
Få en tryggere digital hverdag:
TRUSLER
OG TRENDER
2019-2020
NorSIS


Trusler og trender - 2019-2020
Trusler og trender er en årlig rapport utgitt av Norsk senter for informasjonssikring (NorSIS). Rapporten gir et bilde av de alvorligste og mest relevante truslene for privatpersoner og små og mellomstore virksomheter, inklusive kommuner, slik de fremstår på utgivelsestidspunktet. Den skisserer også de mest fremtredende trendene innenfor datakriminaliteten.
Takk for innspill til rapporten fra informasjonssikkerhetsgruppen i Dataforeningen, Kripos, DNB, Nasjonal Sikkerhetsmyndighet (NSM) og Microsoft. Takk også til Bakke Maskinservice som delte sin historie med oss.
De oppdaterte rådene for en trygg digital hverdag får du på våre tjenester Slettmeg.no og Nettvett.no. Her finner du også egne kurs rettet mot privatpersoner og virksomheter.
2

Innhold

Direktøren har ordet

ØKENDE DIGITAL TRUSSEL – MANGE TROR DE ER IMMUNE MOT ANGREP

Det er en stor utfordring at hele en av fire norske virksomheter tror de er nærmest immune mot dataangrep. Samtidig som trusselen om digitale angrep er økende, gjør heller ikke den enkelte innbygger nok for å beskytte seg mot dette.

NorSIS' årlige rapport om trusler og trender er en oppsummering av de truslene som har preget Norge i året som gikk, og som høyst sannsynlig også kommer til å gjøre det i året som ligger foran oss. Vi ser også nærmere på trendene i det digitale trusselbildet for å gi både enkeltpersoner og de mer enn 500 000 små og mellomstore bedriftene i Norge en mulighet til å sikre sine verdier bedre.

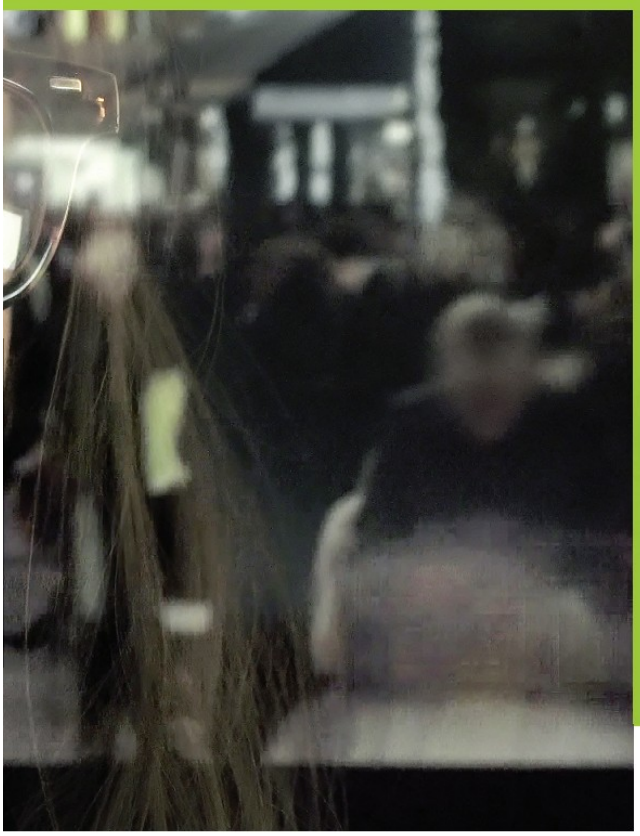
> «Vårt inntrykk er at det har spredd seg en holdning om at det er vanskelig, og nærmest en heldags-jobb, å sikre seg tilstrekkelig mot stadig nye trusler. Slik er det heldigvis ikke.»

For fjerde år på rad ga vi, med støtte fra Justis- og beredskaps-departementet, i september ut rapporten "Nordmenn og digital sikkerhetskultur". Rapporten viser at vi fremdeles ikke er bra nok rustet til å beskytte oss mot de risikoene som et stadig mer digitalt samfunn representerer. Uansett om det er passordbruk, ukritisk åpning av e-poster eller ID-tyveri, har vi fremdeles en vei å gå før vi kan si oss fornøyde. Samtidig viser undersøkelsen at vi opplever mer frykt når vi bruker nettbanken eller deler personopplysninger med det offentlige.

