NSM

Risiko 2023

Økt uforutsigbarhet krever høyere beredskap

Forsidefoto: Forsvaret / NTB

NSMs rapport «Risiko» er én av tre offentlige trussel- og risikovurderinger som utgis i første kvartal hvert år. De øvrige gis ut av Etterretningstjenesten og Politiets sikkerhetstjeneste.

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for nasjonal forebyggende 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 for å avdekke og varsle om cyberangrep mot digital infrastruktur. NSM har også et nasjonalt ansvar for å koordinere håndteringen av alvorlige cyberangrep.

Etterretningstjenesten

E-tjenesten er Norges nasjonale utenlandsetterretningstjeneste. Tjenesten er underlagt forsvarssjefen, men arbeidet omfatter både sivile og militære problemstillinger. E-tjenestens hovedoppgaver er å varsle om ytre trusler mot Norge og prioriterte norske interesser, støtte Forsvaret og forsvarsallianser Norge deltar i, og understøtte politiske beslutningsprosesser med informasjon av spesiell interesse for norsk utenriks-, sikkerhets- og forsvarspolitikk. I den årlige trusselvurderingen «FOKUS» gir E-tjenesten sin analyse av status og forventet utvikling innenfor tematiske og geografiske områder som tjenesten vurderer som særlig relevant for norsk sikkerhet og nasjonale interesser.

Politiets sikkerhetstjeneste

PST er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste, underlagt justis- og beredskapsministeren. PST har som oppgave å forebygge og etterforske alvorlig kriminalitet mot nasjonens sikkerhet. Som ledd i dette skal tjenesten identifisere og vurdere trusler knyttet til etterretning, sabotasje, spredning av masseødeleggelsesvåpen, terror og ekstremisme. Vurderingene skal bidra i utformingen av politikk og støtte politiske beslutningsprosesser. PSTs årlige trusselvurdering er en del av tjenestens åpne samfunnskommunikasjon der det redegjøres for forventet utvikling i trusselbildet.

Om rapporten

Risiko 2023 beskriver hvordan trusselaktører kan utnytte sårbarheter hos virksomheter og i samfunnet, og hvilken risiko dette medfører. I rapporten peker NSM på hvordan myndigheter og virksomheter bør redusere sårbarheter for å gjøre trusselaktørenes jobb vanskeligere.

Risiko 2023 henvender seg til hele samfunnet, men spesielt til ledere og personell med sikkerhetsoppgaver. Målet med rapporten er å gi virksomheter bedre forutsetninger for å se sikkerhetsarbeidet i en større sammenheng. Dette er spesielt viktig for virksomheter underlagt sikkerhetsloven, men også for andre virksomheter. Rapporten inneholder eksempler og anbefalte tiltak som norske virksomheter bør gjøre for best å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Rapporten omtaler også hvordan virksomhetene og myndighetene bør redusere sårbarheter for å gjøre trusselaktørenes jobb vanskeligere.

Rapporten kan lastes ned på nsm.no/Risiko2023

Innhold


EVERGOOD KAFFE
Ring 2 Skøyen
Ring 3 Smestad
20 Skøyen
106

Hva sammensatte virkemidler faktisk betyr

Fjoråret viste på verst tenkelig måte at fred kan bli krise og krig. Samarbeid og styresett i Europa ble satt på stor prøve. Vi svarte med samhold og unison støtte til Ukraina. Men prøven er ennå ikke bestått. Den sikkerhetspolitiske situasjonen i Europa er varig endret. Norges geopolitiske situasjon er aktualisert.

Med krigen i Ukraina kom økt bekymring for sikkerheten i de europeiske landene. Det ble forventet bølger av cyberangrep mot Ukrainas støttespillere. Mens krigen foregår på bakken, og digitale hendelser stadig utfordrer Ukraina, er konsekvensene for resten av Europa mer sammensatt. Grunnleggende verdier og oppfatning av spillereglene i internasjonal politikk er stridens kjerne mellom Russland og Vesten. Også her har Norges rolle blitt viktigere. Vi er den største leverandøren av gass til Europa. Sverige og Finland er på vei inn i NATO, samtidig som vi som nærmeste nabo berøres av Russlands ambisjoner i nord.

Gjennom året har vi opplevd sabotasje av rørledninger som forsyner Europa med gass. Ulovlig droneflyging har fått stor oppmerksomhet. Norge ble rammet av et tjenestenektangrep som var egnet til å skape uro og usikkerhet i befolkningen. I mediene skrives det om personer med tilknytning til Russland som anklages for spionasje i Norge, og i andre europeiske land. Ønsket om å svekke tilliten til styresett og myndigheter i NATO-landene er tydelig. Det skapes uro i befolkningen, det spres falske nyheter, og prisene i Europa stiger over all forventning. Det er uforutsigbare tider, og det krever høyere beredskap.

Hvordan møter vi disse utfordringene? Vi må kjenne dem og de som truer oss og våre verdier. Vi må vite hvordan de påvirker oss, hvilke verktøy de bruker. Deretter må vi få oversikt over verdikjeder, og vurdere risikoen i virksomhetene våre. Vi må starte med tiltakene vi vet fungerer, som tetter hull der angriperne lett får fotfeste. Vi må ta inn over oss at vi har en ny sikkerhetspolitisk situasjon, som kan utvikle seg til det verre.

Vi i Norge har gode forutsetninger til å møte utfordringene som måtte komme hvis vi bruker tiden godt nå. Motstandskraft og robusthet bygges best i fredstid.

I Risiko 2023 fokuserer vi på risikobildet. Nasjonal sikkerhetsmyndighet skal gjøre landet i stand til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler.

Sofie Nystrøm
Direktør

Oppsummering

Vi står i en mer uforutsigbar sikkerhetspolitisk situasjon enn vi har gjort på mange år. Vi må forvente at dette vedvarer eller tilspisser seg. Vi må bygge beredskap på tvers av sektorer og vi må håndtere hendelser effektivt for å sikre oss mot ulike trusler i tiden fremover.

Trusselaktører bruker en rekke virkemidler for å fremme sine interesser på vår bekostning. Sabotasje mot Nord-Stream-ledningene i Østersjøen, høy kartleggingsaktivitet mot kritisk, norsk infrastruktur og flere tilfeller av alvorlig innsidevirksomhet er noen eksempler fra det siste året som belyser spennet av utfordringer vi står overfor. Flere virkemidler kan benyttes samtidig og koordinert mot utpekte mål i et bredt spekter av sektorer. Selv om en virksomhet har god fysisk og digital sikkerhet, så kan trusselaktører utnytte underleverandører som er langt dårligere sikret for å få tilgang til sine egentlige mål. Dette gjør at vi også må sikre oss godt på flankene.

Rikets sikkerhet avhenger også av private virksomheter og individer. Når disse opplever en svakere økonomi, risikerer vi at sikkerheten nedprioriteres samtidig som det oppstår sårbarheter som trusselaktører vet å utnytte. Vår avhengighet av leverandører som understøtter viktige samfunnsfunksjoner må vurderes i lys av den sikkerhetspolitiske utviklingen. Sikkerheten vår blir ikke bedre enn det svakeste leddet i leverandørkjeden.

Samtidig går den teknologiske utviklingen raskere og raskere. Dette bidrar til effektivisering og forenkler hverdagen vår. Parallelt utvikler den digitale sårbarhetsflaten seg, og dette er noe trusselaktører vet å utnytte. Hverken myndigheter, virksomheter eller enkeltindivider er skjermet for denne utviklingen.

