Digitalt selvforsvar – hvordan forstå, forebygge og håndtere cyberangrep

En e-bok fra Tietoevry

September 2024

tietoevry

Først publisert november 2023 Oppdatert september 2024.

Forord

De siste årene har antall dataangrep mot norske virksomheter økt, nærmest fra måned til måned. På toppen av listen over trusler finner vi de såkalte løsepengevirusene, men angrepene omfatter også for eksempel innbrudd der målet er å stjele verdifull informasjon, informasjonskrigføring og såkalte DDoS-angrep (Distributed Denial of Service Attack).

Dette har skapt en situasjon som ingen kan ignorere og som aktivt må håndteres hver dag.

Denne publikasjonen gir en grunnleggende innføring i utfordringen slik Tietoevry opplever den akkurat nå (Situasjonsforståelsen). Risikobildet er komplisert, med stadig nye trusler, Europa er i krig og vi ser et mønster der de kriminelle ofte ligger litt foran. Samtidig skaper utviklingen av ny teknologi, nye sårbarheter – men også verktøyene vi trenger for å beskytte oss.

Vi kartlegger de viktigste truslene som møter oss i dag og prøver å si noe om de nye, som vi må være forberedt på. Og vi er konkrete og tydelige på hva som kreves av eiere, ledelsen og på styrerommet hos norske virksomheter i arbeidet med å sikre at egen IT-avdeling og eksterne samarbeidspartnere får ressurser og rammebetingelser som setter dem i stand til å håndtere risiko og å beskytte virksomheten.

I dette arbeidet er vi avhengig av både maskiner og mennesker; oppdaterte og solide IT-løsninger i samarbeid med kunnskapsrike ansatte som er trygge nok til å navigere trusler og utfordringer på en sikker måte.

I arbeidet med denne e-boken har vi først og fremst skrevet for ledere, styreledere og -medlemmer. Samtidig håper vi at også IT-ansvarlige og andre interesserte finner teksten nyttig – og bruker den som et utgangspunkt for å finne mer informasjon og så sette i gang tiltak i egen organisasjon.

I Tietoevry er vi klare til å sparre med dere, utveksle idéer, hjelpe dere med analyser og testing – og å bygge det forsvaret virksomheten trenger.

Ta gjerne kontakt!

Foto: Michaela Klouda

Sigrun Bock

Head of Cyber Security Professional Services

Tietoevry Tech Services

1. Det handler om tillit

I september i år gikk 21 norske næringslivledere ut i E24 og kalte digitale angrep en av de største truslene norsk næringsliv og samfunn står i overfor i tiden fremover.

De pekte på at cybetrusler vokser i et eksponensielt tempo, omtalte samarbeid som vårt beste forsvar og tok til orde for at digitale hjelmer og vernesko må på i alle bransjer og virksomheter.

At dette er viktig, fikk Norge merke i april 2023. Da benyttet en utenlandsk hackergruppe en såkalt nulldagssårbarhet i programvaren Ivanti Endpoint Manager for å angripe Departementenes sikkerhets- og serviceorganisasjon (DDS) for å komme seg på innsiden av tolv norske departementer. Der holdt de seg i ro frem til sommerferien hadde starter, før de aktivt begynte å søke etter informasjon.

Foto: Getty Images

Til NRK fortalte daværende direktør i Nasjonal Sikkerhetsmyndighet, Sofie Nystrøm, at angrepet var alvorlig, og for avansert til at det kunne vært utført av amatører:

> “
> – Det er tidlig i analysen, men dette er åpenbart en aktør som er ressurssterk. Det dreier seg ikke om gutteromshacking, sier Nystrøm i NSM. – Det er en aktør som har forsøkt å komme seg på innsiden. Først gjennom en hovedinngangsdør, og deretter prøvd å kartlegge hvor arkivene er. Hvor er det noe interessant? De kartlegger verdier, og prøver deretter å få tilgang til nye rom. (NRK, 24. juli 2023)

Selv om dette angrepet på offentlig IT-infrastruktur er var av de alvorligste i 2023, er det på langt nær det eneste. I august samme år brøt for eksempel nettsidene til et tosifret antall kommuner sammen i et DDoS-angrep. Stortinget klarte i samme måned å forhindre et tilsvarende angrep. Og i oktober ble Stavanger kommune hacket av en gruppe som truer med å offentliggjøre en stor mengde informasjon som de stjal i angrepet.

Angrepet på departementene, Stortinget og Stavanger kommune illustrerer et viktig poeng; datasikkerhet handler om å beskytte grunnleggende, demokratiske verdier i det norske samfunnet. Og det som står på spill er ikke bare informasjon eller økonomiske verdier, men den unike, norske tilliten – mellom folk og mellom folket og de som styrer – som garanterer et velfungerende og rettferdig samfunn for alle.

Vi er trygge og de aller fleste har det godt i Norge, og samfunnet og næringslivet fungerer, fordi vi kan stole på hverandre. Dette handler ikke om naivitet, men om en grunnleggende verdi som er fundamentet i den norske samfunnsmodellen.

Tietoevry tar ansvar

Når cyberkriminelle organisasjoner, enkeltindivider eller aggressive nasjonalstater angriper organisasjoner, virksomheter eller institusjoner, risikerer vi at de svekker den tilliten vi er avhengig av for å sikre et velfungerende samfunn. Og fordi Tietoevry leverer IT-tjenester til så mange av de sentrale aktørene i det norske samfunnet – fra banker og bedrifter, via helsevesenet til norske kommuner og frivillige organisasjoner – har vi både en forpliktelse og et ansvar for å ta IT-risiko på største alvor.

Våre kunder leverer infrastrukturen i samfunnet. Våre løsninger, og vår evne til å håndtere risiko, bidrar til verdiskapning og gir trygge rammer i hverdagen for de som bor i landet.

Foto: Getty Images

Sikkerhet er en viktig del av Tietoevrys samfunnsoppdrag. Vi jobber for at samfunnet skal fortsette å være så trygt at alle skal kunne ha tilgang på grunnleggende, digitale tjenester – og stole på at de er trygge å benytte.

Slaget er ikke tapt

I møte med historier om virksomheter som blir utsatt for løsepengevirus og verdikjedeangrep, enkeltpersoner som rammes og samfunnsinstitusjoner som angripes, er det lett å bli sittende igjen med et inntrykk av at det egentlig ikke er så mye vi kan gjøre.

Vi kan beskytte oss som best vi kan og håndtere de angrepene som kommer, men mange føler nok at de kriminelle, enten det er grupper med økonomiske motiver eller stater som er ute etter politisk kapital, ligger et hestehode foran.

Tietoevry mener at en slik holdning er for defensiv – og faren er er at vi spiller ballen rett i bena på alle som har tvilsomme motiver og onde hensikter i de grenseløse nettverkene som nå binder verden sammen.

Vi tror tvert imot, at vi har omfattende kunnskap og erfaring og et rikt arsenal av tiltak som vi kan ta i bruk, både i arbeidet med å forebygge, for å håndtere angrepene som de aller fleste virksomheter nå må regne med at de kommer til å bli utsatt for.

Denne kampen vinner vi imidlertid ikke alene. Beredskapskommisjonens rapport «Nå er det alvor», som ble lagt frem i juni 2023, peker blant annet på behovet for samarbeid mellom det offentlige og det private næringslivet. Samtidig må norske virksomheter bli flinkere, både til å forstå hva de forvalter av verdier som en hackergruppe vil være interessert i, og samtidig være villige til å investere i løsninger og kunnskap som gir reell beskyttelse mot angrep.