Cybersikkerhetsarbeidet er, som i dette eksemplet, fylt av paradokser. Hvorfor frykter vi at noen skal ta over kontoen vår, samtidig som bare 37 prosent benytter seg av noe så enkelt som totrinnsbekreftelse? Hvorfor er vi redde for å miste dataene våre i lammende løsepengevirus, men lar være å sikkerhetskopiere den samme dyrebare dataen?

Kunnskap og opplæring reduserer frykten

NorSIS tror at dette handler om noe så enkelt som kunnskap. Vet vi mer om det vi frykter, så er sjansen større for at vi sikrer oss bedre. Det høres mye vanskeligere ut enn det er. Vårt inntrykk er at det har spredd seg en holdning om at det er vanskelig, og nærmest en heldagsjobb, å sikre seg tilstrekkelig mot stadig nye trusler. Slik er det heldigvis ikke. Sammen med totrinnsbekreftelse, oppdatert programvare, antivirusbeskyttelse og et enda mer bevisst forhold til hva vi legger igjen av opplysninger om oss selv eller vår egen bedrift digitalt, vil sikkerheten bli dramatisk forbedret.



Derfor satser NorSIS på egne tilrettelagte opplæringskurs, rettet spesielt mot definerte grupper. Bare det siste året har vi lansert eget seniorkurs og et kurs rettet mot små og mellomstore bedrifter.

Cyberkriminalitet er en reell trussel for alle

Oppfatningen om at dette ikke rammer meg selv – som en undersøkelse vi gjennomførte i forbindelse med Nasjonal sikkerhetsmåned viste å være mer utbredt enn vi trodde – må vi også legge bort med en gang. Når en av fire virksomheter tror de er immune mot potensielt lammende dataangrep som det kan koste store summer å rydde opp i, viser det at det er behov for informasjon.

De kriminelle som i dag opererer i den digitale verden, er nemlig ikke bare profesjonelle, utspekulerte og grenseløst frekke. De er også interessert i å tjene mest mulig på sin kriminalitet med minst mulig motstand. Derfor angriper de heller det svake punktet i en verdikjede – en liten eller mellomstor virksomhet – i stedet for å prøve seg på den store og godt sikrede virksomheten som denne lille leverer varer eller tjenester til.

36 %

Kunnskap om trusler eller hacking har fått oss til å avstå fra å bruke en nettjeneste

> «Det er en bekymringsfull trend når kjente personer med høy sosial status i sosiale medier nærmest gjør mobbing til noe som kan aksepteres.»

Omdømmetap kan bli mer kostbart enn selve skaden

Risikoen for den angrepne virksomheten er ikke bare den umiddelbare kostnaden med å få systemet sitt opp å gå igjen og den tapte fortjenesten i perioden med nedetid. NorSIS ser stadig oftere at omdømmetapet er det som gjør mest vondt – det faktum at kunder av den lille bedriften mister tillit til dem. Mange store er selvsagt også redde for at angrep mot et

«Når en av fire virksomheter tror de er immune mot potensielt lammende dataangrep som det kan koste store summer å rydde opp i, viser det at det er behov for informasjon.»

svakt ledd i deres verdikjede igjen kan gjøre dem utsatte for angrep. Det er en reell risiko som vi mener altfor få små og mellomstore bedrifter tar inn i regnestykket. Nettopp denne faren for verdikjedeangrep – hvor det reelle målet for angrepet ikke er bedriften som blir rammet, men en større bedrift høyere opp i næringskjeden – er noe av årsaken til at Nasjonal sikkerhetsmyndighet mener mindre virksomheter er ekstra utsatte for dataangrep.

Samtidig som den digitale utviklingen går i ekspressfart, har det også blitt enda mer synlig hvordan sosiale medier påvirker oss alle med sin massive innsamling av data og manipulering av hvordan vi mennesker forholder oss til hverandre sosialt.

Rollemodellene må ta mer ansvar i den offentlige debatten

Krenkelser, som mobbing og annen hets, er blitt en gjenganger. Vi hører daglig om den smerten og følelsen av håpløshet mange sitter igjen med etter å ha blitt utsatt for netthets. Det er selvsagt ekstra vondt når dette rammer barn og unge.

