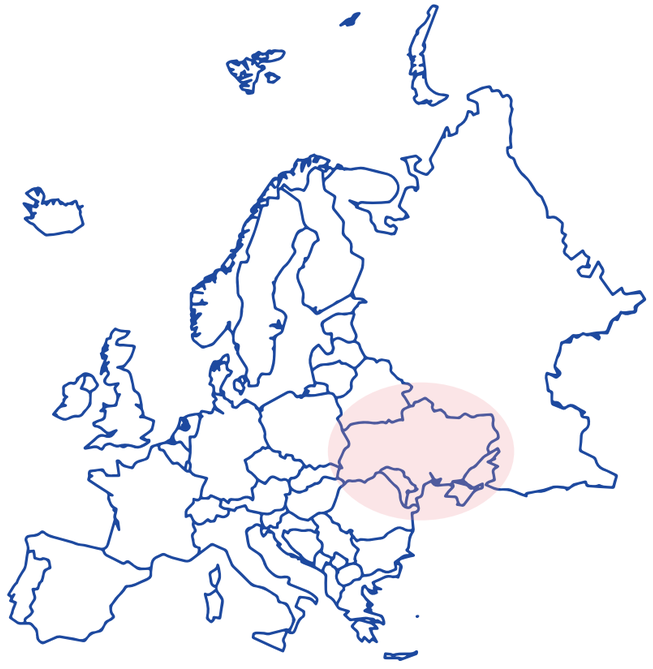
2024 preges av en fortsatt økende global usikkerhet i det digitale domenet, med stater som aktivt gjennomfører cyberoperasjoner for å fremme nasjonale interesser. Veksten i geopolitiske spenninger, spesielt mellom stormaktene, skaper et komplekst og dynamisk trusselbilde. Angrep fra statssponsede aktører, som tidligere var målrettet mot spesifikke strategiske mål, blir stadig mer varierte og omfattende. Med den teknologiske utviklingen følger også nye muligheter for trusselaktører, og dermed flere områder som krever sikkerhetstiltak. Vi ser at både statlige og ikke-statlige trusselaktører blir raskere til å benytte avansert teknologi til sin fordel, og er mer målrettede i sine forsøk. Å raskt kunne tilpasse seg endringer i trusselbildet er derfor viktigere enn noensinne.

» Å raskt kunne tilpasse seg endringer i trusselbildet er derfor viktigere enn noensinne.

De siste årene har vi ikke bare sett samfunnsendringer som påvirker forutsetningene for trusselbildet, men også at trusselaktørenes handlingsrom, risikovilje og evne er i endring. Dette har også betydning for hvordan økt digitalisering og teknologisk utvikling utnyttes.

Vi ser en økning av ressurssterke, opportunistiske trusselaktører i det digitale domenet som er i stand til raskt å endre taktikk og justere sine metoder for å skreddersy angrep mot vår bedrift og våre kunder. Kriminelle aktører med finansielle mål fortsetter å utnytte mulighetene som ligger i samfunnsendringer og teknologiutvikling.

De store endringene i det geopolitiske landskapet kan også føre til at forsyningslinjer må endres fort, blir mer uoversiktlige eller at man må endre underleverandører raskt. Dette kan utgjøre en sikkerhetsrisiko. Konfliktnivået er økende i Midtøsten og deler av Asia. Regionale konflikter kan fort påvirke forsyningssikkerheten. Dette kan ha betydning for tilgangen til spesialisert teknologi. For eksempel i form av tilgjengelighet av varer på løpende kontrakt i andre deler av verden, samt økt leveransetid der handelsruter forlenges og forsinkes. En stødig og robust forsyningskjede blir både vanskeligere – og viktigere – å opprettholde.



Endrede spilleregler – hybrid krigføring

Endringene vi nå ser i Europa påvirker sikkerhetsarbeidet og prioriteringer. Hybride trusler er mer aktuelt nå enn noensinne. Det mange har oppfattet som teoretiske begrep som «hybrid krigføring» eller «gråsonetaktikker», inngår nå i sikkerhetsvurderinger med tilhørende tiltak for alle som hittil ikke har forholdt seg til dette.

Sikkerhetstruende hendelser som er designet til å se ut som tilforlatelige feil – for eksempel sabotasje som framstår som feil på utstyr med ukjent årsak – er noe vi forventer å se mer av i tiden fremover. Dette ser man i økende grad også i Europa, ofte knyttet til kritisk infrastruktur. Det har vært en rekke mistenkelige hendelser som involverer fysisk sabotasje av kritisk infrastruktur i Europa i 2023 og 2024, som da kutting av kommunikasjonskabler i Tyskland og Frankrike forårsaket betydelige forstyrrelser. Disse handlingene anses gjerne som advarsler eller gjengjeldelser mot land som støtter Ukraina. Infrastruktur som rørledninger og undersjøiske kabler, er sårbar for fysisk sabotasje. Russland har tidligere vist vilje til å gjennomføre slike operasjoner for å destabilisere regionen og sende politiske signaler til Vesten.

For å kunne identifisere hva som er hybride trusler er det viktig å følge med på hva som er utenfor normalbildet, også relatert til frekvens og konsekvens. Dette er spesielt viktig i Nordland, Troms og Finnmark, og på Svalbard, Jan Mayen og Bjørnøya. Vi følger også med på endringer i normalbildet i resten av Norge. Mange av våre kunder og leverandører er spredt utover landet, og flere av disse har svært viktige funksjoner knyttet til samfunnsoppdrag. En ytterligere eskalering av sikkerhetssituasjonen i Europa vil trolig øke trusselen for at sabotasje (enten fysisk eller logisk) kan ramme Telenor Norge direkte eller indirekte. Denne usikkerheten må vi håndtere med resiliens, robuste systemer, god deteksjon og beredskapstankegang.

Militær og politisk signalering er utenrikspolitiske pressmidler. Trusselaktørene gir hint om hvilke kapabiliteter de er i stand til å benytte og utfører handlinger for å fremsette en uuttalt trussel. Dette er også brukt for å skape frykt og usikkerhet. Målet er å påvirke politisk beslutningstaking og opinion, uten å måtte benytte militære virkemidler på en slik måte at det kan utløse krig. Både signalering hvor Telenor er et mål, og signalering som påvirker Telenor indirekte, er mer sannsynlig nå enn tidligere.

Russisktilknyttede cyberaktører har i økende grad utført målrettede angrep mot europeisk infrastruktur siden krigen i Ukraina startet. Disse angrepene fokuserer ofte på kritisk infrastruktur og offentlige institusjoner, og har gjerne en sterkere politisk dimensjon enn tidligere. Der hvor tjenestenektangrep (DDoS) er benyttet som angrep, blir det i denne sammenheng ofte benyttet av aktører omtalt som «hacktivister». Slike koordinerte DDoS-angrep har også forekommet i Norge, og blir ofte satt i sammenheng med aktivitet eller politiske beslutninger som Russland motsetter seg. Andre mål har vært selskaper som bidrar aktivt til å støtte ukrainsk side i krigen.

» Sikkerhetstruende hendelser som er designet til å se ut som tilforlatelige feil – for eksempel sabotasje som framstår som feil på utstyr med ukjent årsak – er noe vi forventer å se mer av i tiden fremover.

Finansiell trygghet i en usikker verden

Tekst: DNB

Finansielle tjenester er grunnleggende for samfunnet. Eksempelvis er det å kunne gjennomføre landets forpliktelser globalt, det at befolkningen har økonomiske midler til å kjøpe mat og medisiner i hverdagen og det å få betalt for tjenester man gjør, essensielt for verdenssamfunnet.

I dag er disse tjenestene i stor grad digitale, og det er ikke et alternativ å gå tilbake til gammeldagse metoder. Derfor er robusthet og motstandskraft en av de viktigste hjørnesteinene i finanssektoren, og DNB er den viktigste støttespilleren for dette her i Norge. Krigen i Ukraina har lært oss at selv ekstreme situasjoner løses best med digitale alternativer. Samfunnet er i dag avhengig av at digitale basisfunksjoner fungerer i kriser og krig.

Dette har dessverre blitt høyaktuelt de siste årene med økt global uro. Likevel er fortsatt faren for cyberangrep og økonomisk kriminalitet finansnæringens høyeste trussel. Angrepene og kriminaliteten øker og behovet for godt samarbeid mellom næringslivet og det offentlige er helt essensielt hvis vi skal lykkes i å skape finansiell trygghet i en usikker verden.

FOTO: ISTOCK.COM / WILLIAM87

Det strategisk viktige nord

For enkelte bedrifter som opererer i hele Norge, som Telenor Norge, er det nødvendig å differensiere mellom de forskjellige regionene i landet. Vi i Telenor støtter oss i stor grad på de helhetlige og nasjonale vurderingene som de nordiske etterretnings- og sikkerhetstjenestene legger frem i sine årlige, ugraderte trusselvurderinger. Vi har også et særlig fokus på våre mest utsatte regioner.

For oss er det særdeles viktig å være observante på lokale forhold som kan spille inn på tjenestene vi leverer. Gitt sikkerhetssituasjonen vi nå opplever, og myndighetenes advarsler om hvilke sektorer i samfunnet som er mest trusselutsatt, har vi et ekstra fokus på kunder hvor dette treffer – enten det er i vestlige deler av Norge med sin olje- og gassvirksomhet – eller i nordområdene som er mer påvirket av interaksjon med Russland enn noe annet sted i Norge.

Telenor har en aktiv tilstedeværelse i arktiske strøk. Dette innebærer at vi har et ekstra behov for å vurdere sikkerhet, beredskap og trusselanalyse – med et spesielt fokus på Nordland, Troms, Finnmark, Svalbard, Jan Mayen og Bjørnøya. At sikkerhetssituasjonen her er mer knyttet til hva som skjer med våre naboland, er hevet over enhver tvil. Dette oppleves i det daglige for Telenor, og er den tilbakemeldingen vi får i dialog med lokale myndigheter.

De arktiske områdene har ikke bare klimaforhold som krever særlig robuste tjenester og oppfølging, de er også mer utsatt for sikkerhetspolitiske spenninger. Dette krever en ekstra årvåkenhet. I en tid hvor infrastruktur i Europa er mer utsatt enn tidligere, og hvor spesielt Russland vurderes å utgjøre en hybrid fare, har vi særskilt fokus på hvordan egen infrastruktur er knyttet opp mot annen kritisk infrastruktur. Gjensidige avhengigheter krever beredskap. Både Russland og (i økende grad) Kina er viktige aktører i nordområdene.

» Kommunikasjon er vitalt for å kunne drive krisehåndtering og vil ved en sikkerhetspolitisk krise være svært kritisk å opprettholde.

FOTO: NIGEL KILLEEN / GETTYIMAGES

» På Svalbard står Telenor i en særstilling som en av de største, viktigste og lengst etablerte bedriftene.

På Svalbard står Telenor i en særstilling som en av de største, viktigste og lengst etablerte bedriftene. Vår posisjon og vår drift, vil trolig være av høy interesse for andre land som også har tilstedeværelse her eller som ønsker å etablere seg i regionen. Klimaendringene gjør at isen smelter fortere, og nye sjøveier åpnes. Det øker både militær og sivil trafikk i nordområdene. Arktiske strøk har tidligere blitt vurdert som strategisk viktige for blant andre Russland, og det er god grunn til å anta at sikkerhetssituasjonen har forsterket betydningen av denne regionen. Økt militær tilstedeværelse både fra allierte stater og fra Russland, fører til at dette området vil oppleve en mer spent sikkerhetssituasjon.

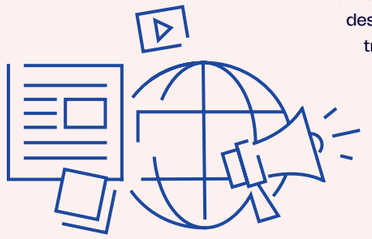
Vi antar at Telenors aktivitet i våre nordlige regioner i tiden som kommer vil være av høyere interesse for utenlandske stater enn tidligere. Dette vil sannsynligvis gi utslag i økt etterretningstrykk – spesielt fra russiske og kinesiske aktører.

Kommunikasjon er vitalt for å kunne drive krisehåndtering og vil ved en sikkerhetspolitisk krise være svært kritisk å opprettholde. Den generelle trusselen mot Telenor Norge vurderes som høyere i denne delen av landet.

Redaktørstyrte medier er viktigere enn noen gang

Tekst: NRK

Spredning av falske nyheter og desinformasjonskampanjer har økt i omfang og er en trussel mot demokratiet. Ved hjelp av AI produseres artikler og bilder som det er vanskelig for mange å se at er falske. Sosiale medier flommer over av syntetiske nyheter og det er vanskelig å stå imot. Målet kan være å lure penger fra folk, eller å svekke folks tillit til media eller andre viktige samfunnsfunksjoner.



NRK har høy tillit og stor oppslutning, og er som allmennkringkaster viktig for å sikre hele befolkningens tilgang til informasjon. Det gjør NRK til et attraktivt mål for desinformasjon og påvirkningsaksjoner. Sikkerhet og kildekritikk er i dagens trusselbilde tett knyttet sammen. NRK må vite hvem som er den egentlige kilden til det vi publiserer.

Det siste året har vi sett flere situasjoner der aktivister har forstyrret direktesendinger for å fremme et budskap. Vi har også sett NRK og NRK-journalisters troverdighet misbrukes gjennom falske nyheter, falske nettsider og annonser til villedning og bedrageri av publikum. Redaktørstyrte medier er viktige i kampen mot falske nyheter og påvirkningsoperasjoner. Tillit er avgjørende, og aldri har NRKs rolle som veiviser i hva som er fakta vært viktigere.

Hvilke endringer ser vi innen cybersikkerhet?

Skillet mellom hva som er statlige og ikke-statlige aktører viskes mer og mer ut. Dette fordi statlige aktører bruker ikke-statlige aktører for å skjule sin tilknytning til ondsinnede handlinger, og fordi metoder deles mellom disse. Vi kan heller ikke lenger med samme grad av sikkerhet forutsi hvilke metoder som vil bli brukt mot oss, basert på hvilke aktører vi tror har interesse for Telenor Norge. Generelt kan vi gjøre oss en del antakelser som vil være relevante for sikkerhetstenkning innen cyberdomenet. Trusselaktørene som er aktive eller kan tenkes å være aktive mot bedrifter som Telenor Norge, vil kunne være interessert i alt fra å skape forstyrrelser, til målrettet innsamling av etterretning, inkludert kartlegging av nettverk for mulige destruktive angrep.