Det er nå korte tidsrammer for å etablere og opprettholde akseptable sikkerhetsnivå i virksomheter og på nasjonalt nivå. Risikovurderinger og sikkerhetstiltak må endres oftere i takt med et stadig endret risikobilde. Dette må ikke gå på bekostning av våre demokratiske verdier. Vi må derfor sørge for at vi har et samfunn som er så åpent som mulig og samtidig så sikkert som nødvendig.

Å imøtegå dagens risikoer krever et omforent situasjonsbilde og effektivt samarbeid for at vi sammen kan verne om våre verdier og samfunnsfunksjoner. Vi må omstille oss raskt, og det stilles større krav til vår evne til å ivareta sikkerheten både nasjonalt, hos virksomheter og blant enkeltindivider.

Eksplosjonene på NordStream rørledningene høsten 2022 viser viktigheten av å beskytte kritisk infrastruktur.

Foto: Ritzau / NTB

Risikobildet

Det nasjonale risikobildet har sjeldent vært i så stor endring som i dag. Krigen i Ukraina, Kinas voksende ambisjoner og utvidelsen av NATO vil få stor betydning for nasjonal sikkerhet. Den hurtige teknologiske utviklingen og digitaliseringen av samfunnet byr på både muligheter og utfordringer. Trusselaktører benytter seg av stadig flere virkemidler for å oppnå sine mål samtidig som våre sårbarheter blir mer komplekse. Vi må oppdatere risikovurderinger og tiltak i takt med endringene i risikobildet. Denne uforutsigbarheten stiller store krav til samarbeid på tvers av virksomheter, sektorer og landegrenser.

Frem til invasjonen av Ukraina var Russland Europas største gassleverandør – nå er det Norge. Sabotasje mot Nord Stream-ledningene i Østersjøen og droneobservasjoner ved norske petroleums- og kraftinstallasjoner viser viktigheten av å beskytte infrastruktur som er kritisk for Norges grunnleggende nasjonale funksjoner. For å kunne beskytte våre viktigste verdier i krise eller krig må sikring mot potensielle trusler planlegges og gjennomføres i fredstid. Samtidig ser vi at gapet mellom trusselen mot oss og sikkerhetsnivået i samfunnet er økende. Dette må reduseres systematisk.

Viktigheten av de grunnleggende nasjonale funksjonene endrer seg kontinuerlig. Når konsekvensen av forstyrrelser i norsk olje- og gasseksport til Europa øker, må akseptabelt sikkerhetsnivå i sektoren etableres i lys av dette. I fjor ble Forsvaret satt inn for å sikre sivil infrastruktur. Kampfly og Sjøforsvarets fartøyer patruljerte og demonstrerte tilstedeværelse rundt olje- og gassinstallasjoner, mens HV-soldater bistod med vakthold på landanlegg. I dag er informasjon om forsvar og beredskap, norske våpenbidrag til Ukraina og ulike forhold knyttet til petroleumssektoren av stor verdi for trusselaktører som Russland. Da øker også beskyttelsesbehovet.

Krigen i Ukraina har vist oss at vi må være forberedt på et bredt spekter av trusler som i dag er vanskelig å forutse. Vi må derfor sikre kritiske samfunnsfunksjoner i flere sektorer mot et bredt spekter av trusler for å skape trygghet inn i en uforutsigbar fremtid.

Virksomheter, myndigheter og privatpersoner blir stadig utsatt for informasjonsinnhenting og påvirkningsoperasjoner fra fremmede etterretningstjenester. Det åpne samfunnet vi nyter godt av utnyttes av trusselaktører. De benytter en rekke virkemidler for å påvirke norske beslutningsprosesser og våre nasjonale sikkerhetsinteresser. Blant annet pekes det på at Russland utnytter eksisterende skillelinjer i samfunnet for å polarisere befolkningen. Disse virkemidlene kan brukes enkeltvis og i kombinasjon. Noen ganger er virkemidlene lovlige, andre ganger ulovlige. De kan være åpne eller fordekte. Dette bidrar til at det er vanskeligere å imøtegå eller avdekke sikkerhetstruende virksomhet.

DEL1

Felles motstandskraft i et komplekst risikobilde

Vi blir stadig utsatt for sammensatte trusler fra aktører som ønsker å utfordre Norges sikkerhet. Virkemidlene som benyttes kan være av mindre betydning isolert sett, men den totale summen utfordrer nasjonale sikkerhetsinteresser. Sammensatte trusler kan omfatte virkemidler som spredning av desinformasjon og cyberangrep, strategiske oppkjøp av norske virksomheter og kartlegging av kritisk infrastruktur. Det kan derfor være vanskelig å se hendelsene i sammenheng. Saker som i seg selv virker små, kan i en større helhet utgjøre en stor risiko.

Definisjon av sammensatte trusler

Sammensatte trusler er en betegnelse på strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt, som kan kombinere diplomatiske, informasjonsmessige, militære, økonomiske, finansielle, etterretnings-messige og juridiske virkemidler for å nå strategiske målsettinger.[1]

Sammensatte trusler kan forekomme i sikkerhetspolitiske gråsoner, der formålet er å skape splid og destabilisering. Virkemiddelbruken kan være bredt distribuert og kombinere åpne, fordekte og skjulte metoder. Virkemiddelbruken kan være rettet mot konkrete aktiviteter eller situasjoner, eller være innrettet mer langsiktig for å skape tvil, undergrave tillit og ved dette svekke våre demokratiske verdier.

Sammensatte trusler er i sin natur komplekse og utfordrer tidlig varsling, omforent situasjons-forståelse samt effektiv og samordnet håndtering.

Utviklingen i risikobildet krever mer samarbeid

For å gjøre Norge bedre i stand til å beskytte seg mot og håndtere sammensatte trusler har Regjeringen opprettet et Nasjonalt etterretnings- og sikkerhetssenter (NESS). I NESS skal Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og det øvrige politiet samarbeide for å styrke vår nasjonale evne til å oppdage og forstå sammensatte trusler og bred virkemiddelbruk – og våre egne sårbarheter – for å sikre god beslutningsstøtte til myndighetene.

1 Meld. St. 9 (2022–2023)

Foto: Forsvaret

Vi er sårbare på flankene

Viktige samfunnsfunksjoner er avhengige av leverandører og underleverandører. Disse kan ha potensielt ukjente og alvorlige sårbarheter. Vi er ikke sikrere enn det svakeste ledd. Dette krever at vi evner å oppdage og avverge sikkerhetstruende virksomhet også i leverandørkjedene vi er avhengige av. Virksomheter som er av avgjørende betydning for grunnleggende nasjonale funksjoner må ta hensyn til den tilspissede sikkerhetspolitiske situasjonen i sine oppdaterte risikovurderinger. Ikke minst må vi skaffe oss oversikt over virksomheters verdier og funksjoner som understøtter nasjonal sikkerhet. Dette er helt nødvendig for å kunne prioritere og ta i bruk riktige tiltak.

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

Utenfor det digitale rom ser vi også at trusselaktører utnytter leverandørkjeder for å oppnå tilgang til sine egentlige mål. Når målet er å ramme en stor virksomhet krever det mindre ressurser å angripe en mindre sikker underleverandør eller enkeltpersoner. Vi ser også at trusselaktører forsøker å skaffe seg tilgang til sensitiv informasjon gjennom tilsynelatende legitime oppkjøp og investeringer i norske selskaper. Med andre ord er det ofte langs flankene eller ytterkantene vi er mest sårbare og nettopp der vi kan være mest utsatt for sikkerhetstruende virksomhet.

