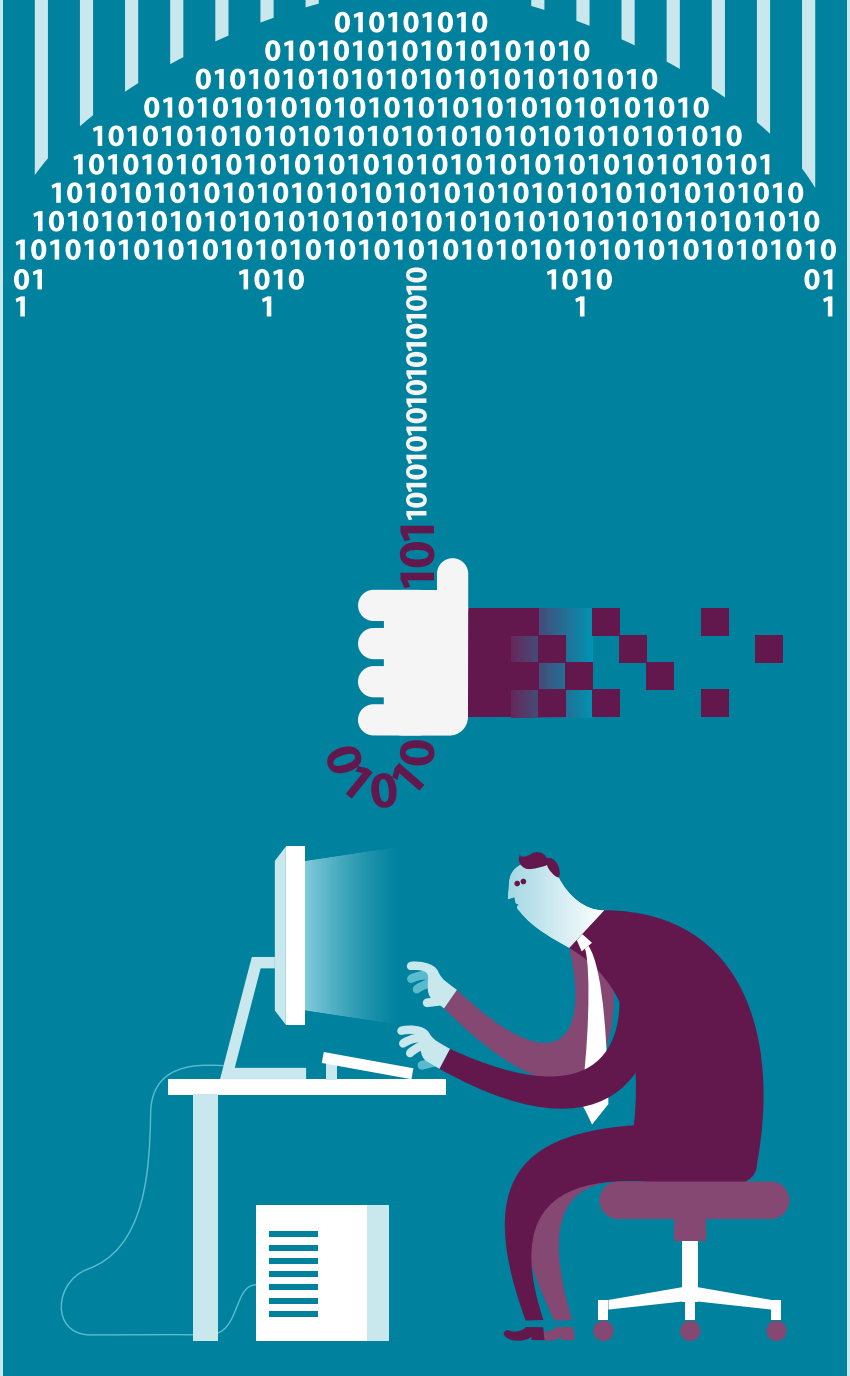
TRUSLER OG TRENDER
2018–19

Hvilke digitale trusler møter oss på jobb og i hverdagen?



Norsk Senter for Informasjonssikring 2018
Skrift: Proxima Nova og Adobe Garamond Pro 10 / 13 pkt
Illustrasjoner: Akindo via GettyImages
ISBN: 978-82-93651-03-1

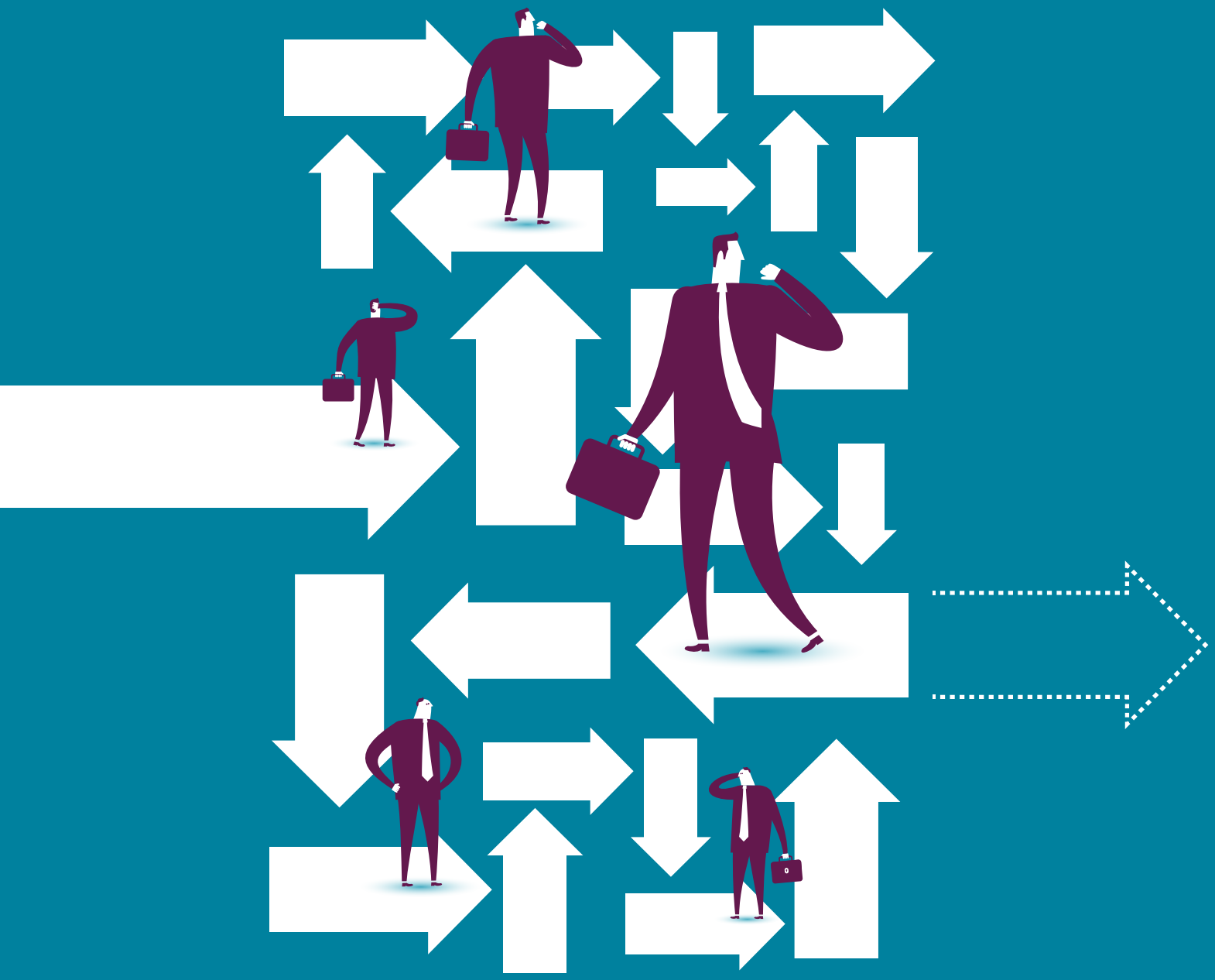
norsis.no

TRUSLER OG TRENDER

2018–19

INNHOLD

TRUSLER OG TRENDER I EN DIGITAL HVERDAG



I denne rapporten presenterer NorSIS hvilke trusler som har vært mest fremtredende det siste året. Vi ser særlig på trusler som treffer små og mellomstore virksomheter og befolkningen. I tillegg til hva som allerede treffer oss, beskriver vi hvilke utfordringer eller digitale trender vi mener samfunnet vil møte fremover.

Arbeidstagere og privatpersoner forventer at leverandører, produsenter, myndigheter og andre hjelper dem å unngå å bli digitalt utnyttet. I tillegg ser det ut til at mange har en forventning om at myndighetene vil hjelpe dem dersom de utsettes for trusler eller hendelser på nett. Myndighetene på sin side, ønsker en digitalisering av samfunnet fordi det er både energi-, ressurs- og kostnadssparende. I hvert fall på sikt. Dette betyr at samfunnet både forventer at virksomheter legger til rette for digitalisering, og at brukerne er villige til å ta i bruk digitale verktøy. For å lykkes med dette, må samfunnet som helhet ha en god sikkerhetskultur, tilstrekkelig kompetanse og høy tillit til digitale verktøy og kanaler. En forutsetning for å oppnå dette, er å kjenne til hvilke trusler en utsettes for, hvilke trusler en kan forvente å møte fremover og ikke minst hvordan disse truslene bør eller skal håndteres.

Hensikten med rapporten er å gi en oversikt over de mest vanlige hendelsene som virksomheter og befolkningen forøvrig bør kjenne til, og inkludere i sine risikovurderinger.

HVA ER EN RISIKOVURDERING?

Å gjøre en risikovurdering handler om å kartlegge sårbarheter og trusler mot seg selv og sine verdier, og ut fra det identifisere uønskede hendelser som kan ramme virksomheten. I virksomhetssammenheng er det en viktig lederoppgave å ta stilling til risiko knyttet til den aktiviteten virksomheten gjennomfører. Ledelsen må gjøre en vurdering om risikoen ved å gjennomføre er for høy, eller om den kan aksepteres med de sårbarheter og eventuelle trusler som er kjent.

Samtidig er risikovurderinger noe alle vi mennesker gjør flere ganger daglig. Bare vi skal koble telefonen vår til et trådløst nett eller krysse gata gjør vi, eller burde vi gjøre, en vurdering av hva denne handlingen betyr for oss og om risikoen den innebærer eller den mulige konsekvensen er verdt å ta.

Digitale trusler kjenner ingen landegrenser. NorSIS kjenner til flere tilfeller der kriminelle utnytter sårbarheter hos små virksomheter for å ramme større virksomheter eller myndigheter. Vi opplever derfor en utfordring i at mange mindre virksomheter ikke forstår at de er et attraktivt offer for ulike trusselaktører.

Konsekvensene av å rammes av en eller flere av truslene beskrevet i rapporten er mange og de er ofte også store. Det kan være alt fra økonomisk tap, i noen tilfeller konkurser, angrep på kritisk infrastruktur eller politiske beslutningsprosesser til psykologiske vansker, ødelagte sosiale relasjoner eller tap av omdømme og tillit.

Truslene er valgt utfra det som møter små og mellomstore virksomheter og privatpersoner i hverdagen. Samtidig er det viktig å understreke at disse truslene like godt kan ramme store selskaper og offentlige myndigheter. Rapporten har en bred tilnærming til trussel-

Risikovurderinger begrenser seg altså ikke til umiddelbar fysisk fare. De omfatter alle uønskede hendelser som kan ramme virksomheten eller den enkelte, knyttet til omgivelser og aktiviteter. En risikovurdering handler om å svare på; Hva kan gå galt? Hva er konsekvensene dersom noe går galt? Hva kan vi eventuelt gjøre for å forhindre det, og hva vil det koste? Hvilken risiko kan vi leve med? Det siste vil si, er handlingen så viktig at vi er villige til å gjennomføre den likevel, selv om vi vet hva konsekvensen blir dersom det går galt. For eksempel å krysse gata. Vi vet at det er en mulighet for å bli påkjørt av en bil eller andre kjøretøy. Samtidig er konsekvensen av å ikke gå over gata som regel større en risikoen ved å gjøre det.

bildet. Dette er viktig fordi bildet blir stadig mer sammensatt. Kildene for rapporten strekker seg fra henvendelser inn til NorSIS, NorSIS egne rapporter, trusselrapporter fra ulike myndighetsorganer til undersøkelser gjennomført i målgruppene og internasjonale rapporter om cyberkriminalitet. Vi har blant annet sett til rapporter fra Etterretningstjenesten, PST, NSM, Europol, NSR, CISCO, Visma og Telenor.

HVA ER DIGITALE OG NETTILKOBLEDE ELEMENTER?

Noen eksempeler på på dette er Smart-TV, mobilapper, førerløse busser, lønns- og fakturasystemer, saksbehandlingssystemer, sensorteknologi, skybaserte arbeidsverktøy, GPS-flåtestyringssytemer og stemplingssystemer.

PÅLOGGEDE OG SÅRBARE – HVORDAN SIKRE EN TRYGG DIGITAL HVERDAG?

I mange år har det vært snakket om tingenes internett og digitalisering av samfunnet. Dette er en villet utvikling, både politisk og samfunnsøkonomisk. Norge regnes som et modent digitalt marked. Det understrekes i mange undersøkelser og rapporter, for eksempel Nasjonal sikkerhetsmyndighet (NSM) sin rapport om IKT-risikobilde[1]. Samtidig viser Vismas digitale index[2] at innføring av ny teknologi hos deres kunder går saktere enn før. Også sammenlignet med andre land. Fra 2017 til 2018 har digitaliseringsgraden kun økt fra 46 prosent til 47 prosent i Norge Til sammenligning har den i Sverige økt med 7 prosent i samme periode, fra 41 til 48.

Regjeringen påpeker stadig at mulighetene IKT og digitalisering gir, skal utnyttes. Myndighetene tar også mange initiativ for gjenbruk av data, digitalisering av arbeidsprosesser og å bedre tilgjengelighet, kommunikasjonskanaler og kunde-, bruker og pasientopplevelser for befolkningen. Samtidig er det utfordringer for å få dette på plass både raskt, sikkert og gjennomsiktig. Det siste handler om at digitalisering skal skje på en måte som bevarer åpenheten om hva som skjer for de som omfattes av endringen.

HVA ER EN VIRKSOMHETS VERDIER?

Virksomhetens verdier kan være alt fra penger, tekniske løsninger og tegninger, kontakt-, kunde eller interessentlister til avtaler eller andre løsninger. Det kan være noe som er spesielt for nettopp den virksomheten eller noe som alle virksomheter har. For eksempel kompetanse om et fagfelt, informasjon som er samlet inn fra andre, sammenstilling av opplysninger, forskningsresultater eller patenter. Verdiene er grunnleggende for virksomheten på den måten at det enten er et grunnlag for å tjene penger som i seg selv kan gjøre dem til et attraktivt mål, eller at verdiene gir innpass til andre aktører.

Med ny teknologi følger nye muligheter, men også nye sårbarheter. Jo flere digitale og etterhvert nett-tilkoblede elementer som tas i bruk, jo mer utsatt er brukerne for at uvedkommende får tilgang til informasjonen deres i eller fra systemer og løsninger.

I arbeidslivet så vel som i privatlivet skjer det en stadig utvidelse av verdikjeder, eller verdinettverk, når ulike enheter kobles sammen. I hjemmet kan det være at mobiltelefonen gjennom ulike apper kobles sammen med smarthøyttaleren, dørlåsen, bilen og gjerne også arbeidsrelaterte systemer som e-post og virksomhetens saksbehandlingssystem.

Både hjemme og i arbeidslivet ser vi at mange virksomheter ikke er klar over at de kan være potensielle ofre for cyberkriminelle. Det kan skyldes en undervurdering av egne verdier og at noen er interessert i disse, eller kanskje en undervurdering av egen sårbarhet. I følge Mørketallsundersøkelsen[3] kan det også skyldes manglende oversikt over egne verdier. I undersøkelsen svarte hele 40 prosent at de oppdaget sikkerhetsbrudd ved en tilfeldighet. Og av alle de som oppdaget sikkerhetsbrudd

1 Nasjonal sikkerhetsmyndighet: *«Et sikkert digitalt Norge – IKT-risikobilde 2018»* https://nsm.stat.nol/globalassets/rapporter/nsm_ikt-risikobilde_2018_web.pdf

2 Visma: *«Digital index 2018 – En undersøkelse om digital modenhet i norske bedrifter»* https://www.visma.no/digitalisering/digital-index/

3 Nærligslivets sikkerhetsråd: *«Mørketallsundersøkelsen 2018»* https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/Mørketallsundersøkelsen/Mørketallsundersøkelsen%202018%20low.pdf

svarte 67 prosent at dette skyldes uflaks eller uhell. Dette understreker hvor viktig det er at virksomheter både kjenner sine egne verdier og forstår hvilke trusselaktører som kan se dem som et attraktivt mål.

En annerkjennelse av hvilke trusler som finnes, god kjennskap til egen verdi, og å inneha en egenevne til beskyttelse er viktig. Særlig fordi NorSIS erfarer at trusselaktørene som møter små og mellomstore virksomheter stadig blir mer profesjonelle og målrettede. Det stiller også større krav til sikkerhetsarbeidet. Dette er en stor utfordring for virksomheter som har lav kjennskap til, lav kompetanse om og få ressurser tilgjengelig til sikkerhetsarbeid. Det er nok dessverre situasjonen hos mange virksomheter i Norge. NorSIS erfarer at selv de som kjøper sikkerhetstjenester eller utkontrakterer sikkerhetsarbeidet til eksterne leverandører, må ha en grunnleggende kompetanse for å sikre egne interesser.

HVA ER SIKKERHETSKULTUR?

Digital sikkerhetskultur handler om å beskytte digitale verdier fra ulike former for trusler som rettes mot innebygde sårbarheter. Den kan derfor forstås som de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til alt som er digitalt. Digital sikkerhetskultur er derfor et sett med handlingsmønstre, og et sett med idéer, holdninger og kunnskaper. I en organisasjon kan digital sikkerhetskultur enten være slik ledelsen ønsker at den skal være, eller ikke slik de ønsker at den skal være. I det siste tilfellet vil sikkerhetskulturen kjennetegnes av lav kunnskap og forståelse for digitale verktøy, uvilje til å bruke disse og manglende tillit til digitale tjenester og teknologi.