Gjennom slettmeg.no jobber NorSIS daglig med denne problematikken. Voksne må i langt større grad gå foran som gode forbilder når de kommenterer i sosiale medier. Det er også en bekymringsfull trend når kjente personer med høy sosial status i sosiale medier nærmest gjør mobbing til noe som kan aksepteres. Om det er ment som underholdning, satire eller humor, er det ikke alltid like enkelt for den oppvoksende generasjonen å få med seg denne «merkelappen» på utspillene.

Skillet mellom jobb og privatliv er som på så mange andre områder også her flytende. NorSIS ser stadig oftere at krenkelser mot privatpersoner også kan få en konsekvens på arbeidsplassen til både den som blir krenket og den som krenker. Kampanjer i ulike lukkede og åpne grupper kan også gå ut over alt fra ansatte i barnevernet til lærere eller andre i stillinger som gjerne

skaper sterke følelser hos mange. Dette setter samfunnet på nye og krevende prøver.

Markedsføring og personalisering nye verktøy for kriminelle

Medietilsynets ferske undersøkelse om tillit til mediene* viser at bare seks prosent av den norske befolkningen oppfatter nyheter på Facebook som tillitvekkende. Samtidig er det en kjensgjerning at profesjonell bruk av både budskap og de mange datapunktene som både Facebook og andre tilbyr sine annonsører, gir en enorm mulighet til å påvirke alt fra beslutningsprosesser til valg. Senest ble dette med all tydelighet vist i NRK-programmet Folkeopplysningen. Dette er et redskap som også vil bli brukt av kriminelle i sin målrettede jakt på penger eller data på nett. Som markedsføring blir kriminalitet langt mer effektiv når den målrettes og spesialtilpasses det intetanende offeret.

* Kritisk medieforståelse i den norske befolkningen, oktober 2019, Medietilsynet

Kunnskap om det digitale trusselbildet, de kommende trendene og dine egne verdier er sammen med en oversikt over hvordan du konkret forholder deg til truslene et svært viktig redskap for å bli trygg på nett. Det er nettopp det Trusler og trender 2019–2020 er.

God lesing!

Peggy Sandbekken Heie
administrerende direktør NorSIS

NOEN AV CYBER-HENDELSENE I 2019

JANUAR

- IT-sikkerhetsselskapet Trend Micro har avdekket at 85 apper i Google Play Store har infisert flere millioner Android-brukere verden rundt. Over ni millioner brukere er rammet, skriver selskapet i en pressemelding.

FEBRUAR

- Visma offentliggjør en rapport som sier at hackere fikk tilgang til deres nettverk ved å bruke stjålet påloggingsinformasjon. Visma er sikre på at hackerne ikke har fått tilgang til noen av kundenes nettverk, som skal ha vært formålet med angrepet. Visma Mamut er en ledende leverandør av administrative programvareløsninger og internettbaserte tjenester til små og mellomstore virksomheter i Norge.

- Australias statsminister opplyser at en «sofistikert, statlig aktør» har hacket landets største politiske partier og parlamentet. Dette skjer kort tid før valget i landet.

- Den internasjonale organisasjonen ICANN, som administrerer internett, kunngjør at det pågår et betydelig angrep mot global internettstruktur.

MARS

- Facebook ber myndighetene om hjelp for å beskytte privatliv og data og hindre valginnblanding og spredning av hatytringer.

- Hydro blir utsatt for et omfattende dataangrep som spredde seg til Europa fra virksomheten deres i USA. Selskapet oppga at det dreide seg om et løsepengevirus. Viruset har slått ut selskapets globale nettverk, og de må flere steder bruke reserveløsninger for kommunikasjon og administrative oppgaver. Kripos åpner etterforskning av angrepet. Storbanken DNB innfører nye tiltak for å hindre at lignende ting skal skje hos dem og for å begrense spredningen dersom det skulle skje.

APRIL

- Rundt en av ti kommuner har vært utsatt for dataangrep som førte til tap av data eller arbeidstid det siste året. Men de sliter med å skaffe IKT-spesialister. Det viser tall fra Statistisk sentralbyrå.

JULI

- En av Norges største kryptobørser, Bitcoins Norge, som selv oppgir å ha 25 000 nordmenn som kunder, hevder å ha blitt hacket, skriver Dagens Næringsliv. De skal ha tapt over fire millioner kroner i et dataangrep.