Stikkordet er samarbeid

Cybersikkerhet forutsetter at alle gode krefter trekke sammen, både i offentlig og privat sektor. Med Innlandet som knutepunkt har Tietoevry engasjert seg, sammen med en rekke andre aktører, i det som heter Norwegian Cybersecurity Cluster – et nasjonalt næringslivssamarbeid ledet av Wanja Bordewich.

–Innlandet har i flere tiår jobbet for å være et nasjonalt knutepunkt for cybersikkerhet med flere nasjonale organisasjoner og arrangement som har tilhold nettopp her, forteller Wanja Bordewich, – og det er også noe av grunnen til at et av Europas største og fremste forskningsmiljøer innen cybersikkerhet er lokalisert i området. Kompetansemiljøet på NTNU Gjøvik, inkludert Center for Cyber and Information Security (CCIS) og Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS), tiltrekker seg kompetanse i verdensklasse. På Gjøvik ligger også Norsis, Norsk senter for informasjonssikring som har blitt en del av NSM og Cyberforsvaret holder til på Jørstadmoen. Bare for å nevne noen.

The primary objective of the Cyber Security Cluster is to develop innovative cyber-security solutions to address the needs of a highly increased threat on our partners digital univers.

Norwegian Cybersecurity Cluster

Det gjelder å bygge tillit, også blant konkurrenter

Klyngetankegangen – som enkelt forklart handler om at virksomheter innen samme bransje eller fagområde gjensidig verdiøker hverandre når de samarbeider– ble opprinnelig introdusert og popularisert av bedriftsøkonomen Michael Porter i boken «The Competitive Advantage of Nations» i 1990. Et norsk eksempel som er mye brukt, er industriutviklingen i Rogaland rundt olje- og oljeservicebransjen.

– Et viktig premiss i cybersikkerhetsklynga som jeg leder, er at det er næringslivsdrevet og verdiskapende. Vi har fokus på innovasjon, produktivitet og på å skape ny omsetning med utgangspunkt i kompetanse og banebrytende løsninger som våre medlemmer og partnere utvikler.

– Det er stor variasjon i modenheten til norske virksomheter og organisasjoner når det kommer til cybersikkerhet. Noen bransjer er generelt mer modne, for eksempel finans, energi og kraft, mens andre er mindre modne i sin sikkerhetskultur. Cybersikkerhet er noe alle trenger i større eller mindre grad, uavhengig av sektor og bør ses på som like naturlig som HMS og økonomi. Samtidig skal vi møte en rekke store utfordringer som for eksempel økende grad av cyberkriminalitet og strengere krav til informasjonssikkerhet og personvern. Alt dette gjør at vi må samarbeide for å sikre vårt digitale samfunn.

Forskning og utdanning

Et viktig fokus for klynga er utdanning og kompetanse. Årsaken er enkel: Norge trenger flere fagfolk innen cybersikkerhet. – To tredjedeler av de som utdannes innen cybersikkerhet, har sin eksamen fra en læringsinstitusjon i Innlandet, enten det er NTNU, Fagskolen, Forsvarets Cyberingeniørskole eller en annen institusjon. Vi jobber også for at IT–lærlinger skal få den kompetansen som trengs, og vi er engasjert i de kortere etter- og videreutdanningsløpene, for dem som allerede er i jobb.

Et annet prioritert område, er samarbeidet mellom offentlig og privat sektor og andre klynger. – Mye av Norges kritiske infrastruktur driftes eller eies av private aktører. Det er en av grunnene til at vi trenger et næringsdrevet samarbeid, som sitter på et bredt spekter av kompetanse og erfaringer, for å finne flere av de gode løsningene på de store utfordringene vi står ovenfor både i næringslivet og samfunnet generelt.

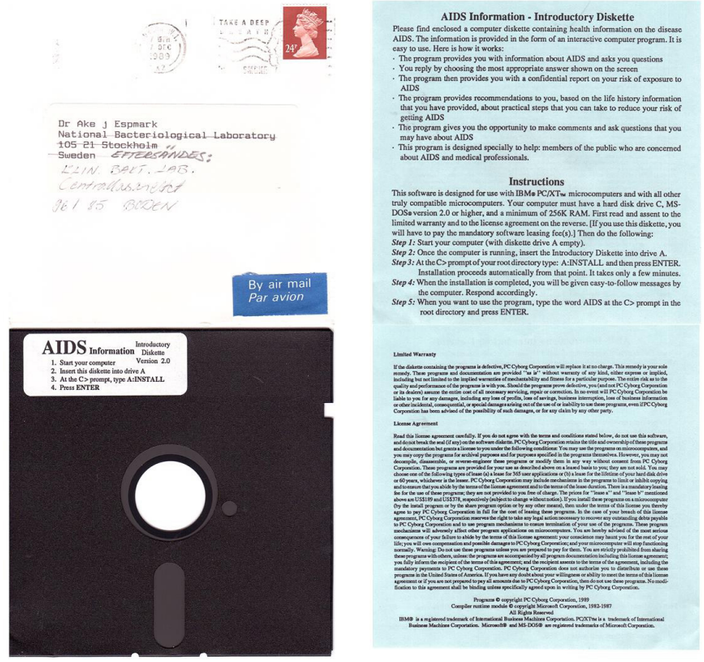
Vår misjon er å bygge en bærekraftig cybersikkerhetsnæring gjennom innovasjon, samarbeid og eksport av ledende løsninger. Vi styrker Norges posisjon som en global leder innen sikker digitalisering, avslutter Guro Storlien Evensen, daglig leder for Norwegian Cybersecurity Cluster.

Wanja Bordewich, klyngeleder, Norwegian Cybersecurity Cluster

2. Situasjonsforståelse: Trusler og trender

I 1989 sendte den Harvard-utdannede evolusjonsbiologen Joseph Popp ut 20 000 floppydisker til deltagerne på Verdens Helseorganisasjons AIDS-konferanse i Stockholm. De som matet disken inn i PC'en og fulgte Popps instruksjoner, opplevde noen dager senere at maskinen frøs og at en melding dukket opp på skjermen der ble de bedt om å sende 189 dollar til en postboks i Panama.

Noen av ofrene, de som hadde egen PC-kompetanse eller IT-ressurser på arbeidsplassen, klarte å jobbe seg rundt programmet Popp hadde sendt dem, men mange mottakere mistet alt de hadde lagret på harddisken. Og i 1989 var kunnskapen om datalagring og behovet for sikkerhetskopiering relativt tynn.



Credit: Olle Gustavsson, via Wikipedia, CC BY-SA 4.0

Det er fortsatt uklart om Popp opererte alene. Å betale for, og så formatere og sende ut over 20 000 floppydisker er en enorm jobb, for ikke å snakke om portokostnadene. Popp ble arrestert i sitt hjemland, Nederland, samme år, og utlevert til USA der han ble stilt for retten, men ikke dømt. Han døde i 2007. I ettertid blir denne hendelsen sett på som det første kjente forsøket på å benytte et løsepengevirus for å svindle til seg penger.

Flere år med digitalisering på 18 måneder

Norge var allerede før pandemien rammet i mars 2020, et av Europas mest digitaliserte land. På EUs The Digital Economy and Society Index (DESI) samme år (basert på data fra 2019) lå vi på tredje plass, etter Finland og Sverige. Indeksen, som i dag er erstattet med Report on the state of the Digital Decade, sier blant annet noe om i hvilken grad offentlige tjenester er digitalisert, utbredelsen av bredbånd og konsum av digitalt medieinnhold. Det er ikke mange land i verden som har realisert potensialet knyttet til digital teknologi og nettverk på en mer effektiv måte enn Norge.