Relatert til ren vinningskriminalitet, ser vi en økning i svindelforsøk rettet mot Telenor Norge og våre kunder. Den teknologiske utviklingen og profesjonaliseringen innen cyberkriminalitet gjør muligheten til å benytte dette mye mer utbredt. Tidligere var man prisgitt egen teknologisk evne for å utføre angrep, nå kan trusselaktører i større grad kjøpe dette som tjenester hos profesjonelle kriminelle.

Ransomware-angrep fortsetter å utgjøre en betydelig trussel mot alle bedrifter. Denne utviklingen krever en styrket respons fra virksomheter gjennom avanserte deteksjons- og gjenopprettingssystemer, og styrket intern (og eventuelt ekstern) beredskap.

Ransomware gjennomføres nå raskere enn noen gang, og evnen til å detektere, rapportere og håndtere indikasjoner på et ransomware-angrep er viktigere enn noensinne. Tidligere har fremgangsmåten vært å kryptere nettverk for å be om løsepenger. Nå ser vi også at dette kombineres med trusler om videresalg av den krypterte informasjonen. Det er viktig å understreke at dette ikke er en garanti for at informasjonen leveres trygt tilbake etter at eventuelle løsepenger er betalt, eller at integriteten i informasjonen er intakt.

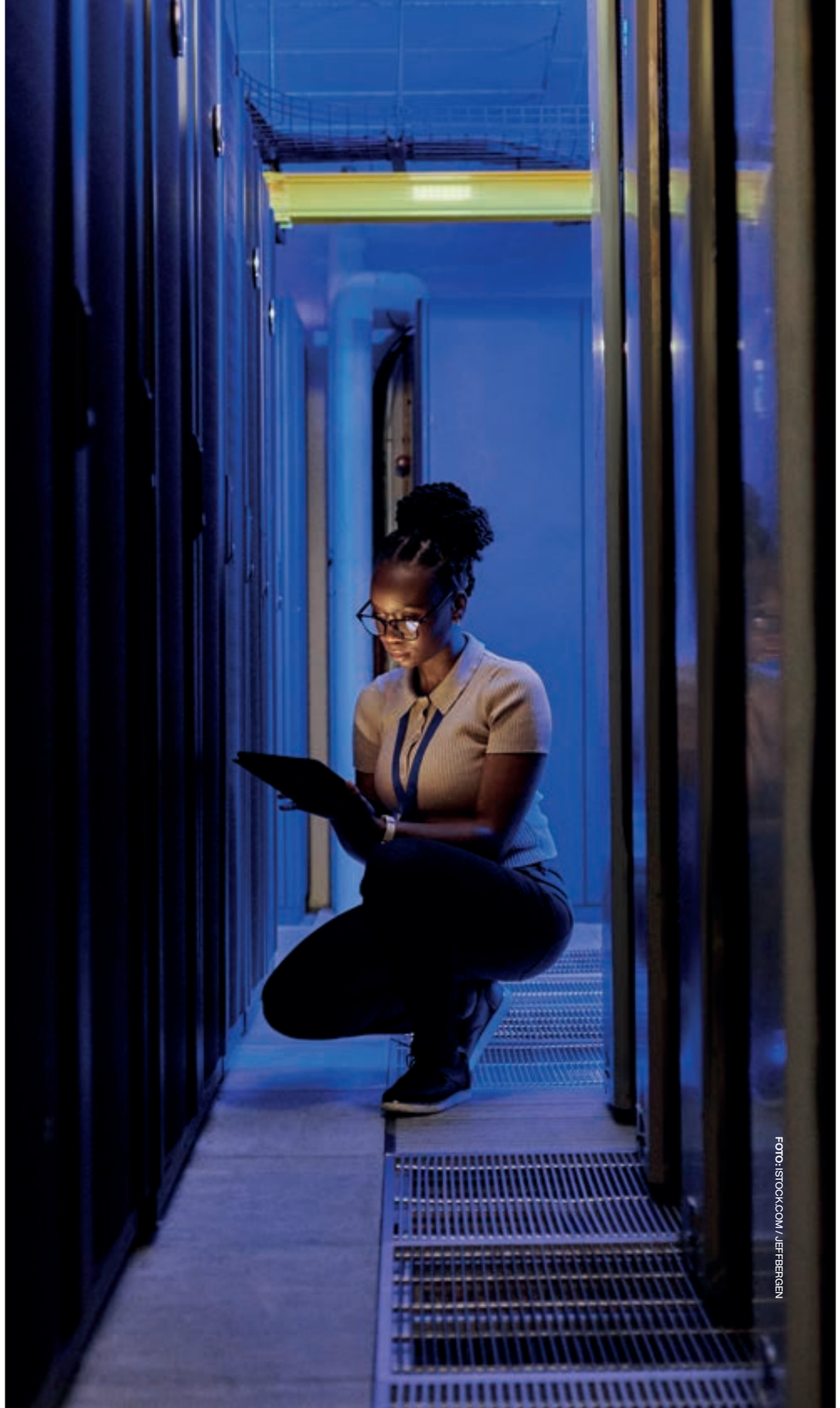


FOTO: ISTOCK.COM / JEFFBERGEN

I likhet med mange andre former for sikkerhetstrusler, ser vi også en økende bruk av målrettede forsøk på sosial manipulering. Man har stadig mindre tid til å oppdage og håndtere forsøk på digitale angrep. Mye av det preventive arbeidet ligger derfor i god sikkerhetskultur i alle deler av bedriften. Hos Telenor Norge er dette noe vi jobber aktivt med hver dag.

For å få innpass i et fremmed nettverk, ser vi også at trusselaktører fremdeles benytter phishing eller spearphishing (målrettet phishing). Phishing som metode er i utvikling og vil trolig fortsette å bli justert for å forbigå endrede sikkerhetsanbefalinger. Vi ser stadig nye metoder her, hvorav bruk av QR-koder i e-post og bruk av iMessage har økt i det siste.

Ved å benytte sosial manipulering, har trusselaktører i andre deler av verden kunnet tilegne seg legitim identifikasjon for å logge på nettverk og utføre spektakulære ransomware-angrep. Slik pålogging er vanskeligere å detektere, fordi det krever at man gjenkjenner unormal oppførsel eller trafikk i nettverket. Man kan ikke lenger basere seg på deteksjon av skadevare. Bevissthetskampanjer og, ikke samt sterke systemer for beskyttelse og verifisering av identitet ved pålogging er svært viktig. Bare én kompromittert påloggingsmetode som gir tilgang på nettverk, kan utgjøre stor skade.

Bruken av skytjenester fortsetter å vokse, og dette gjør skyinfrastrukturen til et mer attraktivt mål for trusselaktører. Trusselaktører benytter også her «legitime innganger» for å infiltrere og manøvrere innenfor skyplattformer. Dette gjør det utfordrende å oppdage sikkerhetsbrudd. Dette understreker behovet for styrket nettverksmonitorering og responsstrategier spesielt tilpasset skyteknologier.

Vedvarende prioritering av sikkerhet samt oppdatering på hvilke trusler som nå gjelder innen cyberdomenet, er viktig for å ha relevante sikkerhetsmekanismer på plass. Rask patching og utfasing av gamle og utdaterte systemer som ikke lenger oppdateres, forblir viktige strategier.

» Man har stadig mindre tid til å oppdage og håndtere forsøk på digitale angrep. Mye av det preventive arbeidet ligger derfor i god sikkerhetskultur i alle deler av bedriften.

Ser du indikatorer på kartlegging?

Indikatorer er «spor» man følger for å komme til riktig konklusjon. Når vi jobber med sikkerhet, er dette et viktig bidrag for å vurdere sikkerhetsrapportering og analysere hva dette kan si om en situasjon. Når vi har indikatorer på at noen kartlegger vår virksomhet, er dette noe som tas på stort alvor. Dette kan gjelde for eksempel fotografering av en installasjon eller mistenkelig kontakt opp mot ansatte. Indikatorer på kartlegging kan sees både i det digitale domenet og det fysiske domenet. Ettersom indikasjoner på kartlegging ikke innebærer noen umiddelbar skade, er det en fare for at dette blir oversett og nedprioritert for å håndtere mer umiddelbare behov.

Kartlegging er ofte blant de første stegene til videre handling for en trusselaktør. Å se etter indikatorer på kartlegging er derfor en viktig start på avvergende sikkerhetsarbeid. I den sikkerhetssituasjonen vi nå befinner oss, er det svært viktig å få med seg nettopp dette.

Kartlegging betyr ikke automatisk at en ondsinnet handling skal gjennomføres, men det kan bety at noen har til hensikt å bruke det senere – eller ønsker å vise at dette kan være en mulighet. For trusselaktører som ønsker informasjon til senere bruk, kan gjentakende kartlegging være nødvendig for å vedlikeholde evnen til å kunne slå til når de ønsker. Indikatorer på kartlegging er derfor svært viktig å ta på alvor, enten det gjelder i det fysiske eller digitale domenet. Kartlegging er en målrettet handling og kan dermed gi verdifull innsikt i hvordan man bør styre sikkerhetsarbeidet. Selv om noe kartlegging kan ha som mål å forstyrre eller avlede oppmerksomhet fra et annet sted, vil det at noen utfører dette, være en indikasjon på at noe er på gang eller at en trusselaktør har fattet interesse.

Bevisstgjøring hos ansatte, kunder og leverandører er viktig for å sørge for at det rapporteres om «mistenkelige hendelser» og på den måten avdekke om kartlegging pågår.

» Bevisstgjøring hos ansatte, kunder og leverandører er viktig for å sørge for at det rapporteres om «mistenkelige hendelser» og på den måten avdekke om kartlegging pågår.

Er du klar?

Beskyttelse av kritisk infrastruktur vil alltid være vesentlig for at et samfunn skal kunne fungere optimalt. Det samme gjelder beredskap for situasjoner hvor samfunnet er satt under press. Dette hjelper bedrifter å bli mer motstandsdyktige mot komplekse trusler.

Beredskapsplanlegging er en absolutt nødvendighet i dagens situasjon preget av hybride trusler. Dette er ikke bare noe bedriftene bør gjøre, men også noe hver enkelt ansatt bør tenke gjennom. Det å vite hvilken rolle en selv har i en krisesituasjon, er svært viktig.

Vet du hva du skal gjøre hvis bedriften din er utsatt for et ransomware-angrep i morgen? Vet du hva du skal gjøre hvis kritiske tjenester er borte? Hvor møter du opp? Hva er din rolle?

I Telenor jobber vi kontinuerlig med disse spørsmålene for å sørge for at kommunikasjonsløsningene vi leverer, skal være tilgjengelige og pålitelige over tid. Vi ser også på hvordan vi skal fungere hvis de som leverer tjenester til oss ikke lenger er i stand til å gjøre dette.

FOTO: ISTOCK.COM / UNISELLER

FOTO: ISTOCK.COM / IGNATIEV

6

Slik angriper de

Ifølge bankene og svensk Økokrim er cyberkriminalitet i ferd med å bli en viktigere inntektskilde enn narkotika for kriminelle nettverk. I dette kapittelet kan du lese om metodene som aktivt brukes mot norske privatpersoner og virksomheter nå.

Dette er de viktigste punktene i årets oversikt:

Phishing-as-a-service
Nye tjenester forenkler jobben for kriminelle

Stjålne brukernavn
og passord samt usikrede servere brukes i cyberangrep mot bedrifter

Kriminelle utnytter fersk informasjon fra LinkedIn

Avlyttingsutstyr
brukes i svindel mot privatpersoner

Safe account-svindel
Kriminelle utgir seg ut for å være fra banken eller politiet

34,6 millioner svindelforsøk via SMS og 22 millioner svindelanrop mot Telenors kunder ble blokkert første halvår

Generativ AI åpner nye snarveier for kriminelle

Tekstmeldinger
sendes via internett for å unngå sikkerhetsfilter

Til venstre: Telenor blokkerte hele 56,6 millioner svindelforsøk via SMS og anrop mot sine kunder i første halvdel av 2024. Bildet er et illustrasjonsfoto.

Da en malaysisk statsborger i fjor ble pågrepet i Oslo med bilen full av avlyttingsutstyr, trodde PST det dreide seg om spionasje.

Det viste seg imidlertid at det hele var et ledd i en omfattende SMS-svindel – og en ny metode for å omgå eksisterende sikkerhetsfiltre.

Det siste året har cyberkriminelle tatt i bruk stadig flere utradisjonelle fremgangsmåter for å nå ofrene sine, enten det er bedrifter eller folk flest.

Godt hjulpet av blant annet kunstig intelligens har det dukket opp nye trusselaktører som står bak phishing-forsøk og andre former for bedrageri. Flere av disse kan knyttes til kriminelle nettverk både her hjemme og i Sverige.

34,6 millioner SMS-er og 22 millioner anrop blokkert første halvår

Det enorme antallet svindelforsøk som stanses av Telenor hver dag, er et tydelig bevis på hvor stort og alvorlig samfunnsproblem nettkriminalitet er. Personene bak svindelforsøkene inngår i velorganiserte kriminelle nettverk som både har kompetanse og ressurser til å gjennomføre sofistikerte angrep i stor skala.

Første halvdel av 2024 blokkerte Telenor hele 56,6 millioner svindelforsøk via SMS og anrop mot sine kunder.

I en spørreundersøkelse gjennomført av YouGov på vegne av Telenor i mars i år svarer 1 av 2 nordmenn over 18 år at de er blitt utsatt for forsøk på digital kriminalitet i første kvartal 2024.

Svindel er en lukrativ inntektskilde for kriminelle, og mange strekker seg langt for å prøve å omgå Telenors og andre virksomheters sikkerhetstiltak. De kriminelle utvikler stadig nye metoder og går langt for å ramme norske virksomheter og privatkunder.

» Første halvdel av 2024 blokkerte Telenor hele 56,6 millioner svindelforsøk via SMS og anrop mot sine kunder.

