NSM

Nasjonalt digitalt risikobilde 2023

Forsidebildet er laget med kunstig intelligens, og tjener to hensyn. Bildet illustrerer sabotasje av kritisk infrastruktur som følge av cyberangrep. Det er et scenario som bekymrer den norske befolkning. I tillegg illustrerer det hvordan kunstig intelligens både kan brukes for å understreke et legitimt poeng, og brukes av trusselaktører til manipulasjon og påvirkning. Forsidebildet er laget av Benjamin Egseth Martinsen ved hjelp av Midjourney, Adobe Firefly i Photoshop og Adobe Photoshop.



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

NASJONAL
SIKKERHETSMYNDIGHET

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for nasjonalforebyggende sikkerhet. Tjenestens hovedoppgave er å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Gjennom rådgivning, forskning, tilsyn, testing og kontrollaktiviteter bidrar NSM til at virksomheter sikrer sivil og militær informasjon, systemer, objekter og infrastruktur med betydning for nasjonal sikkerhet. NSM er ansvarlig for et nasjonalt varslingssystem (VDI) som skal avdekke og varsle om cyberangrep mot digital infrastruktur. NSM har også et nasjonalt ansvar for å koordinere håndteringen av alvorlige cyberangrep.

NSM
NASJONALT
CYBERSIKKERHETSSENTER

Rapporten er utarbeidet av Nasjonalt cybersikkerhetssenter (NCSC) som er en del av NSM og samtidig et partnerskap mellom NSM og ulike offentlige og private virksomheter. Senteret skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot cyberoperasjoner. NCSC har et spesielt fokus på rådgiving knyttet til cybersikkerhet og tekniske sikkerhetsløsninger. NCSC yter også bistand ved håndtering av digitale hendelser og vedlikeholder et nasjonalt cybersituasjonsbilde.

Innhold

Det digitale risikobildet 6

Teknologisk utvikling i en uforutsigbar verden 7

Slik kan en cyberoperasjon ramme din virksomhet 8

Cybersituasjonsbildet i Norge 10

Multifaktorautentifisering - ikke alt er lenger like sikkert 15

Sårbarhetene NSM oftest finner 16

Digitale trender og utviklingstrekk 18

Vi trenger kunstig intelligens for cybersikkerhet 19

Kvanteakopalypse - start forberedelsene nå 22

Cyber i det store bildet 26

Cyberangrep mot kritisk infrastruktur 27

Datasentre og skytjenester - et kontinuitetsperspektiv 30

Leverandørtjenester og uoversiktlighet 32

Når cybersikkerhet blir bedre - øker risikoen for en innsider i bedriften din? 34

Cyberdomenet - slik brukes det mot demokratiske valg 38

Ordliste 42

Det digitale risikobildet

Fabian Helmersen / Forsvaret

Teknologisk utvikling i en uforutsigbar verden

Krig i Europa skaper usikkerhet, og gjør fremtiden vanskelig å forutse. Usikkerheten forsterkes ytterligere av en teknologisk utvikling med stadig hurtigere tempo og utbredelse. Kunstig intelligens utfordrer vår evne til å se forskjell på ekte og falskt, på sant og usant. Vi har allerede sett at mulighetsrommet for maskingenerert kreativitet er stort. Hvor stort det vil være om ett år eller mer, er vanskelig å si. Potensialet til å bruke teknologien i det godes tjeneste er stort. NSM ser med bekymring på potensialet for det motsatte. Alt som kan brukes, vil misbrukes. Flere av grunnleggerne av kunstig intelligens-teknologien har advart mot retningen utviklingen går i.

Samtidig er det, parallelt med utviklingen av kunstig intelligens, et globalt kappløp om kvanteteknologi. Kvanteteknologien utfordrer også vår evne til å forstå tenkelig utvikling. Kvantedata-maskiners overlegenhet kan i verste fall føre til at alle koder knekkes, og at all beskyttelse av informasjon opphører. Noen har kalt dette kvanteapokalypsen. I denne rapporten belyses noen utviklingstrekk og bekymringer rundt både kunstig intelligens og kvanteteknologi.

Kontroll over den teknologiske utviklingen er blant arenaene for konflikt mellom stormakter. Tilspissingen av sikkerhetspolitikken og teknologikappløpet skjer samtidig med at Norges geopolitiske viktighet øker. Både som energileverandør til Europa, og som mottaksland på NATOs forsterkede flanke i nord. Forsvarssektoren er avhengig av sivil støtte og infrastruktur. NSM er enig med Forsvarskommisjonens anbefalinger om behovet for å bedre sikre sivil og militær infrastruktur. Det betyr at det sivile samfunn må være sin rolle bevisst, og ta cybersikkerhet på det høyeste alvor i tiden fremover.

NSM erfarer dessverre at gapet mellom trusselaktørenes kapabiliteter og det forebyggende sikkerhetsarbeidet øker. Det haster å ta i bruk ny teknologi – som kunstig intelligens – i forsvaret av nettverkene våre. For vi vet at trusselaktørene vil bruke teknologien med andre hensikter så raskt de kan. Selv om NSM så langt ikke har sett kunstig intelligens bli brukt i cyber- eller påvirkningsoperasjoner mot Norge, er det trolig bare et spørsmål om tid. NSM påpekte i sikkerhetsfaglig råd at demokratiske land nå står i fare for å bli fraløpt i teknologi-kappløpet. Noen sentrale utfordringer som NSM peker på, er:

- Statlig IT-styring ivaretar hverken koordinering eller behov for samvirke i tilstrekkelig grad.
- Den nasjonale deteksjonsevnen i cyberdomenet er utilstrekkelig – til tross for et velutviklet Varslingssystem for digital infrastruktur (VDI).
- Håndteringsevnen ved store cyberhendelser er begrenset.
- Informasjonssystemer som understøtter grunnleggende nasjonale funksjoner ikke er tilstrekkelig kartlagt, og har ofte ikke etablert et forsvarlig sikkerhetsnivå.
- Cyberoperasjoner kan få økt fysisk slagkraft når industrielle systemer i økende grad kobles til internett.

Erfaringer fra Ukraina har lært oss mye om hvilken rolle cyberdomenet har i konvensjonell krig. Det er nyttig lærdom som kan forbedre vår motstandsdyktighet. Men også andre aktører studerer krigen. Aktører som ikke deler våre verdier. De lærer også.

Årets utgave av nasjonalt digitalt risikobilde søker å bevisstgjøre ledere og IT-personell i private og offentlige virksomheter om viktige trender å følge med på. Trolig har det aldri vært viktigere. Norges rolle i verden, en økt profesjonalisering av cyberoperasjoner, den raske utviklingen innen kunstig intelligens og den sikkerhetspolitiske forverrede situasjonen globalt gjør det digitale cyberrisikobildet mer usikkert enn noen gang tidligere. Nå er ikke tiden for å bli hengende etter. Nå må vi brette opp ermene.

Slik kan en cyberoperasjon ramme din virksomhet

Dette eksemplet er basert på virkelige cyber-operasjoner NSM har håndtert det siste året.

Ola Nordmann er IT-administrator i en privat bedrift som leverer programvareløsninger til både offentlige og private virksomheter. En dag får han en hyggelig henvendelse på LinkedIn fra en hodejeger. Ola oppfordres til å søke en attraktiv og godt betalt jobb hos en større virksomhet i samme bransje. Etter noe dialog over LinkedIn, ber hodejegeren om at kommunikasjonen flyttes til en annen plattform. De flytter derfor samtalene over til WhatsApp. Der mottar Ola Nordmann et dokument tilknyttet jobben de har diskutert.

Dokumentet inneholder spionvare. Hodejegeren har ikke ærlige hensikter. Ola får ikke åpnet dokumentet på mobilen og melder tilbake at vedlegget ikke lar seg åpne. Hodejegeren tipser om at han kan åpne den på en laptop i stedet. Siden Ola allerede er på jobb, åpner han den på laptopen han vanligvis bruker her. Slik installerer han intetanende skadevare på en datamaskin tilknyttet arbeidsgivers infrastruktur.

Dagen etter logger han på jobbens tjenesteportal som benyttes for å yte fellestjenester til de offentlige og private virksomhetene i kundeporteføljen

Skadevaren samler inn brukernavnet og passordet til Ola, og trusselaktøren logger seg på samme portal mens Ola har lunsj.

Spionvare

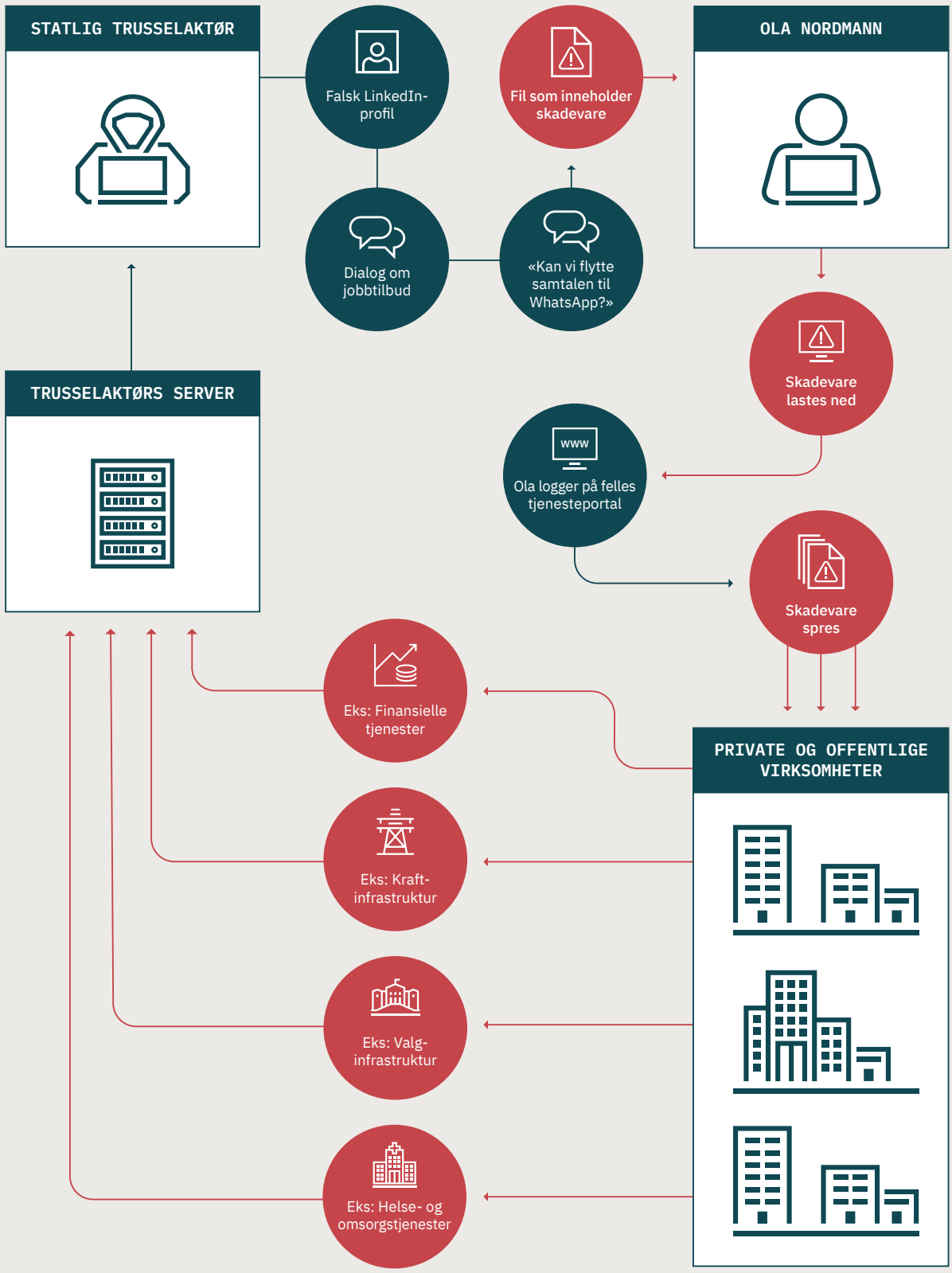
(Eng: spyware). Spion-programvare er en form for skadevare der en programkode, som uten brukerens tillatelse, utfører handlinger med brukerens systemer eller informasjon.

Gjennom stjålne brukerdetaljer kan aktøren bevege seg lateralt til andre bedrifters infrastruktur, og etablere ytterligere skadevare tilpasset målene. Disse kan nå bli offer for løsepengevirus, destruktiv «*wiper*»-skadevare - eller de kan, sakte, over lang tid og usett, bli tappet for sensitiv informasjon og forretningshemmeligheter. Cyberoperasjoner som denne kan dessuten inngå i større og mer komplekse hybride påvirkningsoperasjoner. Sensitiv, stjålet informasjon kan lekkes til offentligheten, potensielt ispedd desinformasjon, på strategisk viktige tidspunkt – for eksempel i forbindelse med et valg.