Foto: Shutterstock

Stadig færre av oss husker hvordan det var å gå på Rådhuset i vinterkulden for å levere selvangivelsen på papir.

En bank i dag er en app, ikke et kontor, og penger er enten et plastkort eller en funksjon på telefonen.

Offentlige skjemaer kommer ferdig utfylt på Digipost eller Altinn, med informasjon fra relevante offentlige registre.

Eiendomsinfo og tinglysingsprosesser er digitalisert og tilgjengeliggjort av det som inntil for noen år siden var statens eget selskap.

En mekaniker på et hvilket som helst verksted i Norge åpner oftere PC'en og så panseret, enn omvendt.

Kommuner kommuniserer digitalt med innbyggerne, som søker om barnehageplass, velferdstjenester eller skolebytte på Internett.

Produsenter av strøm er koblet på den samme infrastrukturen som frakter energien – integrert i én, felles europeisk løsning.

Manuelle prosesser, som innlesing av faktura og betaling av krav, blir automatisert og stadig forbedret ved bruk av kunstig intelligens.

Da pandemien sendte Norge på hjemmekontor, slo norske virksomheter på det de hadde tilgjengelig av digitale løsninger og systemer for fjernarbeid, samarbeid, kommunikasjon og kunnskapsdeling. Fysiske butikker ble til nettbutikker fra en dag til en annen, Oda (som i starten het Kolonial) ble den nye nærbutikken, Über begynte å bruke kunstig intelligens integrert i app'en for å sjekke at kundene virkelige hadde munnbind på, og Bring forteller at de utviklet en digital, berøringsfri signaturløsning på under 24 timer.

Foto: Shutterstock

Estimatene varierer, men det er ingen tvil om at vi under pandemien tilbakela et utviklingsløp på 18 måneder som under normale forhold ville ha tatt årevis. Og det bare fortsetter, noe den rivende utviklingen innen kunstig intelligens og lanseringen av de store, språkbaserte AI-verktøyene, som ChatGTP og Copilot, er gode eksempler på.

Effektiv, men sårbar – angrepsflatene øker

Flere har pekt på at de siste 15-20 årenes IKT-utvikling ikke bare har kastet av seg i form av effektivisering og verdiskapning, men også har en pris i form av økt risiko og eksponering for digitale angrep. En viktig årsak til det er at de digitale angrepsflatene – enheter og funksjoner i en digital løsning der det er mulig for en angriper å komme seg inn – blir stadig større.

Denne utviklingen, som er en direkte konsekvens av digitalisering av nye og eksisterende prosesser, produkter og tjenester, er ikke ny. Den begynte i realiteten med det amerikanske forsvarets utvikling av Arpanet, senere Internett, i 1968, som startet en utvikling av globale, digitale motorveier der veldig mye, og stadig mer, blir digitalisert, oppkoblet og tilgjengelig fra hvor som helst. I dag kaller vi dette Internet of Things (IoT) og den konkrete konsekvensen er at mulighetene for å komme seg på innsiden av et bedriftsnettverk, en offentlig tjeneste eller kritisk infrastruktur er mye større nå enn for bare noen år siden.

Og eksemplene er mange.

- Et hotell i Østerrike som ble utsatt for dataangrep, opplevde at de digitale låsene sluttet å virke. Etter å ha betalt hackerne det de krevde, gikk de tilbake til nøkkelbaserte låser og reduserte den digitale eksponeringen til null.
- Et amerikansk kasino ble frastjålet informasjon om de mest verdifulle spillerne sine av en hacker som kom seg inn via et nett-tilkoblet termometer i et akvarium.
- Den norske sikkerhetseksperten Runa Sandvik – som lenge jobbet for New York Times – ble kjent over hele verden da hun og en kollega klarte å hacke og avfyre en moderne snikskytterrifle uten å være i nærheten av våpenet.
- Utallige angrep og innbrudd skjer fordi ubrukte kontor fortsetter å være operative lenge etter at en ansatt har sluttet eller funksjonen som kontoen er knyttet til, ikke lenger er i bruk.


Foto: Unsplash

Og hvis det ikke er mulig å komme til en virksomheter med digitale virkemidler, er det alltid et alternativ å rette angrepet mot de ansatte – hvor det naturlig nok er noen som ikke rekker å tenke at en e-post fra sjefen eller en SMS fra en kollega ikke er autentisk, før det er for sent.

Drivere i en farlig utvikling

Årsakene til, og driverne i den utviklingen innen cyberkriminalitet og IT-angrep som vi har sett, særlig de siste 10 – 15 årene, er mange. Dette er en kort oppsummering av noen av dem som er med å forme trusselbildet akkurat nå.

Tingenes Internett og større angrepsflater
Det store økningen i eksponerte flater der det er mulig for en kriminell å hacke seg inn i et system, fortsetter å representere en stor risiko. «Internet of Things», som vi på norsk kaller Tingenes Internett, beskriver en utvikling der stadig flere fysiske gjenstander kobles på digitale nettverk ved hjelp av sensorer, som igjen generer data til bruk i styring, overvåking eller analyse. Vi snakker om alt fra laksemærder, foringsmaskiner, skurtreskere og hodetelefoner, via biler til værstasjoner, trafikkameraer, industrielle kontrollsystemer, mobiltelefoner, lysarmaturer og dørlåser.

En faktor som også må med i denne sammenhengen, er mobiliteten blant de ansatte i en moderne virksomhet. Mobiltelefoner, bærbare PC'er, programvare for deling og samarbeid og tilgang på trådløse nettverk, har ført til at kontoret ikke lenger er et sted, men en situasjon. Du er på kontoret når du jobber, ikke der du jobber.

Stadig mer proffe kriminelle
Bildet av den klassiske hackeren som en ung, ensom mann som programmerer virus på gutterommet, er for lengst gått ut på dato. Det har funnet sted en profesjonalisering av cyberkriminalitet som har lagt grunnlaget for en global industri som opererer mer eller mindre på samme måte som en ordinær, kommersiell virksomhet. Resultatet er Ransomware as a Service (RaaS).