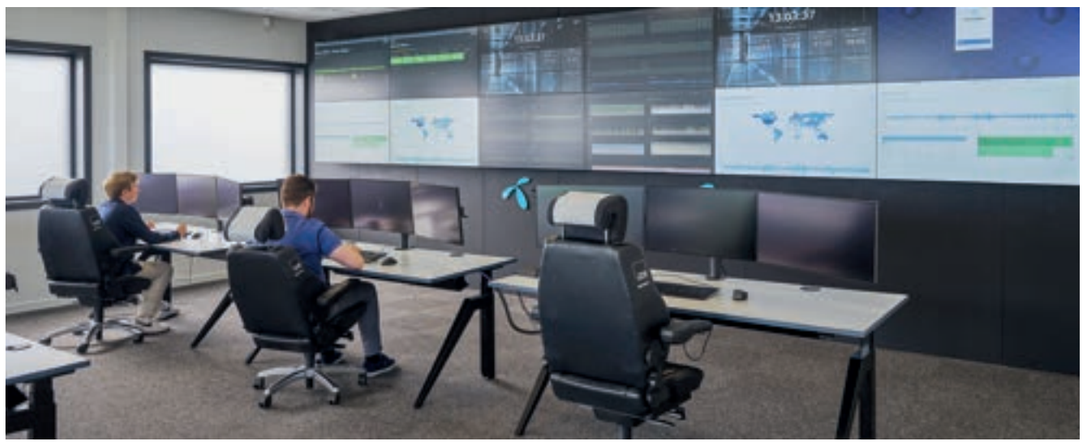


FOTO: HARALD SPJELKAVIK / NEWSLAB

Slik angripes norske virksomheter

Telenors sikkerhetssenter, som monitorerer og beskytter bedriftskunders nettverk og datautstyr, har i snitt håndtert mer enn 20 alvorlige hendelser månedlig den siste tiden.

Dette dreier seg blant annet om avverging av ransomware-angrep og fjerning av såkalte «informasjonstyver» i nettverk, som brukes av kriminelle til å hente ut lister med brukernavn fra bedriften.

I tillegg registreres det hver måned i snitt rundt 140 DDoS-angrep (tjenestenektangrep), som har som mål å overbelaste og lamme servere og nettverk.

Det siste året har sikkerhetssenteret registrert spesielt en dreining i måten norske virksomheter angripes på. Det er spesielt to fremgangsmåter som utmerker seg.

1) Stjeler ansattes brukernavn og passord

En av de mest utbredte metodene som brukes for å angripe virksomheter, er at kriminelle overtar og utnytter virksomhetens legitime brukerkontoer, framfor å utnytte svakheter.

Dette skjer blant annet ved at:

- Angriperne bruker passord som er lekket etter datainnbrudd på andre tjenester, og matcher disse med brukere som har brukt tilsvarende passord på jobbkontoen
- Angriperne tester de mest utbredte passordvariantene mot tusenvis av brukere i ulike bedrifter
- En ansatt blir lurt til å installere en «informasjonstyv» på PC-en, som kopierer ut innloggingsdetaljer og session-cookies
- En ansatt blir lurt til å oppgi brukernavn og passord ved hjelp av phishing

Dersom virksomheten benytter seg av skytjenester kan denne typen angrep få store konsekvenser fordi angriperen lett kan få tilgang til flere ulike systemer via én konto.

Her er effektive mottiltak å benytte seg av tofaktor-innlogging, hardware-nøkler, sertifikatbasert innlogging og passkeys med godkjenning via biometri på PC/mobil.

2) Kommer seg inn via edge devices

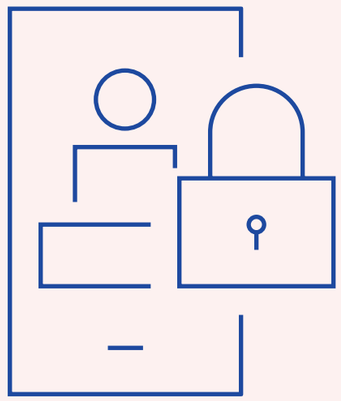
En annen fremgangsmåte angriperne ofte benytter seg av, er å aktivt gå etter såkalte edge devices i virksomhetens nettverk.

Dette er endepunkter i nettverket som er eksponert direkte mot nettet, ofte fordi både ansatte og samarbeidspartnere skal ha enkel tilgang til dokumenter og annen informasjon.

Blant annet dreier dette seg om VPN-endepunkter, MDM-servere, e-postservere og fildelingsservere. Mange av disse har begrensede sikkerhetssystemer, og kan være relativt enkle å kompromittere.

Etter å ha fått tilgang via en slik enhet, kan angriperne hente ut lister med brukernavn og forflytte seg videre innover i nettverket.

For å forsvare seg mot denne typen angrep, er det viktig med god kontroll på tilganger og overvåking av egen ressursbruk i skytjenester. Et godt tips er å ikke ha flere endepunkter med åpen nettilgang enn helt nødvendig.



Utnytter informasjon fra LinkedIn

Flere svindelforsøk den siste tiden tyder på at kriminelle følger nøye med på nettet for å kunne utnytte fersk informasjon til å angripe virksomheter og privatpersoner. Særlig informasjon fra LinkedIn benyttes hyppig, noe Telenor selv har erfart.

Fremgangsmåten foregår nærmest i sanntid: Kort tid etter at en ansatt har oppdatert egen profil med ny stillingstittel, kontaktes HR-avdelingen hos den aktuelle arbeidsgiveren med en e-post der de kriminelle utgir seg for å være den ansatte.

I e-posten blir HR-avdelingen bedt om å oppdatere den ansattes informasjon med nytt kontonummer, slik at neste lønn i realiteten utbetales til de kriminelle.

En lignende metode der fersk informasjon fra nettet brukes til å begå svindel er ved bilsalg på FINN.no. Her kontaktes ofrene med en falsk melding fra Statens vegvesen, og blir bedt om å betale gebyr i forbindelse med salgsmelding eller omregistrering.

Avlyttingsutstyr brukt i svindel mot privatpersoner

Blant verktøyene og fremgangsmåtene som ble brukt i angrep mot privatpersoner det siste året, finner vi også QR-koder, kunstig intelligens, nye nettjenester – og i tilfellet med den malaysiske statsborgeren nevnt innledningsvis, en IMSI-fanger.

Grunnen til at den malaysiske statsborgeren kjørte rundt med avlyttingsutstyr i bilen, var ikke som først antatt for å spionere på myndigheter eller privatpersoner, men fordi det ga ham mulighet til å sende ut SMS-er til forbipasserende uten å måtte ta veien via mobilnettet.

Ved hjelp av en såkalt IMSI-fanger kunne han opprette en direkte forbindelse med alle mobiltelefoner i nærheten. Dermed lyktes han å omgå teleoperatørenes sikkerhetsfiltre – og både AI- og SpamShield-teknologi.

Mange av dem som mottok meldingene var tilfeldig forbipasserende travelt opptatt med julehandel. På den måten økte også sannsynligheten for at flere var uoppmerksomme og dermed responderte raskt og ukritisk på meldinger om uavhentede pakker eller ubetalte regninger.

Foreløpig tyder lite på at slikt utstyr brukes aktivt av kriminelle i stor grad. Likevel illustrerer det hvordan nye metoder tas i bruk for å ta seg forbi sikkerhetsmekanismer på mobilnettet og i IT-systemer.

Tekstmeldinger sendes via nettet: iMessage og RCS

Selv om Telenor blokkerer millioner av e-postsvindler hver måned, har både nordmenns bevissthet rundt mistenkelige lenker og sikkerhetsfunksjoner som blokkerer falske nettsider gjort det mer utfordrende for kriminelle å nå ofre på denne måten.

Det har ført til at mange velger å bruke QR-koder i stedet for lenker når de forsøker å lokke ofre inn på falske nettsider. Quishing er en svindelmetode der ofre blir lurt inn på nettsider som fisker etter påloggings- eller betalingsinformasjon, ved å skanne en QR-kode som ser legitim ut – som for eksempel på en meny eller i en annonse.

Nå er imidlertid tekstmeldinger på mobilen den mest attraktive og effektive metoden for å få nordmenn til å gi fra seg personlig informasjon – rett og slett fordi altfor mange fortsatt lar seg lure.

Antall blokkerte svindel-SMS-er har skutt i været. Alt tyder på at svindlerne merker det godt, for når Telenor blokkerer SMS-er med lenker til falske nettsteder, forsøker de å finne nye veier for å nå målene sine.

Økningen av svindelforsøk som sendes via alternative meldingstjenester har derfor vært stor. Får man en mistenkelig melding via iMessage (iPhone), RCS (Android) eller WhatsApp bør man med andre ord være ekstra varsom.

Meldinger som sendes via iMessage og RCS – altså Rich Communication Services på Android-mobiler – blir sendt med ende-til-ende-kryptering via nettet.

Grunnen til at svindlerne i økende grad bruker slike kanaler, skyldes at Telenor og andre operatører ikke har mulighet til å blokkere slike meldinger, fordi de i likhet med meldinger sendt fra en IMSI-fanger ikke kommer fra mobilnettet – hvor slike lenker i meldinger blir blokkert av sikkerhetsfiltre.

Phishing med uavhentede pakker fortsatt vanligst

Innholdet i phishing-meldingene som sendes i de alternative kanalene kan dreie seg om alt fra spennende jobbtilbud til ubetalte inkassokrav.

Meldinger om en uavhentet pakke eller et problem med en nettbestilling er imidlertid fremdeles vanligst. Disse meldingene brukes gjerne som første ledd i både enkle og mer omfattende bedragerier.

En typisk fremgangsmåte er å lure mottakeren til å tro at det har skjedd noe feil med en bestilling eller levering, for deretter å lokke vedkommende inn på en falsk nettside eller til en samtale med noen som utgir seg for å være fra kundeservice.

Her blir offeret ofte lurt til å gi fra seg BankID eller åpne for fjernstyring av PC-en for å få hjelp med å håndtere hendelsen – hvorpå svindlerne i realiteten tømmer offerets bankkonto.

Selv om phishing med meldinger om uavhentede pakker ikke lenger er noe nytt, er det fortsatt en effektiv metode for svindlerne. Derfor finjusterer de den også kontinuerlig.

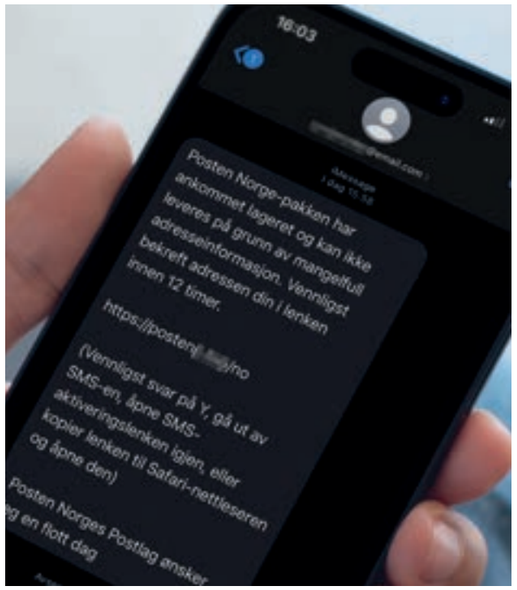
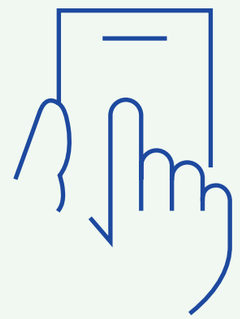


FOTO: TELENOR

Slik ble IMSI-fangeren brukt

- **En IMSI-fanger** er en falsk basestasjon som brukes til å avlytte mobilkommunikasjon ved å bryte inn i kommunikasjonen mellom mobiltelefoner og basestasjonen
- **Utstyret brukes ofte til avlytting og spionasje**, men kan også brukes til å sende ut SMS-er uten at meldingene går via mobilnettet
- **I fjor høst ble en malaysisk statsborger pågrepet** for å ha brukt en IMSI-fanger i en bil til å sende ut svindel-SMS-er til forbipasserende i Bergen og Oslo
- Folk som befant seg i nærheten av IMSI-fangeren fikk tilsendt en SMS som tilsynelatende var fra DHL, Bank Norwegian eller DNB. Herfra ble mottakerne ledet inn til en falsk nettside hvor de ble bedt om å oppgi kortinformasjon og/eller BankID
- **I Norge er det ulovlig** å bruke slikt utstyr for alle andre enn myndigheter innenfor rammen av sine lovlige hjemler



Den siste tiden har det dukket opp flere nettjenester som har effektivisert og strømlinjeformet nettopp phishing-metoden.

Phishing-as-a-service: Svindelverktøy servert på et fat

Den siste tiden har det dukket opp flere nettjenester som har effektivisert og strømlinjeformet nettopp phishing-metoden beskrevet over. Dette har gjort det svært enkelt for kriminelle å skreddersy såkalte «svindelpakker» – selv med begrenset teknisk kompetanse.

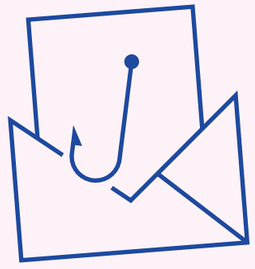
Den nye svindelplattformen Darcula er et godt bilde på nettopp dette.

Plattformen er en såkalt phishing-as-a-service (PhaaS): En brukervennlig nettjeneste som lar kriminelle lage og sende ut meldinger basert på forhåndslagde maler, med såkalte phishing-kit.

I motsetning til eldre phishing-metoder, benytter Darcula teknologi som JavaScript, React, Docker og Harbor – noe som gjør det mulig å hele tiden oppdatere og legge til nye funksjoner uten at brukerne er nødt til å re-installere programvaren.

Phishing-kitene tilbyr brukerne over 200 maler som etterligner merkevarer og virksomheter i mer enn 100 land. Landingssidene holder generelt høy kvalitet og inneholder lokalt språk, logoer og innhold.

Darcula og lignende plattformer benytter seg også av den nevnte omveien via nettet – som gjør at meldingene havner i offerets innboks via iMessage (iPhone) eller RCS (Android).



Slik brukes et phishing-kit:

1. En legitim nettside blir klonet – f.eks. www.telenor.no
2. Innloggings- og/eller betalingssiden byttes ut med et script som stjeler innloggingsdetaljer og/eller kontoinformasjon
3. De modifiserte filene komprimeres i en .zip-fil og lagres som et phishing-kit
4. Phishing-kitet lastes opp til en hacket nettside eller et falskt domene – f.eks. www.telenor-tjenester.top
5. E-post sendes deretter ut med lenker til denne «spoofede» nettsiden

Generativ AI: Åpner nye snarveier for svindlerne

Ikke overraskende har kunstig intelligens begynt å spille en stadig viktigere rolle i hverdagen, både for dem som jobber med IT-sikkerhet og for de kriminelle.

Blant annet sørger ChatGPT – og chatboter spesielt utviklet for kriminell aktivitet, som WormGPT og FraudGPT – for at cyberkriminelle raskt kan tilegne seg informasjon i forkant av et angrep.

Ved å be om all tilgjengelig informasjon om et gitt selskap (for eksempel lister over leverandører og kunder) kan de kriminelle effektivisere datainnsamlingen og profileringen av potensielle ofre.