Kinesisk dominans på verdensmarkedet innenfor enkelte teknologiområder utgjør også en økende utfordring for sikkerheten her hjemme i Norge. De omfattende sanksjonene mot russiske virksomheter har også påvirket norske virksomheters leverandørkjeder. Raske bytter av leverandører og underleverandører kan medføre at det ikke blir foretatt tilstrekkelige risikovurderinger før avtaler med nye leverandører blir inngått. Samtidig har sanksjonene mot Russland belyst utfordringene ved å ha for store avhengigheter til leverandører i land som Norge ikke har sikkerhetssamarbeid med. Etter å ha kartlagt verdier og avhengigheter til leverandørkjeder må vi derfor ta hensyn til at disse kan bli forsøkt utnyttet fra flere hold ved hjelp av en rekke ulike virkemidler.

Leverandøravhengighet til Kina er en sårbarhet som kan utnyttes av kinesiske myndigheter. Omfattende tilstedeværelse fra andre stater i leverandørkjedene til flere av våre viktigste verdier kan utgjøre en risiko for nasjonal sikkerhet.

Det siste året har vi sett en markant økning i antall sikkerhetstruende hendelser. Hendelsene rammer et bredt spekter av virksomheter i forsvarssektoren og i det sivile. For at Norge skal bli bedre til å forebygge trusselaktørers bruk av sammensatte virkemidler, er det nødvendig å øke rapporteringen av hendelser. Dette vil bidra til bedre situasjonsforståelse. Derfor er det viktig å ha et system og rutiner for registrering og håndtering av sikkerhetstruende hendelser. Det bidrar til læring og systematisk prioritering av sikkerhetstiltak.

Grunnleggende nasjonale funksjoner

Grunnleggende nasjonale funksjoner er 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.

Leverandørkjeder

En leverandørkjede omfatter alle ledd i kjeden av leverandører og underleverandører som leverer eller produserer varer, tjenester eller andre innsatsfaktorer som inngår i en virksomhets leveranse av tjenester eller produksjon av varer fra råvarestadiet til ferdig produkt.

Fordekte investeringer og oppkjøp truer nasjonal sikkerhet

NSM er et nasjonalt fagmiljø for motvirkning av sikkerhetstruende økonomisk virksomhet, og har i løpet av året behandlet flere saker knyttet til mulig økonomisk virkemiddelbruk. En stor overvekt av sakene omhandlet leverandørproblematikk, og i mange av sakene kommer leverandøren fra Kina eller har en tilknytning til Kina. Men også Russland og andre stater utgjør en risiko på dette feltet.

Flere stater investerer i og kjøper opp norske virksomheter for å blant annet få innsikt i sensitiv informasjon og teknologi av strategisk betydning. Oppkjøp av norske virksomheter og strategisk plassert eiendom kan derfor være en trussel mot vår nasjonale sikkerhet. Slike økonomiske virkemidler kan benyttes også i kombinasjon med ikke-økonomiske virkemidler som cyber- og påvirkningsoperasjoner. Nasjonalt eierskap og kontroll er et av flere virkemidler som brukes i Norge for å motvirke uønsket oppkjøp som kan gå på bekostning av nasjonale sikkerhetsinteresser.

I dagens sikkerhetspolitiske klima og med de omfattende sanksjonene mot Russland øker risikoen for økonomisk virkemiddelbruk mot Norge. Norske virksomheter som forvalter viktige verdier eller har strategisk plassert eiendom bør være oppmerksomme på fordekte investeringer og oppkjøp fra andre land Norge ikke har et sikkerhetssamarbeid med. Slike økonomiske transaksjoner kan skje gjennom stråselskaper og komplekse selskapsstrukturer og kan dermed være vanskelig å avdekke. Ekstra bevissthet og årvåkenhet rundt problematikken er derfor nødvendig.

Kinesisk økonomisk virkemiddelbruk

Under arbeidet med å bygge en reservevannforsyning til Oslo kommune, avdekket Vann- og avløpsetaten (VAV) at tilbyder i hovedanbudsrunden var et kinesisk firma i et fellesforetak sammen med et spansk firma. Det kinesiske selskapet er kjent for å ha koblinger til kinesiske myndigheter og det kinesiske forsvaret.
Som følge av koblingen til Kina er det risiko for at kinesisk etterretning kan få tilgang til og informasjon om norsk kritisk infrastruktur. NSM bistod Oslo VAV med rådgivning og veiledning om hvordan å beskytte viktige verdier. Dette medførte at den kinesiske leverandøren ikke ble valgt i anbudsrunden.

Vi må sikre nødvendig nasjonalt eierskap og kontroll over kritiske samfunnsfunksjoner.

Foto: Johner Images / NTB

Utnyttelse av cybersårbarheter lar ikke vente på seg

I Norge har vi fra 2019 til 2021 sett en tredobling i alvorlige cyberoperasjoner mot norske myndigheter og virksomheter. Antallet alvorlige og svært alvorlige hendelser har i 2022 holdt seg på et tilsvarende nivå som i 2021. De vanligste angrepene var distribuerte tjenestenektangrep, phishing og kartleggingsaktivitet. Vedvarende phishing- og kartleggingsaktivitet mot norske aktører understreker at disse er attraktive mål, og det er viktig å være bevisst på at kartlegging kan peke frem mot framtidige cyberangrep.

Blant forsøkene på kompromitteringer mot norske mål i 2022 var andelen vellykkede lavere enn i 2021. Det vil også være aktivitet i cyberdomenet som ikke avdekkes, og det er derfor viktig å understreke at fravær av bevis på aktivitet ikke er det samme som bevis på fravær. Flere virksomheter har sikkerhetsarbeidet høyt på agendaen, og har blant annet økt innrapportering om mulige sikkerhetstruende hendelser og iverksetting av sikkerhetstiltak. Dette er en positiv utvikling, men det er fortsatt et gap mellom ønsket sikkerhetsnivå og status i mange virksomheter.

NSM har stadig sett utnyttelse av menneskelige, teknologiske og organisatoriske sårbarheter for å understøtte ondsinnede cyberoperasjoner mot flere norske virksomheter. Samtidig har forsøk på å skaffe seg tilgang til virksomheters datasystemer i hovedsak blitt gjort ved velutprøvde metoder og varianter av sosial manipulasjon, for eksempel phishing-eposter, og automatiserte påloggingsforsøk.

I mai 2022 ble det kjent at en kopi av Norges offisielle eiendomsregister hos karttjenesten Norkart – som henter data fra Statens kartverk – var lekket til en ukjent trusselaktør. Persondata om 3,3 millioner nordmenn hvor navn, adresser, fødselsnummer og informasjon om hva man eier er på avveie.

Persondata om 3,3 millioner nordmenn på avveie

I mai 2022 ble det kjent at en kopi av Norges offisielle eiendomsregister hos karttjenesten Norkart – som henter data fra Statens kartverk – var lekket til en ukjent trusselaktør. Persondata om 3,3 millioner nordmenn hvor navn, adresser, fødselsnummer og informasjon om hva man eier er på avveie. Dersom denne type datasett blir satt i sammenheng med annen tilgjengelig informasjon er det særlig bekymringsfullt.