Uansett utfall er det en rekke tiltak som underveis i angrepskjeden kunne ha stoppet angriperne. NSMs grunnprinsipper for IKT-sikkerhet har en rekke tiltak innen kategoriene: Identifisere og kartlegge, beskytte og opprettholde, oppdage samt håndtere og gjenopprette. Et utvalg av tiltak fra disse kategoriene som kunne risikoredusert cyberangrepet:

- 1.2.3 Kartlegg enheter i bruk i virksomheten
- 2.2.3 Del opp virksomhetens nettverk etter virksomhetens risikoprofil
- 2.3.2 Konfigurer klienter slik at kun kjent programvare kjører på dem
- 2.6.4 Minimer rettigheter til sluttbrukere og spesialbrukere
- 2.6.7 Bruk multifaktorautentisering
- 3.2.3 Avgjør hvilke deler av IKT-systemet som skal overvåkes
- 4.1.1 Etabler et planverk for hendelseshåndtering

NSM grunnprinsipper for IKT-sikkerhet og tilhørende støtteressurser er tilgjengelig på www.nsm.no/grunnprinsipper-ikt



Figur 1: Grafisk fremstilling av et tenkt cyberangrep, basert på saker NSM har håndtert det siste året.

Cybersituasjonsbildet i Norge

Cyberangrep har blitt hverdagskost. Virksomheter må gjøre det de kan for å forhindre, avdekke og håndtere hendelsene når de oppstår. For det er et spørsmål om når - ikke hvis.

Nulldagssårbarheter

Sommeren 2023 ble det kjent at 12 norske departementer var blitt kompromittert gjennom bruk av såkalte nulldagssårbarheter. En avansert trusselaktør hadde over lengre tid tilgang til flere deler av departementenes nettverk – som trolig ikke var tilfeldige mål. «Regjeringen står under angrep», sa statsministeren med henvisning til kompromitteringene.

Nulldagssårbarheter er i praksis nesten umulige å beskytte seg mot. De kjøpes og selges på digitale undergrunnsmarkeder, hvor en symbiose av hackere, kriminelle og etterretningstjenester opererer. Men det hjelper alltid, uansett, å installere sikkerhetsoppdateringer så raskt som mulig, og ha orden på loggfiler. God sikkerhetsarkitektur vil også gjøre det vanskeligere for en potensiell trusselaktør å bevege seg lateralt i nettverket ditt.

Nulldagssårbarhet

- Sårbarhet i programvare som noen får kunnskap om, før produsenten/ leverandøren eller brukerne av programvaren
- Begrepet nulldagssårbarhet spiller på at man har 0 dager til å kunne forberede seg på utnyttelse av sårbarheten

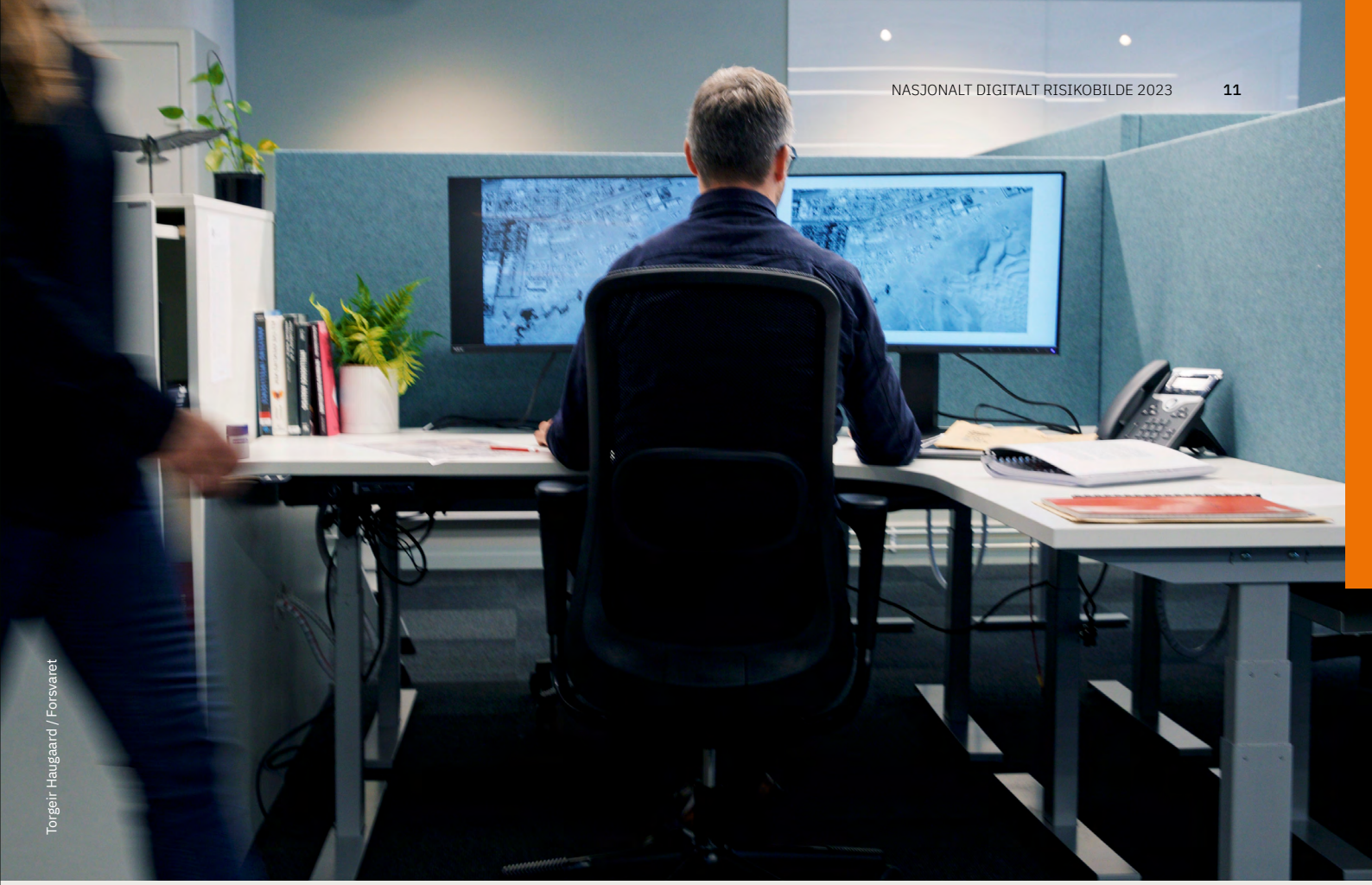
Tjenestenektangrep

Tjenestenekt som angrepsform er langt fra noe nytt fenomen. Det har bare ikke truffet Norge før i den skalaen vi har sett det siste året. Siden sommeren 2022 har NSM registrert en seksdobling i antall tjenestenektangrep sammenlignet med de tre foregående årene samlet. Angrepene har i mange tilfeller ført til at norske nettsteder har vært utilgjengelige, men har ikke fått alvorlige konsekvenser utover dette. Dessverre er nok den massive økningen i antall tjenestenektangrep den nye normalen.

Det finnes gode tiltak mot tjenestenektangrep. Likevel er NSM bekymret for at angrepsformen er i utvikling: Mer sofistikerte teknikker tas i bruk og kan rettes mot sårbare punkter i virksomheters nettverk. Erfaringen fra utlandet er at angrepene blir mer sofistikerte, vanskeligere å oppdage og beskytte seg mot. Tjenestenektangrep kan dessuten inngå som del av større og mer komplekse cyberoperasjoner, hvor tjenestenekt først og fremst brukes for å skape forstyrrelser og avlede oppmerksomhet.

Nye sektorer rammes

Det siste året har bølger av tjenestenektangrep fra prorussiske aktører truffet virksomheter i transport-, finans- og helsesektoren. Dette er sektorer vi ikke tidligere har sett på som typiske mål for denne typen hendelser. Sektorene høyteknologi, næring og offentlig forvaltning er fortsatt de mest utsatte sektorene for cyberoperasjoner i alle former, totalt sett. Tidligere år har NSM observert et høyt trykk av trusselaktivitet mot universiteter og andre virksomheter i sektoren forskning og utvikling. Denne aktiviteten har det siste året avtatt noe.



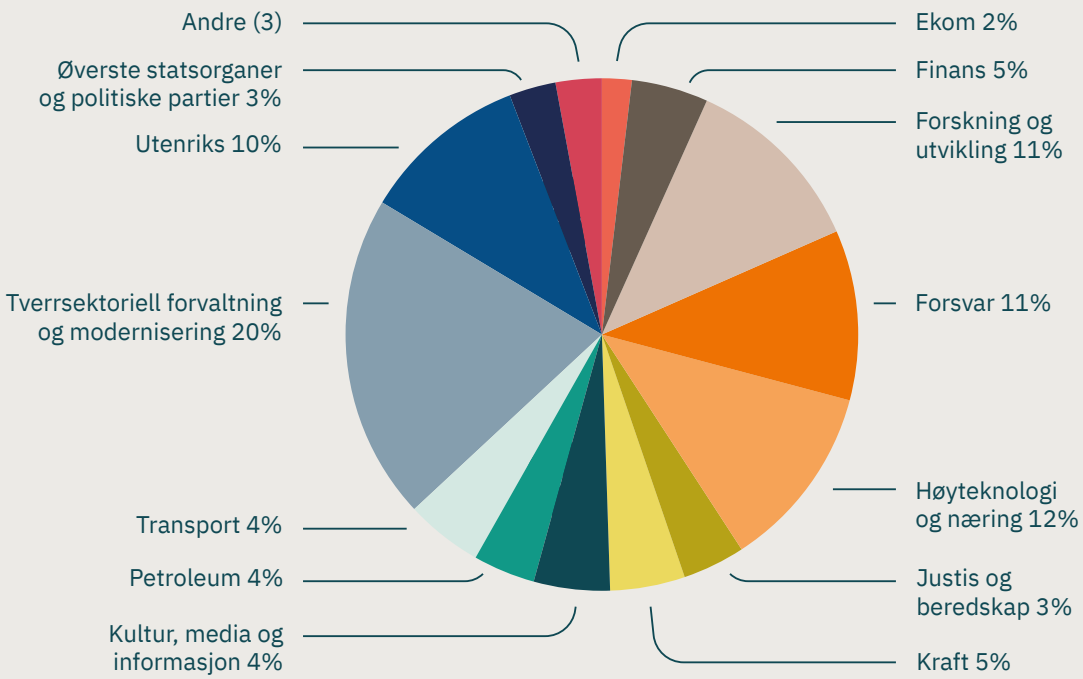
Torgeir Haugaard / Forsvaret

Sektorer med økt trussel-aktivitet	Sektorene med høyest trussel-aktivitet	Sektorer med redusert trussel-aktivitet
• Finans • Helse • Transport • Forsvars-sektoren	• Høyteknologi og næring • Tverrsektoriell forvaltning	• Forskning og utvikling

Forsvarssektoren mer utsatt

NSM har registrert flere og mer alvorlige hendelser i forsvarssektoren det siste året, enn året før. Også forsvarsindustrien har vært rammet av cyberoperasjoner – noen av dem svært alvorlige. Det er naturlig å prøve å forstå utviklingen i lys av Norges støtte til Ukrainas forsvarskrig mot Russland. I mange av tjenestenekt-angrepene mot sektoren oppgir russiskspråklige hack-tivister selv at motivasjonen for angrepene er Norges rolle som støttespiller for Ukraina i krigen. E-tjenesten påpeker også i sin rapport Fokus 2023 at russiske aktører er ute etter informasjon om norsk politikkutforming: «(...) særlig innen forsvars-, utenriks- og sikkerhetspolitikk, og om nordområdene, Svalbard og energisektoren. Forsvaret, militære beredskapsplaner, militær infra-struktur og alliert aktivitet er også ettertraktede mål.»

Figur 2: Prosentandel av registrerte cyberhendelser per samfunnssektor siden sommeren 2022



Rammer oftere flere mål samtidig

Det siste året har vært preget av flere typer cyberangrep mot norske kommuner, med ulik alvorlighetsgrad. Målselv, Vadsø og Sør-Varanger er eksempler på kommuner av stor potensiell strategisk betydning og med en høy andel militært ansatte blant befolkningen. Gjennom lekkede påloggingsdetaljer til en ekstern tjenesteleverandør greide en trusselaktør å komme seg inn i kommunale systemer. Politiets etterforskning tydet på skadevarespredning til flere kommuner.

Digitale trusler er blitt en del av hverdagen. Dataangrep rammer i økende grad flere mål samtidig, på tvers av sektorer, og vi ser at disse angrepene søker sårbarheter i verdikjeder som så kan utnyttes mer målrettet.

-IT-sjef i en av de involverte kommunene

Profesjonalisering av angrep

Internasjonalt beskriver cybersikkerhetsorganisasjoner at alle ledd i en angrepskjede profesjonaliseres. Fra sårbarhetsscanning og phishing-kampanjer til løsepengeangrep, tjenestenektangrep og stjålne brukernavn og passord. Alt kan kjøpes på det mørke nettet*.

I Norge ser vi også tegn til at angrepene blir proffere: Kvaliteten på svindelinnholdet i målrettede e-poster har nådd et urovekkende høyt nivå. Årvåkne, kritiske mennesker kan bli lurt i et svakt øyeblikk. NSM forventer at utviklingen innenfor kunstig intelligens og store språkmodeller* vil skape ytterligere forbedringer og dermed større utfordringer. Teknologiutviklingen vil muliggjøre en type spredning og økt automatisering av svindel, desinformasjon og spionasje på måter vi i dag ikke fullt ut forstår konsekvensene av.

Cybersikkerhet er en kontinuerlig kamp mellom angriperne og forsvarerne. Taktikker, teknikker og prosedyrer utvikles av angriperne. Forsvarerne detekterer, analyserer og utvikler nye forsvarstiltak.