Teknologien har også gjort det enklere å tilpasse og utføre svindelforsøk over landegrenser, med langt mer realistisk innhold på lokale språk enn det som tidligere var mulig uten bruk av store ressurser.

Spor til de kriminelle nettverkene

Kunstig intelligens, PhaaS-tjenester og stadige finjusteringer har i sum gjort de kriminelles fremgangsmåter både mer effektive og lettere tilgjengelig for langt flere enn før. Stadig mer av den digitale kriminaliteten kobles til norske og utenlandske miljøer som tidligere har vært mest forbundet med narkotikakriminalitet.

Ifølge svensk Økokrim tjener svenske kriminelle nå mer på bedragerier enn på narkotikasalg. Bare i fjor tjente svenske kriminelle 5,8 milliarder kroner på bedragerier.

Lite tyder på at tendensen er annerledes her hjemme. Trolig foregår mange av bedrageriene på tvers av landegrensene. Blant annet avslørte SVTs dokumentarserie Uppdrag Granskning nylig et svensk kriminelt nettverk som begikk omfattende bedrageri av eldre i både Sverige og Norge.

Her ble det også brukt phishing-meldinger om nettbestillinger, med påfølgende telefonsvindel der bankkontoer ble tappet – ofte ved at svindlerne utga seg fra å være fra banken, og at de måtte flytte offerets penger over på en «trygg konto».

Safe account- og politisvindel

Her hjemme har politiet i en pressemelding vært ute og advart mot en lignende fremgangsmåte, der de kriminelle ringer og utgir seg for å være fra politiet. I noen tilfeller har de kriminelle også møtt fysisk opp utenfor boligen for å hente ut BankID, bankkort og telefon.

Telenor registrerte i vinter en stor økning svindelanrop, der de kriminelle utga seg å være fra politiet.

I løpet av bare én uke i november fanget Telenors svindelfiltre opp over 1,1 millioner uønskede samtaler. I løpet av en vanlig uke ligger antallet på rundt 400 000. Økningen skyldes i stor grad mange tilfeller av denne typen politisvindel over telefon.

Ifølge politiet arter svindelen seg slik på telefon:

1. Offeret blir først oppringt av noen som utgir seg for å være fra politiet eller Økokrim. Beskjeden er gjerne at offeret holder på å bli svindlet, for eksempel ved at noen har tatt opp lån i vedkommendes navn
2. Deretter settes telefonen over til en annen kriminell, som utgir seg for å være fra banken, og som skal hjelpe offeret
3. Offeret blir deretter bedt om å oppgi BankID og passord, og får beskjed om å flytte pengene over på en sikker konto
4. Svindlerne bruker deretter BankID for å komme seg inn i ofrenes nettbank
5. Blir overføringen stanset, for eksempel av banken, kan svindleren oppsøke offeret hjemme – hvor de ber om kodebrikken til BankID, bankkort, telefon og lignende

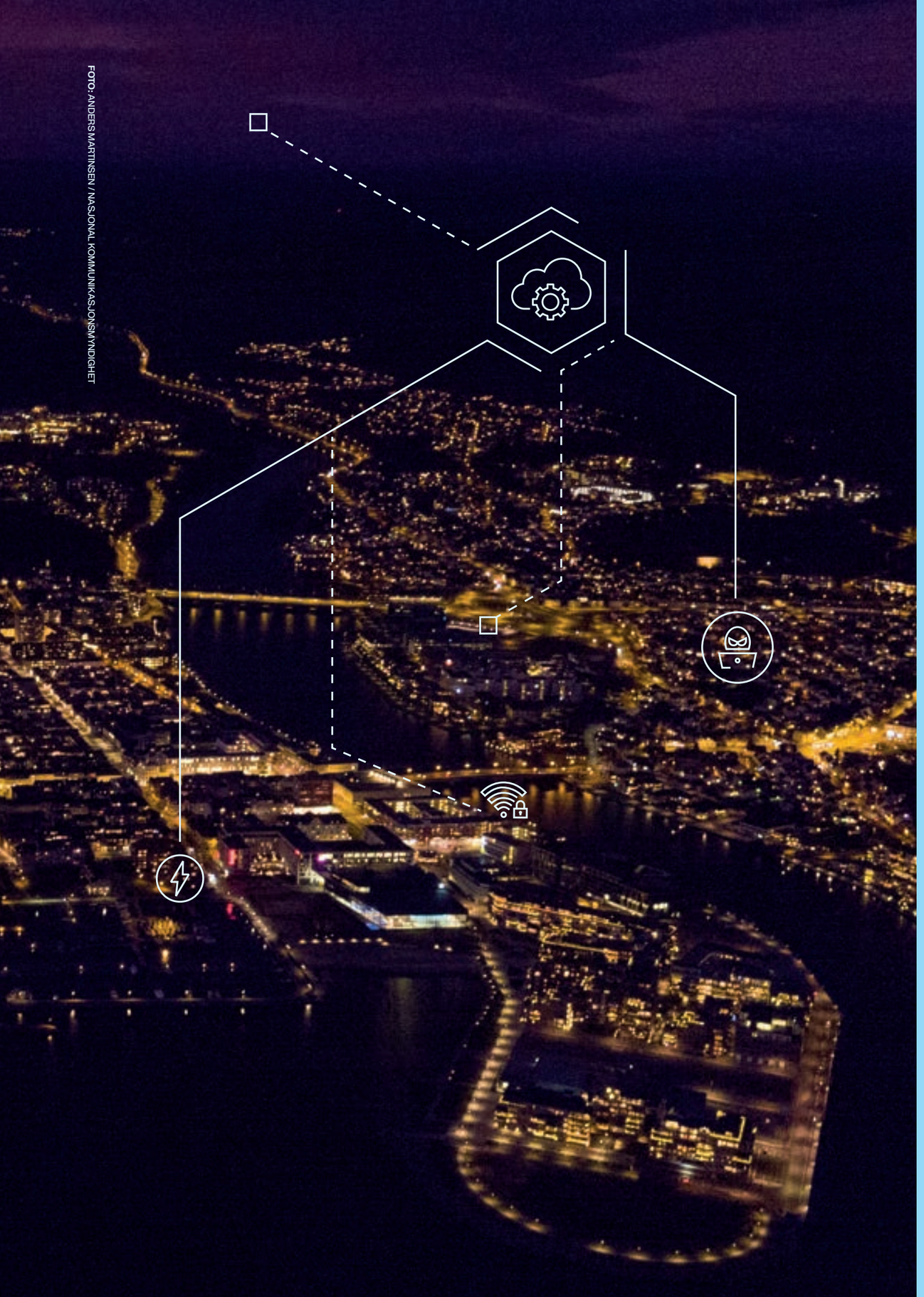


FOTO: ANDERS MARTINSEN / NASJONAL KOMMUNIKASJONSMYNDIGHET

7

Tett samarbeid for digital sikkerhet

Kampen mot digital kriminalitet foregår på flere fronter og ulike nivåer. I dette kapittelet deler Økokrim, Kripos og Nasjonal kommunikasjonsmyndighet noen av sine perspektiver på sikkerhetsåret 2024.

Tekstbidrag fra:
Økokrim,
Nasjonalt cyberkriminalitetssenter (NC3),
Nasjonal kommunikasjonsmyndighet (Nkom)

Felles trusselforståelse er essensielt i bekjempelsen av digital kriminalitet.

Når Kripos, Økokrim og Nasjonal kommunikasjonsmyndighet her deler sine sikkerhetsperspektiver, er nettopp viktigheten av kunnskapsutveksling, felles trusselforståelse og samarbeid mellom private og offentlige aktører et gjennomgangstema.

De tre sikkerhetsaktørene peker blant annet på behovet for økt informasjonsutveksling i kampen mot bedrageri, oppfordrer til å etablere en felles nasjonal trusselforståelse, og viser til hvordan fremveksten av kunstig intelligens og deepfake krever stadig bedre samarbeid mellom offentlige og private aktører.

FOTO: ISTOCK.COM / ECLIPSE_IMAGES

Kripos NC3: Å forstå trusselen

Kunnskapen rundt digitale trusler og kriminalitet må økes for at sikkerhetstiltakene som innføres skal oppnå ønsket effekt. Her kommer Kripos nasjonalt cyberkrimsenter (NC3) inn i bildet.

Kripos NC3 er et nasjonalt senter for etterforskning og bekjempelse av alvorlig digital kriminalitet. For å løse og utvikle vårt samfunnsoppdrag jobber vi kontinuering med en helhetlig kunnskapsbygging langs ulike innsatsspor. Innsatssporene er blant annet metode- og kapabilitetsutvikling. Ved å utvikle nye verktøy og metoder for bekjempelse av digital kriminalitet, økes evnen til å ligge i forkant av kriminaliteten. Etterforskningsbistand til politidistrikt, det private næringsliv og forsterket internasjonalt politisamarbeid, er andre sentrale innsatsområder for NC3.

For å få varig og langsiktige effekter av politiets innsats i det digitale rom er forståelse av trusselen helt sentralt. Derfor produserer Kripos NC3 en årlig ugradert temarapport på cyberkriminalitetsbildet sett fra politiets perspektiv. Innenfor cyberetterretning fokuserer vi på ulike former for cyberrettet og cyberstøttet kriminalitet, men har et særlig fokus på kriminelle konsekvenser av løsepengevirus-nettverk og -aktører, ulike former for datainnbrudd og datatyveri, i tillegg til utviklingstrekk innen AI og dennes betydning for kriminalitetsutviklingen. Gitt utviklingen i den spente sikkerhetspolitiske situasjonen i Europa har også sårbarheter i den cyberfysiske koblingen fått økt oppmerksomhet.

Etablering av en felles nasjonal trusselforståelse er avgjørende for å treffe de rette tiltakene og innsatsen mot den mest alvorlige digitale kriminaliteten. Økt forståelse av samarbeidsflater mellom statlige aktører og kriminelle nettverk har fått og vil fortsette å få økt betydning. Trusselen samfunnet står ovenfor kan ikke fjernes, men den kan reduseres gjennom ulike former for forstyrrelser fra offentlige og private aktører. Samlet sett vil dette forsterke politiets og samfunnets felles evne til å forebygge, varsle, avverge og iretteføre digital kriminalitet.

Økokrim: Situasjonsforståelse og responsevne

For at politiet og andre offentlige og private aktører skal kunne forebygge bedrageri, må det foreligge en omforent og tidsriktig situasjonsforståelse som er basert på et godt kunnskapsgrunnlag.

For lite kunnskapsbygging og informasjonsdeling

Det er i dag få som anmelder bedrageri. Enkelte private foretak har god oversikt over bedrageri som rammer egne kunder. Politiet har frem til nå hatt lite fokus på kunnskapsbygging og har ikke god nok innsikt i reelt omfang, hvilke fremgangsmåter som benyttes og hvor store økonomiske tap bedrageri medfører.

Det er videre lite samarbeid og informasjonsutveksling mellom offentlige etater og private aktører. Regelverket setter begrensninger for effektiv utnyttelse av digitale løsninger som kunne ha understøttet kriminalitetsbekjempelsen. Manglende muligheter for å dele informasjon mellom ulike sektorer i samfunnet utfordrer vår evne til å forebygge, avverge og etterforske bedrageri.

Internasjonale etterforskninger blir enda mer krevende

Det er ressurskrevende å etterforske digital grensekryssende kriminalitet. Regelverket for internasjonalt politisamarbeidet er i stor grad blitt til i en analog tid, myntet på analog kriminalitet. Kriminalitet i det digitale rom med tilpasningsdyktige internasjonale kriminelle blir derfor utfordrende. Økt konfliktnivå og polarisering kan også gjøre internasjonalt politisamarbeid vanskeligere.

FOTO: ISTOCK.COM / DKOSIG

Nasjonal kommunikasjonsmyndighet: Behov for tettere samarbeid mellom offentlige og private aktører

Hvert år svindles virksomheter og privatpersoner for opp mot én milliard kroner. Nå skaper nye svindelmetoder et behov for tettere samarbeid mellom offentlige og private aktører.

Nasjonal ekspertgruppe mot ekomsvindel ble etablert høsten 2023 og utgjør en forsterket offentlig-privat samordning og styring av kampen mot svindel på digitale områder. Gruppen ledes av Nasjonal kommunikasjonsmyndighet i partnerskap med Økokrim. Telenor, Telia, Ice og NRDB deltar fra bransjen. Observatører er Nasjonal sikkerhetsmyndighet, Nasjonalt Sikkerhetsråd, Finans Norge og Digitaliseringsdirektoratet.

Bakteppet er at svindeltrykket er stort på både tale, SMS og Internettbaserte tjenester. Årlig tapes store summer til svindel, viser Finanstilsynets ROS-analyse for 2024. Tall fra Økomkrim viser at det ble anmeldt om lag 26 000 bedragerier i 2023. Mørketallene antas å være store. Svindel ved hjelp av digitale tjenester står for en stor andel.

Gruppen jobber blant annet med å fremme gode og koordinerte spoofing-sperrer på gatewaynivå og gode registreringsløsninger for SMS.

Svindelen utføres av internasjonale kriminelle nettverk. Det er ventet at kunstig intelligens og deepfake vil gjøre det stadig vanskeligere å avsløre svindelforsøk. Dette medfører ytterligere krav til godt samarbeid mellom offentlige og private aktører. Nkom er glad for at Telenor fortsetter å være en sentral bidragsyter i dette viktige arbeidet.

» Det er ventet at kunstig intelligens og deepfake vil gjøre det stadig vanskeligere å avsløre svindelforsøk.

FOTO: ISTOCK.COM / TERO VESALAINEN

8

Utfordringer med dagens beredskaps-organisering – og en mulig løsning

Det finnes i dag ingen mekanismer som ivaretar informasjonsdeling til hele næringslivet under en sikkerhetshendelse. Kan opprettelsen av Næringslivets beredskaps- og sikkerhetssenter være løsningen?

Tekstbidrag fra:
Odin Johannesen,
Direktør i Næringslivets Sikkerhetsråd (NSR)

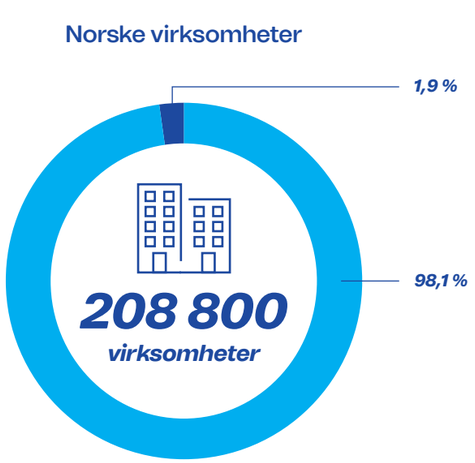
FOTO: ISTOCK.COM/ EZYPIX

På bakgrunn av Forsvarskommisjonens og Totalberedskapskommisjonens rapporter og høringsinnspill, Nasjonalt sikkerhetsfaglig råd, og egne erfaringer har NSR (Næringslivets Sikkerhetsråd) identifisert en rekke utfordringer med dagens organisering av sikkerhets- og beredskapssamarbeidet mellom myndigheter og næringsliv. Disse identifiserte utfordringene er bakteppet for NSRs konseptuelle utvikling av en ny samarbeidsmekanisme om sikkerhet og beredskap.