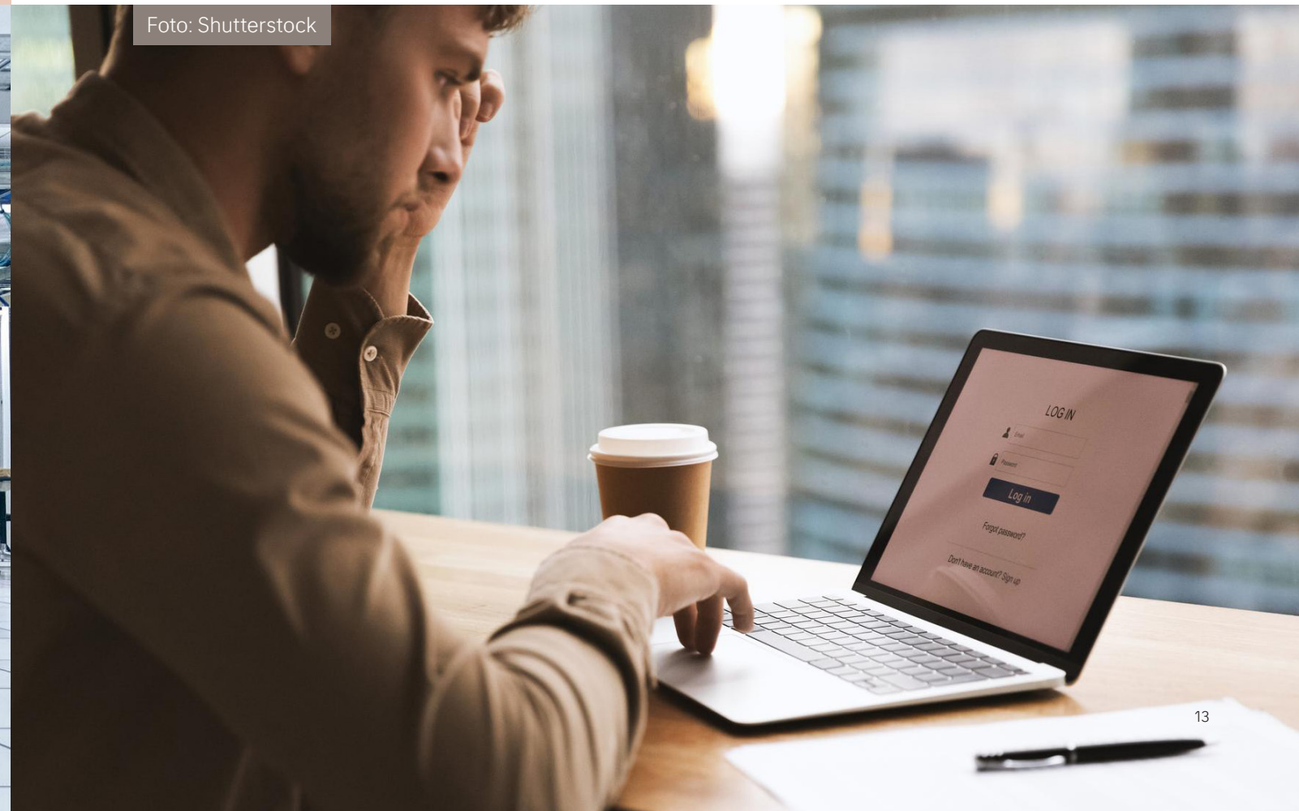


Foto: Shutterstock

De klassiske enkelthackerne finnes selvfølgelig fortsatt, men i stadig økende grad blir norske myndigheter og organisere angrepet av virksomheter som til forveksling likner på dem selv. De kriminelle er godt organisert, de jobber 9 til 4, tar ut ferie og logger av i helgene.

(Funfact: Statistikk viser at de fleste løsepengevirusene settes ut på fredager. Teorien er at de kriminelle avslutter uken med å gjennomføre et antall angrep, tar helgefri og kommer tilbake mandag morgen for å finne ut hva virusene har kastet av seg.)

Noen av disse gruppene gjør hele jobben selv, samtidig som det ikke er vanskelig å få kjøpt ferdig hackede virksomheter som utpresses, informasjon som allerede er hentet ut, bestille nødvendig ondsinnet programvare eller leie inn en virksomhet som tar seg av forhandlinger og kontakt med ofrene. Nylig var det til og med mulig å kjøpe en hel hackervirksomhet med allerede stjålet data, VPN-tilgang til 11 ferdige hackede selskaper, inkludert «spillboken»; oppskriften på hvordan gruppen jobber.

Eieren hadde rett og slett gått lei av å bli plaget av føderale myndigheter og overvåkingen som fulgte med et liv som cyberkriminell.

Hvis «kundene» opplever problemer med varen de har kjøpt, kan de kontakte supportsenteret hos selgeren. Og er de fornøyde, har de anledning til å legge igjen en anmeldelse, omtrent som når du scorer spisesteder på Trip Advisor. Sånn etablerer man tillit i en bransje der ingen stoler på hverandre.

Kryptovaluta utenfor myndighetenes kontroll

En viktig forutsetning for denne profesjonaliseringen, er fremveksten av kryptovaluta. Dette er betalingsmidler og verdier som eksisterer på siden av nasjonalstaten og sentralbankenes kontroll. Bitcoin er på samme tid et viktig verktøy for politiske bevegelser og aktivister i land der de ikke trygt kan bruke den eksisterende finansielle infrastrukturen – og realiseringen av en gammel drøm for alle kriminelle verden over som har savnet et betalingsmiddel som muliggjør både omfattende hvitvasking og sporløs betaling av produkter og tjenester som ikke er lovlige.

Foto: Getty Images

Å sende noen et løsepengevirus på 90-tallet, for deretter å organisere overleveringen av en koffert med løsepenger, var ikke en bærekraftig forretningsmodell. Kryptovaluta har fungert som en disruptiv teknologi i dette markedet. Nå kan en kriminell organisasjon være lokalisert i land som ikke er veldig opptatt av å stoppe dem, gjennomføre angrep på den andre siden av kloden – og få betalt i verdier som ingen kan spore.

Nicholas Weaver, en forsker ved Berkley, har kalt løsepengevirus for et «bitcoinproblem». Han ser ingen annen løsning på dette, enn at myndighetene på en eller annen måte tar kontroll over betalingsløsningen.

Geopolitikk og en ustabil verden

Som styremedlem eller leder i en mellomstor norsk virksomhet som selger marine wireprodukter, lysarmaturer til eiendomsmarkedet, importerer kjemiske løsninger til celluloseindustrien eller er digitaliseringsrådgivere for statlige virksomheter, var den politiske situasjonen i Russland, forholdet mellom Kina og Taiwan eller den økonomiske utviklingen i Nigeria, kanskje ikke det som tidligere sto øverst på dagsorden. Det endret seg dramatisk den 24. februar i 2022.

Dagen før hadde russiske hackere gjennomført et massivt angrep på Ukrainsk infrastruktur, men denne dagen startet Russland sin bakkeinvasjon, en på mange måter logisk videreføring av landets anneksjon av Krim noen år før – som allikevel kom overraskende på store deler av verden.


Foto: Getty Images

Realiteten er at geopolitikk; konflikter, sosiale forhold, klima, teknologi og økonomi i dag er relevante faktorer som påvirker cyberrisiko og trusselbildet også for virksomheter i demokratiske land med en solid infrastruktur og ryddige samfunnsforhold.

Et skremmende og kostbart eksempel på dette, er NotPetya-viruset som rammet land og virksomheter sommeren 2017.

NotPETYA – en massiv, koordinert cyberinvasjon

Bakteppet er konflikten mellom Russland og Ukraina og Russlands annektering av Krim-halvøya i 2014. I årene etterpå opplevde Ukrainia så mange cyberangrep med opprinnelse i Russland, at enkelte politikere mente stormakten brukte sin mye mindre nabo som et testlaboratorium for digitale våpen. Det var for eksempel ikke uvanlig at elektrisitetsnettverket brøt sammen og strømmen forsvant i særlig kalde perioder om vinteren.

27. juni 2017 startet det som i ettertid har blitt kalt «en massiv, koordinert cyberinvasjon» av Ukraina, da hackergruppen Sandworm slapp løs NotPetya-viruset ved å plassere det på oppdateringsserveren hos Linkos Group i Kiev, utviklerne av landets mest populære regnskapsprogramvare. Viruset var bygget over samme lest som et klassisk løsepengevirus fra året før, Petya, men til forskjell fra sin forgjenger var målet til NotPetya-viruset utelukkende ødeleggelse. Og paradoksalt nok benyttet hackerne seg blant annet av et digitalt våpen, EternalBlue, som var stjålet fra NSA (US National Security Agency) tidligere på året.