AUGUST

- FN etterforsker minst 35 hackerangrep som Nord-Korea skal ha utført mot 17 land for å stjele penger til et av landets våpenprogram. I en rapport, som et utvalg under FNs sikkerhetsråd har stått for, går det frem at Nord-Korea ved å

utføre dataangrep mot banker og kryptovalutabørser har greid å stjele om lag to milliarder dollar. Pengene skal ha blitt brukt til å finansiere et av landets program for masseødeleggelsesvåpen, slår rapporten fast.

SEPTEMBER

- Politiet flere steder i landet advarer mot å svare på oppringninger fra telefonnummeret 112. De understreker at politiet aldri ringer fra nødnummeret, og at det trolig er snakk om svindel.

- Facebook opplyser at selskapet har fjernet flere titalls tusen applikasjoner som en del av etterforskningen etter Cambridge Analytica-skandalen.

OKTOBER

- Passordene til over 600 000 nordmenn er gjort tilgjengelige på internett etter hacking av flere store nettsider. Ifølge Adresseavisen har en gjennomgang de har gjort av mer enn 1,4 milliarder e-postadresser og passord knyttet 600 000 av disse til Norge. Lekkasjene er fra teknologiselskaper som LinkedIn og Dropbox, samt flere andre mindre nettsteder.

- Dagbladet, DinSide og Seher.no blir stengt etter at en artikkel med grove, falske utsagn ble publisert. Politiet sikter en ungdom for hacking-angrepet.

NOVEMBER

- Det britiske partiet Labour blir utsatt for et «sofistikert og omfattende dataangrep» på sine digitale plattformer. Ifølge BBC skal det dreie seg om et såkalt tjenestenektangrep (DDoS).

- Skatteetaten utsettes for 100 000 forsøk på dataangrep hver eneste dag. Digitale trusler mot norske bedrifter er overveldende, sier samfunnsikkerhetsminister Ingvil Smines Tybring-Gjedde.

Få oversikt over dine verdier og gjør en risikovurdering

Formålet med en risikovurdering er å først kartlegge egne sårbarheter og trusler mot seg selv og sine verdier, for deretter å iverksette sikkerhetstiltak mot de som vurderes å utgjøre størst risiko.

For å komme i gang med en risikovurdering er det derfor viktig at du får en oversikt over virksomhetens verdier. Det kan være penger, tekniske løsninger og tegninger, kontakt-, kunde- eller interessentlister, avtaler eller andre løsninger.

Cyberkriminaliteten profesjonaliseres

– NORDMENN MER SÅRBARE ENN NOENSINNE

Mens mange av de kriminelle som opererer på nett blir stadig mer profesjonelle og nærmest driver som multinasjonale selskap, er den menneskelige faktor en større sårbarhet enn noensinne.

En av truslene som har skapt overskrifter i året som gikk, pornosvindel, kan illustrere dette. Det startet med likelydende e-poster som høyst sannsynlig ble sendt til hundretusener av nordmenn. På dårlig engelsk ble mottagerne gjort oppmerksomme på at de var blitt filmet mens de så på nettporno. Opptakene ville bli offentliggjort dersom de ikke betalte en sum penger, gjerne rundt 5000 kroner i kryptovaluta.

De kriminelle tok seg også bryet med å få tak i ofrenes brukernavn og passord. Dette var trolig nøkkelen til at mange gikk på limpinnen – selve «beviset» på at offerets datamaskin var hacket. Brukernavn og passord er informasjon som relativt enkelt kan kjøpes på det mørke nettet. Informasjonen stammer fra phishing-angrep eller fra datainnbrudd hvor fangsten har vært brukerinformasjonen til hundretusenvis av nordmenn.

Titusener kan ha blitt lurt av pornosvindel

I perioder i fjor formelig kokte det på telefonlinjene til NorSIS. Et stort antall nordmenn hadde mottatt pornosvindeltrusselen og var i tvil om de skulle ta den på alvor. Ifølge en undersøkelse vi gjennomførte kan så mange som titusener av nordmenn ha valgt å betale til sammen flere millioner kroner til de kriminelle bak den falske trusselen.