Norsk næringsliv er mangfoldig

I Norge har vi 208 800 virksomheter med minst én ansatt. Bare 1,9 prosent er store bedrifter med mer enn 100 ansatte. Resten (98,1 prosent) er små og mellomstore bedrifter, med færre enn 100 ansatte. Rundt en tredjedel av virksomhetene med registrerte ansatte er medlem av en arbeidsgiverorganisasjon.

Det finnes per i dag ingen mekanismer som ivaretar varsling/informasjonsdeling til hele næringslivet under en hendelse. Det er derfor krevende for de ulike sikkerhets- og beredskapsmyndighetene å forholde seg til et komplekst næringsliv, som består av hundretusenvis av enkeltstående bedrifter i en flat struktur.



Det offentlige Norge består av en rekke ulike beredskapsmyndigheter på kommunalt, regionalt og nasjonalt nivå.

Alle de 357 kommunene har etter sivilbeskyttelsen plikt til blant annet å ha en kriseledelse, risikoanalyse og beredskapsplan. På lokalt nivå er det også 275 brannvesen, organisert under kommunene.

På regionalt nivå er det 10 statsforvalterembeter, 12 politidistrikt, og 11 heimevernsdistrikt.

På nasjonalt nivå har man, som følge av ansvarsprinsippet (sektorprinsippet), en rekke myndigheter som har ulike ansvarsområder innenfor sikkerhet og beredskap. Noen eksempler er Forsvaret, E-tjenesten, Politidirektoratet, Politiets sikkerhetstjeneste, Kripos (herunder NC3), Økokrim, Nasjonal sikkerhetsmyndighet (herunder NCSC), Direktoratet for samfunnssikkerhet og beredskap, Kystverket, Direktoratet for atomberedskap, Hovedredningssentralen, Statens Vegvesen, NVE, Meteorologisk institutt, Mattilsynet, Tolletaten, Norges bank, Sjøfartsdirektoratet, Havindustritilsynet, Nasjonal kommunikasjonsmyndighet, samt departementene, og flere andre organer. Alle disse organene kommuniserer med næringslivet på ulikt vis.

På nasjonalt nivå finnes det flere overordnede arenaer for sikkerhets- og beredskapskoordinering. Et sentralt planverk er Nasjonalt beredskapssystem, som består av Beredskapssystem for Forsvaret (BFF) og Sivilt beredskapssystem (SBS). Mange av tiltakene i disse planverkene berører næringslivet direkte og indirekte.

Svært få næringslivsaktører har likevel innsikt i planverket, eller i hvilke tiltak som til enhver tid er iverksatt, fordi begge deler er sikkerhetsgradert. Få i næringslivet er sikkerhetsklarert, og det finnes ingen fullgode samarbeidsmekanismer mellom næringslivet og offentlige myndigheter for slike sikkerhetssaker.

Utfordringer med dagens beredskapsorganisering

Digital sikkerhet har utviklet seg til å være et tema som angår hele samfunnet, og berører alle sektorer.

Digital sikkerhet

Digital sikkerhet er avgjørende for å ivareta velferdssamfunnet, viktige samfunnsfunksjoner og nasjonale sikkerhetsinteresser. Stadig flere tjenester i samfunnet, både offentlige og private, blir digitaliserte. Dette gjør at digitale infrastrukturer og systemer blir bærere av flere og flere verdier for både offentlige, private og frivillige aktører. Samfunnets avhengighet av systemene øker. Risiko og sårbarhet i kompleks teknologi og sammenkoblede systemer, den premissgivende rollen til store internasjonale teknologiselskaper og utviklingen i det digitale trusselbildet har bidratt til at digital sikkerhet har utviklet seg til å være et tema som angår hele samfunnet, og berører alle sektorer.

Næringslivets rolle i arbeidet med nasjonal digital sikkerhet blir stadig mer sentral for forebygging og hendelseshåndtering. Private aktører eier og drifter en stor del av den norske kritiske infrastrukturen. I tillegg har private virksomheter betydelig digital system- og spisskompetanse. Det å avdekke sårbarheter, arbeide med risikoreduksjon og håndtering av hendelser er derfor en felles oppgave for både offentlig og privat sektor.

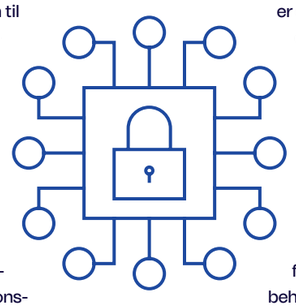
FOTO: TELENOR

Nasjonal sikkerhetsmyndighet (NSM)

Nasjonal sikkerhetsmyndighet (NSM) slår i sitt sikkerhetsfaglige råd fast at situasjonsforståelse er nødvendig for at myndigheter og virksomheter skal kunne møte fremtidige sikkerhetsutfordringer med presise sikkerhetstiltak. Et slikt bilde bygger på kunnskap om det gjeldende trusselbildet, hvilke verdier som må beskyttes og hvilke sårbarheter som kan utnyttes. Myndighetene og virksomhetene har mangelfull situasjonsforståelse på grunn av utilstrekkelig tilgang til trussel- og sikkerhetsinformasjon. Regelmessig rapportering om sikkerhetstilstanden til verdier med betydning for nasjonal sikkerhet danner grunnlag for sektorvise situasjonsbilder. Majoriteten av norsk næringsliv har ikke et eget sektorvis responsmiljø (SRM).

Etableringen av et sikkerhets- og beredskapssenter i og for næringslivet vil styrke evnen til både deteksjon og forebygging gjennom betydelig forbedret situasjonsforståelse.

Justis- og beredskapsdepartementet har et samordningsansvar for digital sikkerhet, og en generell samordningsrolle på samfunnssikkerhetsområdet på sivil side. NSM skal, som det nasjonale fagmiljøet for digital sikkerhet, understøtte og bidra til utøvelsen av sikkerhetsarbeidet i både offentlig og privat sektor. Utøvelsen gjøres av Nasjonalt cybersikkerhetssenter (NCSS). NSR har siden oppstarten i 2019 vært partner i dette samarbeidet. Partnerskapet gir NSR innblikk i den til enhver tid gjeldende sikkerhetssituasjonen, samtidig som vi er en del av et nasjonalt nettverk for kunnskapsformidling om og forebygging av digitale sikkerhetshendelser.



Arbeidet med digital sikkerhet i ulike sektorer er organisert gjennom sektorvise responsmiljøer (SRM). I dag finnes det rundt 20 SRM-er. Kraftbransjen, helsesektoren, justissektoren, Forsvaret, Regjeringen og ekom-sektoren er eksempler på sektorer som har sitt eget digitale responsmiljø. I næringslivet har noen bransjer gått sammen om å etablere egne sentre for digital sikkerhet, slik som for eksempel rederiene (Norma Cyber), kraft- og oljebransjen (KraftCERT), samt finansbransjen (NFCERT). Noen av disse er, eller er i ferd med å bli, formelt utpekt som SRM av ansvarlige departementer.

Den største delen av næringslivet er imidlertid ikke knyttet til et sektorvis responsmiljø. Det betyr at de fleste bedrifter i dag ikke er i et system for varsling og informasjonsdeling om digital sikkerhet. NSR har gjennom sitt arbeid generelt og med Mørketallsundersøkelsen spesielt, etablert et godt bilde av cybersikkerheten i næringsliv og virksomheter på et nasjonalt nivå. Vi er særlig bekymret for digital sikkerhet i små og mellomstore bedrifter, som i dag ikke er en del av de sektorvise responsmiljøene. Disse bedriftene er viktige spillere i verdikjedene til de store virksomhetene i Norge. Vi vet også at det er i denne kategorien vi finner flest virksomheter som heller ikke har et rammeverk og/eller styringssystem for informasjonssikkerhet, noe som ytterligere øker virksomhetens sårbarhet overfor cyberhendelser. I dette bildet er det spesielt viktig med et SRM som kan motta og videresende varsler og råd knyttet til digital sikkerhet på en forutsigbar, kontrollert og sikker måte. Videre er det behov for et SRM som kan motta rapporter fra næringslivet, og vurdere og videreformidle et aggregert situasjonsbilde til myndighetene.

Mange bransjer har oppdaget denne sårbarheten, og ønsker å opprette egne sektorvise responsmiljø. Dette er etter vårt syn

FOTO: ANETTE ASK / FORSVARET

Cyberforsvarets IKT-tjenester (CIKT) på Kolsås. Illustrasjonsfoto.

Forsvarskommisjonen

Forsvarskommisjonen slår fast betydningen av kunnskap og bevissthet om sikkerhetssituasjonen for det grunnleggende beredskapsarbeidet, og at denne informasjonen må deles på tvers av sektorer, inkludert privat sektor, for å bedre forsvarsvilje og styrke forsvarsevnen. Næringslivets og industriens rolle i totalforsvaret bør tydeliggjøres, og knyttes sterkere til strukturene for nasjonal beredskap og krisehåndtering. På samme måte som for skipsfarten, som har en etablert beredskapsstruktur, bør det bygges opp rutiner og prosesser for beredskap og samarbeid med andre sentrale deler av det private næringsliv, herunder transport, IT, digitale tjenester og vitale forsyninger.

» Det finnes per i dag ingen mekanismer som ivaretar varsling/ informasjonsdeling til hele næringslivet under en hendelse.

en uheldig utvikling. Ved å etablere et stort antall små, bransjeorienterte sentre for digital sikkerhet vil man trolig ikke oppnå tilstrekkelig kvalitet og dybde i hvert enkelt senter. Samtidig vil kampen om kvalifisert arbeidskraft bli stor. En ukontrollert utvikling av stadig nye SRM-er er derfor ikke ønskelig i et overordnet sikkerhetsperspektiv.

På oppdrag fra Justis- og beredskapsdepartementet gjennomførte KPMG i 2022 en evaluering av ordningen med sektorvise responsmiljøer (SRM). Formålet med evalueringen var å etablere et beslutningsgrunnlag for den videre utviklingen av SRM-ordningen. Evalueringen viste at det er stor variasjon i modenhet, omfang, kompetanse og innretning mellom de ulike SRM-ene. KPMG anbefaler at det etableres tre standardiserte nivåer av sektorvise responsmiljøer, der minimumskravene øker med virksomhetens betydning for grunnleggende nasjonale funksjoner.

For å møte disse utfordringene arbeider NSR med et nytt konsept for sikkerhet og beredskap i næringslivet. Vi ønsker å etablere Næringslivets beredskaps- og sikkerhetssenter (NBSS). NBSS skal være et senter for styrking av fysisk sikkerhet, digital sikkerhet og beredskap i norsk næringsliv, men ikke erstatte eksisterende samarbeidsordninger mellom næringslivet og offentlige myndigheter der det allerede er velfungerende samarbeidsmekanismer.

NSR tror det er store synergier i å se et senter for digital sikkerhet i sammenheng med et senter for fysisk sikkerhet og beredskap. Evne til å sende og motta varsler til hele næringslivet vil være en grunnleggende funksjonalitet for senteret, uavhengig av hendelsestype. For den store andelen små og mellomstore bedrifter vil trolig snevre avgrensninger mellom fysisk sikkerhet, digital sikkerhet og beredskap fremstå uforståelig. Ved å konsentrere seg om ett senter, skaper man forutsigbarhet hos denne målgruppen. Overfor myndigheter og andre samarbeidspartnere vil også ett senter bidra til at innslagspunktet til næringslivet forenkles.

Direktoratet for samfunnssikkerhet og beredskap (DSB)

Direktoratet for samfunnssikkerhet og beredskap (DSB) er enig med Totalberedskapskommisjonens anbefaling om å inkludere næringslivet i sentralt, regionalt og lokalt beredskapsråd. Samtidig peker de på at det erfaringsmessig har vært krevende å velge ut hvilke næringslivsaktører som skal delta på de ulike samordnings- og krisehåndteringsarenaene: «Arenaene kan ikke romme alle aktørene på grunn av mengden næringslivsaktører veiet opp mot effektiv samordning».

FOTO: ODD SKARBØMYR, DSB, CC BY-ND 2.0

Et essensielt sikkerhetsorgan

Næringslivets beredskaps- og sikkerhetssenter (NBSS) skal styrke samholdet og informasjonsflyten for landets organiserte næringsliv. Dette skal sørge for et sterkere sikkerhetsgrunnlag på tvers av norsk næringsliv.

NBSS ...

... ER ET INITIATIV fra det organiserte næringslivet for å styrke sikkerhets- og beredskapsarbeidet i næringslivet gjennom økt informasjonsdeling og samarbeid, men uten formelt ansvar eller myndighet. Senteret kan ikke pålegge bedrifter tiltak eller binde næringslivets ressurser på noen måte.

... SKAL VÆRE ET KONTAKTPUNKT for offentlige sikkerhets- og beredskapsmyndigheter mot næringslivet, for eksempel ved behov for bistand fra næringslivet, eller ved behov for å dele informasjon til næringslivet.

... SKAL REPRESENTERE OG IVARETA næringslivets fellesinteresser i myndighetenes regionale og nasjonale beredskapsrådsstrukturer.

... SKAL ORGANISERE næringslivets regionale beredskapsrepresentasjon, slik at næringslivet fremstår mest mulig samlet i regionale beredskapsstrukturer. NBSS skal motta innkallinger, referater og situasjonsoppdateringer fra regionale beredskapsstrukturer, samt rapporter fra regionale beredskapskontakter/liaisoner. Denne informasjonen brukes til å bygge et nasjonalt situasjonsbilde som primært skal benyttes til støtte for egen forebyggende virksomhet, men som ved behov kan deles med bedrifter, næringsorganisasjoner og andre aktører.

... SKAL SØRGE FOR at bedrifter, næringsorganisasjoner og andre aktører kan medvirke i det regionale beredskapsarbeidet.

... SKAL BISTÅ de regionale beredskapsrepresentantene med praktisk beredskapsarbeid, herunder varsling og informasjonsdeling, informasjonsmøter og forankring av posisjoner.