DEN MENNESKELIGE FAKTOR

Den enkelte borger får stadig flere digitale enheter både hjemme, på jobb og ellers i hverdagen. Ettersom disse i stadig større grad er knyttet sammen med andre enheter, kan de, om de ikke er tilstrekkelig sikret, brukes for å begå nettkriminalitet. Enten i stor skala for eksempel at de brukes for å angripe samfunnsfunksjoner, eller for å angripe eller utnytte den enkelte bruker. Jo flere tjenester, systemer og enheter og infrastrukturer som kobles sammen, jo lengre blir verdikjedene. Uoversiktlige verdikjeder gjør det vanskelig å iverksette sikringstiltak. Det fortsetter også et samarbeid på tvers av samfunnsfunksjoner for å sikre en enhetlig tilnærming. Alt dette gjør at den enkeltes holdninger og adferd knyttet til digital sikkerhet stadig blir viktigere.

HVA ER EN VERDIKJEDE ELLER ET VERDINETTVERK?

En verdikjede er en sammenkobling av en rekke systemer, for eksempel ulike IT-systemer, saksbehandlingssystemer, apper, GPS-kjørebok, ansattregister, infrastruktur som kabelnett, strømnett eller kommunikasjonskanaler. Infrastrukturen kan også bestå av fysiske transportetapper med tog, lastebil båt eller fly. Deler av verdikjeden være plassert på virksomhetens servere, mens andre deler er plassert i en skyløsning, hos underleverandører, kunder, myndigheter eller andre steder.

Teknologien påvirker mennesket, men mennesket kan også påvirke teknologien. Både ved den enkeltes villighet til å bruke den, og måten den brukes på. For å sikre at mennesker og teknologi jobber best mulig sammen, må den enkelte av oss ha eller få, nødvendig digital kompetanse og forståelse. Uten å vite eller forstå hvilke muligheter og trusler hun eller han kan tenkes å møte ved bruk av digitale eller analoge tjenester, er det vanskelig å sikre eller i det hele tatt bidra til, at ens egen digitalisering er trygg.

Samtidig er det viktig at alle borgere har eller får, et forhold til utviklingen av vår di-

4 NorSIS: *«Nordmenn og digital sikkerhetskultur 2018»* https://norsis.no/wp-content/uploads/2018/11/Nordmenn-og-digital-sikkerhetskultur-2018-web.pdf

5 Politites sikkerhetstjeneste: *«Trusselvurdering 2018»* https://norsis.no/wp-content/uploads/2018/11/Nordmenn-og-digital-sikkerhetskultur-2018-web.pdf

gitale hverdag. På den måten kan vi forstå hva som skjer, hvorfor det skjer og hva som er vår rolle i det som skjer. De som har en faglig interesse av digitaliseringen vil trolig ta en mer aktivt del i den enn andre. Det er også fornuftig å møte denne utviklingen med en sunn skepsis. Det vil si, å stille spørsmål ved ny teknologi, for eksempel bruk, nytte og implementering av ny teknologi. Det er også viktig å være klar over sin egen rolle i implementering av ny teknologi. Først da, kan mennesket få tillit til teknologien og også til de eller dem som implementerer den.

SIKKERHETSKULTUR – HVA ER DET OG HVORFOR BØR ALLE VIRKSOMHETER KJENNE TIL EGEN SIKKERHETSKULTUR?

NorSIS har på oppdrag fra Justis- og beredskapsdepartementet kartlagt den nasjonale sikkerhetskulturen siden 2015. Høsten 2018[4] la vi frem resultatene fra årets måling. For at samfunnet og den enkelte av oss skal bli mindre sårbare for digitale trusler, må vi jobbe målrettet med sikkerhetskultur.

Ledelsen må sørge for at de alle ansatte får nødvendig opplæring, kjennskap til og kunnskap om digitale trusler. Dette kan være alt fra enkle grep som å låse PC-en, bruke skjermfilter og ikke ta med tjenestetelefon på reise, til å vite om og videreformidle informasjon om og kjenne til svindel-, utpressing- og phishing-kampanjer, melde fra om mistenkelige henvendelser, ha rutiner for å dobbeltsjekke endringer i utbetalinger til leverandører, bruke totrinnsbekreftelse for pålogging og å sørge for å holde all programvare oppdatert til enhver tid. Når de ansatte kjenner igjen trusler og håndterer dem riktig, vil de aktivt bidra til å sikre virksomhetens verdier.

Kunnskap om egen sikkerhetskultur gjør det mulig å finne ut hvor ledelsen må sette inn tiltak for å sikre virksomhetens verdier. Dersom sikkerhetskulturen kartlegges over tid, er det også mulig å finne ut om tiltakene virker.

GRENSELØS KRIMINALITET

En av de store utfordringene med kriminalitet i det digitale rom, er at både trender og utviklingstrekk er globale. Dette stiller krav til alle de som skal oppdage, avdekke og eventuelt etterforske denne typen kriminalitet. Det at alle kan bli ofre for cyberkriminelle hvor som helst i verden, uten noen spesiell tilknytning til oss utover en digital tilgjengelighet, øker også sårbarheten til potensielle ofre.

Små og mellomstore virksomheter er ofte enten verdifulle mål i seg selv eller mål på grunn av deres rolle i en verdikjede. Dette bekrefter i PST sin åpne trusselvurdering.[5] Enkelte små og mellomstore virksomheter er hovedleverandører innen en nisje, for eksempel teknologi, industri, produksjon eller annet. Dette kan for eksempel gjøre dem til attraktive mål for spionasje, sabotasje, datainnbrudd, svindel eller utpressing. Andre virksomheter er kanskje et sårbart element i en verdikjede. Et eksempel på hvem som kan være et offer i en slik verdikjede er for eksempel leverandør til en større virksomhet eller myndighet. Det er svært viktig at alle virksomheter innser hvor viktige de er i verdikjeden eller -nettverket. Hvis ikke, kan de bli et mål for noen som ønsker å ramme den eller de virksomhetene eller myndigheten som er på toppen av verdikjeden. Alle virksomheter må sørge for å beskytte egne verdier.

Det krever en helhetlig tilnærming til sikkerhetsarbeidet, uansett hva kjerneområdet for virksomheten er. Alle, fra ledelse til den enkelte ansatt i virksomheten må få nødvendig opplæring og oppmuntres til å utvikle egen kompetanse innenfor sikkerhet. Godt trente og bevisste ansatte er virksomhetens beste middel for å møte digitale trusler i hverdagen. Samtidig må tekniske systemer og hjelpemidler også sikres og oppdateres for å bidra til å sikre virksomhetens verdier. NorSIS opplever at det å få til en slik helhetlig tilnærming til sikkerhetsarbeidet ofte er en stor utfordring i en travel hverdag. Særlig for små og mellomstore virksomheter.

4 NorSIS: *«Nordmenn og digital sikkerhetskultur 2018»* https://norsis.no/wp-content/uploads/2018/11/Nordmenn-og-digital-sikkerhetskultur-2018-web.pdf

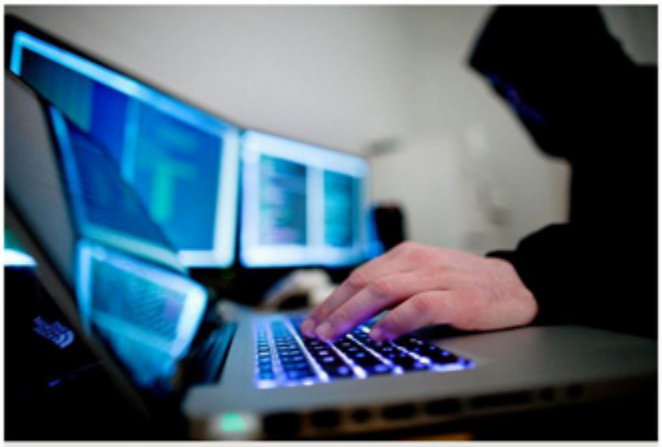
5 Politiets sikkerhetstjeneste: *«Trusselvurdering 2018»* https://norsis.no/wp-content/uploads/2018/11/Nordmenn-og-digital-sikkerhetskultur-2018-web.pdf

Nav får sterk kritikk for svak IKT-sikkerhet

Det er sterkt kritikkverdig at Nav og Kunnskapsdepartementet ikke har sikret tilfredsstillende informasjonssikkerhet, ifølge Riksrevisjonen.

KRITISK: – Det er vesentlige mangler i styringen av informasjonssikkerhet og sikring av IKT-systemer, sier riksrevisor Per-Kristian Foss.

Dataangrep mot Ticketmaster – ber kunder endre passord



Ukjente hackere kan ha fått tak i kortopplysninger og personlig informasjon fra Ticketmasters nettsider. Foto: Thomas Winje Øijord / NTB scanpix Foto: Øijord, Thomas Winje

Alkoposten-brukere er rammet av datalekkasjen. (Ill.: Martin Kynningsrud Størbu)

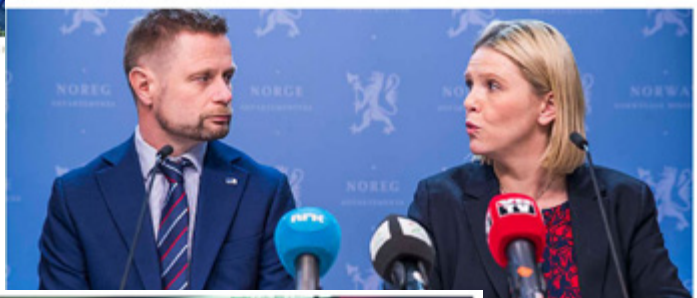
Schibsted bekrefter datalekkasje – 8500 nordmenn rammet

Prøvde å bryte seg inn i datasystemene til Helse Midt

– Mistenker at profesjonelle står bak innbrudd i annet helseforetak.

Norge

Pasientinformasjon kan være på avveie etter dataangrepet



Del (79) Tweet Epost

Stavanger kommune svindlet for en halv million kroner

Kommunen har ved en feil betalt 49.500 euro til svindlere. – Slik svindel er såpass vanlig at den er blitt vanskelig å unngå helt, sier ekspert på IT-sikkerhet.

Lise Marit Kalstad
Journalist

Fordøring utsatt: Ut fra trusselvurderingen til PST sjef Marie Benedicte Bjørnland regner organisasjonsdirektør Ida Munkeby med at NTNU som ofte kunnskapsorganisasjon kan være utsatte for slike typer spionasje.

Daglig data-angrep mot NTNU

– Vi har daglig innbruddsforsøk mot våre datasystemer. Mye er fra land som PST nevner i sin trusselvurdering for 2018, sier organisasjonsdirektør Ida Munkeby.

Nasjonal sikkerhetsmyndighet:

Norske virksomheter mer sårbare for digitale angrep

TRUSLER

LEDELSES- OG DIREKTØRSVINDEL

UHELL, UAKTSOMHET (VANVARE)

ID-TYVERI

SVINDEL (INKLUDERT DATINGSVINDEL)

UTPRESSING

KRENKELSER (MOBBING)

SABOTASJE

SIKKERHET PÅ REISE

SPIONASJE

LEDELSES- OG DIREKTØRSVINDEL

HVA ER DET?

Kriminelle forsøker å få en virksomhet til å overføre penger til dem, enten ved å utgi seg for å være en ansatt i virksomheten, ved å ta kontroll over en ansatts e-post eller en annen kommunikasjonskanal i virksomheten, eller i noen tilfeller gjennom å sende en falsk faktura. Dette rammer ofte små virksomheter som ikke ser seg selv som noe attraktivt mål for slik svindel. Det er viktig å huske på at alle virksomheter som omsetter eller behandler penger kan være et attraktivt mål for en svindler. Alle har sårbarheter som kan benyttes i en svindel.

HVEM STÅR BAK?

Kriminelle som ønsker økonomisk vinning.

HVORDAN UTFØRES DETTE?

Det finnes en rekke ulike metoder for denne typen svindel. En variant er at e-poster «spoofes» eller forfalskes slik at de ser ut til å være sendt fra en direktør eller andre med fullmakt til å godkjenne transaksjoner. Henvendelsen gjelder ofte en «hastetransaksjon». En annen metode som benyttes er at kriminelle kommer seg på innsiden av virksomheten gjennom å ta over tilgangen til en av de ansattes e-post. Det er ofte økonomimedarbeidere eller mellomledere som utsettes for denne typen svindel. Når de uvedkommende har tilgang til e-postkontoen, kan de overvåke e-postkorrespondanse med kunder og leverandører. De kan også sende og svare på e-post. Dersom muligheten byr seg, kan svindleren for eksempel endre kontonummer for en eller flere utbetalinger. I tillegg kan de besvare e-poster på vegne av den virksomheten de svindler, eller utgi seg for å være dennes leverandør eller kunde. NorSIS kjenner til tilfeller der det er sendt falske e-poster, falske fakturaer eller falske SMS tilsynelatende fra virksomhetens leder. Noen ganger følges disse også opp med en telefonsamtale. Endel av disse angrepene er godt planlagte. Det vil si at svindlerne har gjennomført en kartlegging av selskapets ledelse, rutiner og aktiviteter. Denne kartleggingen bruker de til sin fordel. I noen av tilfellene utnytter svindlerne kjente sårbarheter i programvare for å komme seg på innsiden av en virksomhets systemer.

HVA ER MÅLET?

Denne typen svindel gjennomføres først og fremst for økonomisk vinning. Samtidig har det vært tilfeller der de kriminelle har brukt informasjonen de har samlet inn om en virksomhet for å bygge opp kunnskap om en leverandør/kunde. Intensjonen er da som regel å misbruke den innsamlede informasjonen, for eksempel ved å selge den videre til andre kriminelle.

HÅNDTERING

Forebyggende tiltak

Et viktig forebyggende tiltak er å aktivere totrinnsbekreftelse for e-postklienter, arbeidsverktøy, saksbehandlingssystemer og alle andre systemer som benyttes. Det gjør det vanskeligere for uvedkommende å ta kontroll over e-post og andre systemer virksomheten bruker. Det er også viktig å ha og følge, gode interne rutiner for å sjekke om meldinger om for eksempel endring av kontonummer for leverandør eller andre, er reelle. Når dere skal undersøke dette, bør de som har sendt melding om endringen kontaktes i en annen kanal enn den første melding er mottatt i. Det vil si at dere, dersom dere får en e-post om bytte av kontonummer tar en telefon til avsenderen for å bekrefte at dette stemmer. NorSIS er kjent med eksempler på at en sender e-post for å verifisere innholdet i en mottatt e-post, men der svindlerne har kontroll over e-posten. I slike tilfeller bekrefter svindlerne sin egen svindel.

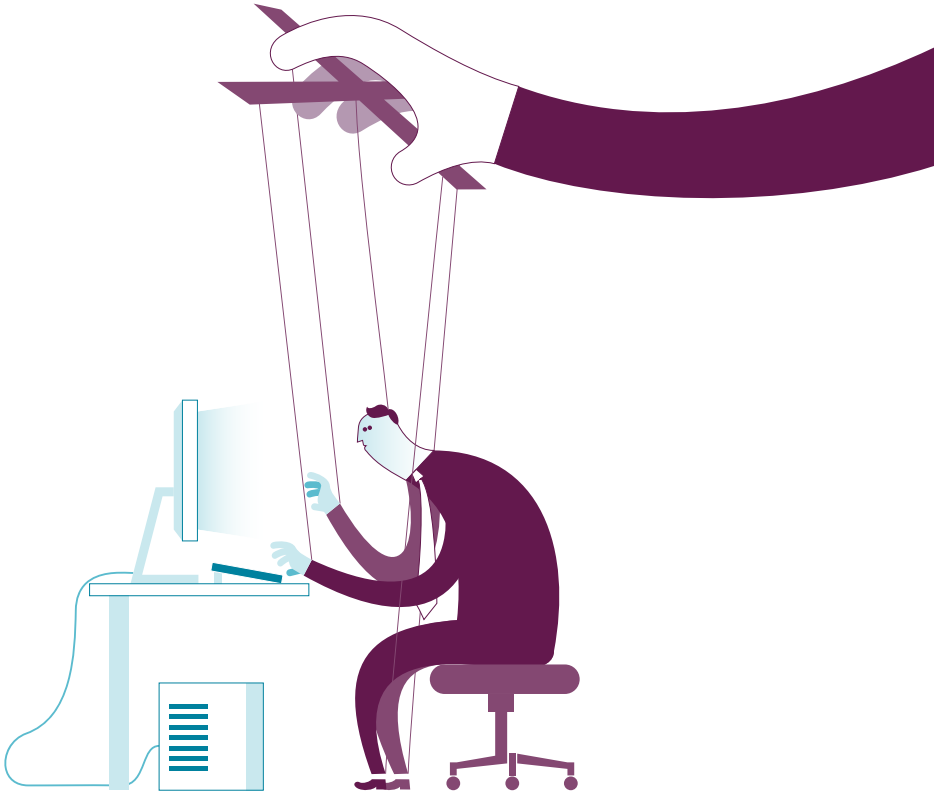
For større virksomheter med egen IT-

avdeling, anbefaler vi å se til NSMs tiltak for grunnsikring mot skadevare.[6] I tillegg er det viktig å ha sikkerhetsovervåking og sikkerhetstesting for å kunne oppdage hendelser og begrense skade. Dersom dere benytter ekstern IT-leverandør, anbefaler vi at dere diskuterer med dem hvordan denne typen svindel kan avverges og oppdages teknisk.

Hvis uhellet er ute

Sikre alle relevante elektroniske spor, og anmeld forholdet til politiet. Meld fra til alle involverte aktører som IT-leverandør, andre kunder som er eller kan være berørt og eventuelt også forsikringsselskap. Forsøk å få oversikt over omfanget av skaden. Hvem har uautorisert eller har hatt uautorisert tilgang til hvilke av virksomhetens systemer, hva er det brukt til og når. Dersom opplysninger er på avveier, meld fra til alle riktige instanser, for eksempel myndighetsorganer og de berørte. Dersom personopplysninger er på avveier må dere vurdere om det skal meldes til Datatilsynet.