Så ble pornosvindelen gradvis foredlet. Den dårlige engelsken ble byttet ut med godt norsk. Svindel-e-postene ble mer truende. De truet med å offentliggjøre video av offeret som så på porno med unge tenåringer. Situasjonen ble enda mer tabubelagt. Svindel-e-posten startet gjerne med «Jeg vet du er pedofil». Flere e-poster kom med vedlegg av de såkalte bilde- eller videobevisene. Disse lot seg naturligvis ikke åpne, rett og slett fordi det aldri eksisterte noen bevis.

> «Ifølge en NorSIS-undersøkelse kan så mange som titusener av nordmenn ha valgt å betale til sammen flere millioner kroner til de kriminelle bak "pornosvindelen".»

Tar i bruk moderne markedsføringsmetoder

På mange områder ser NorSIS at svindlere og utpressere i økende grad benytter de samme metodene som profesjonelle markedsførere for å få ut sine budskap. De definerer og analyserer målgruppene sine. I ytterste konsekvens henter de

inn informasjon om alt fra bosted og inntekt til sivilstatus og interesser. Det er ikke uten grunn at beløpene ved pornosvindel og utpressing gjerne ligger på rundt 5000 kroner. Beløpet er stort nok til at svindlerne kan få inn sin fortjeneste, men lavt nok til at offeret betaler i stedet for å anmelde forholdet.

En pornosvindel anno 2020 kan derfor meget vel bli enda mer målrettet. Det skal ikke mer enn et Google-søk til for å finne ut i hvilken målgruppe svindlerne har størst sannsynlighet for å treffe noen som nylig har sett på pornografi, og dermed kan de øke trusseleffekten.

Minst 50 ble «Olga-svindlet» i 2019

Den såkalte Olga-svindelen er et stjerneeksempel på hvor lett det er å målrette svindelforsøkene. Ifølge DNB het nemlig en overvekt av de som ble lurt til å oppgi BankID og senere svindlet nettopp Olga. Dette er et navn som i dag typisk tilhører noen over 80 år. Ved et enkelt søk på SSBs navnestatistikk, har svindlerne målrettet seg mot eldre kvinner – en gruppe som tradisjonelt har hatt svakere digitale ferdigheter enn landsgjennomsnittet. Så langt har banken registrert rundt 50 såkalte Olga-svindler i 2019. I midten av november tydet imidlertid mye på at bankene sammen med politiet fikk stoppet denne bølgen. Det viser at målrettet innsats og samarbeid mellom flere aktører kan gi gode resultater.

36 prosent

Økningen i bedragerianmeldelser fra næringslivet i 2018

> «Den såkalte Olga-svindelen er et stjerneeksempel på hvor lett det er å målrette svindelforsøkene.»

Akkurat som med Olga-svindelen, er det en klar tendens til at de kriminelle i økende grad tar i bruk direkte dialog som verktøy. Det er sannsynligvis enklere å lure sensitiv informasjon ut av ofrene via en telefonsamtale enn å gå den lange veien med et datainnbrudd. Noen få informasjonsbiter om ofrene er ofte alt som skal til for å øke sjansen for en vellykket svindel. Mennesket er vanedyr. Man kan ofte forutse hvordan vi reagerer på kort og litt lengre sikt på en utpressing eller andre former for kriminalitet. Den menneskelige faktor og vår forutsigbarhet blir svært synlig i møte med profesjonelle og godt organiserte kriminelle.

Styres som et internasjonalt selskap

Det er en kjensgjerning at svindlere og utpressere er blitt langt mer profesjonelle bare det siste året. Det mener vi ganske enkelt henger sammen med at den digitale verden vi lever i også er

blitt mer profesjonell. Akkurat som i en virksomhet handler det om å få mest mulig utbytte med minst mulig innsats. Jobber som andre kan gjøre raskere, billigere og bedre blir outsourcet. Det er enkelt å kjøpe fiks ferdig hyllevare som kan spionere, kryptere eller låse alt som skjer i et IT-system. «Cybercrime as a service» skjer primært på det mørke nettet, og fortsetter å vokse. Kryptert kommunikasjon og betaling i disse kanalene gjør det ifølge Europol* enda mer utfordrende for myndighetene å stoppe markedsplasser for kjøp og salg av kriminalitet.