... SKAL BYGGE et nasjonalt situasjonsbilde, som ved tjenstlig behov skal kunne deles med bedrifter, næringsorganisasjoner, myndigheter og andre aktører. NBSS skal vedlikeholde varslingslister for utsending av slik informasjon. Det er et mål at NBSS skal sikre mest mulig lik situasjonsforståelse mellom aktører på næringslivssiden, og skal kunne ta initiativ til graderte og ugraderte orienteringer til relevante aktører ved behov.

... SKAL VÆRE FORBEREDT på å representere næringslivet i nasjonale råd, forum og utvalg om sikkerhet og beredskap. Det kan for eksempel være i DSBs nasjonale samvirkekonferanser, Sentralt totalforsvarsforum og lignende.

... SKAL HA EVNE til varsling og informasjonsdeling til alle norske bedrifter, basert på offentlige og tilgjengelige data. NBSS skal også ha evne til sikker og fortrolig informasjonsdeling til det profesjonelle beredskaps- og sikkerhetsmiljøet i næringslivet og næringsorganisasjonene, gjennom et nytt system for ugradert informasjonsdeling.

» NBSS skal være et senter for styrking av fysisk sikkerhet, digital sikkerhet og beredskap i norsk næringsliv.

FOTO: ISTOCK.COM / BIM

... SKAL KUNNE TA IMOT varsler fra næringslivet, veilede og eventuelt henvise til riktig myndighet eller bistandsressurs. Varslingsmottaket vil også bidra til at man kan bygge et systematisk og overordnet situasjonsbilde fra næringslivet som kan deles til myndighetene.

... SKAL KUNNE UTVIKLES til et sektorvis responsmiljø/sektorvis cybersikkerhetssenter med meget begrensede ambisjoner for de deler av næringslivet som i dag ikke er underlagt et etablert responsmiljø (nivå 1 i henhold til KPMGs anbefalte nivådeling).

Behovet for et sektorvis responsmiljø for næringslivet handler primært om bedriftenes behov for å bli varslet når myndighetene har behov for å spre sikkerhetskritisk informasjon om digital sikkerhet. I dag eksisterer det ingen varslingssystem som omfatter hele næringslivet. Et cybersikkerhetssenter for næringslivet vil også kunne være innslagspunkt for bedrifter som er rammet av ulike digitale hendelser. Dette vil kunne redusere trykket på Nasjonalt cybersikkerhetssenter, som i større grad vil kunne forholde seg til samfunnskritiske aktører og aggregerte situasjonsbilder fra de ulike sektorvise responsmiljøene.

... SKAL HA OVERSIKT over fagkompetanse og materiell i industrivernet, for å gjøre disse ressursene mer gripbare for myndighetene (samarbeid med NSO).

... KAN HA EN DØGNKONTINUERLIG vaktfunksjon, i første omgang for myndighetene, næringsorganisasjonene og det profesjonelle sikkerhets- og beredskapsmiljøet i næringslivet.

... ER ET FYSISK SITUASJONSSENTER i Næringslivets hus for daglig drift og behandling av gradert informasjon.

... SKAL VÆRE TILGJENGELIG på Nødnett og Nasjonalt begrenset nett, for å ha sikre og redundante kommunikasjonsløsninger med myndigheter og sentrale næringslivsaktører.

Sikkerhets- og beredskapsutfordringene vi står overfor i dag krever en mer helhetlig tilnærming, der samarbeid mellom offentlige myndigheter og næringsliv står sentralt. Etableringen av Næringslivets beredskaps- og sikkerhetssenter er et skritt i riktig retning for å møte disse utfordringene. Gjennom NBSS vil det siktes mot bedre informasjonsdeling og mer effektiv koordinering mellom næringsliv og myndigheter, og styrking av den nasjonale beredskapen. Næringslivet må integreres som en del av Norges totale beredskap, og da er det nødvendig å bygge strukturer for et effektivt og koordinert samarbeid om sikkerhet og beredskap.

» Næringslivet må integreres som en del av Norges totale beredskap, og da er det nødvendig å bygge strukturer for et effektivt og koordinert samarbeid om sikkerhet og beredskap.

Totalberedskapskommisjonen

Totalberedskapskommisjonen mener det er nødvendig å innlemme næringslivet i nasjonal beredskap på en grunnleggende annerledes måte enn det som er tilfellet i dag. Næringslivet er i seg selv en beredskapskapasitet uavhengig av myndighetenes behov for leveranser. Infrastruktur, lagerbeholdninger og produksjon av varer og tjenester er ofte i privat eie, og myndighetene er avhengige av slike kapasiteter i beredskap og krisehåndtering. Næringslivet er ikke representert i råds- og beslutningsstrukturer. Mangel på etablerte fora og kontakt med sentral kriseledelse kan føre til at næringslivet kommer sent i gang med koordinering, informasjonsutveksling og samhandling. Når en krise inntreffer, er hele samfunnet avhengig av at næringslivet både har sterk nok egenberedskap og at næringslivets ressurser er gripbare i krisehåndteringen. For å avverge dette slår kommisjonen fast at næringslivet bør være integrert i den formelle beredskapsrådsstrukturen på sentralt, regionalt og lokalt nivå, og peker på NSR som et naturlig utgangspunkt for integrering av næringslivet i nasjonal beredskapssammenheng.

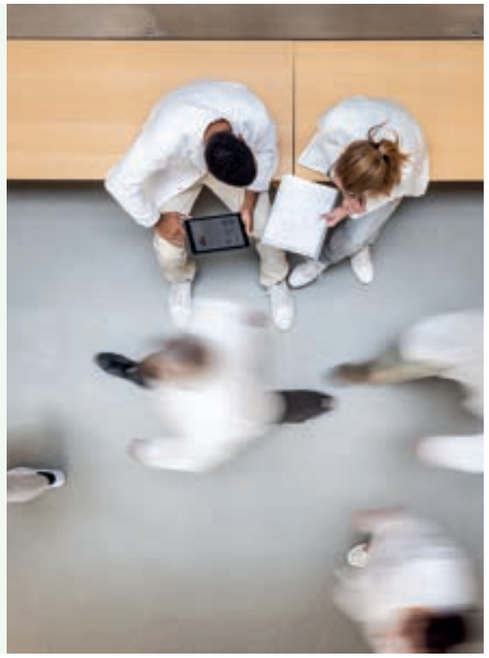


FOTO: ISTOCK.COM / SANJERI

FOTO: ISTOCK.COM / BERK UCAK

FOTO: HARALD PETTERSEN / ©EQUINOR

9

Derfor er *resiliens* den nye sikkerheten

Trusselbildet har tvunget fram endringer i måten landets viktigste virksomheter jobber med sikkerhet. Så hva skjer egentlig hvis NRK, DNB eller Equinor skulle bli angrepet i dag?

Til venstre: Selskaper som Equinor er avhengige av å kunne levere i en unntakstilstand. Det krever robusthet og resiliens.

Trusselbildet mot Norge er mer alvorlig nå enn for bare ett år siden. Det har medført flere endringer i måten noen av Norges viktigste virksomheter jobber med sikkerhet og håndtering av sikkerhetshendelser.

Mye handler om å tilpasse seg for å kunne opprettholde driften, selv i en krise.

– Robusthet og redundans i infrastruktur og systemer har blitt nødvendig for å beskytte seg i dagens trusselbilde. Det samme har evnen til å tåle og komme tilbake fra en alvorlig hendelse, sier Rolv R. Hauge, BCM Manager i Telenor Norge.

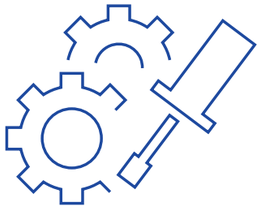
I likhet med mange andre virksomheter har Telenor de siste årene utvidet porteføljen av tiltak for å trygge forretningskontinuitet og evnen til å hente seg raskt inn etter en hendelse.

Modningen innen sikkerhetstenkning har tatt de fleste virksomheter på en reise, mener Hauge.

– I starten handlet alt om å beskytte. Lenge var det å ha en brannmur ansett som god nok sikkerhet. Derfra gikk det til en gradvis erkjennelse av at inntrengning likevel skjer, og at man må ha evne til å oppdage og håndtere hendelser.

– I dag har de fleste flyttet fokus til overlevelse og gjenoppretting etter en hendelse.

Nettopp derfor er resiliens valgt som gjennomgangstema for årets utgave av Digital sikkerhet.



» Robusthet og redundans i infrastruktur og systemer har blitt nødvendig for å beskytte seg i dagens trusselbilde.

i

Dette er resiliens

- Resiliens viser til en virksomhets evne til å tilpasse seg, stå imot og komme seg etter en sikkerhetshendelse.
- En virksomhet eller et system er resilient når det er motstandsdyktig i flere lag, og er i stand til å opprettholde eller returnere raskt til operasjonell drift.
- Begrepene robusthet, motstandsdyktighet og resiliens brukes gjerne om hverandre. Alle disse kan ses på som motsatte begreper av sårbarhet.

FOTO: OLE JØRGEN BRATLAND / ©EQUINOR

Motstandsdyktighet – fra A til Å

Kort fortalt handler resiliens om hele virksomhetens evne til å tåle og komme tilbake fra en alvorlig hendelse, enten det er et cyberangrep eller en naturkatastrofe.

– I de fleste virksomheter er man avhengig av en rekke innsatsfaktorer som inngår i kritiske prosesser. Blir de gjort utilgjengelige på grunn av en hendelse, starter først hendelseshåndteringen – etterfulgt av arbeid med gjenoppretting. Samtidig er man nødt til å tenke forretningskontinuitet gjennom en fase der man mangler kritiske innsatsfaktorer, forklarer Hauge.

Slike tiltak kan ha en rekke former – fra reserveløsninger som gir nær fullt fungerende prosesser og produksjon til nødløsninger som kun sikrer en absolutt minimumsfunksjon.

– Tiltak for å ivareta forretningskontinuiteten og tiltak for å styrke evnen til gjenoppretting må ofte balanseres, og omtales derfor som *business continuity* og *disaster recovery* under fellesbetegnelsen BC/DR.

Samtidig vil alvorlige hendelser ofte utgjøre en krise for virksomheten. Dette fordrer en egen form for ledelse, som både må sørge for riktige prioriteringer og tydelig kommunikasjon underveis.

For å styrke evnen til å gjenopprette, gjennomføre kontinuitetstiltak og utøve kriseledelse, trengs det ikke bare gode planverk, men også trening og testing opp mot ulike scenarier.

Nettopp dette har også vært sentralt i arbeidet til NRK, DNB og Equinor gjennom de siste årene.

Som hos Telenor, er det heller ikke her noe alternativ å sette driften på pause. Blir systemene satt ut av spill, må samfunnskritiske funksjoner fremdeles fungere.

NRK: – Må kunne formidle, uansett

I en hverdag hvor mediehusene stadig utsettes for komplekse DDoS-angrep fra fiendtlige aktører, har konkrete beredskapsplaner og reserveløsninger blitt kritiske. Hos NRK er planverket på plass dersom en krise skulle oppstå på Marienlyst.

– Den største forskjellen på tradisjonell sikkerhetstenkning og å jobbe med resiliens, er graden av kompleksitet. De fleste er i dag avhengig av mange systemer, og det er ikke alltid lett å avgjøre hva som må prioriteres i en krise, sier Øyvind Vasaasen, sikkerhetssjef i NRK.

Som allmennkringkaster har det for NRK alltid vært viktig å ha en reserveløsning tilgjengelig dersom TV- eller radiosendingen plutselig skulle gå i svart. I dag er den delen av NRKs virksomhet som sikrer kriseinformasjon til befolkningen også underlagt sikkerhetsloven.

– NRK må kunne formidle beskjeder fra myndighetene til befolkningen, uansett om vi er i krig eller blir utsatt for et cyberangrep. Kontinuitet og motstandsdyktighet er derfor noe vi jobber med hele tiden, sier Vasaasen.

For 10 år siden etablerte NRK en kontinuitetsplan som blant annet inneholder tiltak for hvordan de fortsatt skal kunne publisere nyheter og informasjon dersom systemene på Marienlyst blir rammet. De siste årene har planverket blitt styrket ytterligere for å tilpasse seg dagens trusselbilde og NRKs produksjonsstruktur.

Selv om teknologien har endret seg mye, holder det ikke å kun sitte med en PC når du skal kringkaste nyheter til hele Norge. Derfor er NRK nødt til å trene på å bruke alternative løsninger.

– Vi har jevnlig sendinger fra det som i dag er vår reserveløsning, rett og slett fordi vi trenger en «varm» løsning. Skulle ting gå i svart på Marienlyst, vil den alternative lokasjonen kunne holde det gående med nyhetsoppdateringer og sendinger til NRK-systemet er oppe og går igjen, sier Vasaasen.

I NRKs egen trusselvurdering peker de ut flere aktuelle trusler akkurat nå – som påvirkning og desinformasjon, aksjonisme, oppetid og publiseringsevne, svekket tillit til innholdet, misbruk av merkevaren, datalekkasjer og informasjonstyveri.

FOTO: HANS A. RØSBACH, CC BY-SA 3.0, VIA WIKIMEDIA COMMONS

– Generelt er det en mer krevende sikkerhetssituasjon for mediehusene nå enn tidligere. Vi utsettes for flere DDoS-angrep fra aktører som ønsker å ta oss ned, samtidig som falske nyheter daglig setter redaksjonene på prøve.

I dag har NRK et eget beredskapsplanverk for å håndtere kriser. I tillegg har de etablert et styringssystem for sikkerhet, inspirert av ISO 27001.

– Vi har styringsdokumenter på virksomhetsnivå, som videre er brutt ned til retningslinjer og prosedyrer. Når vi jobber med prinsipper for sikkerhet, som er vårt overordnede dokument, setter det rammen for sikkerhetsarbeidet i NRK, sier Vasaasen – og forsetter:

– Ofte henger de ulike truslene sammen. Digital sikkerhet handler også om fysisk sikkerhet, og derfor er rutiner på hvem du slipper inn i bygget også en del av den digitale motstandskraften.

Motstandsdyktighet er noe NRK jobber med hele tiden, også i form av å ha bedre operativ IT-sikkerhet og å klare å fange opp forsøk på eventuelle digitale angrep. De siste årene har de styrket IT-sikkerhetsmiljøet betydelig, forklarer Vasaasen.

– NRKs beredskapsplanverk bygger på det nasjonale CIM-systemet. Dette er adskilt fra NRK og vil fungere selv om alt hos oss er nede. Her har NRK planer for ulike situasjoner, helt ned på tiltakskort-nivå.