6 Nasjonal sikkerhetsmyndighet: «*Grunnprinsipper for IKT-sikkerhet*» https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/



UHELL, UAKTSOMHET (VANVARE)

HVA ER DETTE?

Vanvare er når ansatte, ledere eller privatpersoner gjør feil som får, eller kan få, store konsekvenser. Den stadig økende bruken av teknologi og nettverkstilkoblede enheter stiller større krav til oss som brukere av teknologi. Jo mer kompleks teknologien blir, jo større krav stilles det til kompetanse for å bruke denne. En utfordring er at mange ikke vet hvordan de selv kan redusere risikoen for å gjøre feil. Mange er heller ikke i stand til å oppdage at de har gjort en feil. Vanvare eller uaktsomhet kan også føre til at opplysninger kommer på avveier, endres eller blir utilgjengelig.

HVEM KAN STÅ BAK?

Alle som bruker teknologi, og særlig nettverkstilkoblende enheter i jobb eller privat sammenheng.

HVORDAN UTFØRES DETTE?

Dette er rene uhell eller feil. Det kan skyldes mangel på kunnskap eller forståelse eller begge deler. Et eksempel på en slik hendelse er å ikke bytte et standardpassord for en printer, ventilasjonssystem, ruter eller noe annet. For mange slike enheter er det allment kjent hva standardpassordet som enheten leveres med er. Det kreves kun et raskt nettsøk for å finne det. Dersom det ikke endres og en i tillegg synkroniserer enheten opp mot en skytjeneste, kan uvedkommende få tilgang til andres data gjennom tilgang til enheten som benytter standardpassordet. En annen vanlig feil, er å trykke på lenker eller åpne vedlegg med makroer i e-post. Disse fører til at PC-en infiseres med skadevare, for eksempel virus. Lav bevissthet om digitale trusler gjør oss også mer sårbare for sosial manipulering. Det vil si at noen forsøker å lure deg til å oppgi brukernavn og passord eller på annen måte gi dem tilgang til systemer, e-post, løsninger, apper eller lignende. Denne typen hendelser kan også gjøre enkeltpersoner eller ansatte sårbare for utpressing eller digital trakassering.

HVA ER MÅLET MED DETTE?

Dette er ikke bevisste handlinger. Likevel kan det få store konsekvenser for de som rammes. Det er derfor viktig å inkludere håndtering av denne typen hendelser i en risikovurdering.

HÅNDTERING

Forebyggende tiltak

Alle virksomheter bør legge vekt på digital sikkerhetskultur og sørge for god sikkerhetsopplæring av alle ansatte og ledelse i en virksomhet. Både generell opplæring og opplæring i de systemene eller løsningene de ansatte bruker. I tillegg har myndigheter, virksomheter, akademia og alle sektorer et ansvar for å bidra til teknisk opplæring, kompetansebygging og god sikkerhetskultur i hele samfunnet. Vi bør ha gode forbilder innen digital sikkerhet, både på arbeidsplassen vår og i samfunnet forøvrig.

Hvis uhellet er ute

Begrens skaden så langt det lar seg gjøre. Sørg for å lage en oversikt over hvem som kan ha blitt berørt av feilen og meld fra til disse. Kontakt de ansvarlige som kan hjelpe deg, for eksempel IT-ansatte, IT-leverandører, politiet, kunder, leverandører og eventuelt ansvarlige myndigheter. Vurder å anmelde saken til politiet. Dersom personopplysninger er på avveier må dere vurdere om det skal meldes til Datatilsynet.

ID-TYVERI

HVA ER DETTE?

Å utgi seg for å være en annen og gjennom dette forsøke å anskaffe, overføre, besitte eller erverve tjenester, varer, økonomiske goder eller andre fordeler. Ved å bruke noens identitetsbevis, tilgang til systemer eller kontoer eller annen personlig informasjon utgir man seg for å være rette eier av dette. Hensikten kan være alt fra å bestille varer eller tjenester i noens navn til å påføre noen skade utfra et ønske om hevn. For de som rammes er dette ofte svært alvorlig. Oppryddingen er tidkrevende, psykisk belastende og det kan være krevende å bli trodd og å bevise egen uskyld. Ofrene opplever at andre har kontroll over deres liv. I mange tilfeller er personnummeret en del av informasjonen som er på avveier. Dette er det ikke mulig å sperre for å unngå videre misbruk. Dermed er det en åpen mulighet for at svindlerne kan gjenta misbruket av identiteten. Det gjør at offeret aldri vet når neste svindel mot egen identitet kan skje.

HVEM KAN STÅ BAK?

Det kan være kriminelle som ikke har noen relasjon til offeret, men også personer som har tilgang til informasjon for eksempel slekt, partner, naboer eller andre i nær omgangskrets. NorSIS erfarer dessverre at flere ID-tyveri utføres av folk i nær relasjon til offeret. I noen tilfeller er motivet hevn. NorSIS kjenner til saker der ekskjærester eller andre ønsker å ramme noen som hevn. Når virksomheter rammes kan det være utfra et ønske om å ramme dem økonomisk eller å få tilgang til andre verdier virksomheten har. Et eksempel er en sak der noen, ved hjelp av blant annet en virksomhets organisasjonsnummer, bestilte varer til fiktive byggeplasser eller andre steder de kunne hente varene.

HVORDAN UTFØRES DETTE?

Alle metoder som kan gi tilgang på informasjon som gjør at noen kan utgi seg for å være en annen, vil eller kan benyttes i et ID-tyveri. Eksempler på dette er snoking i andres post eller e-postkasser, tilgang til andres PC, mobiltelefon eller nettbrett eller snoking i en virksomhets filstruktur, fag- eller økonomisystem eller felles arbeidsverktøy. I noen tilfeller samles det også inn opplysninger gjennom nett- eller SMS-phishing, sosial manipulering og kartlegging gjennom sosiale medier og andre åpne kilder. I tillegg er informasjon som har kommet på avveier også en potensiell kilde for en ID-tyv. Stjålne eller mistede førerkort, pass eller bankkort kan være utgangspunktet for et ID-tyveri. Slike dokumenter omsettes også gjerne på svartebørs.

HVA ER MÅLET?

Skaffe seg nok informasjon til å ramme enkeltpersoner enten som privatpersoner eller som ansatt i en virksomhet. I noen tilfeller er målet å ramme en virksomhet gjennom misbruk av organisasjonsnummer. Målet er å oppnå fordeler på bekostning av ID-tyveriofferet. Konsekvensen av dette er som regel økonomisk tap, ærekrenkelse, hevn og gjentagende misbruk av stjålet identitet. Det er sjeldent enkeltpersoner som utsettes for ID-tyveri opplever økonomisk tap. Økonomiske tap går heller utover virksomheter som svindles gjennom ID-tyveri. Samtidig opplever mange ofre sosiale og psykiske utfordringer fordi de ikke lenger har kontroll over egen identitet.

HÅNDTERING

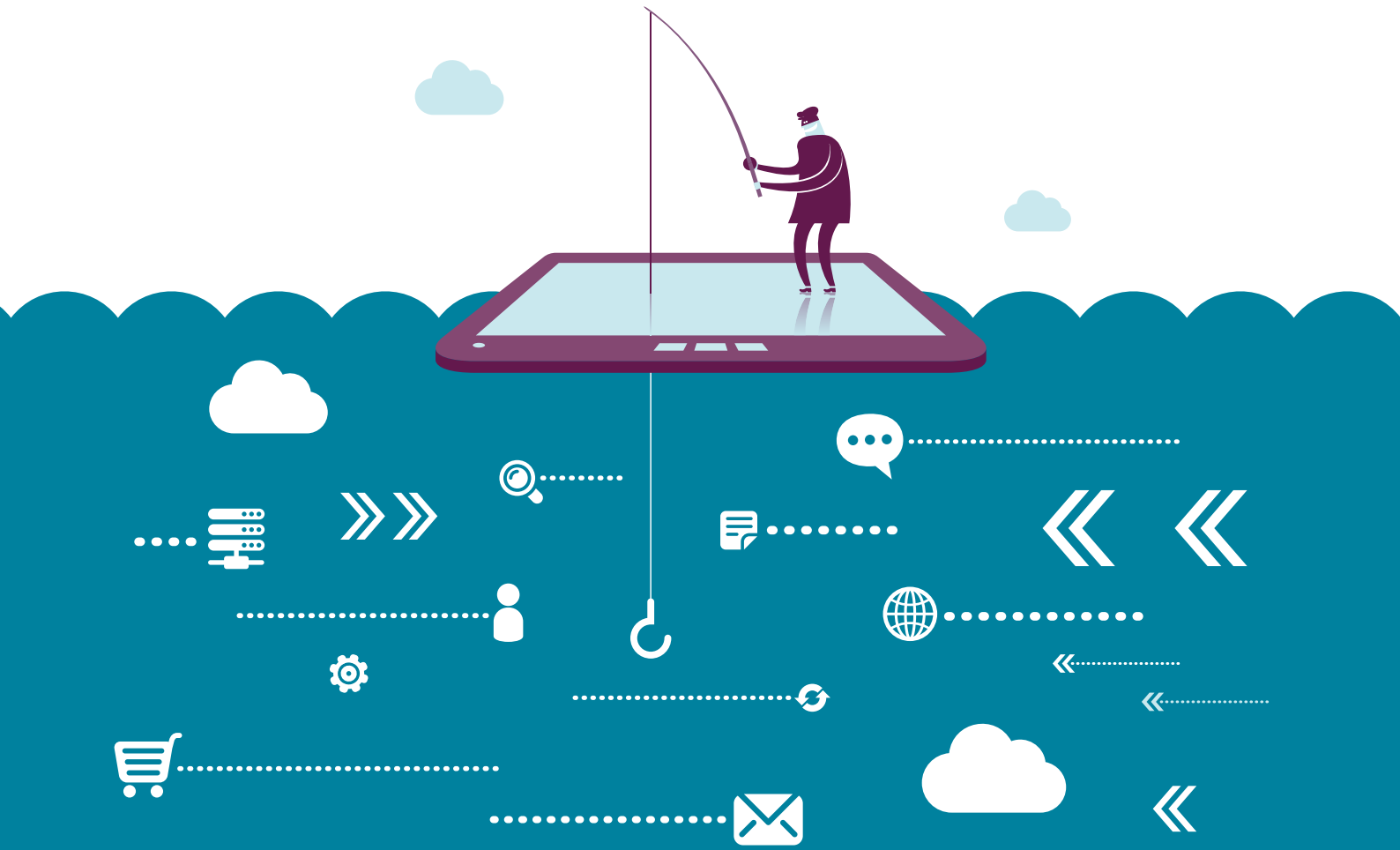
Forebyggende tiltak

Sørge for å sikre digitale kontoer best mulig for å forhindre at uvedkommende får tilgang til informasjon, for eksempel ved å aktivere totrinnsbekreftelse for pålogging. Vær forsiktig med hvem du oppgir personlig informasjon eller virksomhetsinformasjon til. Sørge for å sette seg inn i og å lære opp de ansatte i digital sikkerhet. Da vil de lettere kunne avdekke forsøk på å få tilgang til opplysninger som kan benyttes i et

ID-tyveri. Sørg for å få minst mulig verdipost i postkassa. Bruk digitale postkasser og vær oppmerksom på phishing. Vær også nøye med å ikke publisere bedriftssensitiv informasjon i åpne kanaler.

Hvis uhellet er ute

Sikre alle relevante spor. NorSIS anbefaler å anmelde forholdet til politiet. En anmeldelse er det eneste bindende juridiske dokumentet for å kunne bestride eventuelle krav mot ens person. Varsle banken, forsikringsselskap og andre steder du har konto eller som ID-tyven kan tenkes å kontakte eller misbruke i ditt navn. Følg med på om posten din kommer som normalt og at det ikke gjøres kredittsjekker i ditt navn. Det er mulig å sperre seg for kredittvurdering hos kredittopplysningsselskapene for å unngå dette. Det bidrar til å forhindre at noen kan opprette abonnement eller ta opp lån, åpne kontoer eller lignende i ditt navn. I en virksomhet, gå gjennom alle tilganger som kan være komprimert, be alle bytte passord eller ta andre nødvendige forholdsregler.



SVINDEL (INKLUDERT DATINGSVINDEL)

HVA ER DETTE?

Svindel omfatter alle forsøk på å lure noen til å oppgi passord, konto-, bruker-, pålogging eller annen informasjon, passord eller noe annet som kan misbrukes. Hensikten kan være alt fra å oppnå rask økonomisk vinning gjennom misbruk av et kredittkort, til å forsøke å ramme en virksomhet eller noen i dennes verdikjede, for egen vinning. Det vil si å angripe for eksempel en underleverandør eller kunde av den virksomheten en egentlig ønsker å nå. Ved å komme seg inn i underleverandørens e-post eller andre systemer kan angriperne få tilgang til virksomheten de ønsker å nå.

HVEM KAN STÅ BAK?

Kriminelle som selv skal misbruke informasjonen, kriminelle som ønsker å videreselge informasjonen eller noen i omgangskretsen.

HVORDAN UTFØRES DETTE?

Det finnes svært mange svindelmetoder og disse er også i konstant utvikling. Ofte er metodene lett tilgjengelige og billige å bruke for svindlerne. På den måten kan de oppnå stor vinning med lav økonomisk og ressursmessig innsats. I noen svindelsaker benyttes e-post, SMS eller sosiale medier. Andre ganger mottar offeret falske henvendelser om oppdatering av konto- eller betalingsinformasjon eller falske konkurranser der man fisker etter opplysninger om kontonummer eller kredittkort. Mange av disse svindelsakene misbruker kjente logoer som mange av oss har et forhold til, for å gi et inntrykk av at de er ekte. Noen svindelsaker spiller på sesongrelatert adferd. For eksempel dukker det ved juletider som regel opp en rekke svindelsaker knyttet til uavhentede pakker. I forbindelse med skatteoppgjøret opplever mange falske meldinger fra Skatteetaten om at de har fått igjen penger på skatten.

Mange virksomheter utsettes også for såkalt «spear phishing» som er en mer avansert phishing-metode rettet mot en spesiell bedrift eller ansatt. I tillegg kan metoder som snoking i søppel- eller postkasse og sosial manipulering benyttes både mot virksomheter og privatpersoner.

Ved datingsvindel brukes som regel andre metoder. I slike tilfeller spilles det på tilliten som er bygd opp, gjerne over lang tid. Ved hjelp av sosiale medier, utspekulert sosial manipulering og ofte tett kontakt i private kanaler, bygges det opp en historie som legger opp til at offeret skal sende penger eller gi fra seg betalingsinformasjon. Summene er ofte små til å begynne med, men øker ettersom offeret betaler. Ofrene for datingsvindel er gjerne godt voksne med profiler i sosiale medier eller på datingsider.

HVA ER MÅLET MED DETTE?

Svindel er som regel masseutsendt og rammer tilfeldige ofre. Målet er økonomisk vinning, enten det er snakk om masseutsendte forsøk som rammer tilfeldige ofre, eller mer målrettede forsøk som er mer tids- og ressurskrevende.

VIRKEMIDLER I SVINDELSAKER

NorSIS opplever at de aller fleste varianter av svindel i hovedsak spiller på tre ulike faktorer, frykt, fristelse eller tillit. Dette er klassisk psykologi og benyttes nettopp fordi det er så virkningsfullt for å overbevise mottagerne til å handle slik angriperen ønsker.

Tillit
Dette er det vanskeligste å beskytte seg mot, om du f.eks. får noe tilsendt fra det som ser ut til å være noen du kjenner eller noen du stoler på. I slike tilfeller blir gjerne skepsisen borte. I slike tilfeller er det viktig å spørre seg selv om dette er naturlig for vedkommende. Kjente merkenavn blir ofte utnyttet i konkurranser eller lignende.

Hvis du opplever at noen spiller på en, eller en kombinasjon av disse tre faktorene, samtidig som at de forsøker å få deg til å gjøre noe. For eksempel å trykke på en lenke, installere noe, eller gi fra deg informasjon, så bør du være skeptisk.

Både privatpersoner og virksomheter rammes.

Konsekvensene av personutpressing kan være store, både økonomisk, sosialt og psykologisk. NorSIS kjenner til datingsvindelsaker der offeret har gått personlig konkurs.

HÅNDTERING

Forebyggende tiltak

Siden det finnes svært mange svindelmetoder er det vanskelig å liste opp alt en kan gjøre for å forebygge dette. En generell årvåkenhet vil kunne hjelpe for å oppdage svindelforsøkene og stanse svindelen før den rammer. For å sikre overføring av e-post mellom e-posttjenere, anbefales det å benytte DMARC. NSM har gode veiledninger for hvordan dette gjøres.[7] I tillegg er det viktig å aktivere totrinnsbekreftelse på alle digitale kontoer, systemer og annet en bruker, både privat og på jobb. Det er også viktig å sjekke om avsenderen er den han eller hun utgir seg for å være, unngå å klikke på lenker du synes er mistenkelig eller ikke kjenner avsender av. Vær skeptisk når noen ber deg oppgi personopplysninger, økonomiske opplysninger eller andre opplysninger i skjema eller på nettsider du kommer til fra lenker du får i e-post eller på SMS. Særlig hvis du ikke selv har tatt initiativ til å ta kontakten. Sørg også for at alle ansatte får god opplæring i hvilke trusler de kan møte, både på jobb og privat. Gi dem også opplæring i hvordan de skal håndtere disse truslene. Dersom et tilbud er for godt til å være sant, er det som regel det.

Dersom man er utsatt for datingsvindel er det viktig å kjenne til at dette eksisterer og gjerne også de vanligste metodene som benyttes. En rekke kampanjer i sosiale medier og mediedekning av slike saker har bidratt til å vise at dette er et fenomen den siste tiden. Det kan bidra til at flere som opplever dette søker hjelp eller anmelder saken til politiet.