*viser til ordliste helt sist i rapporten

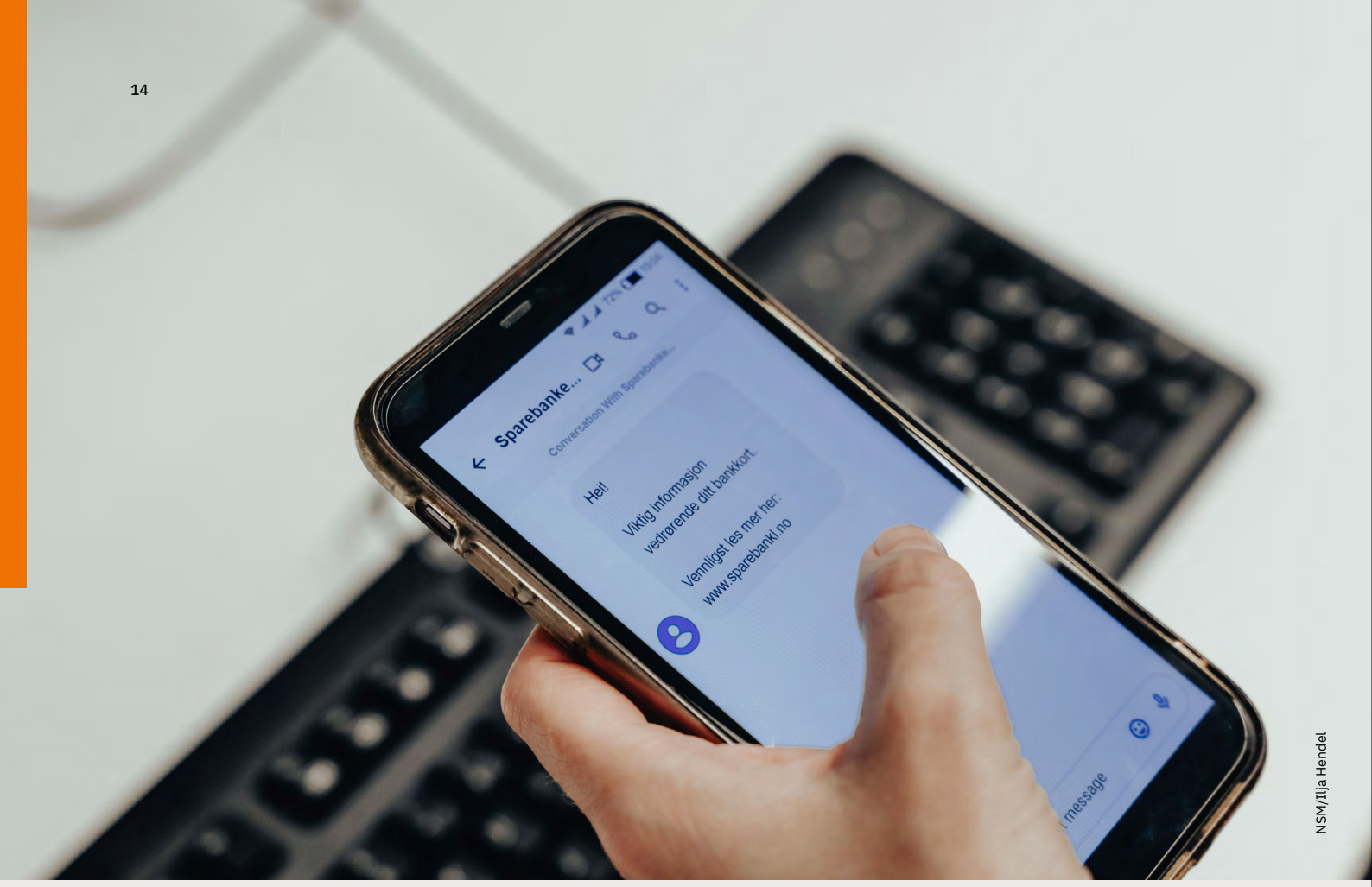
NSM/Ilja Hendel

Multifaktorautentisering

Multifaktorautentisering (MFA) er et aktuelt eksempel. Denne sikkerhetsmekanismen har i mange år vært – og er fortsatt – blant de viktigste tiltakene NSM anbefaler. I dag har de fleste større virksomheter implementert multifaktorautentisering. Men angriperne gir seg aldri: NSM ser – både internasjonalt og i Norge – eksempler på at trusselaktører kommer seg rundt multifaktor-autentisering. Enten ved å utnytte menneskelige eller teknologiske sårbarheter.

Løsepengeangrep

Løsepengeangrep er en arena hvor angriperne har tapt flere slag det siste året. Internasjonalt samarbeid om politietterforskning og ideologiske uenigheter har bidratt til oppsplitting av flere russiskspråklige løsepengeangrep-miljøer. Blockchain-analyser viser at lønnsomheten i løsepengebransjen har gått kraftig ned siden toppårene 2020 og 2021. Dette sammenfaller med at NSM har registrert færre løsepengeangrep mot norske virksom-heter det siste året. Dette betyr likevel ikke nødvendigvis at risikoen avtar. Flere norske virksomheter har blitt rammet det siste året. For mange blir konsekvensene av et angrep omfattende. For noen kan det bety driftsstans og i verste fall konkurs.



NSM/Ilja Hendel

Dynamisk situasjonsbilde

Overordnet utgjør disse ulike momentene et svært dynamisk cybersituasjonsbilde; innbruddsmetoder endrer seg raskt på taktisk nivå, og nye nulldagssårbarheter dukker opp der man minst ønsker dem. Dette er ikke nytt i cyberdomenet. Det nye er den skjerpede sikkerhetspolitiske konteksten vi må innfinne oss med. Flere strategiske faktorer – for eksempel forholdet mellom vestlige land på den ene siden og Russland og Kina på den andre siden – går fortsatt mot en forverring.

I denne situasjonen er det viktigere enn noen gang at alle som beskytter virksomheter mot spionasje, sabotasje, terror og sammensatte trusler, spiller hverandre gode. At vi samarbeider godt og deler informasjon. Bare på den måten kan vi holde forsvarslinjen – sammen.

Nasjonale verdier med internasjonal tilknytning

Da det store sveitsisk-baserte konsernet ABB ble rammet av et løsepengeangrep i mai, fulgte NSM nøye med på hendelsen. Dette var et eksempel på en internasjonal bedrift med komplekse forgreninger til kritisk infrastruktur i flere sektorer over hele verden. Frykten var at konsekvensene av løsepengeangrepet kunne få spredning til grunnleggende nasjonale funksjoner.

Multifaktorautentisering – ikke alt er lenger like sikkert

Det er flere problemer knyttet til bruk av passord som den eneste faktoren for tilgang til kontoer. En angriper kan da:

- lese av passordet ved å fysisk stå bak brukeren
- lure brukeren til å oppgi passordet via phishing som for eksempel anvender nettsider som likner på den ekte nettsiden
- gjenbruke passord som har kommet på avveie
- anvende automatiserte verktøy for å gjette passord («bruteforce»)

Å anvende totrinnsautentisering er et godt steg i riktig retning fra å kun anvende passord til å autentisere med. Typiske eksempler på totrinnsautentisering er engangskode via en mobilapplikasjon eller over SMS. Dette vanskeliggjør angrep der en angriper bruker automatiserte verktøy til å gjette mange passord mot en konto, eller sprer det til et fåtall forsøk over mange kontoer, og forsøk på å autentisere med passord som stammer i fra passordlekkasjer.

Derimot er ikke all multifaktorautentisering like sikker. Et eksempel er et push-varsel der bruker kan trykke ja eller nei på om det er den som forsøker å logge inn. Løsningen bør begrense antall varsler brukerne kan motta slik at en angriper ikke kan bombardere brukerne med push varsler i håp om at noen aksepterer ett av dem, kjent som MFA *bombing* eller *fatigue*. Et annet eksempel er dersom en angriper er i stand til å få tilgang til engangskodene vil de ofte kunne anvende disse som om de var brukeren. Brukerne kan bli utsatt for sosial manipulering der de blir overtalt til å gi i fra seg engangskoder, eller alternativt at de mottar en link som videresender dem til en falsk nettside med et utseende som likner den legitime nettsiden der de blir bedt om å autentisere. Opplæring er derfor spesielt viktig for å hjelpe både ansatte i virksomheter og brukere av tjenester med å avdekke sosial manipulering.

En siste svakhet ved mulitifaktorautentisering, er den tekniske muligheten en trusselaktør kan bruke til å stjele «sikkerhetsbilletten» som utstedes ved vellykket pålogging. Dette kalles MFA *session token*-tyveri, og er en internasjonal trend som sprer seg.

Multifaktorautentisering

Teknologi som åpner for at brukerne kan anvende flere faktorer for å autentisere seg mot en tjeneste. Dette kan bestå av noe du vet (f.eks. PIN-kode), noe du er (f.eks. FaceID, fingeravtrykk) og noe du har (f.eks. adgangskort, kodebrikke). Når to av disse tas i bruk kalles det totrinnsautentisering (2FA)

MFA *bombing / fatigue*

Trusselaktør overstrømmer en bruker med multifaktor autentiseringsforsøk, til brukeren godkjenner forsøket.

Eksempel: Du spammes ned av stadige BankID på mobil-varsler på mobilen din, eller SMS-er som ber deg fullføre innlogging på en annen plattform. Også kjent som MFA *fatigue* eller MFA *spamming*.

MFA *session token*-tyveri

Når en bruker har korrekt logget seg på med sin ID, passord og MFA/2FA, blir en sikkerhetsbillett (*session token*) tildelt brukerens nettleser med en gitt tidsfrist, slik at brukeren kan navigere i en sesjon uten å måtte logge seg inn på nytt. En slik *token* kan stjeles av trusselaktør, som da vil ha tilgang til alle brukerens privileger innenfor tidsfristen.

Gjør innloggingen sikrere

Dersom en nettside tilbyr *WebAuthn* kan dette brukes som et moderne alternativ til tradisjonell passord-autentisering. *WebAuthn* er en spesifikasjon som åpner for at det kan lages en binding mellom brukersiden og nettsiden bruker registrerer seg på. På brukeren sin side blir det lagret informasjon om hvilke nettsider brukeren har en konto på. Dersom en angriper forsøker å lure en bruker til å autentisere mot en falsk nettside vil dette feile.

Sårbarhetene NSM oftest finner

NSM gjennomfører inntregningstester i norske virksomheters informasjonssystemer. Testingen er nøye avtaleregulert mellom NSM og den aktuelle virksomhet, og er forbeholdt de som er underlagt sikkerhetsloven. En inntrengingstest søker å avdekke fysiske, logiske, tekniske, menneskelige og administrative sårbarheter i et informasjonssystem eller ved virksomhetens fysiske lokasjon.

Her har vi oppsummert de vanligste sårbarhetene, og ikke minst - hvordan de kunne vært unngått ved bruk av tiltak beskrevet i NSMs grunnprinsipper for IKT.

Dårlige passord

Mange brukerkontoer har fremdeles **svake passord** som er lette for NSMs pentestere å gjette seg til. NSM registrerer at **passordgjettingsangrep /brute force** stadig rammer norske virksomheter. Flere systemer er konfigurert slik at det er mulig å gjette passord til samtlige brukerkontoer i virksomhetens database. Det er sjelden innført sikkerhetstiltak som begrenser antall forsøk av feilskrevene passord. Selv om omfanget av gjetting vil være lavt, vil man ofte klare å gjette dårlige passord.

Flere virksomheter lager **«passordhuskelister»** og lagrer dem i sitt informasjonssystem, uten å ha kontroll på hvem som har tilgang til den. Ubeskyttede passord er ofte en enkel vei til full kontroll over et informasjonssystem. Mange virksomheter har **uendrede standardpassord** på tjenester og spesialkontoer satt opp av eksterne leverandører. Bruk av standardpassord er uheldig.

Følgende tiltak er anbefalt av NSM:

2.6.3 Benytt et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter
2.6.7 Bruk multi-faktor autentisering
2.6.1 Etabler retningslinjer for tilgangskontroll
2.6.4 Minimer rettigheter til sluttbrukere og spesialbrukere
3.2 Etabler sikkerhetsovervåkning
1.3 Kartlegg brukere og behov for tilgang
2.2 Etabler en sikker IKT-arkitektur
2.3 Ivareta en sikker konfigurasjon
2.6 Ha kontroll på identiteter og tilganger
3.1 Oppdag og fjern kjente sårbarheter og trusler

Slurv med tilganger

NSM finner ofte **eldre administratorkontoer** som ikke er deaktivert. Eldre administrasjonskontoer som tilhørte personer som har sluttet eller ikke tilhører virksomheten, utgjør en sikkerhetsrisiko. NSM avdekker ofte at **administrator- og spesialkontoer** har høyere rettigheter enn nødvendig utføre sin rolle. Disse kontoene gir tilganger som går på tvers av segmenteringen i virksomheten og er derfor attraktive angrepsmål. NSM vet at passord til administrasjonskontoer blir gjenbrukt, noe som øker attraktiviteten ytterligere.

Følgende tiltak er anbefalt av NSM:

2.6.2 Etabler en formell prosess for administrasjon av kontoer, tilganger og rettigheter
2.6.3 Benytt et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter
1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer
1.3 Kartlegg brukere og behov for tilgang
2.2 Etabler en sikker IKT-arkitektur
2.6 Ha kontroll på identiteter og tilganger

Utdaterte systemer

Flere virksomheter kjører **eldre operativsystemversjoner** hvor leverandøren ikke lenger produserer sikkerhetsoppdateringer. Grunnen til dette kan være at maskinene kjører spesialprogramvare eller utstyr som kun fungerer på det eldre systemet.