NotPetya tvang de infiserte maskinene til å starte på nytt, etter å ha kryptert det som kalles «master boots records». Resultatet var at PC'ene ikke var i stand til å finne igjen sitt eget OS og at alt innholdet på disken var utilgjengelig.

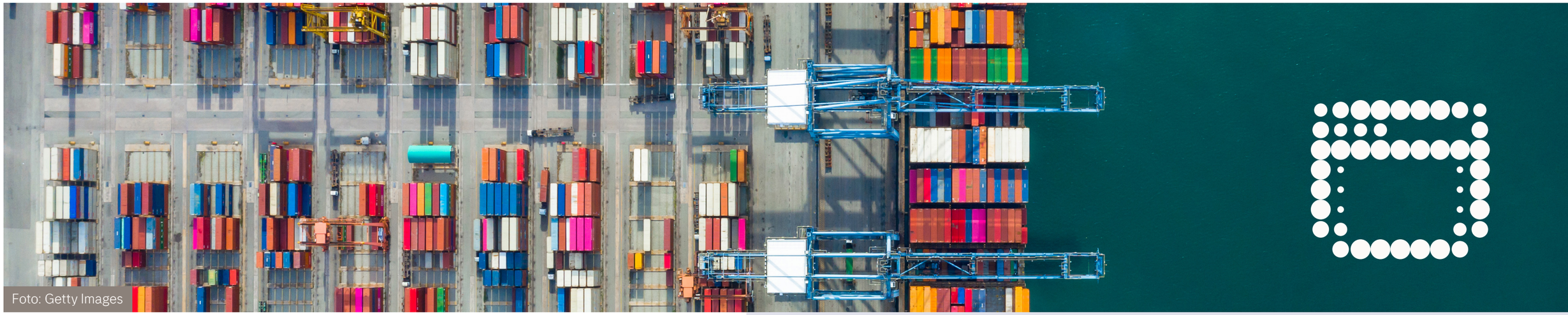


Foto: Getty Images

Viruset spredde seg som en gressbrann, først i Ukrainia, der blant annet landets betalingssystemer gikk ned på noen minutter, og deretter til organisasjoner og virksomheter i resten av verden; et sykehus i Philadelphia, en sjokoladefabrikk i Tasmania, farmasikjempen Merck, TNT Express, Sain-Gobain, Mondelez. Og Maersk.

Den globale logistikkoperasjonen til det danske containerrederiet stoppet helt opp i et angrep som har blitt kjent som det mest omfattende og kostbare noensinne. Maersk har estimert sitt eget tap til over 300 millioner dollar, mens sluttsummen globalt landet på rundt 10 milliarder dollar.

I ettertid har amerikansk etterretning sporet NotPetya-viruset tilbake til Russland og Sandworm-hackerne, som har koblinger til russiske myndigheter. (Russland har aldri innrømmet at de hadde noe med dette angrepet å gjøre.) De har kalt viruset en atombombe, brukt i en begrenset, regional konflikt, med konsekvenser for personer og virksomheter over hele verden.

Og det er her norske styrerepresentanter og ledere gjør lurt i å følge med. For når konflikten mellom Russland og Ukrainia, i form av NotPetya-viruset, representerer en trussel mot infrastrukturen i et moderne samfunn, kan også utenrikspolitiske konflikter i andre deler av verden gi grunn til å heve sikkerhetsnivået i IT-løsningen hos en nettleverandør på Vestlandet, et logistikkselskap i Tromsø eller et hotell i Oslo.

Cyberkrigføring

I lys av Russlands angrep på Ukraina i 2022, har også konseptet «Cyberkrigføring» blitt aktualisert. For det er ikke nødvendig å høre luftvernsirener eller se soldater i gatene for å være under angrep fra et annet land. Og virkemidlene som er tilgjengelige i denne krigsformens verktøykasse, er noe vi må være på vakt mot lenge før en nasjonalstat faktisk oppfører seg truende eller mobiliserer ved grensen.

Cyberkrigføring beskrives som bruk av digitale våpen for å ødelegge fiendens datasystemer. Mange mener at Russlands invasjon av Ukraina ikke startet den 24. februar, men med det digitale angrepet dagen før. Og det var nettopp det som skjedde, både onsdag 23. februar 2022 og i månedene før.

Hybridkrigføring er en type krigføring som kjennetegnes av en kombinasjon av tradisjonelle militære, og irregulære metoder. De omfatter alt fra propaganda, nettmanipulering, undergraving, sabotasje og regulære, elektroniske angrep på IT-infrastruktur og samfunnskritiske virksomheter.

Artikkel 5 i Atlanterhavspakten slår fast at Nato-landene «er enige om at et væpnet angrep mot en eller flere av dem i Europa eller Nord-Amerika skal betraktes som et angrep mot dem alle.». Samtidig er cyberdomenet globalt og grenseløst, og det er vanskelig å bevise at en fremmed makt faktisk har angrepet et Nato-land. Det er derfor fullt mulig å operere i cyberdomene, slik vi må anta at land som Russland, Kina, Nord-Korea og Iran gjør, i stor skala uten at artikkel 5 blir utløst.

Informasjonskrig

Dette er i realiteten kampen om en felles sannhet i et samfunn. Og hvis en fremmed makt klarer å spre så mye desinformasjon eller skape grunnlag for så mye tvil at befolkning ikke lenger tror på offisielle nyhetskanaler, autoritetspersoner eller myndighetene, er det sannsynligvis mulig å få dem til å tro på nesten hva som helst. Denne kampen føres i nyhetskanaler og på sosiale medier for å sikre bred støtte, overtale og fremkalle sympati hos mulige allierte og samtidig spre forvirring, usikkerhet og mistillit i samfunnet.

Norge er et robust samfunn med en høy grad av tillit. Samtidig må vi ta på alvor at informasjon kan misbrukes til å påvirke oss, svekke tilliten vår til politikere, demokratiske institusjoner og myndighetene generelt. Informasjonskrigføring er psykologisk manipulering og et forsøk på å dra motparten sine intensjoner i tvil, og samtidig skape polarisering og splittelse.

En situasjon som er spesielt sårbar i et demokrati, er valg. Et skremmende eksempel er etterspillet i kjølvannet av det amerikanske presidentvalget i 2020, og president Trumps påstander om at valget ble stjålet. I Norge har Forsvarets Forskningsinstitutt tatt akkurat denne trusselen på alvor, og laget rapporten Scenarioer for uønsket påvirkning i forbindelse med norske valg.

De skriver at målet med rapporten er «å utvikle, beskrive og drøfte mulige scenarioer for hvordan informasjonspåvirkning i sammenheng med norske valg kan foregå.» Og selv om vi, så vidt vi vet, aldri har vært i nærheten av omfattende manipulasjon i forbindelse med et valg i Norge, så er det all grunn til å være forberedt på at noen kan komme til å prøve seg, slik verden ser ut i dag.

Foto: Getty Images

Truslene du må forholde deg til

Løsepengevirus

Løsepengevirus utgjør fortsatt en av de vanligste truslene mot norske virksomheter, og kan gjøre enorm skade hvis angrepet er omfattende og sikkerhetstiltakene i forkant mangelfulle.

Løsepengevirus rammer både store og små virksomheter, og skiller ikke på offentlig og privat sektor. Selv om de store virksomhetene generelt sett har blitt flinkere til å kontrollere, overvåke og sikre backup av virksomhetsdata, er det likevel viktig å ha en beredskapsplan som man øver på for å være forberedt dersom et angrep skulle skje.