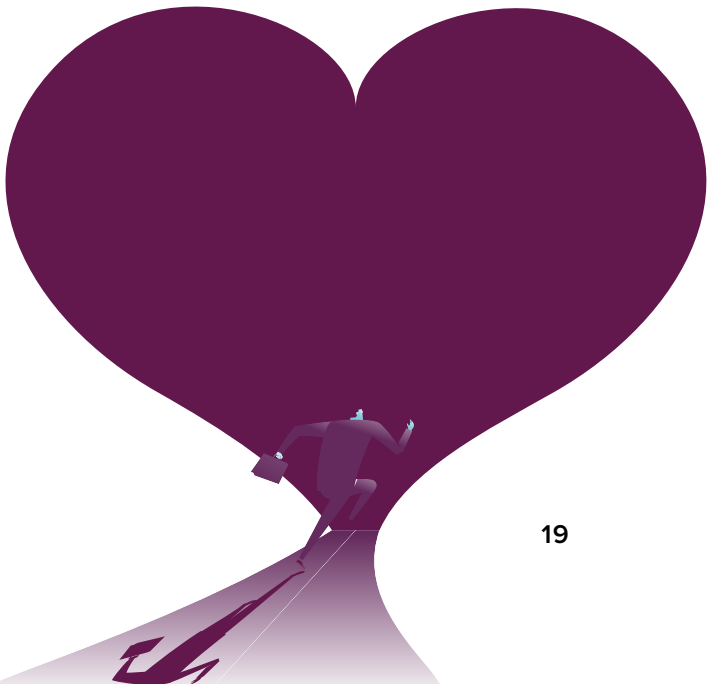
Fristelser
Kan typisk være tilbud om gratis programvare, spill eller lignende. Det er også vanlig med e-poster som oppgir at du har vunnet et større beløp penger, eller andre former for henvendelser hvor det lokkes med seksuelle tilbud.

Frykt
Svindleren forsøker ofte å skremme deg til å gjøre noe. For eksempel kan det dukke opp varsler på skjermen når du surfer, om at det er oppdaget virus på maskinen/mobilen din. For å bli kvitt problemer må du installere et falskt antivirusprogram. Svindlere bruker også ofte frykt for å skape en følelse av dårlig tid og hastverk. Poenget med det er å få deg til å forhaste deg og gjøre som svindlerne vil uten å ta deg tid til å tenke deg om.

HVIS UHELLET ER UTE

Sikre digitale spor, og vurder å anmelde saken til politiet. Forsøk å få best mulig oversikt over hva som har skjedd og eventuelt hvilke opplysninger som er, eller kan være på avveier eller i «gale» hender. Meld fra til de som kan være involvert, som kunder, brukere, leverandører og andre.

7 Nasjonal Sikkerhetsmyndighet: *«Sikrere epost med DMARC»* https://nsm.stat.no/aktuelt/dmarc/



Hello!

I'm a programmer who cracked your email account and device about half year ago.
You entered a password on one of the insecure site you visited, and I catched it.
Your password from [redacted] on momeny of [redacted]

Of course you can will change your password, or already made it.
But it doesn't matter, my rat software update it every time.

Please don't try to contact me or find me, it is impossible, since I sent you an email from your email account.
Through your e-mail, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the internet resources.
Also I installed a rat software on your device and long tome spying for you.

You are not my only victim, I usually lock devices and ask for a ransom.
But I was struck by the sites of intimate content that you very often visit.

I am in shock of your reach fantasies! Wow! I've never seen anything like this!
I did not even know SUCH content could be so exciting!

So, when you had fun on intime sites (you know what I mean!)
I made screenshow with using my program from your camera of yours device.
After that, I joined them to the content of the currently viewed site.

Will be funny when I send these phots to your contacts! And if your relatives see it?
BUT I'm sure you don't want it. I definitely would not want to ...

I will not do this if you pay me a little amount.
I think $819 is a nice price for it!

I accept only Bitcoins.
My BTC wallet: [redacted]

If you have difficulty with this - Ask Google "how to make a payment on a bitcoin wallet". It's easy.
After receiving the above amount, all your data will be immideiately removed automatically.
My virus will also will be destroy itself from your operating system.

My Trojan have auto alert, after this email is looked, I will be know it!

You have 2 days (48 hours) to make a pament.
If this does not happen - all your contacts will get crazy shots with your dirty life!
And so that you do not obstruct me, your device will be locked (also after 48 hours)

Do not take this frivolously! This is the last warning!
Various security services or antiviruses won't help you for sure (I have already collected all your data).

Here are the recommendations of a professional:
Antiviruses do not help against modern malicious code. Just do not enter your passwords on unsafe sites!

I hope you will be prudent.
Bye.

UTPRESSING

HVA ER DETTE?

Kriminelle presser enkeltpersoner for å tjene penger eller til å utføre handlinger vedkommende normalt ikke ville ha gjort. Den kriminelle bruker for eksempel opplysninger, lydopptak, filmer eller bilder av offeret som middel for utpressingen. NorSIS er kjent med at det brukes film og bilder som er tatt i situasjoner der offeret er naken eller i en kompromitterende situasjon. Mange ofre plukkes ut fra datingsider, sosiale medier eller andre nettsteder. Nettopp fordi de er på søken etter nye bekjentskaper. I noen tilfeller blir den som utsettes for svindelen smigret over at en flott kvinne eller mann plutselig tar kontakt.

HVEM KAN STÅ BAK?

Noen som er i en posisjon der de kan utnytte noen for egen vinning eller tilfredsstillelse.

HVORDAN UTFØRES DETTE?

Hvordan dette utføres kommer i an på hva som brukes som pressmiddel, og hvem som står bak utpressingen. I hovedsak dreier det seg om metoder der svindleren viser at hun eller han har psykisk overtak over noen for å få utbetalt penger, utført seksuelle tjenester, tilgang til informasjon eller noe annet. I noen tilfeller har utpresseren funnet materiellet som brukes mot offeret på nett eller i andre åpne kanaler. Andre ganger er materialet høstet gjennom phishing eller dataangrep. Dersom offeret ikke betaler, trues det med at materialet vil spres på nett, i kontaktnettverk, i sosiale medier eller andre kanaler. Som regel spiller utpresseren på flauhet, tabu og skam knyttet til en mulig avsløring av materialet han eller hun har. Henvendelser til NorSIS viser at utpressing ved hjelp av nakenbilder som regel rammer ungdom og helst jenter. Video-opptak over Skype eller andre kanaler, der det er gjort opptak uten at offeret er klar over det, rammer ofte, men ikke utelukkende menn.

Enkelte ofre for datingsvindel har opplevd at de blir presset for penger dersom de nekter å betale, eller ikke er i stand til å betale. Utpresseren kan komme med fysiske eller andre trusler. I noen tilfeller, der et offer for datingsvindel har mottatt penger fra svindleren som igjen har blitt overført til en annen konto, opplever offeret å blir truet med å meldes til politiet for mistanke om hvitvasking. Enkelte ofre har, etter å ha opplevd dette skiftet kontonummer for å hindre at svindleren overfører penger til deres konto. Dette gir svindlere et psykisk overtak.

HVA ER MÅLET MED DETTE?

Utpressing gjøres for å tjene penger på å utnytte enkeltpersoner eller virksomheter. Det rammer ofte mennesker i en sårbar situasjon. Ofrene treffer utpresserne i kjente kanaler som datingsider eller sosiale medier. Ledere bør vite at ansatte som opplever utpressing kan settes i vanskelige situasjoner. I ytterste konsekvens kan utpressing føre til underslag eller andre former for sikkerhetsbrudd i virksomheten.

HÅNDTERING

Forebyggende tiltak

Det er til en viss grad mulig å begrense utpressing ut fra bilder eller materiell på nett eller i åpne kanaler, ved å oppfordre ansatte eller andre til å bruke bedre sikrede eller lukkede kanaler for å dele slikt materiell. Å sørge for å ha ulike passord på alle tjenester og systemer man bruker, er også et viktig tiltak. I tillegg bør totrinnsbekreftelse aktiveres. Å ta opp dette som en problemstilling på skoler, nett og i media med jevne mellomrom, kan også bidra til å gjøre flere oppmerksomme på at dette foregår. Det er også viktig at vi alle er kritiske til hvilke motiver noen har for å ta kontakt med oss på nett.

Hvis uhellet er ute

Avbryt all kontakt med utpresserne, og anmeld forholdet til politiet. Kontakt banken din, i hvert fall hvis du har gitt fra deg informasjon som kan brukes mot deg, for eksempel til økonomisk misbruk i fremtiden. Mange personutpressingssaker er så profesjonelt og utspekulert utført, at det er svært vanskelig å oppdage at man er offer for utpressing. NorSIS mener at det er viktig å møte dem som blir rammet med forståelse fremfor fordømmelse. Alle kan utsettes for svindel når situasjon og metode kombineres på riktig måte.

KRENKELSER (MOBBING)

HVA ER DETTE?

Krenkelser er trakassering, mobbing og overgrep mot enkeltpersoner. Noen blir ofre på grunn av tilfeldigheter, noen fordi de er utpekt eller valgt som offer og andre fordi de jobber et spesielt sted eller har et særskilt yrke. Gjerningspersonen har gjerne personlige grunner til å krenke offeret. Målet er å påføre offeret ubehag eller å begå overgrep mot offeret. Overgrep er særlig knyttet til seksualiserte handlinger utført på nett under tvang eller manipulasjon. Nettovergrep kan noen ganger føre til fysiske møter med fysiske overgrep.

HVEM KAN STÅ BAK?

Krenkelser kan begås av ukjente personer eller personer som kjenner eller har en relasjon til offeret. Krenkelser kan også rettes mot bedrifter, for eksempel av aktivister, brukere eller kunder som er misfornøyde med en service eller med virksomheten generelt.

HVORDAN UTFØRES DETTE?

Krenkelser kan skje gjennom spredning av ondsinnede karakteristikker, falske påstander, åpen eller anonym mobbing eller ved at noen sprer bilder eller annet materiale knyttet til offeret på nett. Noen ganger benyttes materiale eller informasjon som er hentet inn gjennom spionvare, sosial manipulering, åpent tilgjengelig informasjon. Andre ganger har krenkeren eller mobberen selv tatt bilder eller filmen som brukes.

Når virksomheter eller enkelte ansatte som rammes av dette, skjer det gjerne gjennom sosiale medier eller andre nettsteder. Det kan for eksempel være en enkeltperson eller en gruppe mennesker som publiserer ulike påstander, anklagelser eller annet. I endel tilfeller kan det være vanskelig for den eller de som utsettes for dette å imøtegå påstanden. Enten på grunn av nivået eller omfanget av påstandene eller at det å svare på påstanden vil utlevere andre involverte parter. I noen tilfeller, for eksempel inne helsesektoren eller barnevernet, har den eller de ansatte taushetsplikt. Det hindrer dem å svare på påstander som fremsettes om dem. Enkelte nettsteder legger til rette for kanaler der yrkesgrupper vurderes av enkeltpersoner, kunder, pasienter eller brukere. Her er det som regel ikke rom for den enkelte som blir vurdert å få svare på det som fremsettes om han eller hun. Dette stiller krav til redaktørene for slike plattformer. De må sørge for å hindre at dette blir en kanal for krenkelse og mobbing.

HVA ER MÅLET MED DETTE?

Noen rammes tilfeldig og noen rammes på grunn av sitt forhold til den som krenker. Andre rammes på grunn av sin jobb, profesjon, makt, stilling eller rolle. Angrepet kan skyldes hevn, skuffelse, håndtering av ulike saker eller i noen tilfeller hva den ansatte utfører av oppgaver i sin stilling.

HÅNDTERING

Forebyggende tiltak

Det er svært viktig å bygge tillitsforhold til barn og unge slik at de sier ifra til noen, fortrinnsvis en voksen, dersom de opplever krenkelser eller andre ubehageligheter på nett. Også for denne typen hendelser er det viktig å løfte det opp i riktige kanaler. Både på skoler, utdanningsinstitusjoner, i mediene og i samfunnsdebatten forøvrig må dette løftes opp. Da blir vi alle blir klar over at dette foregår. Det er også viktig at voksne er gode eksempler med tanke på hvordan vi omtaler andre og hva vi publiserer om andre på nett. NorSIS mener at det er en utfordring at kommentarfelt på nettaviser, i sosiale medier og andre steder ser ut til å ha fått en «tøffere» tone enn tidligere. Det sender feil signaler til yngre mennesker når voksne er ufine mot hverandre på nett.

Virksomheter bør lage retningslinjer for

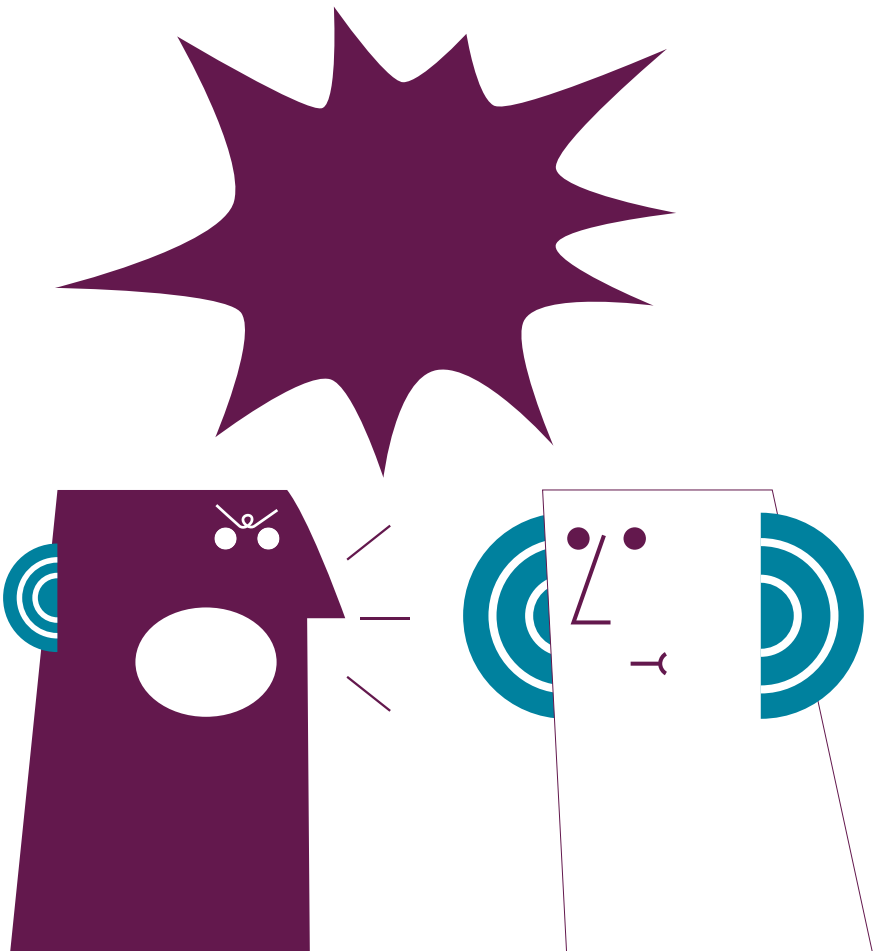
6 Nasjonal sikkerhetsmyndighet: *«Grunnprinsipper for IKT-sikkerhet»* https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

hvordan de beskytter, håndterer og følger opp hendelser der de ansatte opplever dette. De bør også ha policyer og rutiner for hvordan de skal håndtere krenkelser som rammer virksomheten eller de ansatte.

Hvis uhellet er ute

Sikre alle relevante digitale spor, og vurder å anmelde forholdet til politiet. Husk å ta bilde av skjermen dersom krenkelsene fremsettes i apper som Snapchat. Der forsvinner de ellers etter kort tid. Det er viktig at særlig barn og ungdom har noen å snakke med om hva som har skjedd og hva de kan eller bør gjøre. Ta det opp med vedkommende eller si i fra til foresatte dersom du oppdager at noen du kjenner utsettes for dette.

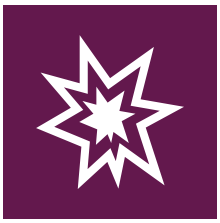
I virksomhetens rutiner for oppfølging av slike hendelser bør det være klart hva som skal gjøres og hvem som skal gjøre det. Å anmelde saken til politiet og å sørge for å støtte den ansatte er to viktige oppgaver i håndteringen av slike saker.



SABOTASJE

HVA ER DETTE?

Forsøk på å ramme virksomheter gjennom å påvirke eller sette systemer, produksjonsanlegg eller kommunikasjonskanaler ut av drift. Motivasjonen kan være å svekke virksomhetens evne til å levere sine tjenester eller produkter. Det kan også være å sette seg selv i en fordelaktig posisjon. Sabotasjen kan være et ledd i en et større angrep som har politiske motiver. Det kan for eksempel være å svekke samfunnet, nasjonal infrastruktur eller virksomhetens omdømme.



HVEM KAN STÅ BAK?

Slike angrep kan utføres av kriminelle, politiske aktivister, terrorister, utro tjenere, vandaler, hevngjerrige eller fremmede stater.

HVORDAN UTFØRES DETTE?

Det benyttes ulike metoder for å sabotasje. Noen eksempler er å slette informasjon, å endre informasjon, å endre konfigurasjon på system, å ødelegge system for eksempel gjennom sosial manipulering, hacking, datainnbrudd, virus og malware, phishing, eller tjenestenektangrep, doxing, Bitcoin mining eller defacing.

HVA ER MÅLET MED DETTE?

Motivene for denne typen angrep er først og fremst avhengig av hvem som utfører det. Det kan være et ønske om å forskyve markedsposisjon, svekke omdømme, skaffe seg informasjon om andre stater eller konkurrenter, skaffe seg konkurransefortrinn, markere territorium eller standpunkt i politisk sak. Det kan også handle om å skaffe seg økonomiske fordeler (Bitcoin mining) eller å ramme noens virksomhet for å fremme egen virksomhet. I dagens samfunn er det å alltid være tilgjengelig for kunder, brukere, leverandører, myndigheter eller andre noe av det viktigste for en virksomhet. Det er derfor svært alvorlig dersom en virksomhets tilgjengelighet rammes, som ofte er tilfellet ved sabotasje.