I 2021 og 2022 førte nulldagssårbarheter i eksempelvis Microsoft Exchange, Atlassian Confluence og Apache Log4j til cyberoperasjoner mot en rekke norske virksomheter, også virksomheter med kritiske funksjoner. Selv om disse og andre sårbarheter er godt kjent, så er det fortsatt mange norske virksomheter som ennå ikke har oppdatert systemene sine og tettet kjente sårbarheter. Utnyttelse av programvaresårbarheter har vært årsaken til en stor del av aktiviteten vi har registrert de siste årene. Man kan i tillegg se en antydning til raskere sårbarhetsutnyttelse, altså at tiden fra en sårbarhet blir kjent til den utnyttes er redusert. Dette viser viktigheten av en bevisst sikkerhetskultur hos både ledere og ansatte i virksomhetene. NSM anser sikkerhetsoppdateringer av programvare som ett av de viktigste sikkerhetstiltakene innenfor cybersikkerhet.

Samtidig er det viktig å være bevisst på at trusselaktørene ikke alltid går direkte på virksomhetenes nettverk. I likhet med andre sikkerhetsområder ser vi at trusselaktørene angriper langs flankene i stedet for å gå direkte på sine egentlige mål. Enkeltpersoner og tredjepartstjenester som virksomhetene er avhengige av, blir utnyttet fordi de blir ansett som enklere mål enn de egentlige målene. Microsoft kan melde at de i løpet av de tre siste årene har sendt ut 20 500 varsler om statlige angrep til sine kunder, hvor 58 prosent var utført fra Russland. Én av fem av disse angrepene var rettet mot oss som forbrukere, og vi ser at avsenderne blir mer og mer treffsikre.

Tar vi ikke inn over oss de økte verdiene og komplekse sårbarhetene i cyberdomenet, øker risikoen for at Kina, Russland og andre trusselaktører skaffer seg tilganger til systemer tilknyttet grunnleggende nasjonale funksjoner uten at vi er klar over det.

Nulldagssårbarhet

En nulldagssårbarhet er en sårbarhet programvareutvikleren ikke har oppdaget eller laget sikkerhetsoppdatering for. Navnet kommer av at når en nulldagssårbarhet først er oppdaget, har programvareutvikleren hatt null dager på seg til å lukke sårbarheten før noen potensielt utnytter den.

Norge utsatt for tjenestenektangrep

Morgenen 29. juni 2022 ble NSM kontaktet av flere virksomheter som opplevde driftsforstyrrelser på nettsidene sine. Årsaken viste seg å være et stort koordinert tjenestenektangrep.

Parallelt med dette sirkulerte meldinger på plattformen Telegram om at flere norske virksomheter var utpekt som mål for tjenestenektangrep fra en kriminell hacktivist-gruppe kjent som Killnet. Gruppen begrunnet angrepet med at «norske myndigheter har avslått Russlands søknad om passasje av varer til russiske bosettinger på Svalbard gjennom det eneste sjekkpunktet på den russisk-norske grensen ved Storskog».

Den påfølgende uken opplevde et stort antall norske virksomheter nedetid på sine nettsider. Senere så vi at Killnet kom tilbake og forsøkte samme angrepsmetode mot forsvarssektoren. Nedetid på nettsider kan være alvorlig dersom det bidrar til å spre mistillit om myndigheters evne til å beskytte befolkningen mot cyberangrep.

Hva er tjenestenektangrep?

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

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

Hjemmekontorløsninger flytter virksomhetenes verdier hjem til folk

Hjemmekontor under covid-19-pandemien muliggjorde fortsatt drift for mange virksomheter til tross for samfunnets nedstengning. Selv om mange etter hvert har vendt tilbake til virksomhetens fysiske lokaler, er hjemmekontorløsninger kommet for å bli – og mange vil tidvis fortsatt benytte seg av muligheten til «å koble seg på» hjemmefra.

Ansattes tilganger til virksomhetens systemer fra hjemmekontoret, eller fra hvor som helst i verden, har samtidig medført at virksomhetene ikke lenger har kontroll på de fysiske og digitale forutsetningene som omgir virksomhetens verdier. Dette gir økt risiko for uautorisert tilgang til verdiene, eksempelvis gjennom bruk av sårbart privat utstyr, gjennom mangelfull sikring av utstyr eller gjennom tilsiktet eller utilsiktet innsideaktivitet. Dette er utfordringer virksomhetene bør ha en bevissthet rundt det kommende året.

Sårbarheten i proprietær programvare

Proprietær programvare, også kalt produsenteid programvare, er programvare hvor brukeren ikke har lov til å undersøke eller endre kildekoden til programvaren. Altså er programvaren hemmelig. I motsetning til programvarer med åpen kildekode, hvor alle selv kan endre denne.

Sårbarheter i proprietære programvarer blir i mindre grad identifisert av brukerne selv, ettersom de ikke har tilgang til kildekoden. Derfor er det desto viktigere at leverandøren selv kontinuerlig jobber med å avdekke sårbarheter. Programvarer med få oppdateringer kan tilsi at det er få som jobber med sikkerheten forbundet med programvaren.

Tilliten i samfunnet utfordres

Bruken av virkemidler som truer nasjonale sikkerhetsinteresser utspiller seg også på sosiale medier. Sosiale medier er en gunstig arena for trusselaktører og andre som ønsker å påvirke oss gjennom desinformasjon og falske nyheter. Algoritmene til sosiale medier forsterker spredningen av innhold som skaper mest engasjement. De skreddersyr innhold som de vet brukeren agerer mest på og sørger for at man får opp lignende innhold. De som trigges av det samme, får opp samme innhold og det skapes såkalte ekkokamre som kan bidra til økt polarisering.

Spredning av desinformasjon og målrettede cyber- og påvirkningsoperasjoner kan ha innvirkning på tilliten som kreves for å opprettholde det politiske systemet vårt. Formålet med desinformasjonen er ikke nødvendigvis å overbevise mottakerne om noe, men på sikt å svekke den politiske stabiliteten. Det samme kan gjelde andre former for sikkerhetstruende virksomhet, som for eksempel tjenestenektangrep. Slike cyberangrep får begrensede konsekvenser på kort sikt, men kan i et langsiktig perspektiv svekke befolkningens tillit til statlige institusjoner og myndigheter.

Tiltak for å beskytte dine verdier

1. **Følg NSMs grunnprinsipper for IKT-sikkerhet, fysisk sikkerhet, personellsikkerhet og sikkerhetsstyring.** Disse gir et godt utgangspunkt for hvordan virksomheter kan beskytte verdiene sine.
2. **Gjennomfør regelmessige øvelser og testing av sikringstiltak for å kontrollere at de fungerer etter hensikten.** Virksomheter bør også dokumentere sikkerhetsarbeidet for å sikre evaluerings- og utviklingsmuligheter.
3. **Kartlegg hvilke verdier som leverandører og underleverandører får tilgang til.** Virksomheter som er omfattet av sikkerhetsloven forutsettes å gjøre det samme for verdier av betydning for nasjonal sikkerhet.
4. **Gjennomfør risikovurderinger ved anskaffelser av varer og tjenester.** Unngå en konsentrasjon av leveranser fra samme leverandør og samme land, særlig hvis det er et land Norge ikke har et sikkerhetssamarbeid med.

Fem effektive tiltak mot cyberangrep

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

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

FORTSATT GJELDENDE

DEL 2

Enkeltindividets viktighet

Enorme mengder med personlig informasjon samles på nett, samtidig som fremmede etterretningstjenester forsøker å rekruttere innsidere. Dette er en stor sikkerhetsutfordring i utsatte sektorer, og bidrar til økt risiko for at individer utnyttes som en sårbarhet. Utenlandske etterretningstjenester leter systematisk etter personer som kan utnyttes eller er villige til å gi dem tilgang til de verdiene de jakter på.