Verdikjedeangrep

Verdikjedeangrep er en risiko mange undervurderer, samtidig som de kan være vanskelige å beskytte seg mot. De skjer ved at en underleverandør eller en partner tar med seg viruset på innsiden av dine systemer og den ondsinnede programvaren kan være alt fra løsepengevirus til spyware.

Små leverandører bruker mindre penger på IT-sikkerhet og har ofte dårligere beskyttelse, mens store virksomheter har sterkere forsvarsmekanismer. De fleste virksomheter har imidlertid små leverandører som de er avhengig av. Da er det viktig å huske at de er eksponert for, og avhengig av sikkerhetsnivået hos underleverandørene de er integrert med. Ofte ser vi at en liten programvareleverandør drar med seg noe på veien inn.

Mange virksomheter har etiske retningslinjer som de også pålegger underleverandører. Flere bør inkludere IT-sikkerhet i partneres forpliktelser og ikke minst «penteste» hele verdikjeden, inkludert samarbeidspartnere.

Phishing

Phishing handler sosial manipulasjon, ofte ved bruk av kunstig intelligens som gjør truslene mer avanserte og som gjør det mulig å produsere skremmende realistiske deepfakes.

Her handler det om hvor gode alle medarbeidere i virksomheten er til å ikke gå i fella når en e-post lokker med en link eller et vedlegg. Phishing-truslene kommer fortsatt på e-post, men nye teknikker basert på kunstig intelligens har økt risikoen for at flere blir lokket til å gå inn på sider eller trykker på linker de ikke skal, eller åpner vedlegg som er infisert.

Der man før lokket med en rabatt eller et tilbud om man trykket på en lenke før en tidsfrist, har de kriminelle gått videre til å utgi seg for å være sjefen eller en kollega, som trenger hjelp med å godkjenne en utbetaling rett før helgen eller ferien.

For å gjøre henvendelsene enda mer troverdige produserer de kriminelle videoer, bilder eller lyd som fører til at offeret i enda større grad opplever at henvendelsen er reell og fra en du faktisk kjenner.

Informasjonstyverier

Cyberkriminelle benytter alle verktøy i kassen, inkludert kunstig intelligens, for å utgi seg for å være personer de ikke er, i jakten p bedriftens verdifulle informasjon. I denne kategorien finner vi også ID-tyverier, der kriminelle stjeler din informasjon og gir seg ut for å være deg øker også. Når de så har klart å stjele den personlige informasjonen, bruker de samme verktøy på nytt for å produsere materiale; tekst, bilder og film, som overbeviser andre om at de faktisk er deg.

Spionasje

På statlig nivå ser vi et stadig mer komplekst risikobilde i kjølvannet av krigen i Europa, der kritisk infrastruktur og digitalt styrte samfunnsfunksjoner, fra sykehus, til vann og avløp, strøm og nettforsyning, kan trues. Samtidig ser vi at spionaktiviteten øker. Ikke med mål om nedstenging og ødeleggelse, men for å stjele hemmeligheter og patenter som representerer intellektuelle verdier for norske virksomheter.

Foto: Shutterstock

Trusler mot operasjonell teknologi (OT)

Litt forenklet kan man si at det digitale universet lenge var delt i to. IT (informasjonsteknologi) på den ene siden – maskinvare og programvare som forvalter, utnytter og verdiøker data eller informasjon. Og OT (operasjonell teknologi) på den andre – enheter og systemer som for eksempel brukes i kritisk infrastruktur, smarte bygg og i industrien for å overvåke, kontrollere og styre fysiske prosesser.

De siste årene har disse to sfærene nærmet seg hverandre, i en utvikling som ofte går under navnet «Industri 4.0». Her handler det om å utnytte den enorme tilgangen på data i digitaliseringens kjølevann, der Internet of Things også omfatter den tidligere så lukkede OT-sfæren. Målet er å strømlinjeforme arbeid, koble sammen og automatisere det som før var isolerte prosesser, utnytte maskinlæring, potensialet i edge computing og utviklingen av såkalte «cyberfysiske systemer».

Foto: Shutterstock

Foto: Getty Images

I et historisk perspektiv har den operasjonelle teknologien har vært mer skjult og beskyttet fra mange av de mindre avanserte, ondsinnede aktørene på nettet. Men i takt med at analoge og lukkede prosesser digitaliseres, blir de også i større grad koblet på og eksponert for aktiviteten på Internett. Og det er når det som tidligere var en diskret bakdør som få visste om, blir til en inngang som flere hackere er i stand til å finne og å utnytte, at faren for at alt fra industrielle produksjonslinjer, energiforsyningen, nødnettet og renseanlegg plutselig slutter å fungere.

Forsøk på å angripe operasjonell teknologi er ikke uvanlig. Virksomhetene som produserer disse hardwarekomponentene som benyttes i alt fra fabrikker og damanlegg til smarte bygg og maskiner, jakter på sårbarheter og løser disse på samme måte som andre IT-virksomheter sikrer sine løsninger og programvare.

Stuxnet – et OT-angrep som tatt ut av en spionroman

Et av de mest omtalte, og spektakulære OT-angrepene vi kjenner til, skjedde for over ti år siden. Bakteppet er som tatt ut av en internasjonal spionroman.

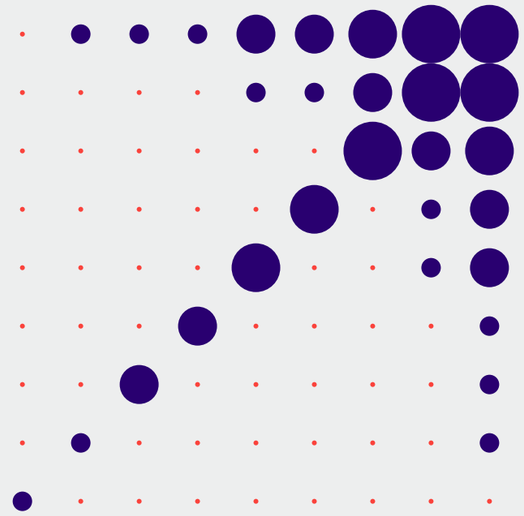
En av Israels og USAs store bekymringer, er muligheten for at Iran skal klare å anrike nok uran til at de kan produsere atomvåpen. Dette ville ha representert en direkte trussel for Israel – et land Iran aldri har anerkjent – og seriøst forrykket den internasjonale maktbalansen. Derfor er også begge landene villige til å gå langt for å forsinke, og helst stoppe, alle iranske forsøk på å utvinne og anrike dette radioaktive grunnstoffet.

Irans atomvåpenprogram er lokalisert til en by og et industriområde, midt i landet, sør for Iran. Fabrikken i Natanz der Israelerne mente produksjonen foregikk, er helt isolert, og ikke koblet til Internett på noen som helst måte. Samtidig visste de at iranerne benyttet moderne gass-sentrifuger i arbeidet med å anrike uranet, og at disse var styrt av Siemens PLC'er – Programmable Logic Controller – en type operasjonell teknologi som kontrollerer prosesser knyttet til maskiner i en fabrikk.

I 2010 observerte ingeniørene i Natanz et problem de ikke forstod; samtidig som måleinstrumentene i kontrollrommet ikke viste tegn til unormal aktivitet, økte hastigheten i tusenvis av sentrifuger så dramatisk, at de moderne maskinene vibrerte og spant i stykker. Et stort antall sentrifuger ble ødelagt, produksjonen stoppet delvis opp og det iranske atomvåpenprogrammet var satt flere år tilbake i løpet av noen uker.