HÅNDTERING

Forebyggende tiltak

Alle virksomheter må ha god oversikt over egne verdier, verdikjeden de er en del av og hvem som er deres potensielle trusselaktører. Dette bør inngå i virksomhetens risikovurdering. Denne bør ligge til grunn for bedriftens sikkerhetsrutiner og for metodene som brukes for å sikre integritet, tilgjengelighet og konfidensialitet i virksomheten. For virksomheter med egen IT-avdeling og leverandører av IT-tjenester, bør NSMs tiltak for grunnsikring mot skadevare følges.[8] I tillegg bør det gjennomføres sikkerhetsovervåking og sikkerhetstesting for å avdekke hendelser og begrense mulige angrep.

Hvis uhellet er ute

Vurder å anmelde forholdet til politiet. Meld fra til alle berørte og andre som trenger å informeres om det inntrufne. Virksomhetens rutiner for håndtering av denne typen hendelser bør inkludere en plan for hvordan slike tilfeller skal håndteres.

8 Nasjonal sikkerhetsmyndighet: *«Grunnprinsipper for IKT-sikkerhet»* https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

SIKKERHET PÅ REISE

HVA ER DETTE?

Adferden og omgivelsene våre endres når vi er på reise. Det kan gjøre oss mer utsatt for uvedkommende som enten ønsker å få tilgang til informasjon vi har med oss, eller som på andre måter ønsker å svindle oss. Det er også vanskeligere for oss å kontrollere omgivelsene våre når vi er på reise.

HVEM KAN STÅ BAK?

Kriminelle med økonomisk vinning som motiv eller andre lands etterretning.

HVORDAN UTFØRES DETTE?

Når man er på reise befinner man seg ofte i områder som er teknisk kontrollert av andre. De som har teknisk kontroll over et område kan ha tilgang til besøkendes anrops- og SMS-logger og kan eventuelt også avlytte den besøkende. Dersom uvedkommende får tilgang til våre digitale enheter, som mobiltelefon og PC, kan de koble på ekstern mobil skadevare. Denne kan gi dem tilgang til innholdet på den kompromitterte enheten. På reise vil en kunne utsettes for overvåking eller gjennomsøkning av bolig, hotellrom, bagasje og kartlegging av hvem en treffer, hvor en befinner seg og annen oppførsel. Dette kan selvsagt skje hjemme også, men når en er på reise kan det være vanskeligere å legge merke til at en kartlegges fordi man er på et mindre kjent eller helt ukjent sted. Det er også en risiko for å utsettes for verving fra spioner. I noen tilfeller kan de som står bak forsøke å lure den reisende inn i kompromitterende situasjoner som kan brukes mot den reisende senere. For eksempel at en politiker oppsøker et bordell.

HVA ER MÅLET MED DETTE?

Denne typen trussel rammes man ofte av på grunn av sitt arbeidssted eller oppgaver. Det gjelder særlig dersom den som utfører overvåking, kartlegging eller informasjonstyveri er ute etter en særlig type informasjon eller opplysninger. I andre tilfeller er den som rammes et tilfeldig offer. Andre igjen rammes på grunn av sin nasjonalitet. Nordmenn og vest-europeere er kjent for å ha god økonomi som kan tilsi at de er gode potensielle ofre for svindlere.

HÅNDTERING

Forebyggende tiltak

Gjør en vurdering av hvor du skal reise og hvilke digitale enheter du absolutt må ha med deg. Tenk også gjennom hva du har lagret på disse enhetene. Ha det som et utgangspunkt at du kan være et mål. Både når du er på internett og der du befinner deg på reise. Det er en god ide å kryptere informasjonen du har med deg, samt å slå av blåtann og trådløs forbindelse. Det gjør det vanskeligere å nå deg. Bruk også andre sikkerhetsmekanismer som for eksempel VPN-løsninger når det er tilgjengelig. Når du kommer hjem bør du be eksperter sjekke enhetene dine. Du bør også endre alle passordene dine dersom de skulle ha blitt fanget opp. En bør også følge UD[9] og NSM[10] sine reiseråd.

Hvis uhellet er ute

Meld fra til arbeidsgiver hvis du mistenker at enheter du bruker i jobb kan ha blitt kompromittert. Vær spesielt oppmerksom på e-poster med vedlegg du mottar i ettertid av reiser. Dersom du oppdager at du er svindlet, anmeld saken til politiet og meld fra til bank, forsikringsselskap og andre du tenker kan bli kontaktet av de som har eller har hatt tilgang til informasjonen din.

9 Regjeringen.no: *«Utenriksdepartementets reiseinformasjon»* https://www.regjeringen.no/no/tema/utenrikssaker/reiseinformasjon/id2413163/

10 Nsm.no: *«Noen råd om informasjonssikkerhet på reise»* https://www.nsm.stat.no/aktuelt/noen-rad-om-informasjonssikkerhet-pa-reise/

SPIONASJE

HVA ER DETTE?

Forsøk på å få tilgang til, sikre eller hente ut informasjon fra en virksomhet, nasjonalstat eller andre. Gjennomføring av phishing eller sosial manipulering rettet mot ansatte i utvalgte virksomheter.

HVEM KAN STÅ BAK?

Konkurrenter, kriminelle, statlig etterretning, hacktivister, terrorister.

HVORDAN UTFØRES DETTE?

Få tilgang til i systemer via skadevare (malware), virus, hacking, datainnbrudd, phishing eller andre operasjoner. Utnytte sårbarheter i systemer eller programvare for å komme inn i dette. Sosial manipulering for å skaffe seg informasjon som kan brukes for å få tilgang til eller inn i en virksomhet. Samle eller spre informasjon i sosiale medier.

HVA ER MÅLET MED DETTE?

Målet kan være å ramme virksomheter, stater, konkurrenter eller et land. Det kan også være et mål å ramme en virksomhets infrastruktur. Både offentlige og private virksomheter kan være mål for spionasje. Bakgrunnen kan være økonomisk vinning, å drive etterretning, å forskyve markedsposisjon eller makt. Bakgrunnen for spionasjen kan for eksempel være et ønske om å skaffe seg tilgang til informasjon og forståelse om ny teknologi for å slippe å utvikle noe selv, men heller komme konkurrenten i forkjøpet. For stormakter kan det være et mål å innhente politisk informasjon. Dette kan gjøre at de sikrer seg makt eller styrker sin egen posisjon på bekostning av andre stormakter.

HÅNDTERING

Forebyggende tiltak

Sørge for å holde alle systemer og all programvare oppdatert. Ha god oversikt over verdikjeden, risiko og sårbarheter i denne samt kontinuerlig jobbe for å redusere risiko der det er mulig. Sikre rutiner og systemer for å oppdage og håndtere eventuelle forsøk på spionasje. Jobbe for å ha en god sikkerhetskultur i virksomheten og at den ansatte får opplæring og kompetanse i IKT-sikkerhet. I tillegg bør virksomheten følge NSMs anbefalinger for grunnsikring.[11]

Hvis uhellet er ute

Meld fra til leder umiddelbart hvis dere oppdager spionasje. Følg ellers virksomhetens rutiner for varsling og håndtering av spionasje.

11 Nasjonal sikkerhetsmyndighet: «*Grunnprinsipper for IKT-sikkerhet*» https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

TRUSSELVURDERING

Truslene vi presenterer i årets rapport er ikke ulike de vi så i fjor. Det er kun noen få endringer i lista. Samtidig melder NSM[12] at samfunnet som helhet utsettes for flere og mer komplekse angrep. De oppfatter trusselaktørene som stadig mer målrettede og at angrepene blir stadig mer avanserte, selv om metodene ofte er de samme som tidligere.

I tillegg ser man at truslene «forandrer» seg eller dukker opp i forskjellige avarter. Et eksempel er hvordan løsepengeviruset med utgangspunktet WannaCry ble til Petya og NotPetya i 2017.

NorSIS ser en utvikling i svindel og utpressingssaker, der svindlerne blir mer «profesjonelle». Utpressingsofre opplever at summen de må betale er så lav, at det oppfattes som mer attraktivt å betale enn å søke hjelp eller melde fra. I løsepengevirussaker vil det å betale en relativt lav sum for å få tilbake virksomhetens informasjonsverdier, systemtilganger eller annet, i noen tilfeller oppfattes som rimeligere enn å risikere å miste verdifull informasjon og i ytterste konsekvens måtte legge ned driften. I slike svindelsaker vil det å søke hjelp kunne oppfattes som mer krevende og belastende enn å betale. Et eksempel på dette er en e-post der avsenderen påstår å ha hacket mottakerens PC og filmet vedkommendes surfing på porno. Dersom mottager ikke betaler, truer avsender med å publisere innholdet for familie og venner. For de som mottar e-posten, er det ofte så skambelagt at noen kan offentliggjøre at de har surfet på porno, at de heller betaler enn å stole på at dette kun er svindel og at det derfor ikke finnes noe kompromitterende materiale å spre.

Ut fra henvendelser inn til NorSIS ser det ut til å være en liten nedgang i antall datingsvindelsaker i 2018. Det kan se ut som det er en utvikling mot at det blir færre saker, men med større svindelbeløp per sak. En nedgang i slike saker er gledelig fordi denne typen svindel er svært ødeleggende for de som rammes. Nedgangen kan skyldes mange oppslag og saker om datingsvindel i mediene. Potensielle ofre kan gjennom denne bevisstgjøringen lettere kjenne igjen svindelmetoden om de utsettes for den. Samtidig opplever NorSIS at ofrene for slik svindel ofte oppfattes som «lettlurte» og i noen tilfelles møtes med at «dette burde de ha skjønt». Det er uheldig, både fordi det stigmatiserer ofrene og fordi det gjør at flere kvier seg for å melde fra om slike saker. Det er svært urettferdig mot ofrene. Når en ser hvor store ressurser enkelte svindlere legger i denne typen svindelsaker, for eksempel ved å bygge tillit over lang tid, kan man forstå at svindlerne i noen tilfeller lykkes. Det er samtidig noen tilfeller der NorSIS har sett at datingsvindel går over til å bli en utpressingssak. For eksempel der noen har betalt ut summer til kontoer som er involvert i hvitvaskingssaker eller annen type svindel, brukes det til å presse dem til å betale mer for å unngå at saken meldes til politiet.

ANGREP PÅ ULIKE STEDER KAN GJØRE DET VANSKELIG Å OPPDAGE TRUSLER

Endel trusler arter seg som rene angrep på enkeltpersoner eller organisasjoner. I slike tilfeller er det den enkelte ansatt eller privatpersonen sine handlinger som utgjør sårbarheten. Et eksempler er hvis en ved uhell eller vanvare, for eksempel gir noen tilgang til passord og brukerkontoer. Enten ved å oppgi informasjon i en phishing-kampanje eller kanskje ved å ikke endre et standardpassord for en nettilkoblet enhet. Dette kan i tur gi innpass til andre nettilkoblede enheter.

Vanvare, dårlig sikring av egne enheter eller manglende forståelse av risikobildet kan også ramme oss alle på reise. En oppfører seg annerledes og er gjerne på et ukjent sted. Det kan gjøre det vanskelig å gjenkjenne trusselaktører eller oppfatte at de finnes. De fleste bruker enheter på tvers av roller og oppgaver. En mobiltelefon brukes som regel til alle oppgaver fra jobb og sosiale medier til å logge seg inn i nettbanken. Sommerens mange medieoppslag om at regjeringsmedlemmer og andre politikere har brukt tjenestetelefoner på reise til land med andre styresett enn vårt, er gode eksempler på dette.

Grunnen til at noen virksomheter ram-

12 Nasjonal sikkerhetsmyndighet: *«Et sikkert digitalt Norge – IKT-risikobilde 2018»* https://nsm.stat.no/globalassets/rapporter/nsm_ikt-risikobilde_2018_web.pdf

mes av for digitale angrep kan være at risikovurderingene deres er mangelfulle. For eksempel hvis de ikke har iverksatt kjente og anbefalte tiltak for sikring av systemer, som hindrer kjente angrepsmetoder. Et eksempel på et slikt tiltak er å benytte DMARC eller lignende, for å hindre svindel av e-post. NSM anbefaler dette og beskriver prosessen i sin veileder om sikrere e-post.[13] Telenor sier riktignok i sin årsoppsummering[14] at deres nett i Norge på grunn av god grunnsikring har gått klar av mange slike angrep. For eksempel WannaCry som herjet i svært mange land i 2017. Dette gjelder imidlertid først og fremst virksomheter. Samtidig sier Proofstep i artikkel i Computerworld[15] at resultatet av deres undersøkelse av norske virksomheter, viser at mange er dårlige på implementering av DMARC. Dette understreker hvor viktig det er at alle gjør gode risikovurderinger, og er klar over hvilke tilgjengelige tiltak som eksisterer for å håndtere de risikoene som finnes.

KRITISK NÅR TILGJENGELIGHETEN RAMMES

Både Europol[16] og Cisco[17] fremhever i sine rapporter at mange opplever at angripere etter å ha fått innpass i en virksomhet, bruker systemet for bitcoinminig. Dette er tilsynelatende vanskelig å oppdage, men kan gå utover hastighet, produksjon og tilgjengeligheten til en virksomhet. Nedetid og utilgjengelighet er også ofte konsekvensen av sabotasje og tjenestenektangrep. Dette er ofte svært alvorlig for de som rammes. I vår digitale hverdag er tilgjengelighet stadig viktigere og ofte et kritisk element for en tjenesteleverandør, logistikkoperatør eller nettbutikk.

Direktør- og ledelsessvindel er stadig utbredt. I Mørketallsundersøkelsen oppgis det at de som utfører denne type svindel ser ut til å være villig til å legge mer tid og ressurser i å målrette svindelen. NSM og PST ser at slike angrep ofte utnytter kjente sårbarheter for å komme på innsiden av virksomheter. Når de oppnår det, for eksempel at de har kontroll over en ansatts e-postkonto, er det lettere å for eksempel endre kontonummer for utbetalinger eller kjøre falske fakturaer gjennom systemet. En stor utfordring med denne typen angrep, særlig for små virksomheter, er at det er liten hjelp å få for de som rammes. Noen sier også at det å la seg lure av slik svindel er noe man ikke ønsker at kunder, leverandører eller konkurrenter skal vite om. Derfor dysses det ned for at ingen skal finne ut av det. At politiet ved Kripos i november 2018 gikk ut i media og oppfordret alle som har opplevd denne typen svindel til å fortelle dem om det, åpent eller anonymt, er et viktig og tydelig signal om at politiet tar denne typen saker på alvor.

ID-tyveri er en egen trussel. Samtidig erfarer NorSIS at den ofte utføres som en metode i kombinasjon med andre trusler eller angrep. NorSIS kjenner for eksempel til saker der direktørsvindel eller utpressing er gjennomført ved å først utføre et ID-tyveri mot en ansatt eller privatperson. At noen tar over en annens identitet, enten som arbeidstager eller privatperson, er svært ødeleggende for den som rammes. Det kan medføre en kamp for å renvaske seg samtidig som man ikke har kontroll over hvem som har mulighet til å misbruke ens identitet eller andre opplysninger eller når. Det er derfor svært alvorlig for den som rammes.

Trusselbildet viser oss at vi daglig utsetter oss for mange sårbarheter. NSM understreker at de stadig lengre verdikjedene og det stadig større kompleksiteten i det digitale rom, er den største sårbarheten i samfunnet i dag.

ALLE ER ATTRAKTIVE MÅL UANSETT EGEN KJERNEVIRKSOMHET

NorSIS opplever at mange virksomheter er mer opptatt av egen kjernevirksomhet enn å sikre sine verdier. Dette støttes i stor grad av Næringslivets sikkerhetsråd sin Mørketallsundersøkelse. I en travel hverdag er det ikke vanskelig å forstå. Samtidig får det dessverre ofte uheldige konsekvenser. For eksempel ved at virksomhetene blir sårbare for digitale angripere. Sikkerhetsarbeidet må forankres i en virksomhets ledelse. Vi ser ofte at dette arbeidet

13 Nasjonal sikkerhetsmyndighet: *«Grunnleggende tiltak for sikring av e-post»* https://nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/u-02-grunnleggende-tiltak-for-sikring-av-e-post---endelig.pdf

14 Telenor: *«Digital sikkerhet – sterkere sammen»* https://www.telenor.no/om/digital-sikkerhet/

15 Computerworld: *«Norge sikrer ikke e-posten»* http://www.cw.no/artikkel/siste-nyheter/norge-sikrer-ikke-e-posten

16 Europol: *«INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2018»* https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

17 Cisco: *«Small and mighty»* https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf

ikke har en top-down-prosess, men at ansatte med ansvar for IT eller sikkerhet er de som i realiteten står for beslutningene.

Virksomheter som utsettes for cyberkriminalitet vil trolig innse alvoret i det de utsettes for en sikkerhetshendelse. Vi antar derfor at de vil iverksette en rekke tiltak i etterkant av hendelsen. Tiltak som totalt sett hadde vært langt billigere om de hadde vært satt i system før noe skjedde. Jo tidligere man tar tak i et problem i en prosess, jo billigere blir endringene å gjennomføre.

Det er likevel gledelig at man i Mørketallsundersøkelsen stadfester at seks av ti virksomheter sier at de har gjennomført aktiviteter for å øke de ansattes sikkerhetsbevissthet. Selv om dette er mer vanlig i store virksomheter enn i små virksomheter, betyr det at flere forstår at opplæring av ansatte er grunnleggende for å møte dagens trusler. Videre konkluderer Mørketallsundersøkelsen med at virksomheter som har et styringssystem for informasjonssikkerhet er mer opptatt av å lære opp ansatte enn de som ikke har et slikt styringssystem. Det indikerer at de som setter av tid og ressurser nok til å få på plass et styringssystem for IKT-sikkerhet, ser helheten i sikkerhetsarbeidet på en annen måte enn de som ikke kan prioritere dette lengre. Respondentene som ikke har et styringssystem for informasjonssikkerhet oppgir i større grad enn andre at hendelsen skyldtes manglende teknisk utstyr eller kompetanse til å hindre trusselen. Det viser at selv om trusselen oppdages uten et styringssystem, er det få som vet hvordan den skal håndteres. Det understreker hvor viktig det er at den enkelte virksomhet har oversikt både over egne verdier og over hvilket risiko- og trusselbilde de befinner seg i og hvordan de skal møte dette.