Alle komplekse programvarer inneholder feil. Virksomhetene må vare bevisst at programvarene de bruker kan være sårbare og ha **utdaterte programvare og protokoller.** Ved å utnytte slike sårbarheter kan en aktør ta kontroll over en maskin eller en bruker. IoT-enheter, nettverksutstyr og tjenester som er internett-eksponerte er spesielt utsatte.

Følgende tiltak er anbefalt av NSM:

1.2.4 Kartlegg programvare i bruk i virksomheten
2.1.2 Kjøp moderne og oppdatert maskin- og programvare
2.5.4 Isoler utstyr som er sårbart og har lav tillitt
1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer
1.2 Kartlegg enheter og programvare
2.2 Etabler en sikker IKT-arkitektur
2.3 Ivareta en sikker konfigurasjon
3.1 Oppdag og fjern kjente sårbarheter og trusler

Les mer her: www.nsm.no/grunnprinsipper-ikt

Digitale trender og utviklingstrekk

NSM/Ilja Hendel

Vi trenger kunstig intelligens for cybersikkerhet

.. men vi trenger også cybersikkerhet for kunstig intelligens.

Kunstig intelligens kan være vår tids mest revolusjonerende teknologi, og et paradigmeskifte i det globale samfunnet. Men hva kan vi forvente av den i cyberdomenet, og kan vi virkelig stole på den?

I den banebrytende artikkelen «Computing Machinery and Intelligence» i 1950, stilte Alan Turing for første gang fundamentale spørsmål som skulle bane veien videre for kunstig intelligens. Her introduserte han et spill, imitasjonsspillet, som for første gang utforsket et grunnleggende eksperiment om hvorvidt en tredjepart er i stand til å skille menneske fra maskin. Så, over 70 år senere, 30. november 2022, ble Chat-GPT* offentliggjort av OpenAI. De fleste har fått med seg oppmerksomheten som fulgte.

Etter kort tid fulgte en internasjonal mediestorm som varslet både arbeidsrevolusjoner og KI-apokalypser. Senere har bildet blitt mer nyansert. Språkmodellene er imponerende virkelighetstro, men har problemer med å resonere logisk og kan hallusinere fakta som bare er oppspinn. Språkmodeller er en del av en større verktøykasse i kunstig intelligens som i takt med algoritmisk utvikling og kraftigere maskinvare er i stand til å utføre nye oppgaver. Dette får konsekvenser også for cybersikkerhet.

Kan finnes usynlige bakdører

Å forstå hva kunstig intelligens kan gjøre og ikke gjøre er viktig. Men inntoget av kunstig intelligens har gitt oss et helt nytt problem. Når vi overlater viktig arbeid til kunstig intelligens, hvem er det som garanterer for sikkerhet og safety? Kunstig intelligens har blitt et nytt mål for cyberangrep som utnytter helt nye typer sårbarheter.

Skal du gå til innkjøp av kunstig intelligens-programvare for oppgaver i cybersikkerhet må du kjenne til begrensningene til hva kunstig intelligens kan gjøre, tenke nøye gjennom hva slags problem du ønsker å løse, og vite at kunstig intelligens-løsningen du får faktisk løser dette problemet.

I 2022 ble det demonstrert i praksis at en tredjepart tjenesteleverandør kan plante en kryptografisk bakdør* i modellen den er satt til å trene av en kunde, som er umulig å oppdage i etterkant og bare kan utnyttes av de som kjenner til den hemmelige nøkkelen. Altså, å oppdage bakdøren er like vanskelig som å knekke den aller mest avanserte kryptografien vi har i dag. En bakdør kan plasseres inn gjennom manipulasjon av programvaren som utfører treningen eller direkte med hensikt av leverandøren selv. Bakdører kan også oppstå gjennom forgiftning* av treningsdata, altså at noen med vilje prøver å villede kunstig intelligens-modellen ved å fôre den feil data. Målet med en bakdør kan være å påvirke modellen til å endre adferd i bestemte situasjoner, som å utføre en uønsket handling, eller lekke sensitiv informasjon den er trent på.

Vær varsom med datasett

Sårbarheter kan altså utnyttes i hele kunstig intelligens-leverandørkjeden fra treningsdata til modeller og programvare. NSM er involvert i utvikling av teknologi som på sikt kan gjøre en tredjeparts leverandør av modelltrening i stand til å legge ved en digital kvittering. Kvitteringen beviser at modellen den har trent for deg er et korrekt resultat av en spesifikk maskinlærings-algoritme, trent på nøyaktig den dataen du som kunde sendte inn. Tilsvarende teknologi kan brukes til å garantere at programvaren du bruker til å evaluere modellen gjør alt korrekt. Man må være varsom ved kjøp av treningssett fra en tredjepart, da tukling med treningssettet kan få målrettede effekter i modellen. Man bør også tenke nøye gjennom om man har trent på sensitiv data, før man deler tilgang til en modell med andre.

Aktiv forvirring og ondskapsfulle eksempler

Selv om programvare og treningssett ikke har feil og mangler, så kan likevel modellen ha egne svakheter. Noen sentrale utfordringer i kunstig intelligens har i det siste blitt løftet:

- Motstandsdyktighet mot manipulering
- Hvordan hindre lekkasje av sensitive treningsdata

Gjentatte ganger har det blitt vist at det ikke er vanskelig å lure kunstig intelligens som brukes til klassifisering. Et eksempel: Å få et bilde av en katt til å bli klassifisert som et hus. Dette kan gjøres gjennom små endringer på datafilen (f.eks. en JPG), som får kunstig intelligens-systemet til å tro at dette er et hus. Eksempler som er laget for å lure klassifisering kalles for ondskapsfulle eksempler og er en potensiell sårbarhet som trussel-aktører kan utnytte til å omgå kunstig intelligens-deteksjon. Hva om den samme teknikken brukes til å forvirre den kunstige intelligensen til hva som definerer bildet av en alliert eller fiende i et våpensystem? Systemet er sannsynligvis fortsatt 100 prosent treff-sikkert, men det kan føre til katastrofale feil, basert på aktiv forvirring av den opprinnelige klassifiseringen.

Data og kunstig intelligens-samarbeid

Det er mange tilfeller hvor to parter identifiserer at den andre sitter på data som komplementerer sin egen, og at et samarbeid rundt maskinlæring vil gi et bedre resultat enn de får hver for seg. Samtidig kan det være konkur-ransehensyn eller regulering som gjør det vanskelig å dele data i klartekst med hverandre. Løsninger som muliggjør sikker maskinlæring på sensitiv data fra flere parter er et viktig område NSM arbeider med. Nye tekno-logier i kryptografi er med på å løse disse problemene på helt nye måter.

Kan vi detektere kunstig intelligens?

Debatten rundt Chat-GPT har reist spørsmål ved om det i det hele tatt er mulig å avdekke om adferd eller innhold (f.eks. tekst) er fra kilden vi forventer, eller om den er laget av kunstig intelligens. Generativ kunstig intelligens* kan brukes til å orkestrere operasjoner designet for å manipulere en fokusgruppe på subtile måter over lengre tidsperioder, som f.eks. påvirkning gjennom sosiale media. Det kan være imitasjon av tekst, bilder, video, eller helt andre former for kommunikasjonsmedium. Selv om generativ kunstig intelligens til en viss grad er designet for å imitere virkeligheten, så er den fortsatt begrenset av noe. Og det er dette noe NSM, og mange flere, systematisk forsker på.

Milliardsatsing på kunstig intelligens

Regjeringen annonserte i september at forsknings-innsatsen på kunstig intelligens skal styrkes med én milliard kroner de neste fem årene.

– Kunstig intelligens og maskinlæring kommer til å forandre samfunnet på måter vi fortsatt ikke forstår eller klarer å kontrollere. Styrking av forskningsinn-satsen er avgjørende for at vi skal sikre at utviklingen skjer på en måte som er i tråd med våre verdier som samfunn, sier statsminister Jonas Gahr Støre.

Regjeringen starter også et større arbeid på tvers av departementer og sektorer for å se på tiltak for kompetanse, datasett og infrastruktur for forskning og innovasjon på og med fremtidens databehandling.

Forsvaret

Kvanteapokalypse – start forberedelsene nå

Gjennom de siste 50 år har kryptografien utviklet seg stadig raskere. Nå står vi overfor et vitenskapelig paradigmeskifte. I verste fall kan alt vi trodde var kryptert, bli åpnet på et øyeblikk. Hva skjer når alle koder knekkes? Det er dette som populært kalles kvanteapokalypsen.

Kryptografi er fagfeltet man snur seg mot om man på en eller annen måte behøver å sikre kommunikasjon fra uvedkommende. Dette er det mest grunnleggende og desidert eldste fagfeltet i cybersikkerhet, med en historie som kan spores tilbake til før Kristus. I Norge begynner overgangen til moderne kryptografi på 1930-tallet, med mye hemmelighold. Siden den gang har vi gjennomgått en internettrevolusjon og flyttet oss fra hemmelighold og mystikk til åpenhet i forskning og internasjonale standarder i kryptografi. I dag krever vi at enheter snakker sammen på tvers av formfaktor og teknologi, og fra ulike produsenter. Arbeidet med kryptoalgoritmer, protokoller og det vitenskapelige grunnlaget for sikkerheten foregår ikke lenger bak lukkede dører, men gjennom internasjonale samarbeid mellom industri, akademia og myndigheter. NSM jobber med mange spørsmål innen kryptografi og fungerer som et bindeledd mellom industri og akademia.

Dagens koder vil bli knekt

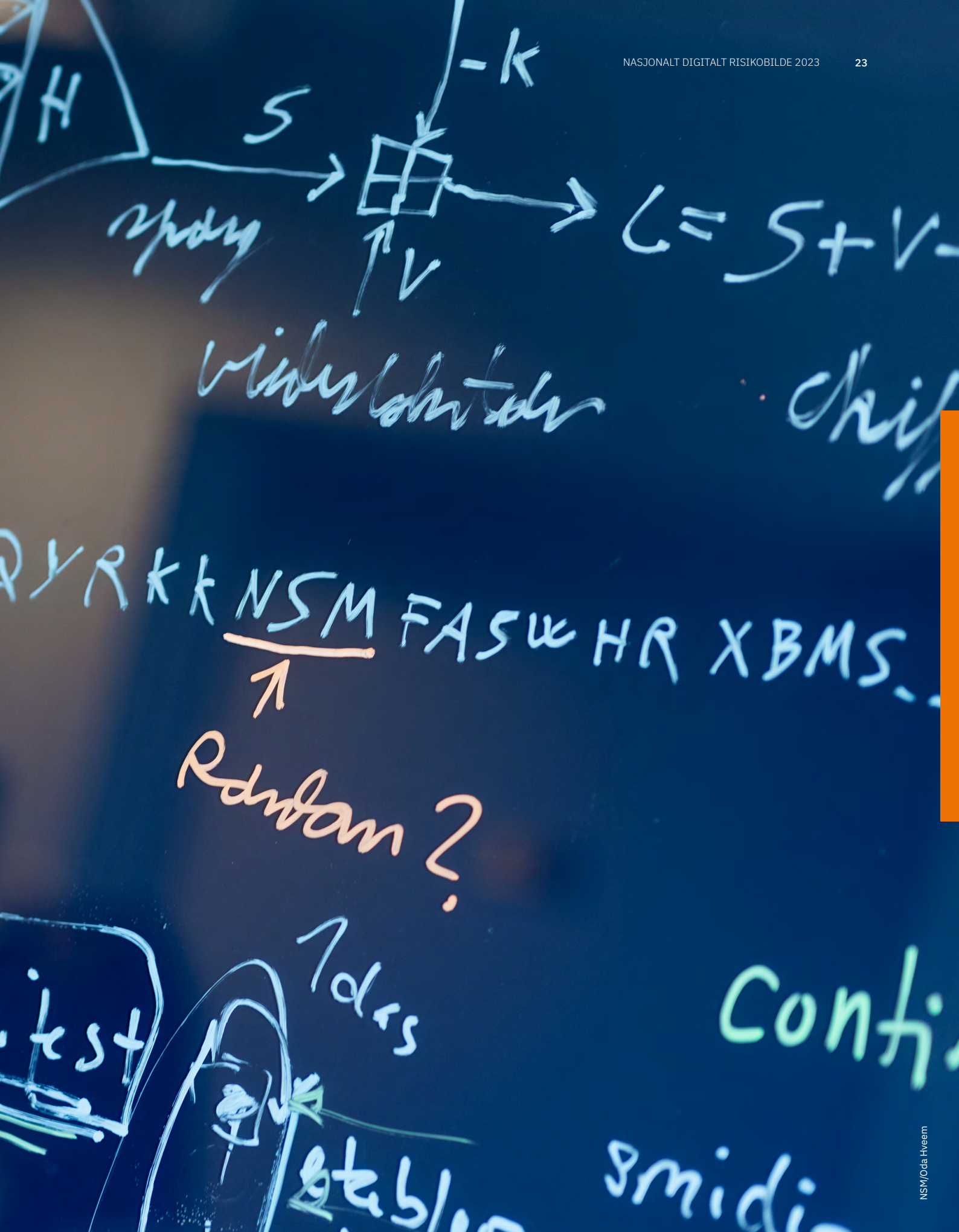
Alt fra kredittkort og F-35 kampfly til moderne dørlåssystemer er i dag avhengig av at de kryptografiske mekanismene i bunn er sikre. Alt dette står nå overfor en trussel som historisk sett er i rivende utvikling: En kryptoanalytisk relevant kvantedatamaskin*.