Innsidevirksomhet

I løpet av 2022 har media omtalt en rekke saker om mulig innsidevirksomhet. I Sverige ble et brødrepar som jobbet i de svenske sikkerhetstjenestene dømt for grov spionasje. En ansatt i den tyske etterretningstjenesten er siktet for å ha delt svært sensitive og hemmelige opplysninger om vestlige etterretningsoperasjoner i forbindelse med Russlands krigføring i Ukraina. Også i Norge har innsidere blitt avdekket. Samtlige av disse har til felles at de er siktet eller tiltalt for å ha jobbet på vegne av Russland. Etterretningstjenesten og PST peker på at trusselaktørene er svært interessert i flere forskningsområder ved norske universiteter, og at disse institusjonene utnyttes for å kartlegge potensielle kilder.

Den bakenforliggende intensjonen og motivasjonen for at en person velger å bli en innsider er sammensatt og kompleks. Felles er at det er tilstedeværelse av en eller flere menneskelige sårbarheter. Noen eksempler på motivasjon er ideologisk overbevisning, lojalitetskonflikt, økonomiske insentiver og forhold på arbeidsplassen. Sårbarhetene til en potensiell innsider kan også utnyttes i form av utpressing fra en trusselaktør. I tillegg kan lav eller manglende sikkerhetsmessig bevissthet øke risikoen for at personer kompromitterer sensitiv informasjon og blir ubevisste innsidere.

Man må ikke nødvendigvis ha tilgang til sikkerhetsgradert informasjon eller sitte i en sentral toppstilling for å være et verdifullt mål for fremmede etterretningstjenester. Ikke alle er seg bevisst hvilken betydning informasjonen de besitter kan ha for nasjonal sikkerhet. Ettersom Norges samarbeid med Russland har opphørt innenfor en rekke områder, vurderer PST at norske borgere og virksomheter i tiden fremover vil være mer utsatt for tilnærmingsforsøk fra russisk etterretning. I tillegg opplever flere å stå i en vanskelig økonomisk situasjon med dyrere utgifter på lån, mat og strøm, som kan gjøre enkelte ansatte mer utsatte for innsidevirksomhet.

Innsidevirksomhet kan oppstå gjennom hele ansettelsesperioden. Det er derfor viktig at virksomheter følger opp sitt personell gjennom hele ansettelsesforholdet, slik at motiver for innsidevirksomhet eller andre omstendigheter som kan benyttes som pressmiddel, kan avdekkes og håndteres fortløpende.

Hva er en innsider?

En innsider forstås som en nåværende eller tidligere ansatt, konsulent eller innleid som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap.

Innsideren kjenner virksomhetens rutiner, prosesser og sårbarheter, og kan benytte kunnskapen for å skade virksomheten til fordel for annen virksomhet, stat, eller til egen vinning. Innsideaktivitet kan gjennomføres direkte og på egenhånd, eller på vegne av en ekstern aktør. Eksterne aktører kan være statlige, ikke-statlig eller andre enkeltindivider. Disse aktørene kan søke å utnytte personer med tilgang til en virksomhets eller stats verdier for å oppnå egne mål.

Kommersiell digital sporing utfordrer nasjonal sikkerhet

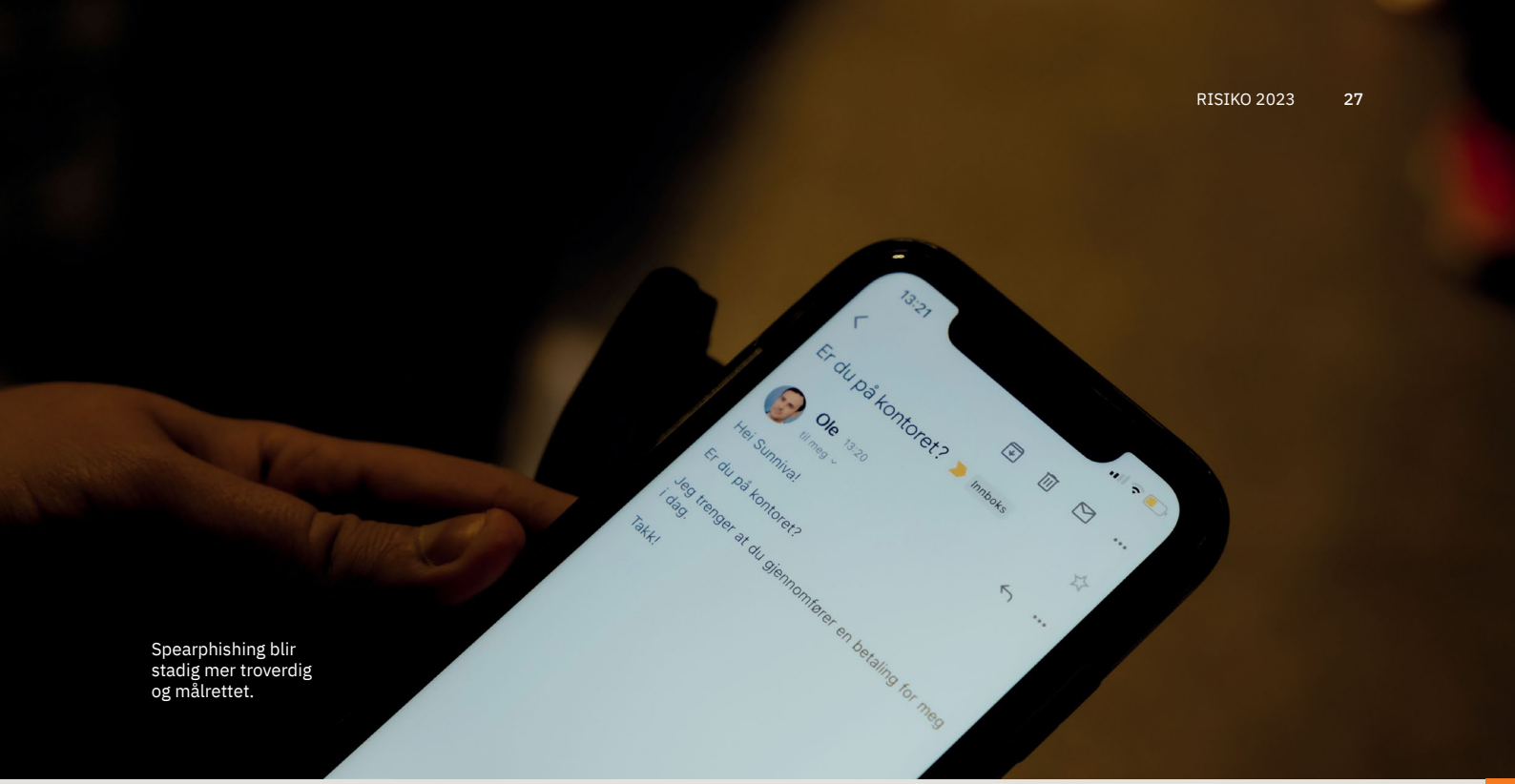
Det anslås at det i år vil være 29,3 milliarder enheter koblet til internett. I 2018 var tallet 18,4 milliarder. Sammen med utviklingen av skytjenester og smartløsninger fører dette til at vi legger igjen enorme mengder digitale spor som lagres og selges videre i et globalt marked. Brukerdata sier mye om hvem vi er og hva vi er interessert i og har derfor stor verdi for kommersielle aktører som ønsker å gi oss målrettet og skreddersydd reklame. Dette er ikke bare en personvernutfordring, men også en utfordring for nasjonal sikkerhet.