I forkant av denne hendelsen, hadde dataviruset Stuxnet infisert systemene til fire IT-leverandører som alle hadde en eller annen kobling til Natanz-anlegget, og som utviklet løsninger for maskin- og prosesstyring. På disse systemene gjorde ikke viruset særlig skade, men i det programvaren kom seg på innsiden av Natanz, gikk det først i skjul over en lengre periode, før det våknet til liv og tok kontroll over sentrifugene.

Hvordan Stuxnet kom seg på innsiden av et «air gapped» anlegg i Iran, isolert fra nettet som det var, er fortsatt en gåte. En av teoriene er at en av ingeniørene har fått med seg viruset inn på en PC han og de andre deltagerne på en internasjonal konferanse hadde fått gratis. Og i koden som viruset var skrevet med, fant analytikere en rekke spor, hint og antydninger som indikerte at den ondsinnede programvaren var et samarbeidsprosjekt mellom USA og Israel.



3. Handlekraft og motstandsbevegelse

Over fire uker etter at IT-leverandøren ble rammet av et løsepengevirus, ligger den lille rørleggerbedriften fortsatt nede for telling.

Ingressen som sto på trykk i Digi den 1. november 2023 var dramatisk. Saken handlet om en IT-leverandør i Innlandet som ble angrepet i oktober i fjor, og som ikke har klart å gjenopprette kundenes data fra sikkerhetskopiene, som også er korrumperte. Konsekvensene var store. Rørleggerbedriften som uttalte seg i saken fortalte at de hadde mistet tilgangen på alt av systemer, dokumenter og prosjekter og at de hadde vært nødt til å jobbe med penn og papir. 35 ansatte hadde fått permitteringsvarsel, de var i ferd med å miste et kjempeoppdrag som de ikke hadde mulighet til å by på – og de er bare en av flere av IT-leverandørens kunder som er i en liknende situasjon.

Det er lett å miste motet. Inntrykket mange sitter igjen med – og kanskje spesielt på leder- og styrenivå – er at en virksomhet er relativt hjelpeløs i møte med kriminelle og internasjonale cybergjenger. De ligger tilsynelatende alltid et hestehode foran, utnytter sårbarheter som ennå ikke er oppdaget eller blir stadig mer avanserte når de lurer ansatte til å slippe dem inn i virksomhetens systemer – eller kommer seg inn på egen hånd.

Og det faktum at løsepengevirus og utpressing ikke bare fortsetter, men øker i omfang, er i seg selv en bekreftelse på at mange velger den enkle løsningen; de betaler.

Foto: Getty Images

Å betale er ingen løsning

De som betaler, begir seg inn i et utfordrende landskap. De bidrar til finansiering av ny kriminalitet og signaliserer samtidig at de er sårbare for nye angrep. Det finnes heller ingen garanti for at data som leveres tilbake, ikke er kompromittert. I verste fall er slutten på det ene angrepet, starten på det neste.

Markedet er også i stadig økende grad oppmerksom på den økonomiske risikoen knyttet til cyberkriminalitet og har sannsynligvis allerede begynt å prise denne inn i verdivurderingen av en virksomhet. Å gi etter for kriminelle er ikke nødvendigvis noe som styrker markedsverdien eller tilliten til selskapet, i hvert fall ikke på lang sikt.

Myndighetene i en rekke land er også tydelige på at de ikke anbefaler at en virksomhet gir etter og betaler. I Australia vurderer de en lov som forbyr det.

Og det er ingen automatikk i at et forsikringsselskap vil dekke tapene. I land som USA, Storbritannia og Frankrike har myndighetene signalisert at de ønsker å forby forsikringer som dekker tap knyttet til løsepengevirus – fordi de som betaler bidrar til nye angrep.

Selv om dette er en beslutning virksomheten selv må ta, er det Tietoevrys posisjon at det ikke er en god løsning å betale det de kriminelle utpresserne krever. I stedet vil vi jobbe for at virksomheter generelt, og våre kunder spesielt, delvis iverksetter tiltak som forebygger og reduserer muligheten for at noen kommer seg på innsiden av IT-systemene og delvis at de er så godt forberedt hvis det skjer, at situasjonen kan håndteres og skaden begrenses.

Et første tiltak er å forstå hva risikoen innebærer, og hva konsekvensene av et løsepengevirus eller et tyveri av informasjon vil være. Deretter sette i verk forebyggende tiltak. Og så til slutt ha planene klare for hva som må gjøres for å redusere konsekvensene hvis virksomheten allikevel blir angrepet.

Identifisere, beskytte, oppdage og håndtere

I Tietoevry jobber vi hver dag med å redusere risikoen for cyberangrep på våre egne systemer og hos våre kunder.

I møte med ledere og IT-ansvarlige som er overveldet av oppgavens kompleksitet og størrelse, er et av våre viktigste budskap at det nytter å beskytte seg. Det handler om å bygge inn effektive kontroller og tiltak gjennom hele organisasjonen og den tilknyttede verdikjeden i et puslespill der alt henger sammen med alt. Og selv om det overordnede bildet er komplekst, er det alltid mulig å starte med de enkleste bitene.

I arbeidet med IT-sikkerhet og risikohåndtering er det én ting som er viktigere enn noe annet: system og struktur. Med utgangspunkt i en kartlegging av risiko og sårbarheter, der man blir seg bevisst konsekvensen av at IT-løsningen går ned eller informasjon blir stjålet, er det mulig å få hjelp til å beskytte seg, overvåke trusler og – i verste fall – håndtere en situasjon. Og de som har tenkt igjennom «worst case» på forhånd, er nesten alltid de som ender i et «best case».

Et rammeverk for handling

I møte med kunder der tema er IT-sikkerhet, er det ett rammeverk for sikkerhet og risikohåndtering som stadig dukker opp, og som Tietoevry aldri nøler med å anbefale. Det er utarbeidet av Nasjonal Sikkerhetsmyndighet (NSM) og går under navnet NSMs grunnprinsipper for IKT-sikkerhet.

De 4 kategoriene som de 21 grunnprinsippene er organisert i, bygger på det etablerte NIST- rammeverket, der NIST står for National Institute of Standards and Technology. Andre standarder som ofte benyttes er ISO 27001.

Rammeverket som disse grunnprinsippene utgjør, er en stor kunnskapsbank, tilgjengelig for flere enn bare de mest tekniske rollene i en organisasjon, samtidig som det representerer en praktisk metodikk og en måte å jobbe med IT-sikkerhet på. På nettsidene til NSM finnes et introduksjonskurs til rammeverket, og vi opplever at kunder og andre vi snakker med går fra å føle seg overveldet, til å ha en mer praktisk og overkommelig tilnærming til risiko og IT-sikkerhet etter å ha tatt kurset.

NSM er Noregs direktorat for forebyggjande nasjonal trygging. Direktoratet gir råd om og gjennomfører tilsyn og andre kontrollaktiviteter på sivil og militær side knytta til sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning. NSM har også eit nasjonalt ansvar for å avdekkje, varsle og koordinere håndtering av alvorlege IKT-åtak.

NSM sine hjemmesider

NSMs grunnprinsipper for IKT-sikkerhet

Den beste måten å tilegne seg kunnskapen og metoden på, er å sette seg inn i informasjonen som NSM tilbyr på hjemmesidene sine. Den er lett tilgjengelig og gratis og et konstruktivt startpunkt for alle virksomheter, også de små og mellomstore.