Kvantedatamaskiner er datamaskiner som utnytter egenskaper ved fysikkens aller minste bestanddeler. Dette er partikler som oppfører seg svært annerledes enn det vi er vant med, og disse egenskapene kan utnyttes til å lage kvantedatamaskiner. Mange antar i dag at en kvantedatamaskin vil bli bygget innen år 2030. Denne vil være i stand til å knekke mye av dagens kryptografi. Med andre ord: Alt det vi trodde vi kunne holde hemmelig, vil bli lest som en åpen bok av den som greier å utvikle den første kvantedatamaskinen.

NSM oppfordrer derfor alle virksomheter til kryptosmidighet når de planlegger oppgradering av IT-systemer. Om en kryptoanalytisk relevant kvantedatamaskin dukker opp i 2030, vil en betydelig andel av dagens IT-systemer være direkte sårbare mot angrep og avlytting. Det er viktig å være klar over at en aktør kan masselagre kryptert kommunikasjon i dag for så å bryte seg gjennom krypteringen til klarteksten den dagen kvantedatamaskiner blir tilgjengelig. Derfor er disse systemene allerede sårbare mot en kvantedatamaskin.

Forskningskappløpet er i gang

En kvantedatamaskin kan bli nyttig til å løse problemer innen områder som finans og kjemi lenge før den blir kraftfull nok til å forsere kryptografi. Dagens offentlige forskning er naturligvis også motivert av slike anvendelser og ikke av å forsere kryptografi. Kvanteinformatikk har blitt et viktig forskningsområde, og som med utvikling av tradisjonelle algoritmer, så krever ikke utvikling av kvantealgoritmer tilgang til en kvantedatamaskin. Vi kan utvikle nye algoritmer på tavla i dag som vil kunne brukes til å løse problemer på en kvantedatamaskin når den kommer. Det forskes derfor mye på å utvikle nye algoritmer som utnytter effekten i en kvantedatamaskin, og som løser problemer på andre og bedre måter enn tradisjonelle algoritmer. Hvordan kvante-algoritmer og kvantedatamaskiner kan utnyttes i resten av cyberdomenet er et pågående spørsmål. Men det vi vet er at dette har blitt et kappløp både mellom bedrifter og mellom nasjoner, hvor målet er å ha den dominerende kapabiliteten i den andre enden av tunnelen.



NSM/Oda Hveem

Pass på implementeringen

De dagligdagse angrepene som forbigår krypto handler vanligvis ikke om sårbarheter i selve kryptoalgoritmene, men i at utviklerne av et produkt har implementert kryptografien på en dårlig måte, i praksis feil. Dette ble kalt «feil bruk» i 40-tallets andre verdenskrig kryptoanalyse, og var hovedgrunnen til at de allierte var i stand til å forsere krypterte kommunikasjonslinjer. Dette er ikke uvanlig innen cybersikkerhet, og har rot i at det er ekstremt vanskelig å implementere kryptografi på en sikker måte i et produkt. Så når man skal velge leverandør av et kryptoprodukt, så er det ikke først og fremst sikkerheten til selve kryptoalgoritmene man bør bekymre seg for, men leverandørens evne til å implementere hele systemet sikkert. Heldigvis gjelder dette også for designere av skadevare og kryptovirus. Vi har sett mange suksesshistorier hvor dårlig håndverk hos de kriminelle har satt oss i stand til å gjenvinne et kryptokapret IT-system uten tilgang til nøkkelen, nettopp på grunn av feil bruk.

De nye standardene for internettkryptering vil ha helt andre typer for feil bruk enn de gamle, og implementasjonssårbarheter i kvanteresistent kryptografi er derfor høyt på agendaen fremover. NSM bidrar i denne prosessen.

Start arbeidet nå

Men hva nå? Alle er enige om at vi må forflytte oss til kvantesikre IT-systemer så raskt som mulig. **NSM anbefaler at norske virksomheter som har planlagt innkjøp av store IT-systemer bør vurdere om leverandøren har konkrete realistiske planer for migrasjon til kvantesikker IT.** Uten dette vil man stå i fare for å oppleve store endringskostnader i fremtiden dersom nye lover krever bruk av kvanteresistent kryptografi for beskyttelse av sensitive opplysninger.

Løsninger er på vei

Om man ønsker å beskytte informasjon i lang tid fremover, bør man allerede i dag planlegge for overgangen til kvanteresistente IT-systemer. Å bytte ut kryptoalgoritmer med nye kvantesikre standarder, eller innføre andre risikoreduserende tiltak som hybrid kryptering, medfører store kostnader. Derfor anbefaler NSM at eiere av informasjonssystemer med en viktig nasjonal funksjon

- A.utpeker en ansvarlig som kan redegjøre for kvantesårbare algoritmer i egne systemer
- B.tar høyde for potensielle merkostnader for å oppnå kvantesikkerhet når man vurderer leverandører av informasjonssystemer opp mot hverandre.

National Institute for Standards and Technology (NIST) har nylig publisert konkrete forslag til standarder. Disse er resultatet av et intensivt arbeid siden 2017. NSM har deltatt aktivt i dette internasjonale standardiseringsarbeidet og representerer også Norge i krypto-spørsmål i NATO.

Vil du vite mer? NSM har publisert en kort veiledning som kan hjelpe virksomheter med migrasjons-prosessen. Se våre nettsider nsm.no/kvantemigrasjon for mer informasjon.

NSM med nytt kryptosenter

I oktober 2023 åpnet senter for anvendt kryptologi i NSM. Senteret skal samle nasjonal kompetanse innenfor kryptologi og styrke samarbeidet mellom myndigheter, akademia og kryptoindustrien. Formålet er at Norge skal opprettholde og videreutvikle nasjonal krypto-kompetanse og være rustet til å møte fremtidens utfordringer innenfor kryptologi.

Det er derfor naturlig at senterets første prosjekt vil dreie seg om migrasjon til kvantesikre kryptoalgoritmer. NSM har arbeidet med kvantesikker kryptografi i flere år, og vi følger det internasjonale arbeidet med å utvikle nye kryptoalgoritmer. Disse skal sørge for at IT-arkitekturen er sikker, selv når kvantedatamaskiner blir en realitet. Å bytte til disse kan bli et omfattende arbeid som de fleste må gjennomføre. I våre øyne har vi foreløpig god tid, men alle parter må kartlegge sine systemer og nettverk for å identifisere hvor krevende det vil bli å foreta et bytte. I sikkerhetsfaglig råd anbefaler NSM å videreutvikle kryptosenteret til et nav for kompetanse og industri-utvikling på viktige teknologiområder som kvanteteknologi, bioteknologi og kunstig intelligens. Det nasjonale innovasjonssenteret for sensitive teknologier skal samle fagpersoner fra myndigheter, akademia og industri for å utvikle og ta i bruk sikkerhetsløsninger som ligger i forkant av teknologiutviklingen. **Formålet er å se på:**

- Hvordan vi som nasjon kan sikre oss mot trussel-aktørers bruk av ny teknologi (f.eks. forebyggende tiltak mot digitale angrep som utnytter kunstig intelligens)
- Hvordan vi kan styrke sikkerheten med bruk av ny teknologi (f.eks. bruke kunstig intelligens for å avdekke og stoppe digitale angrep)
- Hvordan vi best kan utnytte ny teknologi for å gi sikrere, bedre og mer effektive samfunnstjenester

Cyber i det store bildet

NSM/Tija Hendel

Cyberangrep mot kritisk infrastruktur

Kan det skje i Norge?

Cyberangrep mot kritisk infrastruktur i energi- eller petroleumssektoren kan medføre samfunnskonsekvenser som strømutfall eller stans i gassleveranser. Når Norge nå er en kritisk gassleverandør til Europa, bør scenarioet være dimensjonerende for sikkerhetsarbeidet i sektoren.

Ukraina har blitt utsatt for slike cyberangrep gjentatte ganger: I 2015, 2016 og sist i februar 2023. I februar førte angrepet mot energisystemer til strømutfall i store områder. Løsepengeangrepet mot Colonial Pipeline i USA i 2021 medførte betydelige samfunnskonsekvenser, da distribusjon av drivstoff stanset opp. SolarWinds-angrepet i 2020 fikk nasjonale konsekvenser da norske kraftselskaper ble berørt. Alle disse hendelsene viser kompleksiteten i systemer og nettverk i kritisk infrastruktur, og hvor store samfunnskonsekvenser et cyberangrep kan medføre.

Nye verktøy utvikles stadig

Trusselaktørene utvikler kontinuerlig sine metoder og verktøy. **De siste årene er det avdekket cyberverktøy som er tilpasningsdyktige til styring- og kontrollsystemer som brukes i flere sektorer – også i Norge.** Vi må øke motstandsdyktigheten og implementere robusthet i hele livsyklusen til digitale systemer som anvendes i kritisk infrastruktur. Bare slik kan vi opprettholde driften og sikre kraftforsyning og energisikkerhet. Spesielt risikoutsatt er angrepsflatene som kritisk infrastruktur har mot internetteksponerte tjenester. Denne angrepsflaten er det kritisk å sikre for ikke å bli utsatt for spionasje og sabotasje som kan forstyrre energiforsyningen av gass til Europa eller kraftforsyningen nasjonalt.

Norsk sokkel en kritisk gassleverandør

Det meste av norsk gass eksporteres i flere tusen kilometer med rørledninger til Europa. Etter Nord Stream-sabotasjen i Østersjøen i september 2022 ble norsk sokkel en kritisk gassleverandør til Europa. Dette har resultert i at det er etablert en grunnleggende nasjonal funksjon* (GNF): Transport av gass i rør til Europa.

Styring og kontroll av kraftproduksjon, kraftdistribusjon, samt produksjon av olje og gass utføres i stor grad av operasjonell teknologi og industrielle kontrollsystemer. Disse systemene og tilhørende fysiske prosessers tilgjengelighet og integritet er spesielt viktig, både for energisikkerhet nasjonalt og for produksjon av gass til Europa.

Energiproduksjon består av komplekse leveranse- og verdikjeder hvor kompleksiteten og digitale sårbarheter øker i takt med teknologiutviklingen. Integrasjon mellom IT-systemer og OT-systemer øker i form av mer deling av sanntidsdata, og tilgjengeliggjøring av kritiske industrielle systemer og prosessdata. Tilgang på sanntidsdata fra produksjonsmiljøer i kombinasjon med skytjenester er moderniseringsdrivere som medfører økt sårbarhet og risikoområder for operasjonell teknologi.

Kontrollsystemer potensielt mer sårbare

Fjerntilgang til industrielle kontrollsystemer gir økt tilgjengelighet for smart vedlikehold og produksjonsoptimaliseringer. Disse fjerntilgangene må sikres med gode tiltak for å hindre at trusselaktører får tilgang til sårbar operasjonsteknologi som produserer og distribuerer energi. I cyberdomenet deles kontaktflater mellom leveransekjeder, men også trusselaktører utnytter eksponerte funksjoner i cyberdomenet.

Risikoen øker i takt med teknologiutviklingen. Kompetanse-gapet øker og flere kritiske systemer og funksjoner tjenesteutsettes. Dette medfører økt leveranseavhengighet til eksterne OT-leverandører med ekspertise og kompetanse på industrielle systemer som inngår i kritisk infrastruktur.

Operasjonell teknologi

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

Kompleksitet og motstandskraft

For å sikre nasjonen mot fremtidens digitale risikobilde må motstandskraften økes. Det må iverksettes flere tiltak, både menneskelige, tekniske og organisatoriske. Sikkerhetstiltakene som skal sikre verdier må være robuste og tilpasset det til enhver tid gjeldende trussel- og risikobildet. Det medfører at tiltak må herdes, og ekstra barrierer må implementeres ved økt trussel og risiko. Vi står fremdeles i en spent sikkerhetspolitisk situasjon med krig i Ukraina.

Kritisk infrastruktur og digitale systemer, da spesielt internetteksponerte systemer og tjenester, er sårbare. Trusselaktørene har kapabilitet til å drive sabotasje gjennom digitale angrep som kan sette vår infrastruktur og grunnleggende nasjonale funksjoner ut av spill. Å bygge robusthet må utføres etter en god plan og over tid. Tiltakene er både ressurskrevende og tidkrevende å implementere på en god måte.

Energitrilemmaet

En annen nasjonal utfordring er energitrilemmaet, som er omtalt i NSMs sikkerhetsfaglige råd: Norge har satt en rekke klimamål og spesielt reduksjon av C02. Dette medfører økt behov for elektrifisering av norsk sokkel, men også innføring av større vindparker, både havvind og på land. Flere innretninger på norsk sokkel er blitt elektrifisert og forsynes med strøm fra land, noe som gir lavere CO2-utslipp. Dette betyr også økt avhengighet av kraft fra land til våre innretninger til havs. Med økt utbygging og økt oppmerksomhet mot lave CO2-utslipp står vi nå overfor et energitrilemma: på den ene siden vil vi imøtekomme lave utslippskrav, og samtidig øker vi avhengigheten av og tilgangen på stabil kraft for våre innretninger. Elektrifisering av sokkelen må sikres på en forsvarlig måte og ikke minst bygge på robuste og gode løsninger som gir trygghet for både norske og europeiske forbrukere av norsk energi.

Den store utfordringen er å balansere hensyn til klima og miljø, økonomi og forsyningssikkerhet og samtidig å ivareta nasjonale sikkerhetsinteresser

- NSMs sikkerhetsfaglige råd, 2023

Autonomi, krav til redundans, samt tilgang på kraft og ekom er viktige faktorer og avhengigheter til de fleste digitale systemer. Men er disse avhengighetene verdivurdert og risikovurdert? Er systemer og sikkerhetstiltak motstandsdyktige nok, og dimensjonert for fremtidig digital krig og sabotasje?