Fremmede etterretningstjenester kan benytte det store volumet av kommersielt tilgjengelige brukerdata for å manipulere og utpresse personer som sitter på verdifull informasjon. Brukerdata kan understøtte cyberoperasjoner, innsidevirksomhet, påvirkningsoperasjoner og spearphising. Når brukerdata sammenstilles med informasjon som arbeidsgiver eller enkeltpersoner deler offentlig, kan det danne et svært omfattende og detaljert bilde av enkeltpersoners identitet og handlemønster. Denne formen for informasjonsinnhenting blir sjelden avslørt, har lav risiko for aktøren, og muliggjør skreddersydde og svært troverdige tilnærmingsforsøk eller cyberoperasjoner. NSM har den siste tiden sett flere cyberangrep hvor enkeltpersoner blir kontaktet av tilsynelatende troverdige personer på sosiale medier, og dermed lurt til å trykke på linker eller vedlegg som har gitt trusselaktørene tilgang til virksomhetenes systemer.

Informasjon om ansatte på en virksomhets nettside kan også skape sikkerhetsutfordringer. For kunder og samarbeidspartnere er det nyttig å vite hvem man kan kontakte av ansatte og hvordan. Utfordringen er at denne informasjonen også kan brukes til målrettede phishing-forsøk og personlige tilnærmingsforsøk, og inngå som del av større kartleggingsaktivitet. Virksomheter må gjøre en bevisst vurdering rundt hvor mye informasjon om ansatte som deles offentlig, samtidig som ansatte oppfordres til å tenke over hva de deler på sosiale medier.

Hva er spearphishing?

Spearphishing er som regel e-poster som er målrettet utformet for å lure mottakeren. E-postens innhold og utforming fremstår som relevant og legitim for mottakeren. Eksempler på dette er nyhetsbrev fra kjente avsendere eller innkallinger til møter og konferanser med vedlegg. Lenkene eller vedleggene inneholder ondsinnet kode som aktiveres om mottaker klikker på eller åpner vedlegget.



Spearphishing blir stadig mer troverdig og målrettet.

Norsk forsker utsatt for spearphishing

En forsker ved et norsk forskningsinstitutt ble kontaktet av en aktør som utga seg for å være vestlig journalist med sammenfallende fagfelt som forskeren. Journalisten bygget tillit og relasjon gjennom overbevisende dialog og utveksling av fagartikler. Via en tilsynelatende legitim lenke ble forskeren ledet til en spearphishing-side som hadde til hensikt å gi journalisten urettmessig tilgang til forskningsinstitusjonens nettverk og servere. Det viste seg at journalisten jobbet under falskt dekke for en fremmed etterretningstjeneste. Spearphishing-forsøket ble muliggjort av offentlig tilgjengelig informasjon som den fremmede etterretningstjenesten brukte til kartlegging, målutvelgelse og gjennomføring av angrepet.

Tilganger og deling av brukerdata

I forbindelse med klimatoppmøtet COP27 høsten 2022 utviklet egyptiske myndigheter en egen app for deltakerne på konferansen. I tillegg til nasjonale delegasjoner, deltok blant andre ikke-statlige organisasjoner og klimaaktivister.

Utover å skulle registrere fullt navn og passnummer, krevdes det også at man samtykket til å dele høyoppløselige posisjonsdata. Appen fikk også tilgang til telefonens bildebibliotek og kontaktlister og den kunne potensielt brukes til å aktivere opptak av lyd og video.

NSM anbefalte derfor å ikke installere appen på en telefon som er koblet til virksomhetens informasjonssystemer eller personlig e-post eller sosiale medier. COP27-appen er imidlertid godkjent av både Apple og Android, noe som kan gi en falsk trygghet i produktet. Andre apper kan ha tilsvarende tilganger til data på telefoner og nettbrett og kan selge dataen videre til både kommersielle og statlige aktører. Man trenger ikke nødvendigvis bli utsatt for et cyberangrep for at svært personlige og sensitive data kan komme på avveie.

Risikoreduserende tiltak mot innsidevirksomhet

1. **Skap et helhetlig system for å styrke personellsikkerheten.** Dette innebærer å vurdere den menneskelige faktoren i alle deler av sikkerhetsarbeidet og innarbeide mulige konsekvenser av innsidevirksomhet i virksomhetens risikovurdering.
2. **Ivareta personellsikkerheten før, under og etter ansettelse.** Dette innebærer å sikre at risikoreduserende tiltak iverksettes i alle ledd av ansettelsesforholdet, herunder bruk av bakgrunnssjekk.
3. **Sørg for at virksomheten har tilstrekkelig sikkerhetskompetanse og -ressurser.** Dette er nødvendig for å kunne beskytte virksomhetens verdier mot innsidevirksomhet, men også for at virksomheten skal settes i stand til å følge opp sårbarheter som oppstår hos ansatte.
4. **Legg til rette for god sikkerhetskultur.** Dette innebærer å gjøre personellsikkerhet til en naturlig del av virksomheten, øke forståelse av sikkerhetsregler og rutiner samt tilrettelegge for oppfølging av ansatte for å avdekke misnøye eller andre forhold.
5. **Håndtér hendelser, evaluér tiltak og lær av erfaringene.** Ved sikkerhetsbrudd bør virksomheten identifisere hvilken rolle personen på innsiden har hatt, og virksomheten bør arbeide systematisk for å lære av erfaringer og bruke lærdommen til å styrke arbeidet med å forebygge, avdekke og motvirke innsidevirksomhet.

Tiltak mot digital sporing

1. **Lag interne retningslinjer for nettaktivitet i virksomheten.** Det bør blant annet inkludere en beskrivelse av hvor mye informasjon man deler om sine ansatte og om virksomheten på internett.
2. **Skru av Wi-Fi, roaming, bluetooth, og posisjonstjenester når de ikke brukes**
3. **Unngå bruk av åpne Wi-Fi-nettverk**
4. **Gi apper minimal tilgang til mikrofon, kamera og lokasjonsdata.** Det kan avsløre hvor du arbeider, hvor du bor og hvilke lokasjoner du besøker, selv om du ikke bruker navigasjonsapp.
5. **Bruk sporingsfrie nettleser-alternativer, og/eller slett informasjonskapsler (cookies) i nettleseren jevnlig**
6. **Benytt en VPN-løsning operert av egen virksomhet eller en annen aktør du aksepterer at ser dine data.** VPN betyr virtuelt privat nettverk og krypterer trafikken du sender og mottar via din VPN-leverandør.

DEL3

Teknologisk utvikling og sikkerhet

Stadig flere ting rundt oss blir koblet til internett. Kunstig intelligens begynner å gjøre sitt inntog, og avanserte kvantedatamaskiner er under utvikling. Samfunnsviktige tjenester blir mer og mer avhengige av skyløsninger og satellittbaserte tjenester. Rask teknologiutvikling gir et hav av nye muligheter for å effektivisere og automatisere samfunnet. Samtidig øker sjansen for at ny teknologi utnyttes av aktører som er ute etter å ramme oss. Derfor må vi, allerede nå, tilrettelegge for at fremtidens teknologi gagner både samfunnet og nasjonale sikkerhetsinteresser.

5G og skytjenester øker kapasitet og redundans

Innføringen av 5G innebærer nye muligheter, blant annet når det kommer til mobile distribuerte skyløsninger. I dag er det flere sårbarheter knyttet til den samlede nasjonale avhengigheten til utenlandske skyleverandører og til store, sentraliserte datasentre som huser mange viktige verdier. Ved å bygge ut distribuerte, små datasentre vil man oppnå pålitelig tilgang til lokal datakraft og mobiltelefoni og øke robusthet og autonomi i fred, krise og krig. Det vil være spesielt viktig for virksomheter med en rolle i totalforsvaret eller som understøtter andre viktige samfunnsfunksjoner.