Mørketallsundersøkelsen oppgir at menneskelig feil ofte er grunnen til sikkerhetsbrudd. Enten at noen har gjort feil, at det mangler sikkerhetsbevissthet hos ansatte eller at prosesser og rutiner ikke er fulgt som har ført til sikkerhetsbrudd. Dette viser at det er svært nødvendig å øke bevisstheten og kunnskapen om sikkerhet. Både i den enkelte organisasjon, utdanningsløpet, akademia og i samfunnet forøvrig.

Dersom dette følges opp i et styringssystem, er det i tillegg til å både lettere oppdage sikkerhetsbrudd eller trusler, og å se hvilket behov den enkelte virksomhet har for opplæring og kompetanseutvikling av de ansatte. Det understøtter også NSMs oppfordring om å i best mulig grad hjelpe sluttbrukeren til å unngå å gjøre feil.

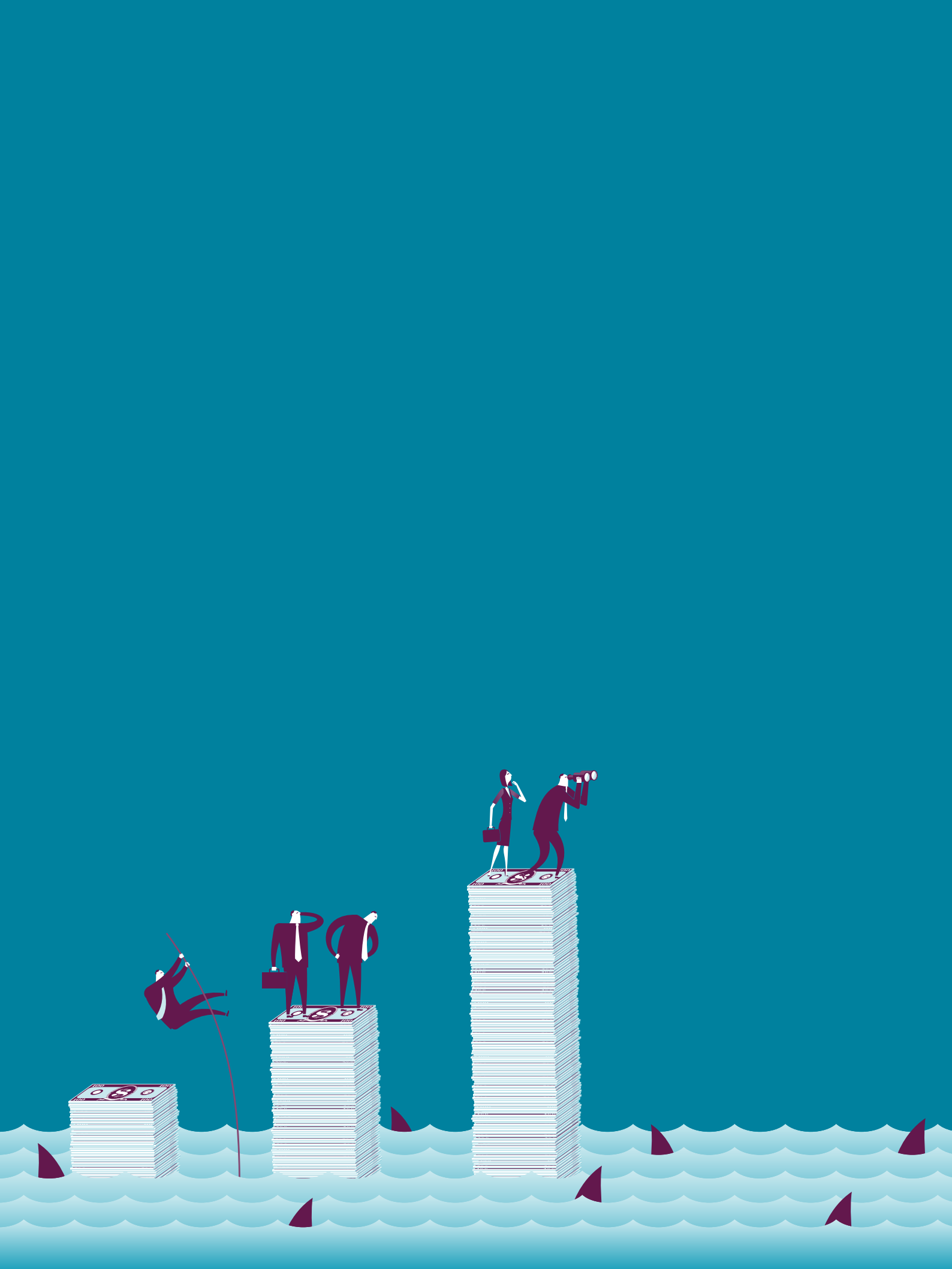
UTFORDRINGER

Et annet viktig funn i Mørketallsundersøkelsen er at industri, overnattings- og serveringssteder samt tjenesteytende næringer har lavest modenhet for å oppdage og avdekke sikkerhetsbrudd. Under 50 prosent av disse oppdager sikkerhetsbrudd umiddelbart.

Dette funnet tyder på at denne gruppen er en viktig målgruppe å nå for alle organisasjoner, næringslivsaktører og myndigheter som jobber med forebyggende IKT-sikkerhet. Mørketallsundersøkelsen antyder at en årsak til at nettopp denne typen næringer scorer så lavt på å oppdage sikkerhetsbrudd, er fordi deres kjernevirksomhet ligger så langt unna grunnleggende sikkerhetsarbeid og sikkerhetsrutiner. Det er forståelig at en vaktmester, kelner eller pakkemaskinoperatør ikke tenker på eller trenger å forholde seg til totrinnsbekreftelse eller oppdatering av programvare i det daglige. Samtidig er alle de aller fleste av disse også teknologibrukere etter jobb. Der har de behov for å kjenne til totrinnsbekreftelse, passordbruk og patching for å være sikre digitale brukere.

En annen utfordring, særlig for små virksomheter uten egen sikkerhets- eller IT-kompetanse, er å ha god nok bestillerkompetanse. For å gjøre gode innkjøp av utstyr, systemer, leverandører og nettverk må man vite noe om det man skal kjøpe inn. Særlig for de som ikke selv har sikkerhetskompetanse internt er det viktig å sørge for å ha systemer som er best mulig rustet mot kjente og potensielle trusler. For å sikre at hendelser virksomheten utsettes for både oppdages og håndteres riktig rent teknisk. I tillegg bør virksomheten sikre at den har en god avtale med leverandøren av dette systemet. Avtalen bør for

eksempel sikre at virksomheten får hjelp ved behov dersom den ikke har intern kompetanse for dette. Dette er imidlertid ofte utfordrende i praksis, nettopp fordi slike innkjøp krever kompetanse. Det er derfor svært viktig at små eller mellomstore virksomheter gjør grundig forarbeid og kanskje også søker hjelp før de gjør slike innkjøp.



TRENDER

SAMMENKOBLET TEKNOLOGI

Dette er i utgangpunktet en videreføring av fjorårets trend, tingenes internett. Samtidig ser vi at samfunnet har kommet mye lengre i sammenkobling av nettilkoblede enheter det siste året. Stadig flere enheter kan kobles på nett. I tillegg har det åpnet seg en rekke nye muligheter for bruk av kunstig intelligens, for eksempel for bruk av maskinlæring. Dette er det også mange som har tatt i bruk. Dette gjør det mulig å samle inn, behandle og finne sammenhenger og mønstre i stadig større datamengder. Maskinlæringen styres av algoritmer som lærer av resultatene fra det som innhentes. På bakgrunn av denne læringen endres eller tilpasses videre innsamling og sortering. Datamengdene hentes og samles gjerne inn fra et utall ulike steder ved hjelp av tingenes internett.

Et eksempel på sammenkoblingen av tingenes internett og kunstig intelligens er hvordan Google Maps registrerer kjøremønstre og utfra dette kan forutse hvor lang tid det tar å kjøre en rute akkurat når du søker den opp. Dersom du søker opp ruta mellom Trondheim og Værnes vil tiden Google foreslår at dette vil ta å kjøre, variere ut fra når på døgnet du gjør søket. Biler har også gått gjennom en interessant teknologisk utvikling, eller nesten en teknologisk revolusjon de siste årene. Tesla er et eksempel på en helautomatisk og nettilkoblet enhet. I tillegg benyttes kunstig intelligens i Tesla til å lære om kjøreadferd, kjøremønstre og alt annet som kan måles i en bil. Læringen fra hver enkelt Tesla sammenstilles og brukes som læring for alle Tesla-er.

NSM[18] forutser at kunstig intelligens vil benyttes i sikkerhetsarbeid fremover. Både som en metode for å analysere sikkerhetsrisiko, fange opp påloggінger i systemet opp mot tilgangsstyringen og å overvåke om en bedrifts utstyr kobler seg på nett utenom den eller de struktur bedriften opererer. Hvis dette oppdages, bør nettilkoblingen ettergås for å sikre at det ikke er uvedkommende som forsøker å koble seg på virksomhetens nett. NSM understreker samtidig at vi må forvente at også trusselaktører og angripere vil benytte mulighetene i for eksempel automatisering i sine angrep mot stater, bedrifter, organisasjoner eller privatpersoner.

STADIG LENGRE VERDIKJEDER MED ULIK TEKNOLOGI OG FLERE AKTØRER

Når stadig flere ulike systemer kobles sammen i stadig lengre verdikjeder, er det lett å miste kontrollen. Først og fremst mister en oversikt og kontroll over hvor opplysningene og informasjonsverdiene våre er. Virksomhetens verdier kan plutselig være tilgjengelig for andre enn før ettersom verdikjeden utvides. Samtidig mister en oversikt over hvem en er avhengige av og ikke minst hva som er virksomhetens sårbarheter. For eksempel kan det tenkes at en programkode utvikles et sted, konfigureres et annet sted, implementeres et tredje sted og leverer tjenester til et fjerde sted.

I tillegg til at denne sammenkoblingen stiller krav til høyere kompetanse om sikkerhet hos den enkelte virksomhet, stiller den også større krav til samarbeid og koordinering av sikkerhetsarbeidet mellom virksomheter. Enten ved at stadig flere virksomheter bidrar inn i samme verdikjede eller gjennom avhengigheter mellom virksomhetenes verdikjeder.

NSM[19] påpeker at sammenkoblingen også innebærer ulik teknologi. Det stiller krav til at en har en helhetlig forståelse for de ulike teknologiene. Både i risikovurderingene som gjøres, informasjonsflyten mellom aktører, og i håndteringen og oppdatering av alle ledd i verdikjeden eller verdinettverket. Denne sammenkoblingen og disse avhengighetene går på tvers av domener. Digitale løsninger er avhengig av nettbaserte løsninger og fysisk produksjon er avhengig av nettbaserte løsninger. I tillegg er avhengighetene ofte gjensidige. Telekom trenger strøm og strøm trenger telekom.

Det betyr at til tross for at sikkerhet er et ledelsesansvar, må alle fagområder, sektorer og roller involveres. I tillegg må en sørge for å ha en helhetlig tilnærming til sikkerhet både med tanke på kompetanse, systemer, portefølje og

18 Nasjonal sikkerhetsmyndighet: *«Et sikkert digitalt Norge – IKT-risikobilde 2018»* https://nsm.stat.no/globalassets/rapporter/nsm_ikt-risikobilde_2018_web.pdf

19 Nasjonal sikkerhetsmyndighet: *«Et sikkert digitalt Norge – IKT-risikobilde 2018»* https://nsm.stat.no/globalassets/rapporter/nsm_ikt-risikobilde_2018_web.pdf

tjenester. Sikkerhet må prioriteres. NSM mener også at de som får dette til, kan bruke sikkerhet som et konkurransefortrinn.

HVA BETYR TRENDENE FOR VIRKSOMHETER, ANSATTE OG PRIVATPERSONER?

Når en mister oversikten over hvem som vet eller har tilgang til hva, mister en også oversikten over hvem som kan være trusselaktører. Det helhetlige bildet blir vanskelig å forholde seg til, kanskje særlig for små virksomheter. Det er lett å tenke at en kun er en liten, ubetydelig aktør uten å innse at en plutselig er en inngang til en annen virksomhet.

Denne nye utfordringen med avhengigheter krever at virksomheter samarbeider om sikkerhet for å unngå at en sikkerhetshendelse hos en aktør, får konsekvenser eller på noen måte påvirker andre aktører. I november 2018 opplevde Microsoft en hendelse, som medførte at virksomheter som var avhengige av Microsofts Azure plattform og som hadde tatt i bruk sikkerhetsmekanismen totrinnsbekreftelse, ikke fikk logget på sin sky-tjeneste. Dette er et eksempel på hvordan en avhengighet, som virksomheten selv i liten grad kan påvirke (og der de i og for seg hadde gjort alt riktig), likevel kan ramme dem. I form av nedetid, utilgjengelighet og store tap i produksjon. Manglende kompetanse til å se avhengigheter mellom virksomheter og manglende evne, og-eller vilje til å informere og koordinere, vil være fremtredende sårbarheter i tiden framover.

HVEM ER TRUSSELAKTØRENE OG HVILKE KONSEKVENSER KAN TRUSLENE FÅ?

Tekniske angrep kan utføres av så og si alle som har eller får tilgang til de tekniske verktøyene som brukes for å gjennomføre angrepet. Slike angrep krever ofte kun enkle, og kanskje til med automatiserte verktøy. Angrepene kan gjøres globalt på tvers av verdensdeler og landegrenser. Det kan derfor være vanskelig å oppdage denne typen angrep. Særlig dersom angriperne utnytter sårbarheter vi ikke kjenner til eller dersom den virksomheten som rammes egentlig ikke er hovedmålet for angrepet. Den økte kompleksitet i verdikjeden kan gjøre det mulig for angripere å unngå en direkte knytning mellom handlingen, trusselaktøren og virksomheten som rammes.

I og med at tingenes internett og kunstig intelligens brukes i leveranser av samfunnskritiske tjenester som strømnett, telekom og finansielle tjenester, kan et suksessfullt angrep få svært store samfunnsmessige konsekvenser. Dersom strømnettet går ned i hele eller deler av landet vil det ikke bare kunne gi store fysiske konsekvenser for innbyggerne. Det vil også bidra til å svekke tilliten til digitale tjenester. Når så mye av samfunnet vårt er digitalisert og regjeringen ønsker økt digitalisering, er det svært viktig å beholde den enkeltes tillit til digitale tjenester.

SAMMENKOBLING AV SVINDELMETODER

En annen fremtredende trend er sammenkobling av ulike svindelmetoder. Som nevnt opplever vi at angriperne stadig blir proffere. Det gjelder også for metodene de benytter. Gjennom å kombinere bruk av teknologi, tilgjengelighet og tilstedeværelse og virkemidler som frykt, fristelse og tillit, blir angrepene også stadig mer målrettede. Et eksempel på dette er når sammenkobling av informasjon hentet fra tidligere datainnbrudd, for eksempel lister over brukernavn og passord, benyttes til utpressing via e-post. Trusselaktørene kombinerer da stjålne data og utpressing. Tiltross for at mye av dette gjennomføres automatisk, som sammenstilling av e-postadresser mot brukerkontoer eller passord, oppfattes dette av mottageren som om det er personlig tilpasset til nettopp den.

Et annet eksempel er at svindlerne tilpasser utpressingsbeløpet til mottageren. Det vil si at privatpersoner kreves for lavere summer enn virksomheter. Slik at det er realistisk at de har råd til å betale. Som nevnt tidligere har summen

som kreves, ofte vist seg å være avgjørende for offerets vurdering av om hun/han skal betale eller søke hjelp. Sesongbetont svindel er et annet eksempel. Ved å sende ut melding om tilbakebetaling på skatten i juni eller hentelapper på posten ved juletider tilpasser man svindelforsøkene til mottageres forventninger og omgivelser. I forbindelse med innføringen av nye personvernregler fikk NorSIS henvendelser fra folk som mottok phishing eller andre svindelforsøk fordekt som oppdatering av personvernerklæring eller personopplysninger.

Det at mottageren forventer en slik henvendelse eller mottar flere lignende henvendelser samtidig, kan gjøre vedkommende mer villig til å oppgi opplysninger ved å klikke på en lenke eller lignende. NorSIS ser også en tendens til at enkelte angrep benytter andre kanaler enn e-post fordi det har høyere tillit hos mottageren. Det å motta en tekstmelding fra Telenor, Apple eller Samsung med en lenke for å oppdatere telefonene virker mer troverdig enn å få en slik lenke via e-post. I disse tilfellene utnyttes også tilliten mottageren har til kjente merkevarer og leverandører.

Denne typen svindel, der mottageren skal klikke på en lenke eller installere noe på telefonen sin kalles gjerne smishing. Tiltross for at dette, som regel er lettere å spore tilbake til avsender enn e-postsvindel og som regel koster noe mer ressurser for dem å gjennomføre, kan det se ut til at denne typen svindel er på fremmarsj. En rekke kjente aktører opplever at deres merkenavn eller tjenester misbrukes i smishing. Enten under dekke av at aktøren inviterer kunder til en konkurranse med attraktive premier eller at SMS som kommunikasjonskanal misbrukes ved kjøp og salg av produkter eller tjenester. Her utnytter angriperne for eksempel brukerkontoer på ulike plattformer, medlemskap i kundeklubber eller annen tilknytning til en aktør for å kommunisere med ofrene for svindelen. De misbruker ved dette både ofrenes tillit til den kjente aktøren de utgir seg for å være, og tilliten til kommunikasjon over SMS. Flere av aktørene som utsettes for en slik misbruk av deres merkenavn mener å se en økning i denne typen svindel via SMS. De mener at dersom flere hadde benyttet SMS som hovedkanal i sin kommunikasjon med kunder og brukere, ville dette vært en enda større problem enn det er i dag. Det jobbes derfor mye på tvers mellom de som utsettes for dette og leverandørene av SMS-tjenester, samt politiet for å forsøke å hindre denne typen svindel.

HVORDAN FOREGÅR DENNE UTVIKLINGEN?