Colourbox

Datasentre og skytjenester – et kontinuitetsperspektiv

Samfunnet er kritisk avhengig av informasjon om infrastruktur og innbyggere, som helsedata, økonomi og finans, samt sikkerhets- og beredskapsinformasjon. I tillegg kommer IKT-systemene som lagrer og behandler denne informasjonen. Disse IKT-systemene driftes og forvaltes i ulike datasentre spredt ut over hele landet, Europa og verden for øvrig.

Datasenter

Et datasenter er en installasjon hvor digitale tjenester produseres, det vil si prosesseres og lagres. I disse sentrene innplasseres servere, nettverks- og lagringsutstyr.

Erfaringer fra Ukraina

Datasentre og infrastruktur som understøtter kritiske IKT-tjenester er fundamentale for å opprettholde et moderne samfunn. I den senere tid, og spesielt etter Russlands militære angrep på Ukraina, har fokuset på kontinuitet på et nasjonalt nivå og risiko knyttet til tap av samfunnsviktige data og IKT-tjenester økt. Dette kom tydelig frem i dagene før invasjonen i Ukraina: Det ukrainske parlamentet vedtok lovendringer som muliggjorde å flytte data og IKT-tjenester ut av landet, samtidig som enkelte skytjenestetilbydere bidro med teknisk bistand og løsninger for å migrere. Dermed klarte ukrainske myndigheter og virksomheter fortsatt å støtte landets befolkning, på tross av store fysiske ødeleggelser som følge av krigen.

Eksempelet fra Ukraina illustrerer noen av fordelene med moderne skyteknologi. Mulighetene til raskt å flytte store datamengder og dynamisk endre kapasitet for prosessering ga her kontinuitet i en svært kritisk situasjon.

Forberedelser i fredstid

Et annet eksempel er Estland som i 2017 signerte en avtale om å etablere egne datasentre i Luxemburg for å sikre kontinuitet av samfunnskritiske funksjoner i tilfelle naturkatastrofer, digitale angrep eller krig på estisk territorium. Avtalen sikrer Estland full kontroll over dataene, serverne og datasenteret, til tross for at plasseringen er innenfor Luxenbourg sitt territorium.

For å understøtte den svenske regjeringens ambisjoner om å utnytte digitaliseringens muligheter samt å øke den digitale robustheten, har man i Sverige etablert «Program 2032». Det har som mål å etablere et nasjonalt system bestående av sikre datasentre med tilhørende kommunikasjonsinfrastruktur, og har tatt frem ulike datasenterkonsepter og forslag til hvor datasentrene skal plasseres.

Den siste tids hendelser rundt om i verden, og andre lands tiltak og innsats, har påvirket hvordan vi i Norge ser på våre digitale verdier og betydningen av å beskytte dem. Dette kommer blant annet til uttrykk gjennom oppdatering av datasenterstrategien, hvor sikkerhet er tatt inn som eget tema, utredningen av en nasjonal skytjeneste, datasenterveileder for kommunesektoren, og reguleringen av datasenterbransjen. Sammen gjør dette at staten nå har flere initiativ som bidrar til å strukturere, samordne og forhåpentligvis redusere den digitale risikoen i samfunnet.

Beredskap

Datasentre utgjør både digitale og fysiske mål som må sikres tilstrekkelig for å tåle ytre påkjenninger gjennom hele krisespekteret. Dette gjelder spesielt for de datasentrene som rommer data, informasjon og systemer som samfunnet er mest avhengige av. Det er derfor viktig at virksomhetene kartlegger sine digitale verdier og vurderer eventuelle skadefølger om tjenesten av en eller annen grunn bortfaller, og plasserer verdiene i datasentre med tilstrekkelig sikringsnivå.

For enkelte av disse verdiene vil man til dels være avhengig av datasentre som har et høyere kontroll- og sikkerhetsnivå enn det man i hovedsak har sett at det kommersielle markedet i Norge tilbyr. Det er først og fremst sivile aktører som bygger den digitale infrastrukturen innen ekom og datasenter. Dette gjøres ut ifra kommersielle strategier og resultatkrav som ikke nødvendigvis sammenfaller med samfunnets behov for sikkerhet. Samtidig erfarer NSM etter publiseringen av NSMs datasenterrapport i 2022 at enkelte aktører innen sektoren nå ønsker å etablere datasentre som imøtekommer deler av det som ble belyst i rapporten. Initiativene vil bidra til å understøtte samfunnskritiske virksomheters behov til blant annet sikkerhet, eierskap og geografisk plassering, og dermed bidra til økt nasjonal kontroll.

Et utvalg av faktorer som påvirker den nasjonale kontrollen er:

Geografisk plassering	Den geografiske plasseringen av et datasenter vil påvirke hvilken jurisdiksjon datasenteret er underlagt.
Eierskap	Avhengig av eierstruktur vil staten i større eller mindre grad kunne påvirke forvaltningen av et datasenter.
Personellsikkerhet	Dersom et datasenter (eller IKT-systemer i slike) blir underlagt sikkerhetsloven kan man stille krav om adgangs- eller sikkerhetsklarering av personell.

Datasenter og nasjonal skytjeneste

Som en del av NSMs utredning for en nasjonal skytjeneste (KVU) og i lys av den pågående krigen i Ukraina, vil et viktig beredskapstiltak være å etablere tjenesten i flere datasentre geografisk spredt i Norge. Datasentrene må ha tilstrekkelig grad av redundant infrastruktur som binder de sammen, høyt tilgjengelighetsnivå og egenskaper som sikrer nasjonal og regional autonomi i tilfelle bortfall av internett.

Data og systemer må kunne migreres ut av landet uten å miste nasjonal kontroll. NSM ser verdien av å inngå bilaterale avtaler, med ett eller flere land, for å kunne etablere sikre og kontrollerte datasentre for strategisk viktige data. Det bør samtidig etableres arkitekturprinsipper som sikrer høy grad av portabilitet og reduserer risiko for innlåsing av informasjon og tjenester. I dag er det foreløpig de store skyleverandørene som er teknisk tilrettelagt for migrering over landegrenser, men da uten nasjonal kontroll og mulig risiko for innlåsing. Det bør derfor vurderes ordninger for alternative løsninger som bør baseres på universelle kjøremiljøer og følge «beste praksis».

Ved innføringen av en nasjonal skytjeneste vil enkelte hevde at konsentrasjonsrisikoen for samfunnskritiske IKT-tjenester øker. NSM erfarer samtidig at statlige virksomheters overgang til moderne skytjenester er preget av et fåtall leverandører. Man kan derfor stille spørsmål om man allerede i dag har en konsentrasjon av data og tjenester. Denne har i så fall oppstått ukontrollert eller ubevisst, samtidig som skytjenestene i liten grad er underlagt nasjonale kontrollmuligheter og påvirkning.

Leverandørkjeder og uoversiktlighet

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

- NSMs sikkerhetsfaglige råd 2023

En verdikjede beskriver ressurser, prosesser og aktiviteter som inngår i produksjonen av en vare eller tjeneste. Aktivitetssettet til en produksjonsbedrift kalles en verdikjede. Leverandørkjeden er den delen av verdikjeden som omfatter aktiviteter utført av leverandørene.

Ordet kjede er en foreldet tenkemåte for det digitale domenet. Med digitalisering og utbredelsen av internettet er modellen verdikjede supplert av verdinettverk, og for den typen virksomhet som driver med problemløsing kalles aktivitetssettet for verdiverksted. Dette betyr at rollene til aktørene kan være mer nyanserte enn leverandør eller kunde, og leveranser kan gå begge veier.

Administrasjon og styring av leverandørkjeder er en del av fagområdet logistikk. Over tid har leveransekjeder økt i kompleksitet. Når virksomhetskontinuitet er avhengig av digitale tjenester som er tjenesteutsatt stopper virksomhetens tjenesteproduksjon i samme øyeblikk leverandøren ikke kan levere sin tjeneste. En følge av dette er at styring av digitale leverandørkjeder må være en del av virksomhetens helhetlige risikostyring, og må underlegges den samme kontroll og oppfølging som alle leverandører.

Utfordringen er at digitale leverandørkjeder er uoversiktlige. Et eksempel er programvare, hvor det i dag er utstrakt bruk av åpen kildekode. Avhengig av hvilken bransje det gjelder blir det anslått at mellom 75 og 90 prosent av applikasjonene inneholder åpen kildekode. Hvor stor andel av kildekoden som er åpen kildekode vil variere mellom forskjellige typer applikasjoner.

Leverandørkjedeangrep – et eksempel

Leverandørkjeden: Produksjon av åpen kildekode kan skje med en forretningsmodell hvor en gruppe utviklere danner et verdiverksted. Den som utvikler en ny programvaremodul kan bygge på programvaremoduler andre utviklere har publisert og vedlikeholder, og andre utviklere kan bruke den nye programvaremodulen.

Et mulig angrep: Et verdiverksted som beskrevet over vil som regel bruke et felles utviklingsmiljø eller -plattform hvor den enkelte utvikler er ansvarlig for å sikre sin egen brukertilgang og muligheten til å endre kildekode og publisere nye versjoner av sine egne programvaremoduler. Dersom en trusselaktør får adgang til utviklerens brukerområde og publiserer en ny versjon som inneholder skadevare, kan dette forbli uoppdaget over lengre tid. Dersom den kompromitterte modulen brukes av andre programvaremoduler i verdiverkstedet kan også disse modulene bidra til å spre skadevaren.

Leveranse av skadevare: Applikasjoner som bruker en eller flere av modulene som nå inneholder skadevare vil etter hvert oppdateres og dermed er skadevaren levert og vil kjøre på systemene til de som bruker disse applikasjonene. Et enkelt innbrudd på kontoen til en utvikler kan føre til at applikasjoner som brukes på et stort antall systemer inneholder skadevare.

Særtrekk for et leverandørkjedeangrep

For en virksomhet som blir utsatt for leverandørkjedeangrep kan dette beskrives som en digital innsidetrussel. Virksomheten har selv anskaffet og startet skadevaren i sine egne systemer, og på den måten blir flere sikkerhetstiltak satt ut av spill.

For trusselaktøren er leverandørkjedeangrep en multiplikator. De fleste stegene i et cyberangrep gjennomføres mot en virksomhet, leverandøren. Multiplikatoren er at det siste steget i angrepet skjer hos leverandørens kunder, og i praksis utføres det siste steget av kundene selv.

Kunstig intelligens i leverandørkjedene

Kunstig intelligens er allerede tatt i bruk ved utvikling av programvare, blant annet i form av programmeringsverktøy med en innebygget digital assistent som kan fungere som en partner ved parprogrammering*. Dermed blir leverandørkjeden for kunstig intelligens som brukes i slike verktøy en del av leverandørkjeden til programvaren som blir utviklet, og må underlegges risikostyring av leverandørkjedene for å unngå at kunstig intelligens blir en digital innsidetrussel.

Bedre risikostyring av leverandørkjedene

Kildekoden til en applikasjon deles gjerne inn i moduler, og kan beskrives som en trestruktur hvor hver modul kan være avhengig av en eller flere moduler på lavere nivå. Moduler utviklet som åpen kildekode er ofte avhengige av andre moduler utviklet som åpen kildekode. Resultatet er at en enkelt applikasjon kan ha flere lange avhengighetskjeder til kildekode utviklet av mange forskjellige personer eller prosjekter.

Det er nødvendig å skaffe tilstrekkelig oversikt og et grunnlag til å gjennomføre en løpende risikovurdering og skape en mulighet for å iverksette korrigerende tiltak når det varsles om sårbarheter. En mulig løsning er å etablere standardisert system for digitale stykklister (software bill of materials). Dette er en problemstilling som det har vært arbeidet med i minst ti år og som i praksis krever at tilstrekkelig mange land stiller samsvarende krav om denne typen dokumentasjon av programvare.

Digitale stykklister vil gi bedre oversikt over hvilke komponenter et system består av, og en mulighet til å følge opp varsling om sårbarheter. For at dette skal fungere i praksis krever det at flere internasjonale standarder kommer på plass og at disse brukes aktivt av både leverandører og kunder. En kritisk faktor er nye sårbarheter blir rapportert og registrert, slik at de kan kyttes til de digitale stykklistene.

Velger virksomheter å bruke skytjenester med programvare-som-en-tjeneste (SaaS) er det stor sannsynlighet for at også disse applikasjonene inneholder åpen kildekode. Det er nødvendig at også digitale tjenester får et krav om transparens med bruk av digitale stykklister.

Det kan også være ulemper knyttet til digitale stykklister. Leverandører ønsker å beskytte forretningshemmeligheter. Det er heller ikke ønskelig å gi trusselaktører bedre mulighet til å lete etter kjente eller nye sårbarheter som kan utnyttes i et angrep.

Ny europeisk regulering

Enkelte utfordringer med leverandørkjedene er adressert i EUs NIS2-direktiv. EU-kommisjonens forslag til et rammeverk for digitale produkters og tjenesters robusthet (Cyber Resilience Act) inneholder bestemmelser om bruk av digitale stykklister. Denne reguleringen vil bruke internasjonale standarder og dermed kan vi forutsette at den i tilstrekkelig grad vil samsvare med lignende regulering i USA.

Det gjenstår mye arbeid med å tilpasse standarder og utvikle verktøy, men det er helt nødvendig å etablere bedre sikkerhet mot digitale innsidere som beveger seg gjennom uoversiktlige leverandørkjeder. NSM har fulgt denne utviklingen over tid. Det er et internasjonalt arbeid som pågår, og som nærmer seg vedtatt regulering i Europa.