Mobilt 5G-nett for soldater

Forsvaret jobber med prosjekter hvor mobile 5G-basestasjoner er en viktig del av kommunikasjonen under militære operasjoner. Egne mobile basestasjoner gjør det mulig å etablere nett for eksempelvis Heimevernets innsatsstyrke og andre totalforsvarsaktører om lokale basestasjoner er slått ut. FFI forsker på hvordan mobile basestasjoner kan benyttes under naturkatastrofer, som store ras (slik som skjedde i Gjerdrum desember 2020).

Konseptvalgutredning av nasjonal skytjeneste

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

I januar 2023 ga NSM innspill til en konseptvalgutredning (KVU) for etablering av nasjonal skytjeneste etter oppdrag fra Justis- og beredskapsdepartementet (JD). Her utredes blant annet hvorvidt staten bør ta eierskap i digital infrastruktur, plattformer, plattformutvikling og standardutvikling.

President Joe Biden inspiserer en kvantedatamaskin hos IBM i New York.

Foto: Eirin Schaff / NYT / NTB

Norge må henge med i kvantekappløpet

Norske virksomheter som er avhengige av digital sikkerhet, kan bli rammet av flere problemstillinger rundt regnekrafts- og kvanteutviklingen. Stadig økende regnekraft reduserer sikkerhetsnivået i dagens kryptoalgoritmer. Utviklingen av kvantedatamaskiner vil utfordre sikkerheten kryptoalgoritmene representerer. Dette kan bety en framtid hvor kvantedatamaskiner gjør mesteparten av dagens krypteringer ubrukelig.

Kvantedatamaskin

En kvantedatamaskin er en maskin som utfører logiske operasjoner basert på kvantemekaniske prosesser. Ved å benytte seg av kvantebits istedenfor bits, vil bestemte typer problemer (slik som faktorisering av store tall) kunne løses mye raskere enn med vanlige datamaskiner.

Det finnes i dag kryptografi som antas kvanteresistent og som er i ferd med å bli standardisert til offentlig bruk. For de aller fleste vil innfasing av kvanteteknologi medføre få sikkerhetsutfordringer. Leverandører som eksempelvis Google og Microsoft tar del i standardarbeidet og vil ta høyde for utviklingen der hvor det er nødvendig i sine tjenester, selv om dette kan ta tid å gjennomføre. Samtidig finnes det mange virksomheter som har spesialutviklede løsninger hvor det ikke er tatt høyde for integrasjon av nye algoritmer. Det vil derfor være viktig å få rede på hvordan sikkerheten kan ivaretas i slike løsninger. For fremtidige anskaffelser vil det være viktig å sikre at man har dekket behovet for kvanteresistente algoritmer.

Kunstig intelligens-fenomenet ChatGPT gikk som en farsott denne vinteren.

Kunstig intelligens skaper unike muligheter og utfordringer

I løpet av det siste året har flere for første gang blitt introdusert for maskinlæring som på egenhånd produserer unike bilder, skriver tekster eller koder basert på brukerens behov. Mye tyder på at utvikling innen kunstig intelligens og maskinlæring vil bidra sterkt med å effektivisere og skape nye muligheter for både virksomheter og myndighetsorgan i tiden som kommer. Kinesiske aktører både i sivil og militær sektor ligger langt framme i utviklingen av brytningsteknologi som kunstig intelligens, robotikk og autonome systemer.

Innenfor kunstig intelligens er mye fortsatt nytt og ukjent. Potensialet i teknologien er enormt, både for hvordan vi selv tar den i bruk og for hvordan trusselaktører kan utnytte den for å ramme oss. Kunstig intelligens kan styrke den defensive evnen ved å trenes til å oppdage, varsle om og håndtere cybertrusler. Samtidig kan man se for seg at kunstig intelligens eksempelvis kan trenes for å lage og distribuere skadevare som stadig endrer seg for å unngå å bli oppdaget av virksomhetenes sikkerhetsmekanismer. Som ledd i en påvirkningsoperasjon kan kunstig intelligens brukes til å sammenstille og tolke store mengder informasjon på svært kort tid, og produsere svært gode tekster uten at innholdet nødvendigvis er til å stole på. Dette kan i nær fremtid gjøre det enda mer utfordrende for enkeltpersoner, virksomheter og myndighetsorgan å skille mellom hva som er og ikke er troverdige kilder til informasjon.

Brytningsteknologi

Brytningsteknologi (av eng: «disruptive technology») er en banebrytende teknologi eller produkt som vesentlig endrer måten forbrukere, bransjer eller bedrifter opererer på.

Kunstig intelligens

Kunstig intelligens handler om datamaskiners evne til å utføre «handlinger, fysisk eller digitalt, basert på tolkning og behandling av strukturerte eller ustrukturerte data, i den hensikt å oppnå et gitt mål. Enkelte systemer for kunstig intelligens kan også tilpasses gjennom analyser og vurderinger av hvordan tidligere handlinger har påvirket omgivelsene»[2].

2 EUs ekspertgruppes definisjon for kunstig intelligens

Satellittbaserte tjenester må sikres

Satellittbaserte tjenester står sentralt i teknologiutviklingen og gir kostnadseffektive løsninger for blant annet overvåkning, navigasjon, kommunikasjon og myndighetsutøvelse. I et krise-krig-perspektiv vil tilsiktede handlinger mot satellittbaserte systemer få stor betydning for samfunnets funksjonsevne og totalforsvarets operative evne. Infrastruktur for rom, både den i rommet og den på bakken, er sårbar for sikkerhetstruende virksomhet[3]. Vi har flere ganger vært vitne til frekvensforstyrrelser av globale satellittbaserte navigasjonssystemer (GNSS) i Troms og Finnmark de senere årene. Etterretningstjenesten rapporterer at trusselaktørene satser betydelige ressurser på teknologi som antisatellittvåpen og evne til tjenestenektelse.

Antall satellitter i bane forventes å bli mangedoblet i løpet av få år, og skillet mellom sivile og militære satellitter blir stadig mindre tydelig. Flerbruksmulighetene kan gjøre det vanskelig for andre å se hva som er det fulle formålet med en satellitt.

Lavbanesatellitter

De siste årene har vi vært vitne til en viktig utvikling innen kommunikasjonssatellitter i lav jordbane (low earth orbit). Et eksempel på dette har vært bruk av den sivile satellitt-tjenesten Starlink i Ukraina. Den har bidratt til at både befolkningen, militære og politiske beslutningstakere i Ukraina kunne kommunisere med omverden under stadige russiske angrep. Systemene kan bidra til bedre og mer redundant kommunikasjon både i konfliktområder og områder med lite utbygd infrastruktur.

3 Eksempler på denne typen destruktive handlinger være fysisk ødeleggelse, cyberangrep, støysending (jamming), narring (spoofing), innsidetrussel og sammensatte virkemiddelbruk.

Mer enn 1000 raketter har blitt skutt opp fra Andøya siden åpningen i 1962.

Foto: NASA Earth Observatory / Wikimedia Commons

For virksomheter og myndighetsorgan som er avhengig av satellittbaserte tjenester, vil det å identifisere nye måter å skape redundans i satellittbasert kommunikasjon og andre tjenester stå sentralt i arbeidet om å redusere risikoene på dette området i tiden fremover. Store avhengigheter til gammel teknologi, samt rask innføring av ny teknologi utgjør en stor risiko for at nye sårbarheter og verdier knyttet til nasjonal sikkerhet ikke blir avdekket i tide. For å sikre nasjonal egenevne og kontroll bør myndighetene stimulere til rombaserte tjenester og kapabiliteter som både ivaretar nasjonale sikkerhetsinteresser og tilrettelegger for næringsvirksomhet.