Vasaasen mener det viktigste tiltaket de har gjort for å styrke beredskapen er å ha slike konkrete planverk – og å bruke planverket jevnlig.

– Mange tenker nok litt for ofte at de ikke trenger å bruke kriseplanverket, fordi de kan løse situasjonen uten det. Veldig ofte viser det seg at ting kunne vært løst bedre om man fikk mer systematikk bak valgene og handlingene sine. Det er en mye mer effektiv måte å jobbe på, understreker han.

» Vi utsettes for flere DDoS-angrep fra aktører som ønsker å ta oss ned, samtidig som falske nyheter daglig setter redaksjonene på prøve.

DNB: – Redundans i alle ledd

Til tross for et dystert digitalt trusselbilde, kan ikke finansnæringen gå tilbake til analoge løsninger. Hos DNB har et robust dybdeforsvar sørget for en nedgang i alvorlige cybersikkerhetshendelser.

Også Norges største bank har de siste årene hatt stort fokus på kontinuitetsplanlegging og robusthet. For dem er det ikke noe alternativ til det digitale.

– Det handler ikke lenger bare om å få på plass IT-systemet igjen, men om hvordan man kan operere under slike forhold, sier Anders Hardangen, sikkerhetsdirektør i DNB.

I løpet av 2023 håndterte DNB 20 208 cybersikkerhetshendelser. Banken håndterte også elleve hendelser med «høyt potensial for negativ påvirkning på DNB».

Begge deler er færre enn foregående år, noe som primært skyldes arbeid med å gjøre konsernets IT-systemer mer resilient, mener Hardangen.

– Takket være et robust dybdeforsvar klarer vi å stoppe flere angrep i en tidligere fase, og at de i tillegg får færre konsekvenser. Når vi utvikler nye produkter og tjenester i dag, tenker vi redundans hele veien. Det samme gjelder måten vi treffer kundene på.

I finansnæringen har kravene til oppetid og å kunne levere digitale tjenester vært viktig i flere tiår. Utviklingen av risikobildet i nyere tid har imidlertid ført til endringer, også i DNB.

– De mange angrepene med løsepengevirus har vist at alle kan rammes, og at de forretnings- og kundemessige konsekvensene kan bli enorme. Russlands aggresjon er en annen faktor som har understreket viktigheten av å ha gode kontinuitetsplaner og alternative løsninger, sier Hardangen.

– Det er mye som er viktig i hverdagen, så i en krise er man nødt til å prioritere. På de kapabilitetene vi prioriterer, må vi være motstandsdyktige og ha gode alternativer som fungerer også under suboptimale forhold.

De siste årene har DNB fornyet hele rammeverket for forretningskontinuitet og gått for en internasjonal standard der de har definert de mest kritiske tjenestene og funksjonene i virksomheten.

– Her handler det om å legge opp et strukturert løp med konsekvensanalyser, risikovurdering, etablere kontinuitetsplaner og teste dem. Dette er krevende i et stort digitalt økosystem, og mye handler om å prioritere det viktigste først og sørge for at det er godt nok.

For et finansforetak som DNB er det ikke noe alternativ til det digitale. For DNB handler det derfor om å finne digitale løsninger som kan dekke de sikkerhetsmessige behovene deres.

– Vi kan ikke gå 50 år tilbake til kontanter og bankkontorer på hvert hjørne. Til det beveger det globale finansmarkedet seg for fort i dag. Selv i ekstremsituasjoner som i Ukraina, ser vi at det å opprettholde digitale finanstjenester ble eneste løsning, fordi det ble for farlig å frakte kontanter.

– Som samfunn er vi helt avhengig av informasjon og å ha kraft- og telekom-infrastruktur i bunn. Som finansforetak er vi avhengig av at digitale tjenester fungerer – også i en unntakstilstand, sier Hardangen.

FOTO: EKELY VIA GETTY IMAGES

» For et finansforetak som DNB er det ikke noe alternativ til det digitale. For DNB handler det derfor om å finne digitale løsninger som kan dekke de sikkerhetsmessige behovene deres.

Equinor: – Ikke nok bare å stå i krisen

Forandringer i det geopolitiske bildet og et økt fokus på det fornybare markedet, er blant grunnene til at Equinor nå utfører endringer i beredskapsorganisasjonen. Selskapet ser nå mer holistisk på sikkerhetsutfordringene.

Et annet norsk selskap som er avhengig av å kunne levere i en unntakstilstand, er Equinor.

Norges største energiselskap har også vært med på noen av de mest alvorlige sikkerhetshendelsene i norsk næringsliv, som gisselaksjonen ved In Amenas i Algerie i 2013.

Med en bred internasjonal tilstedeværelse og operasjoner som tidvis har høy potensiell risiko, er beredskap og krisehåndtering en integrert del av det meste selskapet foretar seg.

Samtidig har endringer i det geopolitiske bildet, underleggelse av sikkerhetsloven og selskapets dreining mot det fornybare markedet bidratt til kursendringer i sikrings- og beredskapsarbeidet.

– For å tilpasse oss har vi gjennomført flere justeringer i beredskapsorganisasjonen. Vi har også utviklet og trent på nye scenarioer som gjenspeiler den geopolitiske situasjonen vi står i, sier Asbjørn Ringstad, beredskapsdirektør i Equinor.

Equinors sin rolle som leverandør av energi til Europa innebærer også forpliktelser som strekker seg utover Norges grenser.

– Mye dreier seg om å kunne stå i kriser lenger enn det vi har vært vant til. I tillegg gjennomfører vi øvelser og koordinerer på tvers av privat og offentlig sektor.

Ringstad forklarer at Equinor i dag har en holistisk tilnærming til sikkerhet og beredskap.

FOTO: MIKE MORLEY VIA GETTY IMAGES

FOTO: OLE JØRGEN BRATLAND / ©EQUINOR

– Kort fortalt er det en erkjennelse av at alt henger sammen. For å kunne håndtere og lære av hendelser på en best mulig måte, må vi også forstå hvorfor og hvordan de oppstår. Da må vi samarbeide tett og ha åpne linjer mellom fagmiljøene.

Equinor har derfor organisert seg på en måte som gjør at ledere med ulike ansvarsområder – innen cybersikkerhet, fysisk sikkerhet, personellsikkerhet, beredskap og forretningskontinuitet – sitter i samme ledergruppe, nettopp for å sikre god og helhetlig risikoforståelse.

– I dag handler mye om eksterne trusler som påvirker våre operasjoner. Dette er gjerne tett koblet til den geopolitiske situasjonen, som vi har liten påvirkningskraft på – men som vi like fullt må forberede oss på konsekvensene av, sier Ringstad.

Å bygge robusthet og resiliens har de siste årene vært sentralt, spesielt knyttet til cybertrusselen.

» Å bygge robusthet og resiliens har de siste årene vært sentralt.

– Dette er en tilnærming som vi nå også tar med oss inn i det totale beredskapsarbeidet. Våre komplekse operasjoner gjør det krevende å raskt finne alternative løsninger for å kunne opprettholde drift, om man ikke er trent og forberedt.

– For oss blir det derfor viktig at vi gjør dette arbeidet i forkant, at vi øver og er bevisste på prioriteringer i samspillet med våre partnere. Det skaper den robustheten som vi er ute etter, og gjør at det uforutsigbare blir mer forutsigbart i en krisesituasjon.

Når alt kommer til alt, er det viktigste at man har en sterk kultur i organisasjonen, mener Ringstad.

– Vi har en sterk kultur når det gjelder øvelser og trening. Den forankringen finner du hos alle ledere og konsernsjefer. Vår CEO trener på sin rolle i beredskapsorganisasjonen fire ganger i året. Denne kulturen er og vil alltid være bærebjelken i alt vi foretar oss, avslutter Ringstad.

10

Har vi tid til å vente

I en digital hverdag der alt er sammenknyttet, er ekom-infrastruktur livsnødvendig. Med den skjerpede trusselsituasjonen mot Norge og Norden betyr det at næringslivet må integreres tettere i Totalberedskapen. Flere felles løsninger for sikkerhet, utholdenhet og robusthet må utvikles i en nordisk og alliert ramme.

Til venstre: I vårt budskap til beslutningstakere understreker Telenor i årets rapport at vi hverken har tid eller råd til å la være å utnytte de store mulighetene som ligger i nordisk samarbeid både militært og sivilt.

FOTO: ISTOCK.COM / NAUMOID

Den sikkerhetspolitiske situasjonen er mer usikker og farlig enn på flere tiår. Trusselsituasjonen i og mot Norge har endret seg mye på kort tid. I vårt naboland Sverige ber forsvarssjefen befolkningen være mentalt forberedt på krig. Leverandører av kritisk infrastruktur må derfor forberede seg på scenarier som før var utenkelige. Dette innebærer et økt fokus på resiliens – både for å øke egen motstandskraft og for å ivareta kunder og eget samfunnsansvar. Næringslivet må integreres tettere og flere felles løsninger for sikkerhet, utholdenhet og robusthet må utvikles i en nordisk og alliert ramme. Vi har ikke tid eller råd til å la være å utnytte mulighetene som ligger i et nordisk samarbeid.

Økt motstandskraft

Ekombransjen utgjør fundamentet for digitalisering av Norge, og det er industriaktører i et internasjonalisert næringsliv som bygger, drifter og utvikler ekomnettene. Disse nettene er avgjørende for at kritiske tjenester innen kraft, finans, transport, helse og mange andre sektorer fungerer – hele tiden.

Vi ser et stadig økende antall trusler mot virksomheter som leverer kritisk infrastruktur. Telenor ser med stor uro på at Russland i Ukraina systematisk bryter ned sivil infrastruktur som strøm, betalingsløsninger, transportsystemer, bredbånd og mobil. Sabotasje mot gassrørledninger i Østersjøen, kabler i jernbanenettet i Tyskland og senest under OL i Frankrike har vært en vekker fordi det samme kan skje i Norge. Et mulig angrep mot kommunikasjonstjenester og nettverk vil kunne få betydelige samfunnsmessige konsekvenser. Uten mobiltelefon eller internett vil vi ikke være i stand til å kommunisere, og en rekke tjenester vi for lengst har gjort oss helt avhengige av i hverdagen vil slutte å fungere.

Motstandskraft og sikkerhet i ekom-infrastrukturen er derfor ikke overflødig luksus, men livsnødvendig. Derfor styrker vi i Telenor vårt interne arbeid med resiliens ytterligere. Robust og sikker kommunikasjon er avgjørende for krisehåndtering og samfunnssikkerhet i den øvre del av konfliktspekteret. Trusselbildet vil kunne endres raskt og denne usikkerheten må vi lære oss å håndtere. For å beskytte vår digitale grunnmur, vil vi fortsette å investere i redundante systemer og cyberforsvar. Det vil kreve god beredskap, en oppdatert situasjonsforståelse og gjennomtenkte løsninger.

Tilgang på kompetanse

Det er en økende utfordring med tilgang på kompetanse på teknologi- og sikkerhetsfeltet. Det er knapphet på slik spesialkompetanse i Norge i dag, særlig gjelder dette tilgang på kompetent personell som samtidig kan sikkerhetsklareres. Telenor mener at et nordisk samarbeid med en mer harmonisert sikkerhetslovgivning og klarering på områder som understøtter kritiske sivile funksjoner, vil kunne bidra til nødvendig skala og dermed i større grad stimulere de multinasjonale teknologileverandørene til å etablere kompetansemiljøer i Norden. Ut over å bidra til regionens digitale motstandskraft, vil dette også kunne styrke nordisk innovasjons- og konkurranseevne.

Om Telenor 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. Det gir oss et betydelig samfunnsansvar og betyr at vi må levere stabile og trygge tjenester i fred, konflikt, krise og krig. Vi tar denne forpliktelsen på alvor og er opptatte av å sikre kontroll med eierskap hos leverandører til kritisk infrastruktur, og har bestemmelser om dette i avtaler med leverandører og partnere. Vi erkjenner at vi er et mål for avanserte trusselaktører. Vi har fokus på å integrere sikkerhet og beredskap i alle våre prosesser og ser stor verdi av en god og transparent dialog med myndighetene for å ivareta nasjonal sikkerhet. Vår virksomhet er underlagt sikkerhetsloven.

Integrer næringslivet

Telenor har i flere år tatt til orde for å få næringslivet tettere integrert i Totalforsvaret. Det er derfor svært positivt at anbefalingene fra Forsvarskommisjonen og Totalberedskapskommisjonen så tydelig erkjenner viktigheten av integrasjon av næringslivet som beredskapsaktør og ressurs. Langtidsplanen for Forsvaret påpeker det er «nødvendig å tenke nytt om hvordan næringslivsaktører bedre kan integreres i totalforsvaret». I tillegg er det relevant for næringslivet at forsyningsloven nå er erstattet av næringsberedskapsloven som innebærer eierskapsnøytralitet og at tjenester også er omfattet.

Større næringslivsaktører innen finans, olje og gass, kraft, mat og ekom har egne kompetansemiljøer og kapasiteter som er betydningsfulle for opprettholdelse av samfunnssikkerhet og statssikkerhet nettopp fordi de eier og forvalter kritisk infrastruktur. De har en naturlig rolle i totalforsvaret. De bidrar med innsikt og kompetanse om de kritiske sivile funksjonene de er med å opprettholde, og på den måten bidrar de til å oppfylle Norges forpliktelser knyttet til NATOs syv grunnleggende forventninger til motstandsdyktighet (NATOs «Seven Baseline Requirements»).

Et mer effektivt og revitalisert totalforsvar vil kreve en betydelig videreutvikling av rammene for samarbeidet. Telenor har god erfaring med samarbeid inn mot statsforvaltere og fylkesberedskapsråd, samt kommuner. Vi mener det fortsatt er mye å hente ved å i større grad formalisere totalforsvarsarbeidet på strategisk nivå. Vårt viktigste innspill er at de mest sentrale næringslivsaktørene bør integreres i Kriserådet på fast basis.

> ***Tre forhold er grunnleggende for et godt totalforsvar:***
>
> God motstandsdyktighet i samfunnet, tverrsektoriell situasjonsforståelse og vilje og evne til gjensidig støtte og samarbeid.

Etter Telenors vurdering er det fortsatt en generell utfordring at næringslivet i utilstrekkelig grad er inkludert i relevant beredskapsplanverk. I tillegg er sikkerhetsloven ikke i tilstrekkelig grad implementert hos underlagte virksomheter i alle sektorer. Den største praktiske utfordringen for mer samarbeid på tvers er – slik NSM har understreket – knyttet til at virksomheter ikke har tilstrekkelig tilgang til trussel- og sikkerhetsinformasjon eller til løsninger for sikkerhetsgradert samhandling. Dette er et myndighetsansvar å rydde opp i, og det haster.