Når cybersikkerhet blir bedre – øker risikoen for en innsider i bedriften din?

Trusselaktører som ønsker å ramme norske virksomheter gjennom spionasje, manipulasjon eller sabotasje, kan i dag ofte gjøre dette enklere og med langt større nytte og effekt gjennom det digitale domenet – sammenlignet med nytten og effekten av å måtte rekruttere en person på innsiden av virksomheten.

Cybertrusselaktørers stadige herjinger med virksomheter og infrastruktur i Norge og andre land, har samtidig bidratt til økt bevissthet om nødvendigheten og betydningen av cybersikkerhet. Både offentlige og private virksomheter har forstått at cybersikkerhet må prioriteres – dersom konkurranseevne, leveranser, funksjoner og tjenester skal opprettholdes. Gjennom økt satsing på ulike menneskelige, teknologiske og organisatoriske tiltak, vil virksomhetene i større grad evne å forhindre og motvirke trusler og sårbarheter i cyberdomenet. Spørsmålet er om en slik forventet styrket sikkerhet og beredskap mot eksterne cybertrusler, samtidig vil bidra til en økt trussel på innsiden av virksomhetene; vil innsiderisikoen øke?

Innsiderisiko

Innsiderisiko handler om personer som kan komme til å utnytte sine legitime tilganger til virksomhetens verdier for uautoriserte formål. En innsider kan være en nåværende eller tidligere ansatt, konsulent eller innleid, som har eller har hatt en legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne tilgangen på en måte som påfører virksomheten tap eller skade.

Flere typer innsidere

På et overordnet nivå kan det skilles mellom den ubevisste og den bevisste innsideren. Den ubevisste innsideren er den som uforvarende åpner et vedlegg med skadevare, som feilaktig videreformidler data som ikke skulle vært videreformidlet, eller som skjødesløst lar være å forholde seg til sikkerhetskrav og sikkerhetsoppdateringer. Denne gruppen innsidere står for **over halvparten av innsidehendelser mot digitale verdier,** ifølge en større internasjonal studie av innsidetrusselen.

Ifølge samme studie står den bevisste innsideren for litt over **en fjerdedel av innsidehendelsene**. Den bevisste innsideren er en person som med forsett utnytter sine legitime tilganger for ondsinnede formål – på vegne av seg selv eller andre. Dette kan være en person drevet av egne motiv som misnøye, hevn, ideologi eller økonomi. Eller det kan være en person som er presset eller rekruttert av en statlig eller ikke-statlig trusselaktør. Innsidere kan drives av en kombinasjon av flere av disse faktorene, som gjerne forkortes MICE – Money, Ideology, Compromise, Ego.

Innsiderisiko ved bedret cybersikkerhet

Norske virksomheters økte fokus på og arbeid med cybersikkerhet, vil kunne bidra både til en sterkere sikkerhetskultur internt i virksomhetene og til en styrket motstandsdyktighet mot eksterne trusler. Samtidig vil sikkerhetsløsninger som eksempelvis zero trust og passordfri pålogging, kunne gjøre det vanskeligere for eksterne cybertrusselaktører å få innpass i virksomheters systemer. **En generelt bedret cybersikkerhet vil dermed kunne øke betydningen av personer med fysisk tilgang til virksomheters digitale verdier.** Den bevisste innsideren kan med andre ord bli mer attraktiv og verdifull for en trusselaktør – for å kunne installere skadevare, hente ut informasjon, manipulere datainnhold eller ødelegge data og dataavhengige prosesser.

For den enkelte virksomhet vil innsiderisikoen kunne bli ytterligere påvirket av øvrige trender og utviklingstrekk:

- **Hjemmekontoret**, som har brakt virksomhetenes verdier hjem til folk, har samtidig medført at virksomhetene ikke lenger har kontroll på de menneskelige, teknologiske og fysiske forutsetningene som omgir virksomhetenes verdier. Dette skaper nye sårbarhetsflater som kan forsterke risikoen knyttet til samtlige innsidekategorier.
- **Migrasjon til datasentre og skytjenester** vil for mange virksomheter styrke den digitale sikkerheten. Samtidig vil ett datasenter ofte forvalte og ha tilgang til mange virksomheters verdier. En innsider i et datasenter og hos en skytjenesteleverandør kan således være gull verdt for en ondsinnet aktør. Bedret cybersikkerhet i kombinasjon med økende verdikonsentrasjon i datasentre, kan dermed øke betydningen av en innsider.
- **Informasjonssystemer** som er utilgjengelige via internett, kalt *air gapped*, er ofte systemer som forvalter sensitive og skjermingsverdige data. Rekrutterte innsidere kan ofte være trusselaktørers eneste vei inn til slike ettertraktede verdier. Trusselaktører kan imidlertid også ha kapasitet til å utnytte teknologiske sårbarheter hos en virksomhet fra en posisjon i fysisk nærhet til virksomhetens lokaler, kalt næraksessoperasjoner.
- **Sårbarhetstrenden.** Antallet kjente digitale sårbarheter har økt hvert år siden 2017, og det finnes i dag mer enn 78000 kjente utnyttbare sårbarheter. Virksomheters digitale sikkerhet handler derfor mye om viljen og evnen til å holde tritt med sårbarhetsutviklingen gjennom løpende sikkerhetsoppdateringer. Sårbarhetsutnyttelser som fortsatt bidrar til vellykkede cyberoperasjoner, vil kunne dempe trusselaktørers behov for å rekruttere innsidere.
- **Fokuset på innsiderisiko** i den enkelte virksomhet vil kunne påvirke en nåværende eller fremtidig innsiders kost-nytte vurderinger. Konkrete tiltak med sikte på å forhindre, avdekke og håndtere innsidevirksomhet vil kunne evne både å forebygge og avskrekke fremtidig innsideaktivitet.

Svensk brødrepar dømt for spionasje

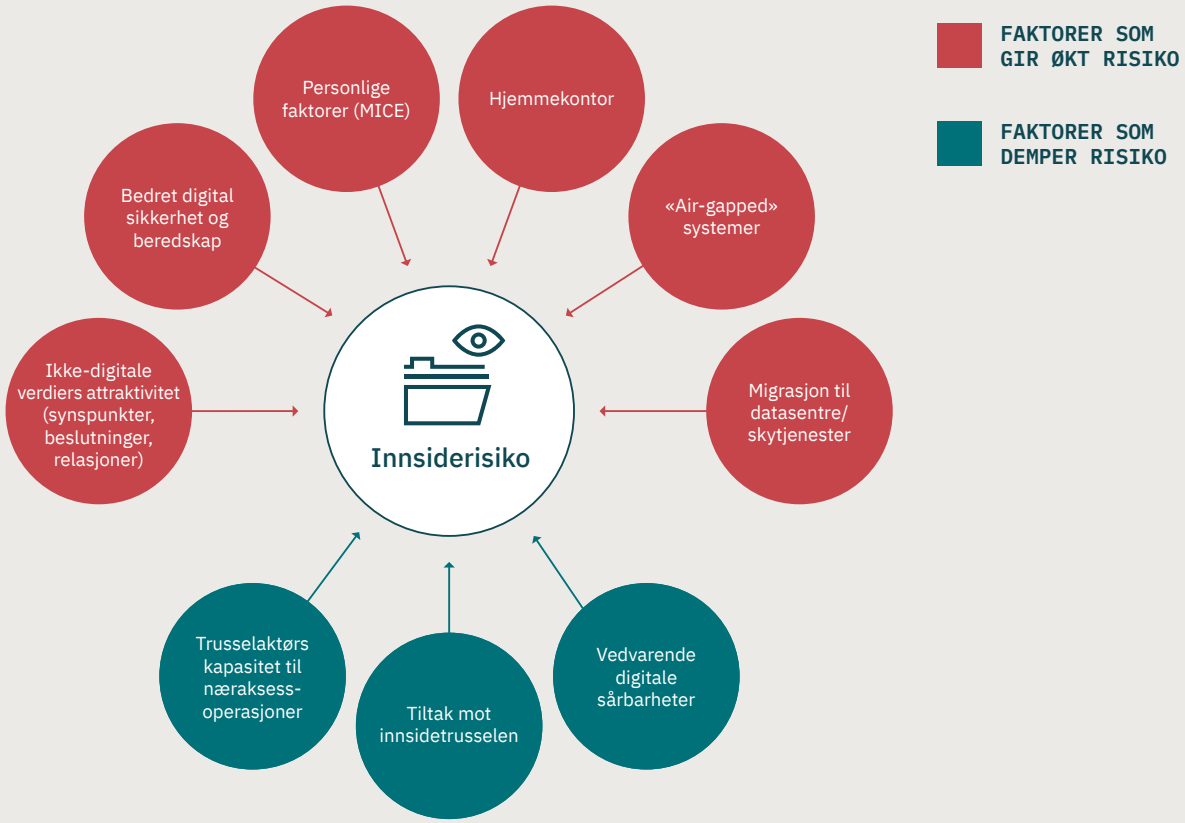
To svenske, iranskfødte brødre ble i Sverige dømt for grov spionasje til fordel for den russiske militære etterretningstjenesten GRU.

Den eldste broren (42) ble tidligere i år dømt til livstid i fengsel. Han hadde i flere år jobbet for det svenske etterretningspolitiet Säpo og den svenske militære e-tjenesten Must. Den yngste broren (35) ble dømt til ni år og ti måneders fengsel. Ifølge tiltalen har de to spionert for GRU siden 2011. Begge nekter straffskyld.

USA: Innsider i telekom blokkerte dissidenter

Siden 2018 skal en innsider i et amerikansk telekomselskap, på oppdrag fra kinesiske sikkerhetsmyndigheter, først ha kartlagt og senere blokkert USA-baserte kinesiske dissidenters bruk av telekomselskapets digitale plattform. Åtte ansatte i kinesiske myndigheter var blant de siktede i saken, som ifølge amerikansk påtalemyndighet «illustrerer risikoen for innsidere».

Figur 3: Faktorer som har innvirkning på innsiderisiko



Innsiderens metoder

En bevisst innsider kan benytte en rekke ulike metoder for å hente ut og videreformidle sensitive data fra virksomhetens systemer. Dette kan dreie seg om eposter sendt til illegitime mottakere, bruk av eksterne lagringsmedier, internettbaserte opplastingsmuligheter, bruk av meldingstjenester og app'er, kommunikasjon gjennom sosiale medier og konferanseplattformer, oppkobling til eksterne enheter via WiFi og Bluetooth, eller bruk av flere brukerkontoer tilknyttet det samme utstyret eller den samme tjenesten – eksempelvis servicepersonell som logger seg på med det ene og samme utstyret hos mange oppdragsgivere. Virksomheters kontroll på bruken av eksterne lagringsenheter vil være ett viktig tiltak for å forhindre uautoriserte uttak av data.

En innsider vil også kunne benytte ulike metoder for å skjule aktivitet og hindre deteksjon. Dette kan eksempelvis dreie seg om å lagre data med et annet navn, i et annet filformat, på et lokalt område; det kan dreie seg om å gjemme sensitiv informasjon i et ikke-sensitivt dokument; eller det kan benyttes steganografi, en metode som skjuler informasjon i annen informasjon – for eksempel en tekst skjult i et bilde. Å forhindre bruk av steganografi-applikasjoner er derfor et tiltak som virksomheter bør vurdere.

En innsider kan også ramme en virksomhets tilgang til sine data. Uten å ramme dataenes konfidensialitet eller integritet, kan insideren eksempelvis fjerne kritisk programvare og på den måten gjøre dataene utilgjengelige for brukerne eller kundene. En innsider med lederfunksjon eller administratorrettigheter vil også kunne endre eller slette informasjon som sporer eller logger brukeratferd – og dermed utmanøvrere virksomhetens egne tiltak mot innsidere. Én person alene bør derfor ikke kunne ha mulighet til å gjøre vesentlige endringer i systemer og logger.