Oppsummerende tiltak for god anvendelse av ny teknologi

1. **Sett deg inn risikoen som er forbundet med tjenesteutsetting eller å ta i bruk ny teknologi i virksomheten.** Økt kunnskap om verdier og sårbarheter i teknologien gjør at man kan iverksette gode risikoreduserende tiltak.
2. **Virksomheter hvor dette er relevant bør planlegge for kvanteresistente algoritmer i sine systemer og leverandørkjeder slik at dette behovet dekkes i tide.** Samtidig anbefales virksomheter å oppdatere eldre typer krypteringsalgoritmer til dagens standarder.
3. **Jevnlig kvalitetssikre modeller for kunstig intelligens man bruker i virksomheten for å sikre seg mot manipulasjon av modeller og data.** Det er særlig viktig å forstå risikoen som er forbundet med bruk av disse modellene som har tilgang til eller bygges på sensitiv informasjon.
4. **Virksomheter som er avhengig av satellittbaserte tjenester bør vurdere behovet for reserveløsninger, inkludert rutiner og alternative prosedyrer for å sikre seg redundans.** Dette vil særlig gjelde for samfunnsfunksjoner som er avhengige av presis navigasjon, posisjonering og tid. Både virksomheter og myndigheter må vurdere mulige løsninger. Sektormyndigheter og departementer bør følge opp at dette skjer.

DEL 4

Så åpent som mulig, så sikkert som nødvendig

Det å finne balansegangen mellom åpenhet i samfunnet og internasjonalt samarbeid på den ene siden, og nasjonale sikkerhetshensyn på den andre siden er utfordrende. Særlig når den sikkerhetspolitiske situasjonen tilspisser seg. Både innenfor forskning og andre samfunnsområder kreves det en fortløpende kvalifisert vurdering for å dra linjen mellom ønsket om åpenhet og behovet for sikkerhet. Nivået for akseptabel risiko kan være vanskelig å stadfeste, og i stadig endring.

Gjennom enkle googlesøk er det mulig å finne mye informasjon om kritisk infrastruktur i Norge. Ulike åpne kilder kan til sammen danne et bilde som vil være svært nyttig for kartleggingsaktiviteten til en trusselaktør.

Det har vært rettet oppmerksomhet mot at data om den norske havbunnen og informasjon om norsk kraftinfrastruktur er åpent tilgjengelig. Russiske forskningsskip har hatt mulighet til å seile fritt langs norskekysten og kartlegge norsk kritisk infrastruktur langs havbunnen i lang tid. Ett av de største russiske oljeselskapene, Rosneft, har i en årrekke hatt tilgang til data om den norske havbunnen. Selv om mye av dataene ikke er sensitive hver for seg, kan trusselaktører utnytte den samlede informasjonen på bekostning av norske sikkerhetsinteresser. For eksempel kan også åpne tilgjengelige kart om transformatorstasjoner sammenstilles med annen tilgjengelig informasjon. Til sammen gjør dette at hvem som helst kan tilegne seg detaljert informasjon om norsk kraftinfrastruktur.

Konsekvensene av å tilgjengeliggjøre informasjon må hele tiden veies opp mot behovet for åpenhet. Norske myndigheter og virksomheter jobber tett sammen. De bruker dagens situasjonsbilde for å identifisere hva det er behov for å skjerme, og hvilke man eventuelt kan fortsette å dele åpent. I samarbeid vurderes hva som til enhver tid er akseptabelt risikonivå. På samme måte må virksomheter vurdere egne verdier i lys av oppdatert informasjon om trusler og sårbarheter.

Dette gjelder også for norske universiteter som bruker laboratorieutstyr og gjennomfører forskning innenfor områder som er viktige for å sikre våre nasjonale interesser. Eksempler er forskning innen olje og energi, elektronisk kommunikasjon (ekom), forsvarsmateriell og annen flerbruksteknologi.

I fjor skrev norske medier om at forskere ved NTNU og det kinesiske universitetet National University of Defence Technology (NUDT) har utgitt forskning sammen i en årrekke. NUDT er direkte underlagt Kinas sentrale militærkommisjon. Betydningen av at internasjonalt forskningssamarbeid er sentralt for akademia blir vurdert i lys av at trusselaktørene prøver å utnytte denne tilgjengeligheten gjennom både åpent og fordekt samarbeid, for å finne det risikonivået som kan aksepteres ved et slikt samarbeid.

Et finsk og svensk NATO-medlemskap vil bety mye for samarbeidet om sikkerheten i Norge. Her ser vi Jonas Gahr Støre sammen med Ulf Kristersson (Sverige) og Sanna Marin (Finland).

Foto: Lauri Heikkinen / Wikimedia Commons

Dagens trusler fra fremmed etterretningsvirksomhet, verdiene forskningsinstitusjoner besitter og sårbarhetene knyttet til den nødvendige åpenheten utgjør en betydelig risiko for at flerbruksteknologi faller i feil hender. Det er derfor viktig å finne en god balanse slik at vi kan ha det så åpent som mulig, men samtidig så sikkert som nødvendig.

Flerbruksteknologi

Flerbruksteknologi omfatter teknologier og produkter som kan anvendes både til sivile og militære formål (av engelsk «dual use technology»).

Tiltak for å sikre balansegang mellom åpenhet og skjerming

1. **Vurdering av skjerming og informasjonsdeling** må inngå i virksomheters risikostyring. Dette inkluderer rutiner for opplæring og bevisstgjøring om risikoen knyttet til ulovlig kunnskapsoverføring. Særlig viktig vil det være å kartlegge relevante krav i regelverk som virksomheten er pliktig å følge. Dette krever en klar og tydelig ansvarsplassering i virksomheten.
2. **Hva som kan ligge åpent tilgjengelig, og hva som må skjermes,** må være basert på en risikovurdering. Denne bør oppdateres jevnlig og ved endringer i risikobildet.

Bidra til å forbedre det nasjonale situasjonsbildet

Avvik fra normalen må varsles til myndighetene. Gjør dere kjent med hva som skal varsles, til politiet, PST, NSM eller andre. Det viktigste er ikke hvem varselet går til eller hvordan det er formulert, men at det skjer. Lag deres egne rutiner for varsling slik at ansatte er trygge på hva de skal gjøre.

Varsler om uønskede hendelser eller mistanke om dette er avgjørende for den nasjonale situasjonsforståelsen. Varslingsplikten til NSM omfatter all aktivitet, eller mistanke om aktivitet, som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser, uavhengig om den er lovlig eller kriminell. Virksomheter uten varslingsplikt oppfordres også til å ha en lav terskel for å rapportere til NSM om slik aktivitet. Gjennom rapportering forstår vi bedre det som skjer rundt oss, slik at vi kan iverksette de riktige tiltakene, små eller store. Ofte er ikke en hendelse isolert fra en annen.

Hvordan varsler du NSM?

Telefon
02497
(24/7)

E-post
cyberhendelser:
cert@ncsc.no

E-post
sikkerhetstruende
virksomhet og hendelser:
varsel@nsm.no

Sikkerhetsgradert informasjon må ikke inngå i varselet.

Foto: Ilja Hendel
Design: Tank Design

NASJONAL
SIKKERHETSMYNDIGHET

Postboks 814,
1306 Sandvika
Tlf. 67 86 40 00

Tlf. 67 86 40 00
nsm.no/risiko2023
www.nsm.no