Ettersom sammenkoblingen av metoder får utvikle seg videre, er det grunn til å anta at angripere og trusselaktører vil gå enda lengre i å tilpasse både budskap og kanal til mottagere. For eksempel vil trolig en iPhone-bruker motta en annen tekst enn Android-brukeren. Det er også sannsynlig at angrepene tilpasses til den enkeltes adferd på nett. Kunnskap om hvilke nettsteder den enkelte besøker kan for eksempel brukes for å svindle den enkelte.

Mnemonic ser en tendens til at angrep er mer skreddersydd til store virksomheter eller organisasjoner. Angrepene utføres på en slik måte at det kan være vanskelig å avsløre dem som et angrep. Deres spådom er at slike angrep etterhvert også vil benyttes for å ramme små virksomheter.

HVILKE KONSEKVENSER KAN DENNE TRENDEN FÅ?

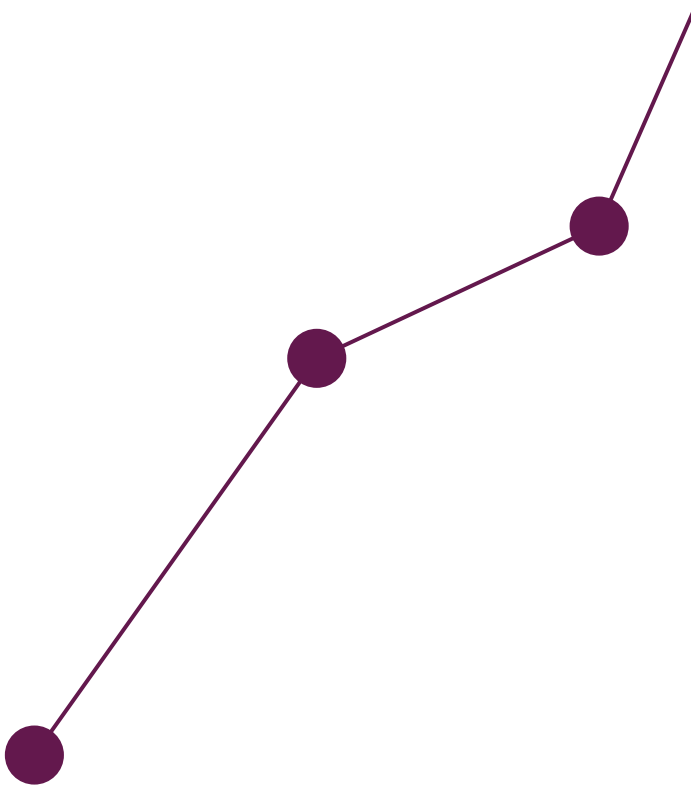
En økt skepsis til digitale henvendelser vil sannsynligvis også vil medføre en økt skepsis til legitime tjenester på nettet. NorSIS sikkerhetskulturmåling,[20] avdekket økt frykt for å bruke nett, både private og offentlige nettsteder og nettbank siden første måling av dette i 2015. Dette støttes også i en undersøkelse BuyPass gjennomførte høsten 2018.[21] Det er et tegn på at vi må imøtegå denne frykten. Samfunnet digitaliseres i stadig større grad. Det er en positiv og villet utvikling. Likevel er en slik utvikling avhengig av at brukerne har tillit til verktøyene, metodene og aktørene som er involvert for at vi best mulig skal kunne benytte de gode dette kan

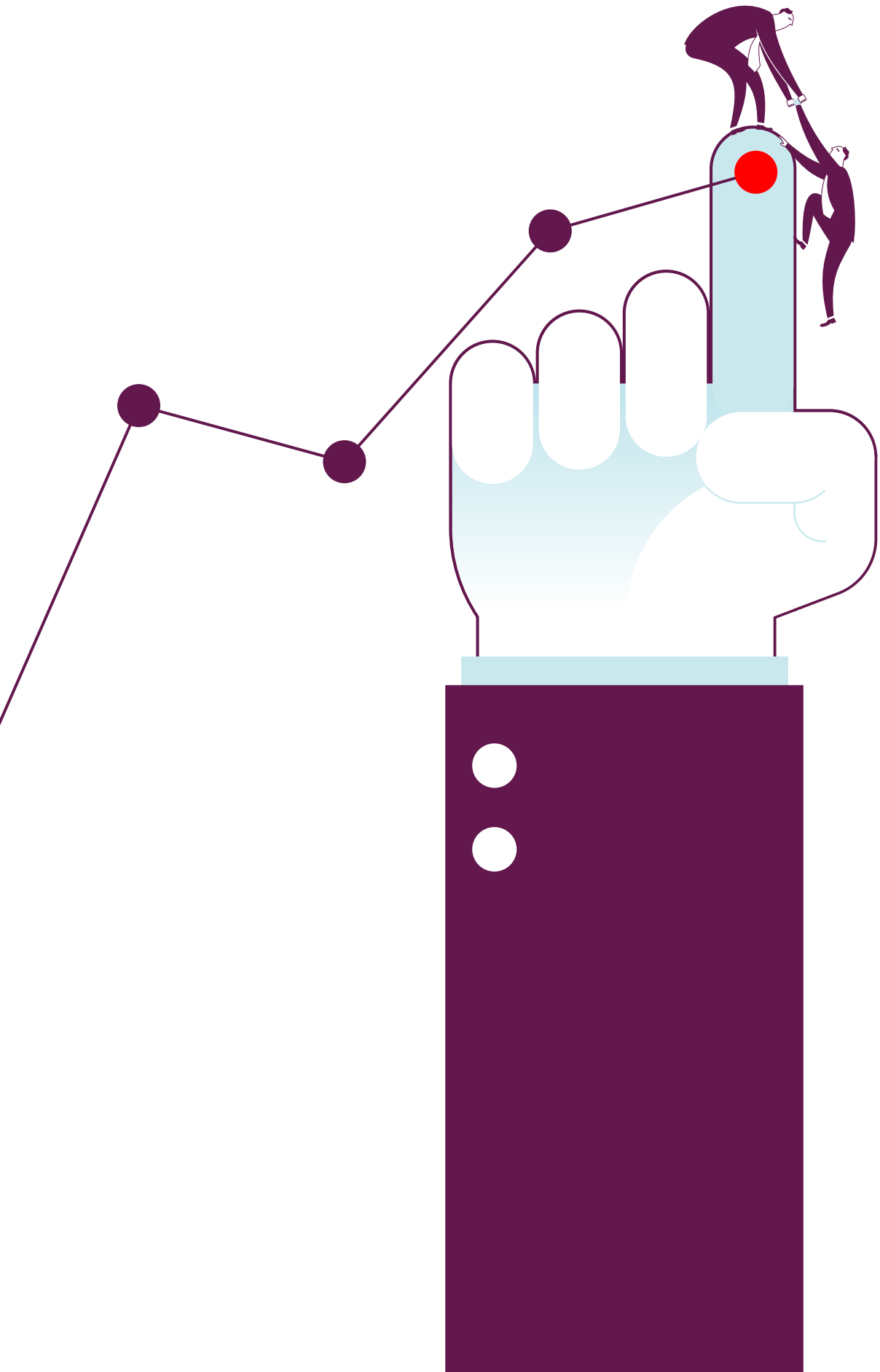
20 NorSIS: «*Nordmenn og digital sikkerhetskultur 2018*» https://norsis.no/wp-content/uploads/2018/11/Nordmenn-og-digital-sikkerhetskultur-2018-web.pdf

21 BuyPass: «*Økt frykt for netthandel*» https://www.buypass.no/nyheter/okt-frykt-for-netthandel

gi oss. Det er derfor viktig å bygge kunnskap om hvordan svindel kan avsløres, og hvem som kan tilby hjelp dersom man fortsatt er usikker. Det er viktig at alle får denne typen kunnskap og opplæring. Hvis ikke kan vi stå i fare for å få et digitalt klasseskille.

Ofrene for digitale angrep opplever som regel konsekvenser fra økonomisk tap til psykologiske reaksjoner eller en kombinasjon av disse. Dette kan være krevende å takle. Det kan også være utfordrende å forstå for andre som ikke har opplevd det samme. NorSIS mener derfor at opplæring og kompetanse kombinert med en åpenhetskultur knyttet til pågående svindelforsøk i samfunnet generelt er nødvendig. Uavhengig av om offeret har handlet i vanvare, blitt utsatt for sosial manipulering, gått på et phishing forsøk eller opplevd datainnbrudd er vedkommende erfaring viktig å dele med andre som kan utsettes eller utsette seg selv for det samme.





VURDERING AV TRENDENE

De aller, aller fleste av oss lever et liv preget av digitale hjelpemidler og verktøy. Det betyr at svært mange er eller vil bli utsatt for en eller annen type dataangrep på kort eller lang sikt. Derfor er det viktig å ha en oversikt over hva eller hvem som kan tenkes å forsøke å ramme vår digitale hverdag. Ettersom både teknologier og svindelmetoder stadig kobles sammen, er samfunnet og alle digitale brukere på vei inn i et svært komplekst og ukjent terreng. Det gjør det vanskelig å forutse hvilke trusler og sårbarheter vi vil stå overfor fremover. Utviklingen går svært raskt og det er vanskelig å vite om den stiger lineært eller eksponentielt når vi blander sammen tingens internett og kunstig intelligens.

TILLIT ER GRUNNLEGGENDE FOR SUKSESSFULL DIGITALISERING

Tillit er en forutsetning for vellykket digitalisering. En god sikkerhetskultur bidrar til å bygge tillit til digitale tjenester. Dersom både virksomheter og den enkelte av oss har tillit til at opplysninger som behandles digitalt, behandles på en god måte og at myndighetene kan hjelpe med utfordringer, kriminalitet, misbruk eller andre utfordringer, kan samfunnet høste godene av digitaliseringen. Det at frykten for å bruke internett er økende kan ha mange årsaker, men helt overordnet er det svært uheldig. Det må derfor være et mål for samfunnet og myndighetene å redusere denne frykten og på den måten bidra til å gjenopprette, og på sikt, øke befolkningens tillit til nettbruk og digitalisering.

BEHOVS- ELLER TEKNOLOGIDREVET UTVIKLING?

Den digitale utviklingen har lenge vært drevet frem av tilgjengelig og mulig teknologi. Analyse av brukerbehov har ikke vært den viktigste driveren for digitalisering. Samfunnet vårt er bygd opp slik at vi må ha en balanse mellom lovverk, tilgjengelige metoder, løsninger og teknologi, og tilnærming til problemløsning. Dette er for å sikre at vi ivaretar alles interesser og bevarer alles tillit til samfunnet. Istendenfor en slik balanse ses teknologiutvikling og digitalisering ofte som et mål i seg selv, heller enn et middel for å oppnå bedre velferd, mer innovasjon og bedre effektivitet.

HVORDAN SKAL DEN ENKELTE ANSATT, BEDRIFTSLEDER ELLER PRIVATPERSON MØTE DISSE TRENDENE?

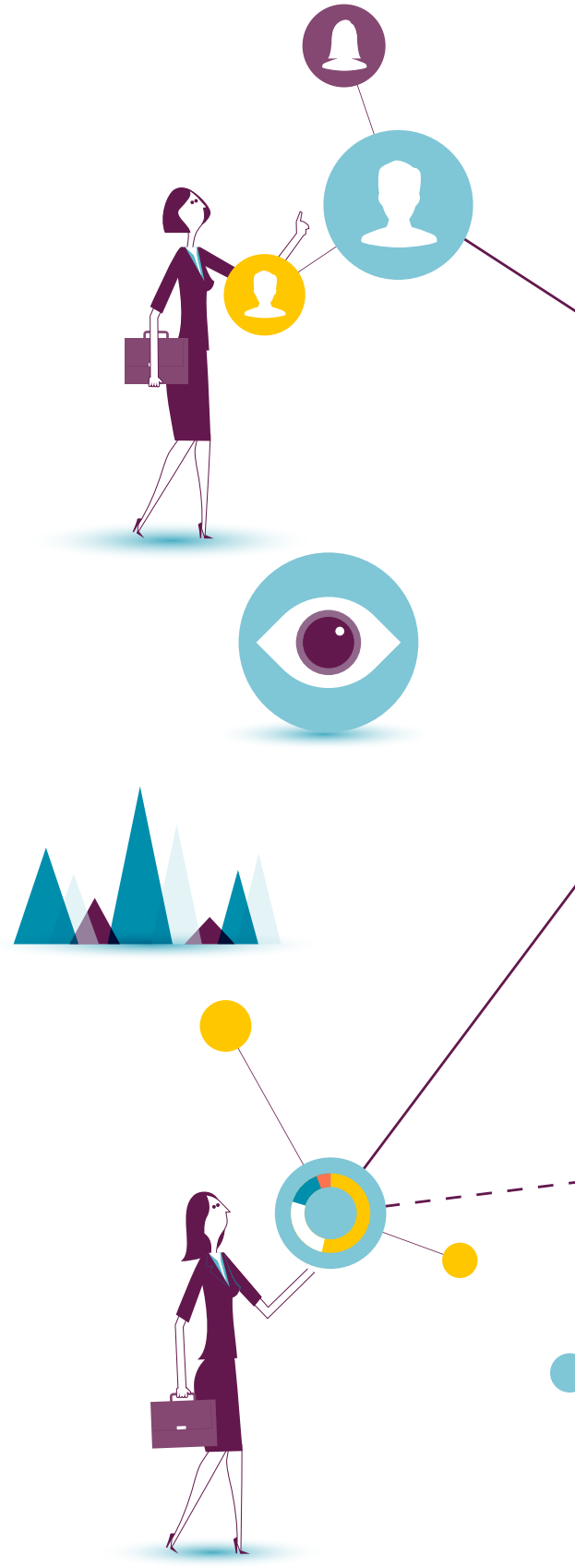
Det viktigste en leder kan gjøre, er å sørge for kontinuerlig opplæring og kunnskapsoverføring hos sine ansatte. Det er også viktig med intern åpenhet om sikring av opplysninger og en kultur der alle oppfordres til å melde fra om ting som avviker fra normalen. Dette kan vi oppnå gjennom gode systemer som reduserer muligheten for brukerfeil,[22] systemer som ikke behandler flere opplysninger enn nødvendig, god tilgangskontroll, gode sletterutiner og kontinuerlig oppdatering. For å håndtere stadig mer komplekse verdikjeder, må alle organisasjoner, som et minimum, sørge for god informasjonsflyt mellom virksomhetene i kjeden, men også en koordinert håndtering og gjenoppretting. I tillegg bør alle bygge kompetanse i eller på verdikjedene og etablere samarbeidsfora om sikkerhet i sin sektor, bransje, lokalmiljø eller tilsvarende. Det må også settes av tilstrekkelige til å undersøke årsaken til sikkerhetshendelser.

Utviklingen stiller også stadig nye og ofte høyere krav til risikovurderinger i den enkelte virksomhet. Alle virksomheter må i større grad enn før vurdere sin risiko i samspill med må omkringliggende og andre hendelser som kan påvirke dem. Det kan være alt fra samarbeidende aktører, leverandører eller kunder til hvilke sikkerhetsvurderinger virksomhetens egen ansatte gjør. En ansatts digitale adferd hjemme kan i noen tilfeller få konsekvenser for arbeidsstedet eller vedkommendes adferd på jobb. Det er derfor god risikohåndtering at en bedrift gir sine ansatte opplæring i hvordan de skal være tryggere på nett hjemme. Gjennom opplæring, fokus på sikkerhetskultur i virksomheter, å forsøke å informere best mulig om

22 Nasjonal sikkerhetsmyndighet: *«Et sikkert digitalt Norge – IKT-risikobilde 2018»* https://nsm.stat.no/globalassets/rapporter/nsm_ikt-risikobilde_2018_web.pdf

hvilke trusler som rører seg, kan privatpersoner, ansatte, ledere og alle andre borgere bli tryggere digitale brukere.

I tillegg må samfunnet og myndighetene bli flinkere til å følge opp anmeldelser og straffe de som driver med slik svindel. Siden nettkriminalitet ikke kjenner noen landegrenser må også politiet må jobbe stadig mer målrettet og globalt i sin håndtering av nettkriminalitet.



HVORDAN MØTER SAMFUNNET DE DIGITALE TRUSLENE OG TRENDENE?

OVERORDNEDE FØRINGER FRA MYNDIGHETENE MED INNVIRKNING PÅ SIKKERHETSARBEIDET

Det er utfordrende for myndighetene å styre den digitale utviklingen gjennom tradisjonelle metoder som utredningsarbeid, felles strategier eller lovregulering. Tradisjonelt har lovutvikling vært den vanligste metoden å styre utviklingen av samfunnet i ønsket retning. Samtidig krever disse metodene og særlig lovregulering, at myndighetene kommer tidlig inn i prosessen. Når det gjelder teknologiutvikling er dette utfordrende både på grunn av at lovarbeid tar lang tid og at samfunnet tilsynelatende aksepterer at det er teknologiutviklingen som driver samfunnet fremover og skaper stadig nye behov hos virksomheter og i befolkningen. Samtidig skaper digitaliseringen stadig nye behov, verktøy, metoder og tilgjengeliggjør informasjon som forbigår, utfordrer og synliggjør behovet for nye lover knyttet til grunnleggende plikter og rettigheter. For eksempel plikten til å sikre nasjonal infrastruktur og retten til personvern.

Derfor har det de siste årene kommet flere lover, både nasjonalt og fra EU/EØS som skal regulere store deler av den stadig mer digitale hverdagen vår. 20. juli i år fikk Norge ny personvernlov som implementerer EUs personvernforordning (GDPR) i norsk rett. Det var kun noen få uker etter at regjeringen i juni, vedtok ny sikkerhetslov som trer i kraft 1.1.2019. I tillegg ble forslag for ny lov for etterretningstjenesten sendt på høring i november 2018.

> «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 (jf. Sikkerhetsloven § 1-5 nr. 2). En forutsetning for at sistnevnte virksomheter omfattes av loven er imidlertid at det enkelte departement innenfor sitt ansvarsområde fatter vedtak om at loven skal gjelde for virksomheten (jf. Sikkerhetsloven § 1-3).