Telenor er positive til etablering av tettere samarbeid med utvalgte selskaper om beredskap og krisehåndtering. At det skal etableres en «totalforsvarskontakt til Næringslivets hus eller tilsvarende næringslivsklynger» er et første skritt og kan innebære forbedring. I tillegg vil et tydeligere mandat for Sentralt Totalforsvarsforum (STF) gi effekt for samarbeid på direktoratsnivå. For å få effekt må styring og rammer for samarbeid i større grad formaliseres, særlig knyttet til arenaer og mekanismer for toveis informasjonsdeling. Det trengs betydelig fart og retning for den samfunnsreformen det er å revitalisere totalforsvaret.

Fem råd fra Telenor for bedre å integrere næringslivet i Totalforsvaret:

1. **Integrer de mest sentrale** næringslivsaktørene i Kriserådet på fast basis
2. **Etabler en funksjon** på myndighetsnivå for økt evne til å bygge tverrsektoriell situasjonsforståelse
3. **Gi sentrale aktører** i næringslivet mer oppdatert tilgang til trusselinformasjon
4. **Styrk arbeidet** med motstandsdyktighet i kritiske sivile samfunnsfunksjoner
5. **Sørg for systematisk** integrering av næringslivet i relevant planverk, samt militær og sivil øving og trening

Beredskapskrav i anskaffelser

Økte forventninger til næringslivet om å planlegge for totalforsvarets behov medfører økte kostnader. I en rapport fra Svensk Näringsliv fremheves et viktig dilemma: at økonomiske resultater alltid er avgjørende for private selskaper. Muligheten et selskap har for å overleve og utvikles avhenger av muligheten til å få betalt for arbeid og oppgaver som utføres og tjenester som leveres. En utfordring for både større og mindre næringslivsaktører som har kapasitet og ønsker bidra til økt sikkerhet, beredskap og motstandskraft, er at det er svært få kunder som har insentiv eller vilje til i hverdagen å betale sine leverandører for at varer eller tjenester skal kunne leveres kontinuerlig under krig.

For næringslivsaktører er derfor forutsigbare rammevilkår og mer langsiktig forutsigbarhet i kontrakter viktig for å kunne fatte beslutninger om investeringer som understøtter totalberedskap. Forsvarets Forskningsinstitutt (FFI) har i rapporten «Fra kjøttkaker til cyberspace – muligheter og utfordringer ved strategisk samarbeid for forsvarssektoren» understreket at en særskilt utfordring er levering av tjenester i øvre del av krisespekteret. Det stiller helt andre krav til både myndigheter og næringsliv og vil kreve nye samarbeidsformer og arbeidsmetoder. I dag er det fortsatt slik at sentrale næringslivsaktører i for liten grad systematisk trekkes med for å understøtte militær og sivil øving og trening. Dette kan muliggjøres i rammen av strategiske partnerskap og kan gi et mer langsiktig perspektiv.

Företags förutsättningar att överleva och utvecklas beror på möjligheten att få betalt för den verksamhet som utförs. Den vara eller tjänst som ingen långsiktigt vill betala för kommer inte att finnas kvar, utan konkurreras ut. Affärsverksamheter med allt för hög risk i relation till potentiella vinster och verksamheter som påverkas av högre kostnader än konkurrenter kan långsiktigt inte överleva. Ökade förväntningar på företag att planera för totalförsvarets behov leder till ökade kostnader. Mycket få kunder har incitament eller vilja att betala sina leverantörer i vardagen, för att varor eller tjänster ska kunna levereras kontinuerligt under krig.

Fra Svenskt Näringsliv:
Konkurrenskraftiga företag stärker försörjningsberedskapen och totalförsvaret

Øvelse Digital 2025

DSB har fått i oppdrag å lede planleggingen, gjennomføringen og evalueringen av Øvelse Digital 2025. Øvelsen skal planlegges i tett samarbeid med Nasjonal Sikkerhetsmyndighet (NSM). Målet med øvelsen er å styrke samfunnets evne til å motstå digitale angrep. Øvelsen skal gjennomføres høsten 2025 og vil involvere virksomheter fra sivile sektorer, Forsvaret og privat næringsliv. Øvelsen skal bidra til å teste totalforsvarets evne til å avdekke, håndtere og koordinere en kompleks digital hendelse på tvers av sektorer. Øvelsen vil videre teste totalforsvarets evne til å kommunisere og samvirke under håndteringen av konsekvensene av den digitale hendelsen.

Fra DSB: *Totalforsvarsøvelse - Øvelse Digital 2025*

Sikkerhetslovgivning skaper grensehindre

I alle nordiske land har myndighetene på ulikt vis skjerpet lovgivning og regulering knyttet til nasjonal sikkerhet. For telekomoperatørene og deres nordiske leverandører er det en stor utfordring at de nasjonale sikkerhetslovene i Norden ikke spiller sammen. Trenden har gått feil vei de siste årene. Dette har dessverre ført til fragmentering og færre muligheter for næringslivsaktører til å bygge sikkerhet basert på felles nordiske løsninger. Trenden har også implikasjoner for leverandørene våre, som de senere år har forsøkt å etablere «Center of Excellence» i Norden – en organisering som står i fare for ikke lenger å fungere.

Det er etablert mekanismer for sikkerhetsklarering av ressurser på tvers av Norden. Men det er ulike krav og praksis for hvilke stillinger eller roller som krever klarering, det er ulike klareringsnivåer i Norden (f.eks. er Adgangsklarering et særnorsk nivå), nivået BEGRENSET omfattes ikke av ordningen, GNFer og myndighetenes direkte utpeking av objekter med tilhørende graderingsnivåer er en særnorsk ordning, og informasjon om GNFer og skjermingsverdige objekter er ikke gradert i de andre nordiske landenes lovgivning. Med andre ord så er manglende symmetri i de nordiske landenes sikkerhetslovgivning kombinert med forskjellig praksis på implementeringen av denne sikkerhetslovgivningen på sammenlignbare virksomheter i hvert enkelt land, et kraftfullt hinder mot effektiv samhandling på tvers av landegrensene.

Telekom er en internasjonal og teknologidrevet bransje, med i all hovedsak utenlandske utstyrsleverandører. Disse leverandørene har som regel et antall kontorer i ulike land, hvorav flere er lokalisert utenfor både Europa og NATO. Det er naturlig og nødvendig for alle operatører å benytte disse leverandørene til å utvikle, vedlikeholde og supportere de plattformer de selger. Det er verken praktisk gjennomførbart, kvalitetsmessig ønskelig, eller økonomisk forsvarlig å benytte andre leverandører enn utstyrsleverandørene. Samtidig er det svært utfordrende å sikkerhetsklarere/autorisere en leverandørkjede fra ende til ende.

Med et stadig større antall virksomheter som underlegges sikkerhetsloven vil denne utfordringen øke snarere enn å avta. I tillegg vil den treffe alle sektorer som er underlagt sikkerhetsloven (ekom, kraft, helse, nødetater og andre). Dette representerer et tilbakeslag for nordisk samarbeid, innovasjon og effektiv konkurranse, og bør vekke en alvorlig bekymring hos ansvarlige myndigheter.

Telenor er også opptatt av – slik også Meld. St. 9 (2022–2023) understreker – at nasjonal «kontroll» ikke må defineres som nasjonalt «eierskap», da vi ivaretar både nasjonale og egne interesser innenfor en ramme som inkluderer Norden/NATO.

Ta i bruk mulighetene i nordisk samarbeid

Telenors viktigste ønske for bedre beredskap er et nordisk initiativ for å imøtegå hindre for nordisk samarbeid. Det er viktig å utforske løsninger for i større grad å benytte knappe personalressurser mellom nordiske naboland og benytte tekniske løsninger og infrastruktur som fiber og datasentre på tvers av land i Norden. Det 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.

Telenor har forventninger til at norske myndigheter i den kommende Totalberedskapsmeldingen tar konkrete initiativ til å følge opp totalberedskapskommisjonens forslag om samarbeid om digital sikkerhet og økt beredskap i Norden. Et slikt samarbeid vil kreve endringer og harmonisering av nasjonale regelverk. Industrien i Norden kan bidra til løsninger i en nordisk og alliert ramme innen samarbeidsområder som mobile kjernenett, datasentre og transportnett for å understøtte behov i både militær og sivil sektor. Det haster med å komme i gang.

Om nordisk integrasjon:

Regjeringen ser et klart behov for at Norge har en størst mulig grad av felles tilnærming med våre nordiske allierte til sivil støtte til militære styrker. På militær side er det allerede innledet et tett samarbeid. Det forutsettes imidlertid også tett samarbeid og avklaringer direkte mellom sivile sektorer i de tre landene. Det pågår allerede et beredskapssamarbeid mellom enkelte sivile sektorer og aktører og motparter i nordiske land. Eksempelvis er det inngått avtaler om krisehandel og forsyningssamarbeid mellom Norge, Finland og Sverige. Regjeringen ser behov for ytterligere å styrke Norges sivile beredskapssamarbeid med Finland og Sverige for å støtte opp under kollektiv evne til å yte effektiv sivil støtte til militære styrker i krig.

Fra: *Prop. 87 S (2023–2024) Forsvarsløftet – for Norges trygghet – Langtidsplan for forsvarssektoren 2025–2036*

Har vi tid til å vente

Øve og trene realistisk

For å forberede oss på å møte et annet alvor i våre nærområder, må vi øve og trene på scenarier som før var utenkelige. Det betyr å øve nærmere daglige utfordringer og reelle scenarier som speiler trusselbildet, og vi må øve på tvers av sektorer. Kun på den måten vil vi oppnå bedre forståelse av hvordan virksomheter er gjensidig avhengige av hverandre og få innsikt i omfanget av faktiske kriser og deres mulige ringvirkninger.

For beredskapsarbeid og øvelser er hovedkonklusjonen i NOU 2012:14 fortsatt relevant knyttet til «viktigheten av risikoforståelse, og at man arbeider med en risikobasert tilnærming». Risikoforståelsen bestemmer om man øver, hva man øver på, og hva man lærer av øvelser. Godt forberedte øvelser kan fungere som en dynamisk form for tilsyn. Etter øvelsen har aktørene praktiske erfaringer som gir en dypere innsikt i utfordringer og endringsbehov.

Telenor har siden 2017 arrangert «Øvelse Bukkesprang» i samarbeid med Cyberforsvaret. Dette er Norges største og tverrsektorielle «live fire»-øvelse i digital hendelseshåndtering. I 2023 ble også Nasjonal sikkerhetsmyndighet (NSM) med som samarbeidspartner. Målet med øvelsen er å styrke totalforsvaret av Norge. Øvelsen er unik i norsk sammenheng, og et viktig bidrag til den digitale totalberedskapen.

Telenor ønsker bedre samhandling innen hendelseshåndtering, og sikkerhetsøvelser som i langt større grad involverer næringslivet. Vi har fortsatt få øvingsarenaer som samler på tvers av sektorer og tester evne til samvirke, samhandling, ledelse og koordinering. Og vi trenger i høyeste grad en sterkere integrering av næringslivet. En annen vesentlig mangel er fraværet av felles plattformer for informasjonsdeling.

Justis- og beredskapsdepartementet har gitt DSB ansvar for å planlegge og gjennomføre Øvelse Digital 2025. Som Telenor tidligere har tatt til orde for, vil økt bruk av øvelser kunne bidra til styrket tverrsektorielt samvirke og ledelse på strategisk, operasjonelt og taktisk nivå. Øvelser er også en god arena for å bygge kjennskap til hverandres kapabiliteter og arbeidsmetodikk, samt utvikle nettverk og relasjoner mellom nøkkelpersoner hos kritiske totalberedskapsaktører. Øvelse Digital 2025 har potensial til å inkludere sentrale næringslivsaktører, og bidra til viktig grunnlag for forbedring.

Vilje til endring

Det er svært viktig for Telenor å kunne benytte egne ansatte over hele Norden, å kunne bruke leverandøransatte i våre fire markeder og å kunne dele tekniske løsninger og infrastruktur på tvers. Vi er forberedt på å ta ytterligere ansvar for sikkerhet og beredskap i nordområdene. Vår ambisjon er å beskytte kommunikasjon, innhold og kritisk infrastruktur.

I en stadig mer komplisert verden, med økende press på talent og kompetanse, og økende konsentrasjon av leverandørmarkedet med stadig lengre forsyningskjeder, blir hvert enkelt land i Norden hver for seg for små. Telenor tror på et felles nordisk regime for sikkerhetsklarering og autorisasjon av personell. Det bør også jobbes målrettet med å legge til rette for at operatørene bygger robuste nordiske løsninger knyttet til transportnett, mobilkjernenett og datasenter.

Et tett teknisk samarbeid mellom bedrifter og organisasjoner over landegrensene krever resultatorientert lederskap. Det vil kreve en harmonisering av sikkerhetslovgivning og samarbeid mellom nasjonale regulatører på et helt annet nivå enn det vi ser i dag.

Et samlet Norden i NATO gir et historisk godt sikkerhetspolitisk fundament for å endre holdninger og kultur. Med langt tettere sikkerhetssamarbeid på tvers av den nordiske regionen har vi helt andre forutsetninger for å sikre et effektivt, sikkert og robust totalforsvar. Vi har ikke tid til å vente.

Kommisjonens viktigste anbefaling er at ledere på alle nivåer i forvaltningen systematisk arbeider med å styrke sine egne og organisasjonenes grunnleggende holdninger og kultur knyttet til:

- Risikoerkjennelse
- Gjennomføringsevne
- Samhandling
- IKT-utnyttelse
- Resultatorientert lederskap

Fra: *NOU 2012: 14 - Rapport fra 22. juli-kommisjonen*

Telenor vil:

- → **Tettere integrere** sentrale aktører i næringslivet i den nasjonale beredskapsstrukturen
- → **Styrke sikkerhetssamarbeidet** om klarering og autorisasjon av nordiske statsborgere med et felles nordisk regime for sikkerhetsklarering
- → **At krav til nasjonal autonomi** operasjonaliseres slik at det muliggjør å benytte personell på tvers av Norden samt dele tekniske løsninger og infrastruktur for økt robusthet og motstandsdyktighet
- → **At det stilles krav om å ivareta** langsiktige beredskapshensyn og nasjonale sikkerhetsinteresser i offentlige anskaffelser
- → **Styrke nasjonal kompetanse** og kapasitet til å føre tilsyn med AI

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/2024