Virksomheters arbeid med innsiderisiko

Forebygging av innsiderisiko forutsetter en helhetlig tilnærming med både menneskelige, teknologiske og organisatoriske tiltak. Virksomheter bør som et minimum:

- Inkludere en vurdering av innsidetrusselen i sine risikoanalyser
- Innføre et innsiderisikoprogram for bevisstgjøring, forebygging, avdekking og håndtering
- Etablere tekniske løsninger som evner å forhindre, monitorere og ettergå uautoriserte forsøk på å hente ut, manipulere eller sabotere sensitive virksomhetsdata

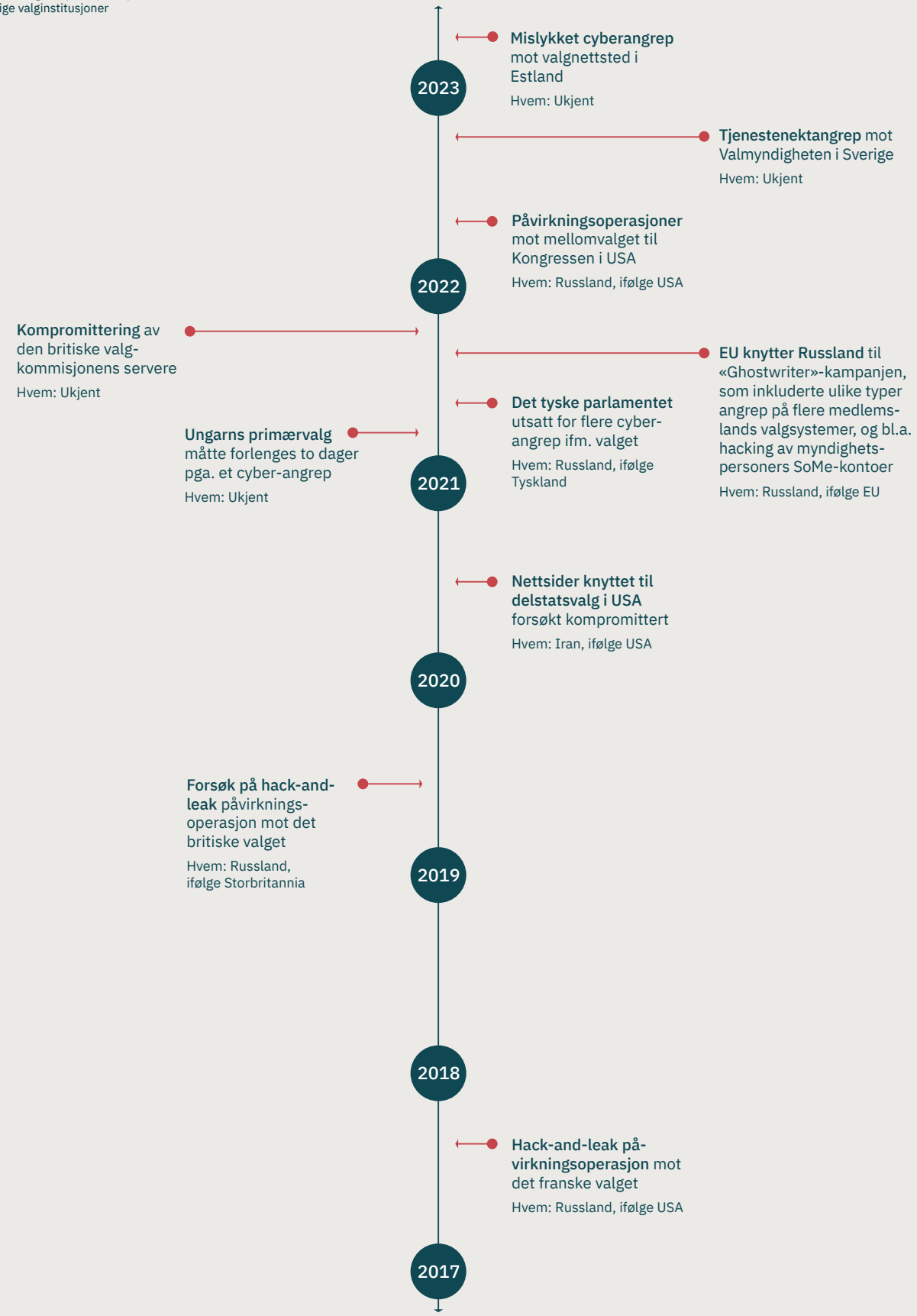
NSM/Ilja Hendel

Cyberdomenet – slik brukes det mot demokratiske valg

Demokratiske valg gjennomføres i Norge annethvert år og handler om hvem som skal styre landet nasjonalt og lokalt i en kommende fireårsperiode. For stater som påvirkes særskilt av norsk politikk i ulike spørsmål, fremstår valgpåvirkning som en unik mulighet til å kunne forme de neste fire års norske beslutninger i ønsket retning. En annen motivasjon for å påvirke nasjonale eller lokale valg kan være å undergrave tilliten og legitimiteten til selve demokratiet. Russlands og Kinas hacking av Stortinget i henholdsvis 2020 og 2021 synliggjorde at demokratiske institusjoner og norske folkevalgte er mål for autoritære stormakters etterretningstjenester. At trusselaktører bruker digitale sårbarheter og ny teknologi for å undergrave demokratiske prosesser har en lang rekke land erfart i de senere år. Senest under gjennomføringen av det svenske riksdagsvalget i september 2022 ble Valmyndigheten utsatt for tre tjenestenektangrep – altså en form for sabotasjeforsøk. Og ved mellomvalget til Kongressen i USA samme år skal russiske aktører nok en gang ha gjennomført påvirkningsoperasjoner mot valget, ifølge amerikansk etterretning.

Valgdirektoratet

Figur 4: Et utvalg av cyberoperasjoner mot vestlige valginstitusjoner



NSM/Tija Hendel

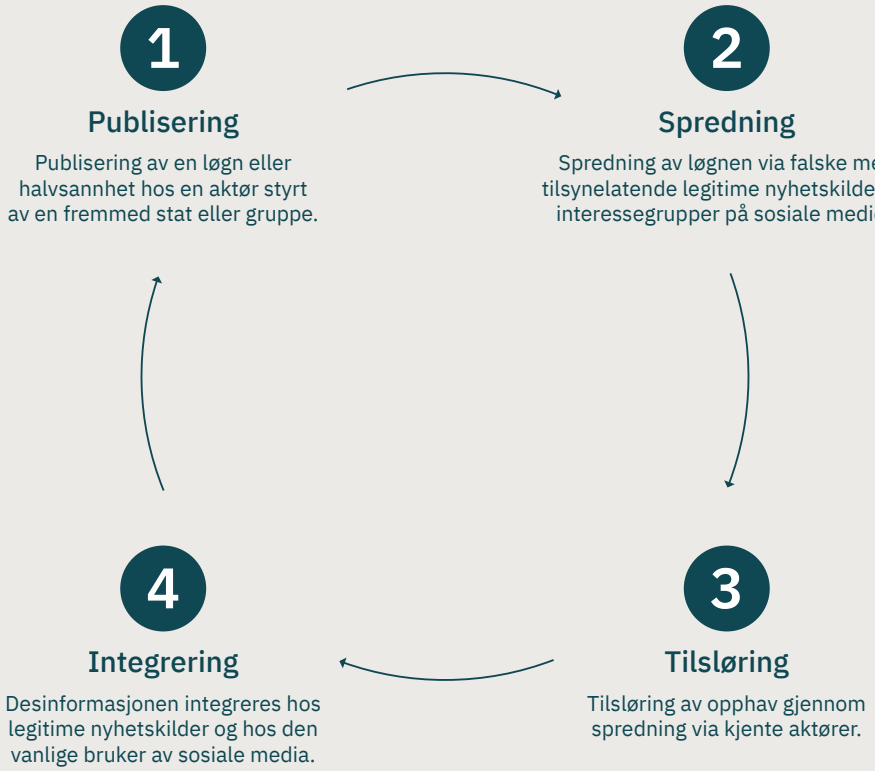
Ettersom demokratiske valg avholdes regelmessig og til fastsatte tidspunkt, gir dette trusselaktører tid til planlegging. Forberedelser til ondsinnede cyber-operasjoner mot demokratiske valg kan derfor foregå måneder og år i forveien. Slike cyberoperasjoner vil i hovedsak kunne rette seg mot tre hovedmål: Velgere, partier/politikere og selve valggjennomføringen. Cybertrusselaktivitet mot ett av disse målene vil som oftest også få konsekvenser for de øvrige målene.

Velgere kan påvirkes av falsk, manipulert eller ikke-kontrollerbar informasjon som produseres av en trusselaktør. Slik desinformasjon kan raskt få stor spredning via ulike digitale plattformer – og eksempelvis forsterke konfliktlinjer eller skape økt usikkerhet. For to år siden etablerte en ukjent aktør falske domener for samtlige partier på Stortinget. Slike falske nettsider eller eposter som etterligner reelle partiers profiler, kan benyttes til å innhente påloggingsinformasjon så vel som til å spre både desinformasjon og ondsinnet skadevare. Gjennom såkalt *deepfake* tekst, lyd eller bilde kan en trusselaktør gi inntrykk av at en person har sagt eller gjort ting denne personen aldri har sagt eller gjort.

Partier, kandidater og deres administrative medhjelpere kan utsettes for ulike typer ondsinnede cyberoperasjoner. Målet kan være å påvirke, forstyrre eller sabotere interne partiprosesser samt kommunikasjonen med velgerne. Dette kan påvirke tillitsforhold innad i partier så vel som velgeroppslutningen. Trusselaktører kan skjende eller manipulere partiers nettsider og kandidaters digitale profiler. Før stortingsvalget i 2021 ble eksempelvis en kandidats profil på sosiale medier manipulert til å fremstå som støtte for en terrorgruppe. Dette er en type misbruk som NSM håndterer gjennom sin beredskapsordning for sosiale medier.

Politikeres e-poster kan bli kompromittert i den hensikt å grave frem opplysninger som kan misbrukes. Publisering av slik *hack-and-leak*-informasjon, som kan være en blanding av ekte og manipulert innhold, kan påvirke valgprosesser. Typiske eksempler er hackingen av det demokratiske partiet i USA i 2016 og Emmanuel Macrons valgkampanje i Frankrike i 2017. Gjennom trussel om lekking av ufordelaktig eller sensitiv personinformasjon vil kandidater også potensielt kunne presses til å endre politiske standpunkter til fordel for en trusselaktør, eller til å trekke sitt kandidatur.

Figur 4: desinformasjonens vei til spredning via troverdige nyhetskilder.



Valggjennomføringer kan bli forsøkt sabotert ved at den digitale valginfrastrukturen utsettes for løsepengeangrep eller tjenestenektangrep – slik Sverige opplevde i 2022. Trusselaktører kan også utnytte sårbarheter og skadevare for å manipulere digital valginfrastruktur – eller leverandører til slik infrastruktur – hvilket kan skape usikkerhet om valgets legitimitet. I oktober 2022 avdekket den britiske valgkommisjonen mistenkelig aktivitet i sine datasystemer. Det viste seg at hackere hadde infiltrert disse systemene første gang allerede i august 2021. Trusselaktører hadde under angrepet tilgang til valgkommisjonens kontrollsystemer, epostsystemer og kopier av velgerregistre. I forkant av Stortingsvalget 2021 måtte en kommunal PC som var planlagt benyttet i valggjennomføringen, byttes ut etter å ha blitt infisert med ondsinnet skadevare. Hendelsene i Storbritannia, Norge og andre land synliggjør at digital valginfrastruktur er mål for ondsinnet aktivitet. Det er derfor avgjørende for demokratiet å beskytte slik infrastruktur.

Motstandsdyktighet mot påvirkning, manipulasjon og sabotasje av demokratiske prosesser

- **Velgere** må være bevisste på ulike digitale påvirkningsmetoder og kritisk vurdere informasjonsinnhold. Bruk av troverdige kilder for å verifisere informasjon er viktig før informasjonen deles og spres videre via sosiale medier.
- **Partier og kandidater** må være bevisste på at eget publisert innhold kan manipuleres og at epostkommunikasjon kan kompromitteres og misbrukes. En hendelseshåndteringsplan må være klar når trusler rammer og sårbarheter utnyttes.
- **Valginfrastrukturen** utgjør grunnmuren i demokratiske valg og må sikres fysisk, digitalt og personellmessig. Dette gjelder ikke minst i kommunene, der selve valggjennomføringen foregår. Sikkerhetstiltak i kommunene bør standardiseres og følges opp sentralt. På valgdagen er redundans og back-up-løsninger avgjørende dersom ordinære løsninger svikter.

*Ordliste

Det mørke nettet: eng: The Dark Web Begrep for en del av internettet en må bruke dedikerte nettlesere, som The Onion Router (TOR) for å nå. Såkalt løk-ruting muliggjør en høyere grad av anonymitet i kommunikasjonen.

Store språkmodeller: eng: Large Language Models (LLMer) er avanserte maskinlæringsmodeller som er spesialisert på å forstå og generere naturlig språk. Disse modellene er trent på enorme mengder tekstdata, noe som gjør at de kan lære seg et bredt spekter av språklige mønstre, strukturer og kontekst.

Chat-GPT: Chatbot lansert av OpenAI i november 2022. Chat-GPT står for Chat Generative Pre-trained Transformer, og ble lansert som en prototype 30. november 2022. Trolig den mest kjente av de store språkmodellene, som tar i bruk generativ kunstig intelligens.

Bakdør: En bakdør er innenfor IT en vei inn i et system som er åpnet av uvedkommende, og som ikke er kjent av systemets eier. Gjennom en slik bakdør kan noen for eksempel få tilgang til å lese, endre eller slette informasjon.

Dataforgiftning: Når feilinformasjon blir matet til kunstig intelligens for å skape sårbarheter. Dataen som mates kunstig intelligens-modellene er utformet for å fordreie logikken til kunstig intelligens.

Generativ kunstig intelligens: En type kunstig intelligens som er i stand til å generere noe helt nytt som ikke finnes fra før. For å få til dette har de kraftigste modellene bak generativ kunstig intelligens tilgang til enorme mengder data.

Kryptoanalytisk relevant kvantedatamaskin (KRK): En kvantedatamaskin som har nok fysiske q-bits til å knekke dagens offentlig-nøkkelkryptograf.

Grunnleggende nasjonal funksjon (GNF): En GNF er definert som «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser», jf. sikkerhetsloven § 1-5, nr 2.

Parprogrammering: En arbeidsmetode hvor to programmerere arbeider sammen på en arbeidsstasjon. Den ene programmereren kan erstattes av kunstig intelligens.

*Trykk ordet du søkte på for å gå tilbake til teksten.

Design: Tank

Utsatt for et dataangrep?

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

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

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

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

Se NSMs nettsider for kontaktinformasjon.

NASJONAL
SIKKERHETSMYNDIGHET

Postboks 814,
1306 Sandvika

67 86 40 00
nsm.no/NDIG2023