PERSONOPPLYSNINGSLOVEN (EUS PERSONVERNFORORDNING, FORKORTET GDPR)

Loven gjelder for alle virksomheter som behandler personopplysninger. Det betyr at alle virksomheter som har en eller flere ansatte må følge loven.

Noen av de viktigste endringene fra gammel til ny personopplysningslov er tydeliggjøring av at ansvaret for å følge loven ligger hos den enkelte virksomhet. Loven stiller også krav til at nye systemer eller tjenester skal utvikles etter kravene til innebygd personvern. I tillegg styrkes de registrertes rettigheter, alle offentlige og flere private virksomheter plikter å opprette personvernombud og databehandlere får en selvstendig plikt til å følge regelverket. Fra forordningen ble vedtatt i EU i april 2016 til den ble vedtatt og senere implementert i norsk lov i 2018, har mange virksomheter lagt ned en betydelig innsats for å sin etterlevelse ny personopplysningslov. For noen skyldes dette at de ikke etterlevet gjeldende personopplysningslov. For andre skyldtes det at de nå må følge flere nye krav til behandling av personopplysninger.

SIKKERHETSLOVEN

Sikkerhetsloven gjelder for alle statlige, fylkeskommunale og kommunale organer. I tillegg gjelder den for virksomheter som behandler sikkerhetsgradert informasjon eller som råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for «grunnleggende nasjonale funksjoner». Hvilke virksomheter som omfattes av loven er det opp til departementene å bestemme. Det avhenger av hvilke grunnleggende nasjonale funksjoner som finnes i den enkelte sektor og

den enkelte virksomhets rolle i dette bildet. Det er derfor vanskelig å forutse hva dette vil bety for små- og mellomstore virksomheter. Samtidig er det verdt å merke seg at NSM eller andre myndighetsorganer trolig få en veiledningsplikt overfor små eller mellomstore virksomheter som omfattes av sikkerhetsloven.

NIS-DIREKTIVET

Et EØS-relevant EU-direktiv som ble vedtatt i EU 16. juli 2016. Direktivet pålegger medlemsstatene, EØS og EFTA-landene å sørge for at landets IKT-sikkerhet gjennom å få på plass en strategi for sikkerhetsarbeidet, etablere sikkerhetsberedskapsenheter (CSIRT) og pålegge IKT-sikkerhetskrav og varslingsplikt for operatører og leverandører av samfunnsviktige tjenester. Dette skal gjennomføres både på strategisk nivå og CSIRT-nivå. Norge oppfyller NSM i stor grad oppgavene direktivet gir. NorCERT oppfyller også i stor grad funksjonene som tillegges det nasjonale CERT-et. NIS-direktivet ligger til grunn for deler av ny norsk sikkerhetslov. I tillegg har regjeringen tatt flere initiativ til å få på plass strategier, handlingsplaner og tverrfaglig samarbeid om IKT-sikkerhet for å oppfylle kravene i NIS-direktivet.

ULIKE MYNDIGHETSINITIATIV FOR SIKKER DIGITALISERING AV NORGE

FELLES CYBERKOORDINERINGSSENTER (FCKS)

FCKS ble opprettet i 2017 og består av NSM, Etterretningstjenesten, PST og Kripos, ledet av NSM. Formålet med samarbeidsorganet er å styrke nasjonal evne til effektivt forsvar mot og håndtering av, alvorlige hendelser og kriminalitet i det digitale rom. Virkeområdet til FCKS er alvorlige hendelser i det digitale rom. FCKS skal koordinere partenes innsats ved handtering av hendelser, herunder bidra til mer effektiv bruk av nasjonale ressurser, styrke informasjonsdeling, samt ivareta koordinert varsling til og frembringelse av helhetlige beslutningsgrunnlag til overordnede myndigheter.

STYRKING AV POLITIET MED NASJONALT CYBERSENTER (NC3)

NC3 opprettes i januar 2019 under ledelse av Olav Skar Jørgensen. I første omgang skal NC3 samle enkeltfunksjoner som allerede ligger i andre deler av politietaten og planmessig utvikle oppdrag, evner og struktur for å bidra til å håndheve «lov om politi» også i det digitale rom. Målrettet og kontinuerlig samarbeid med statlige og private aktører er suksessfaktor, og NC3 ønsker å opprette et døgnbemannet kontaktpunkt for informasjonsdeling og førstelinjerespons, så snart som mulig.

NASJONALT CYBERSIKKERHETSSENTER

Høsten 2018 kunngjorde NSM at de oppretter et Nasjonalt cybersikkerhetssenter i 2019. Senteret etableres som en del av NSM. Ambisjonen er at det skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot cyberangrep. Det vil være et nasjonalt kontaktpunkt og et «nav» for cybersikkerhet, og vil samarbeide tett med IKT-sikkerhetsmiljøer i blant annet næringslivet, kraftsektoren, finanssektoren, helsesektoren, politiet, E-tjenesten, ulike sektormyndigheter, akademia og internasjonale partnere.

DIGITAL 21

En styringsgruppe leverte september 2018 64 anbefalinger for digitalisering til oppdragsgiver Nærings- og fiskeridepartementet.[23] Tiltakene går på tvers av bransje og forskningsmiljø og. De skal følges opp av Nærings- og fiskeridepartementet, Kunnskapsdepartementet og Kommunal- og moderniseringsdepartementet.

NASJONAL STRATEGI FOR DIGITAL SIKKERHET

En gruppe nedsatt av Justis- og beredskapsdepartementet jobber med en strategi og handlingsplan for digital sikkerhet.[24] NorSIS deltar i dette arbeidet. Arbeidet er ventet ferdigstilt i begynnelsen av 2019.

23 Digital 21: *«Digitale grep for norsk verdiskaping – Samlede anbefalinger»* https://digital21.no/wp-content/uploads/2018/09/Digital21_strategi_2018.pdf

IKT-SIKKERHETSUTVALGET

Utvalget er nedsatt av Justis- og beredskapsdepartementet for å styrke den nasjonale IKT-sikkerheten. Dette skal de gjøre ved å vurdere av om eksisterende regelverk på IKT-sikkerhetsområdet er godt nok og ivaretar de nye digitale samfunnsutfordringene. Utvalget skal også vurdere organisatoriske spørsmål og andre virkemidler enn rettslige for å styrke IKT-sikkerheten. I desember 2018 la utvalget frem sin utredning I NOU 2018:14.[25] Utvalget anbefaler at det utvikles en ny lov for IKT-sikkerhet, at det stilles krav til IKT-sikkerhet i alle offentlige anskaffelser og at det etableres et nasjonalt sikkerhetssenter.

SIKKERHET ER IKKE LENGER BARE ET NASJONALT ANLIGGENDE

Sammenkoblingen av teknologi går som regel på tvers av både landegrenser og verdensdeler. Når teknologi og fysiske enheter kobles sammen i et alltid tilgjengelig nettverk kan det åpne for at enkelte aktører får mye makt. Et eksempel på det er analyseselskapet Cambridge Analytica. Cambridge Analytica benyttet blant annet Facebook for å samle inn opplysninger uten at de som eide opplysningene visste om det. Dette ble gjort gjennom plugins utformet som personlighetstester. På denne måten samlet de inn enorme mengder opplysninger om folk over hele verden fra en rekke ulike kilder. Deretter sorterte og sammenstilte de disse, bygde profiler som de solgte videre. Når denne masseinnsamlingen ble satt i system gav den ny, viktig innsikt. Innsikten ble brukt til å bygge profiler som ble benyttet for å påvirke valgkampen i USA da Donald Trump ble valgt som president og avstemmingen om Brexit i Storbritannia. Dette var mulig fordi en utfra så store datamengder kunne trekke slutninger om tilbøyelighet til å stemme opp mot andre preferanser, meninger, oppfatninger og demografi. Dette ble blant annet brukt av de som drev oppsøkende virksomhet for å «fiske stemmer» på døra. Da dette ble oppdaget ble det en stor skandale. Både for Facebook som hadde latt dette skje og for Cambridge Analytica som gikk konkurs. Facebook fikk også høsten 2018 massiv kritikk for en avsløring i New York Times[26] om at de ikke har tatt sitt ansvar for å hindre falske nyheter, falske rykter og politisk desinformasjon som kan påvirke demokratiet.

Utfordringen med slike saker er at dette påvirker maktprinsippet og maktbalansen i samfunnet. Enkelte aktører får enormt mye makt fordi de gjennom kombinasjon av ny teknologi har tilgang til opplysninger og kombinerer disse på nye måter. De store selskapene med denne typen makt anklages for å bruke makten de har til å manipulere markedet, kunden og brukeren Dette gjør at det er viktig å se myndighetsutøvelse, lovverk og tilnærming til muligheter og utfordringer i et globalt perspektiv.

INTERNASJONALT INITIATIV FOR Å MØTE CYBERSIKKERHETSTRUSLER

En rekke av tiltakene beskrevet over som har direkte nasjonal effekt og påvirkning, stammer fra EU initiativ. I tillegg til dette er det verdt å nevne «The Paris Call for Trust and Security in Cyberspace»[27] Frankrikes statsminister Emmanuel Macron gikk i november 2018 i front for et nasjonalt cybersikkerhetsinitiativ. Alle som har underskrevet avtalen skal arbeide sammen for økt forebygging og motstand mot ondsinnet nettaktivitet. Dessuten hindre spredning av ondsinnet programvare, beskytte tilgang til og integriteten til internett, samt samarbeide for å hindre elektronisk valgpåvirkning. De skal også forbedre sikkerheten i digitale produkter og tjenester og samarbeide om å styrke internasjonale standarder.

HAR LOVREGULERING, STRATEGIER, UTREDNINGER OG ANDRE INITIATIV HATT NOEN EFFEKT?

En rekke aktører som jobber med sikkerhet, både på myndighetssiden og i næringslivet, sier at arbeidet med og innføring av nye direktiv eller lover allerede ser ut til å ha hatt en effekt på enkelte virksomheters tilnærming til

24 Regjeringen.no: *«Nasjonal strategi for IKT-sikkerhet»* https://www.regjeringen.no/no/aktuelt/nasjonal-strategi-for-ikt-sikkerhet/id2592996/

25 Regjeringen.no: *«NOU 2018: 14. IKT-sikkerhet i alle ledd — Organisering og regulering av nasjonal IKT-sikkerhet»* https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/

26 NY Times: *«Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis»* https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html

27 France Diplomatie: *«Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace»* https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

sikkerhetsarbeid. Dette kan skyldes at arbeid for å sikre etterlevelse har gitt dem kompetanse de ikke har hatt tidligere. Det kan også skyldes effekten av det arbeidet de må gjøre for å etterleve regelverket. Motivasjonen for å igangsette arbeid knyttet til disse er vanskelig å fastslå og kan være alt fra redsel for økonomiske seksjoner til tap av omdømme eller ønske om å bruke etterlevelse som et konkurransefortrinn. Samtidig tror vi at vi på langt nær alle effekter av disse lovreguleringene er synlige ennå. Dette er likevel en positiv endring fordi det har ført til at virksomheter som ikke har hatt noe forhold til sikkerhet og personvern nå har fått det.

I følge Mørketallsundersøkelsen i 2018 håndterer virksomheter med en strukturert tilnærming til sikkerhet og risiko uønskede hendelser bedre enn andre virksomheter. Derfor lykkes de i større grad med å redusere konsekvensene av slike hendelser. Det betyr at det er bra at myndighetene setter sikkerhetskrav til større deler av privat næringsliv. Samtidig er det usikkert hvilke vurderinger som gjøres for å avgjøre om virksomheten er en del av en grunnleggende nasjonal funksjon eller ikke.

Når det gjelder sikkerhetsloven er NorSIS vurdering at kompetanse innen sikkerhet, spesielt til å vurdere risiko i komplekse infrastrukturer vil være en mangelvare for nasjonen framover. Dette støttes av flere aktører som for eksempel Abelia.[28] Den kompetansen som finnes vil i stor grad bli kjøpt opp av de store industrikonsernene, og offentlige virksomheter. Mindre virksomheter vil slite med å skaffe slik kompetanse, og derfor også slite med å få gjennomført gode risikovurderinger for sin del av den sammenknyttede infrastrukturen.

Mørketallsundersøkelsen viser også at nær halvparten, 48 prosent, av de spurte virksomhetene har gjort endringer eller forbedringer i arbeidet med personvern og IKT-sikkerhet som følge av innføringen av nytt personvernregelverk (GDPR). NorSIS mener dette lover godt for at den nye personopplysningsloven vil ha en positiv innvirkning på virksomheters sikring og behandling av opplysninger fremover.

Når det gjelder strategier, handlingsplaner og opprettelse av nye koordinerende sentre er det vanskelig å se for seg at disse vil ha noen negativ effekt på arbeidet med sikkerhet fremover. Samtidig viser alle disse ulike løpene at dette er et bredt og sammensatt fagfelt med mange aktører og interessenter. Det er derfor viktig med en helhetlig og godt koordinert tilnærming til problemstillinger, utfordringer, løsninger og målgrupper. Ikke minst for å se alle disse initiativene i sammenheng. Dette gjenstår å se om disse parallelle initiativene kan oppnå det og bidra til en tryggere digital hverdag.

28 Regjeringen.no: *«Høringssvar til sikkerhetsloven»* 181001 – Høringssvar – Abelia – Forskrifter til ny sikkerhetslov.pdf

DIREKTØREN HAR ORDET

2018 har vært et år uten de helt store hendelsene knyttet til IKT-sikkerhet. Imidlertid har året vært preget av økt og målrettet svindel mot både SMB-markedet og innbyggeren.

EGENEVNE

Små og mellomstore virksomheter må ta innover seg de truslene de står ovenfor, og erkjenne at de også er et mål for datakriminalitet. Virksomhetene må iverksette risikoreduserende tiltak mot digitale trusler. En risikovurdering skal i størst mulig grad dekke de kjente truslene som eksisterer. Det er de ekstraordinære truslene som man ikke kan forutse, som er vanskeligst å iverksette tiltak mot. Ingen av hendelsene som ble oppgitt i Mørketallsundersøkelsen kan refereres til som «black swans». Dette betyr at mange av hendelsene burde vært forutsett i en risikovurdering og tiltak burde vært iverksatt. Virksomhetene har et eget ansvar for å øke sin egenevne for å beskytte seg. De truslene vi har vurdert som aktuelle i årets utgave av «Trusler og trender 2018-2018» er et utgangspunkt for en trusselvurdering. Samtidig må enhver virksomhet kjenne sine verdier for å kunne treffe riktige tiltak.

MYNDIGHETENES SATSING

Årets kartlegging av innbyggernes sikkerhetskultur viser en generell økning i frykt for digitale trusler og datakriminalitet. Politiet har besluttet å etablere et Cybercrimesenter, som kalles NC3. NorSIS synes det er på tide at dette kommer på plass, da vi gjennom år har påpekt at denne type kriminalitet også må få fokus. Både med tanke på kompetanse, prioritet og organisering.

Det er viktig for samfunnet som helhet at innbyggerne har tillit til digitaliseringen. En generell frykt for digitale tjenester gagner ikke Norge som en digital nasjon. Den sittende regjering har en uttalt politikk for å ta vare på et samfunn med små forskjeller og tillit mellom folk. Økt digitalisering og bruk av teknologi endrer ikke de overordnede målene for samfunnet. Ei heller de grunnleggende behov for individer, virksomheter eller samfunn, men det er viktig å huske på at forutsetningene endrer seg. Vi må ha virkemidler som bidrar til å nå målene og som skaper en tillit mellom folk og samfunnet som helhet. I satsningene som kommer på IKT-sikkerhetsfeltet fremover er det viktig å tenke helhet og maksimere effekten ved et utstrakt samarbeid mellom offentlige etater og sivile organisasjoner. Man må ville og tørre å tenke nytt.

KOMPETANSEHEVENDE TILTAK

Vi i NorSIS ønsker å rette en stor takk til våre samarbeidspartnere i Nasjonal Sikkerhetsmåned. 330 virksomheter deltok og 265.000 ansatte mottok opplæring via NorSIS sine aktiviteter. Flere virksomheter hadde egne aktiviteter og kompetansehevende tiltak. Alle bidrag i oktober medfører økt fokus og bevisstgjøring av digitale trusler og tiltak. Årets tema var sikring av e-post og nettsvindel.

IKT-sikkerhet skal ikke ha fokus bare i oktober, men gjennom en særlig stor bevisstgjøring en måned i året, bidrar vi alle til å sette ytterligere fokus på temaet. Nytt i årets Sikkerhetsmåned var kurs rettet mot innbyggeren. Kurset passer for alle og er ment som en grunnleggende innføring i IKT-sikkerhet. Det ligger på nettvett.no. Vi oppfordrer alle til å iverksette de tiltak som ble formidlet i Nasjonal Sikkerhetsmåned 2018. Særlig gjelder dette innføring av totrinnsbekreftelse der det er mulig.

Med ønske om et sikkert 2019!

Peggy Sandbekken Heie – Administrerende direktør, NorSIS

Rapporten presenterer det NorSIS erfarer har vært de mest fremtredende truslene det siste året. Vi ser særlig på trusler som treffer små og mellomstore virksomheter og befolkningen. I tillegg til hva som allerede treffer oss, beskriver vi hvilke trender vi mener samfunnet vil møte fremover og hvilke utfordringer det innebærer. Truslene som beskrives i årets rapport er: ledelses- og direktørsvindel, uhell, uaktsomhet eller vanvare, ID-tyveri, svindel, utpressing, krenkelser eller mobbing, sabotasje, sikkerhet på reise og spionasje. Trendene vi beskriver er sammenkobling av teknologier og sammenkobling av svindelmetoder.

Norsk senter for informasjonssikring (NorSIS) er en uavhengig ekspertorganisasjon som arbeider for å fremme kunnskap om cybertrusler, effektive sikkerhetstiltak og god sikkerhetspraksis.

Vi informerer om trusler, gir råd om hvordan forebygge datakriminalitet, gir veiledning til de som føler seg krenket på nett og tilrettelegger forum og aktiviteter som bidrar til økt informasjonssikkerhet.

Teknologiveien 22
2815 Gjøvik
+47 40 00 58 99
Org.nr. 995195003
www.norsis.no
post@norsis.no