Her er en kort oversikt:

1. Identifisere og kartlegge

1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer

1.2 Kartlegg enheter og programvare

1.3 Kartlegg brukere og behov for tilgang

2. Beskytte og opprettholde

2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser

2.2 Etabler en sikker IKT-arkitektur

2.3 Ivareta en sikker konfigurasjon

2.4 Beskytt virksomhetens nettverk

2.5 Kontroller dataflyt

2.6 Ha kontroll på identiteter og tilganger

2.7 Beskytt data i ro og i transitt

2.8 Beskytt e-post og nettleser

2.9 Etabler evne til gjenoppretting av data

2.10 Integrer sikkerhet i prosess for endringshåndtering

3. Oppdage

3.1 Oppdag og fjern kjente sårbarheter og trusler

3.2 Etabler sikkerhets-overvåkning

3.3 Analyser data fra sikkerhets- overvåkning

3.4 Gjennomfør innterengingstester

4. Håndtere og gjenopprette

4.1 Forbered virksomheten på håndtering av hendelser

4.2 Vurder og klassifiser hendelser

4.3 Kontroller og håndter hendelser

4.4 Evaluer og lær av hendelser

Modell fra NSM sine hjemmesider.

1. **Identifisere og kartlegge**. Denne fasen handler om å få en oversikt over egen virksomhet, blant annet styringsstrukturer, ledelsesprioriteringer, leveranser, IKT-systemer og brukere. Målet er blant annet å kartlegge hva som må sikres og hvem sitt ansvar det er å gjør det.
2. **Beskytte og opprettholde**. Sette i verk tiltak og implementere løsninger som beskytter virksomheten i dag og over tid.
3. **Oppdage**. Løpende oppdage og fjerne kjente sårbarheter i IT-løsningen, samt avdekke avvik fra ønsket tilstand
4. **Håndtere og gjenopprette**. Håndtere sikkerhetshendelser effektivt ved å være forberedt på dem.

Start med en plan for uønskede situasjoner

NSMs grunnprinsipper burde være overkommelig å sette seg inn i for de fleste virksomheter. Og ROI, for å snakke i økonomiske termer, er høy hvis noe skulle skje. Men frem til alt er på stell og hvis du føler behov for å ta grep umiddelbart, er arbeidet med en enkel plan for hva som må være på plass i tilfelle en uønsket situasjon oppstår, også et godt sted å starte for IT-ansvarlige, i samarbeid med ledelsen. Og kanskje er det en så beskjeden start som skal til, for at dere setter i gang med det litt større arbeidet med grunnprinsippene til NSM.

I arbeidet med en enkel plan er virksomheten nødt til å sette ord på hvordan et dataangrep kan se ut og hva konsekvensene i det daglige vil være. Se for dere at IT-systemet, økonomiløsning, e-post, server og intern chat ikke lenger er tilgjengelig. Det er to dager til lønnsutbetaling, det er midt i faktureringsperioden, flere ansatte har viktige leveranser de kommende dagene – og ingenting virker.

Å sette ord på en slik situasjon, diskutere hva den innebærer og på forhånd bli enige om de første tiltakene man gjør (hvordan kundene skal informeres, hva de ansatte skal gjøre den dagen og hvem som har ansvar for hva), skaper et betydelig forsprang på en virksomhet som ikke har gjennomført en slik øvelse. For arbeidet med en beredskapsplan og trening på scenarioer er ofte en trigger for å finne ut hva virksomheten må ha på plass hvis det verste skulle skje. Det tvinger organisasjonen til å ta stilling til hvem som skal eie cyberangrepsscenariet og til å sette ord på hvem som har oversikt over systemene, hvilken kompetanse dere har og hva dere mangler.

IT-sikkerhet er et leder- og styreansvar

En utfordring for mange norske virksomheter er at de ikke har tenkt godt nok igjennom hvem som har det overordnede ansvaret for IT-sikkerheten. Cybersikkerhet blir ofte lagt til IT, fordi det handler om data. Realiteten er imidlertid at for å bli tatt på alvor og for at det som noen ganger oppleves som litt omstendelige sikkerhetsprosedyrer skal ha legitimitet, så må IT-sikkerhet forstås av og være daglig leders ansvar.

En del av dette ansvaret innebærer å sikre at organisasjonen har tilstrekkelig og god sikkerhetskompetanse som jobber strukturert og målrettet med å forebygge risiko. Samtidig er det ikke et mål at ledere skal bli datasikkerhetseksperter, men de må forstå så mye at de kan stille de riktige spørsmålene for få et faktabasert beslutningsgrunnlag som de kan planlegge med utgangspunkt i.

I denne sammenheng opplever Tietoevry at det ofte glipper i overgangen mellom ambisjoner og konkrete tiltak, som krever budsjetter og ressurser. De som er ansvarlige må få tid til å gjøre jobben, nødvendige systemer og løsninger må kjøpes inn, og ekstern kompetanse koster penger - på samme måte som rekruttering av nye ansatte med riktig bakgrunn må inn i budsjettplanleggingen.

4. Kilder, ressurser, organisasjoner og aktører

En rekke offentlige aktører og organisasjoner har fokus på sikkerhet generelt, og cybersikkerhet spesielt – og deler med seg av kunnskap, råd og metoder.

Hvis du vil lese mer om trusselbildet og hva du kan gjøre for å beskytte deg, er dette fine steder å følge med på:

Politiets Etterretningstjeneste (PST)

Introduksjon til nasjonal trusselvurdering 2024

Etterretningstjenesten i Forsvaret

Fokus 2024 – Etterretningstjenestens åpne vurdering av aktuelle sikkerhetsutfordringer for Norge.

Nasjonal sikkerhetsmyndighet

Digital sikkerhet – kunnskap og ressurser

Nasjonalt digitalt risikobilde 2024

Norsk senter for informasjonssikring

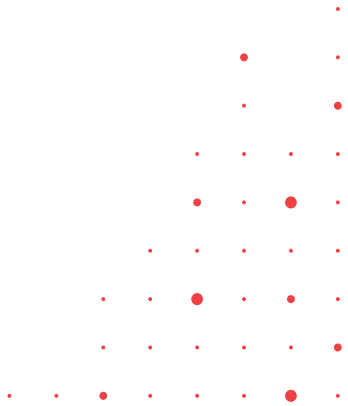
Kunnskap, råd, kurs og tiltak

Andre ressurser:
Næringslivets Sikkerhetsråd, Norwegian Cybersecurity Cluster, Tietoevry-bloggen

Om oss

Tietoevry skaper meningsfull teknologi som bidrar til å gjøre verden bedre. Vi er et ledende teknologiselskap med en solid nordisk arv og global kapasitet. Basert på våre kjerneverdier åpenhet, troverdighet og mangfold, jobber vi sammen med våre kunder for å utvikle digitale fremtider hvor virksomheter, samfunn og mennesker kan vokse.

Våre 24 000 eksperter globalt er spesialisert innen sky, data og programvare, og betjener tusenvis av kunder innen næringsliv og offentlig sektor i mer enn 90 land. Tietoevrys årlige omsetning er på rundt 3 MRD Euro og selskapet er børsnotert på NASDAQ i Helsinki og Stockholm, i tillegg til Oslo Børs.
www.tietoevry.com



Kontakt oss

Tietoevry Norge AS
Snarøyveien 30
Postboks 4
1360 Fornebu

tlf. 23 14 50 00
tietoevry.com/no