I likhet med ordinære virksomheter, følger også de kriminelle pengene. Det er grunnen til at Norge som et rikt og svært digitalisert land også i tiden fremover sannsynligvis vil være et attraktivt mål. Sikkerhetsselskapet Symantec har tidligere trukket frem nettopp Norge som ett av de landene i verden som er mest utsatt for e-poster som inneholder skadevare.

Leier løsepengevirus for under 600 kroner dagen

En av de store truslene i året som gikk, spesielt mot SMB-markedet, har vært løsepengeviruset. Dette er et ondsinnet program som typisk ender opp på virksomhetens servere ved at en ansatt klikker på en lenke og laster ned skadevare fra en e-post. Når det ondsinnede programmet blir åpnet, krypteres alt som ligger på serveren. Virksomheten får beskjed om at alle filene er låst og utilgjengelige for dem, helt til de betaler en gitt sum i løsepenger.

56 %

Andelen bedrifter som har vært angrepet eller forsøkt angrepet med ondsinnede e-poster

> «Ifølge Europol har antallet verdikjedeangrep økt med hele 78 prosent innenfor enkelte sektorer i 2018. De tror det vil bli enda mer av denne typen angrep i tiden fremover.»

Slik ondsinnet programvare er tilgjengelig for en billig penge på det svarte markedet. Ifølge en fersk rapport fra sikkerhetsselskapet Flashpoint** kan denne type «exploit kits» leies for så lite som 80 dollar om dagen. For en uke må du ut med opptil 700 dollar.

Europol omtalte nylig løsepengevirus som den største trusselen for datasikkerheten i Europa.

Det finnes ingen konkrete tall på hvor mange som er blitt rammet, men ifølge Næringslivets sikkerhetsråds KRISINO-undersøkelse*** for 2019 oppgir 15 prosent av de spurte virksomhetene at de har vært utsatt for løsepengevirus i løpet av de 12 siste månedene. Med rundt en halv million små og store virksomheter i Norge utgjør dette med andre ord et enormt problem. Det synes heller ikke å bli mindre i uoverskuelig fremtid.

Dobling i investeringsbedrageri og kraftig økning i datingsvindel

Målet med mange av truslene i NorSIS' oversikt er på et eller annet vis å skaffe seg direkte tilgang til penger. Ifølge tall fra DNB økte datingsvindel med hele 75 prosent de 10 første månedene i fjor. I alt fikk de inn 478 enkeltsaker på dette. Såkalt investeringsbedrageri økte også i fjor til hele 947 saker. Det er mer enn det dobbelte av hva det var i 2018. Mengden som ble svindlet ved hjelp av såkalte phishing-e-poster, der du blir lurt til å gi fra deg påloggingsinformasjon eller personlige opplysninger på falske nettsider, var enorm, uten at DNB kan si akkurat hvor stor den er da disse angrepene treffer forbrukere hele tiden under ulike merkevarer.

DNB-tallene for de 10 første månedene i fjor viser også at antallet fakturasvindel og såkalt direktørsvindel var omtrent på samme nivå som året før, men beløpene det ble svindlet for økte. I november har det ifølge dem vært en økning i antall saker knyttet til direktørsvindel ved bruk av kompromittert e-post.

Et energiselskap i Stavanger-regionen skal i høst ha blitt svindlet for 150 millioner kroner ved direktørsvindel.

Data og opplysninger er mer verdt enn noensinne

Den valutaen som flest jakter i det illegale markedet i dag, handler også om penger, men på en mer indirekte måte. Personopplysninger, data om virksomheter som organisasjonsnummer og lignende har de siste årene blitt en verdifull vare. Ditt brukernavn og passord, eller for den saks skyld dine helseopplysninger, er også attraktive – både for tilsynelatende seriøse virksomheter og de kriminelle.

Opplysninger om helsen din kan være nyttig både for forskning og til målrettet digital reklame. På det mørke nettet selges også fulle identiteter, inklusive helseopplysninger, fødselsdato, navn på nære slektninger og finansiell informasjon, som fulle identitetspakker (såkalt fullz). Disse brukes til alt fra ID-tyveri til utpressing.

Angriper det svakeste leddet i en verdikjede

Med den voldsomme digitaliseringen hvor alt fra kaffetrakter til vaskemaskin og ventilasjonsanlegg er koblet mot nett, har vi som samfunn fått verdikjeder som er mer sårbare. Stadig flere prosesser er koblet til nett, enten det gjelder fakturering i virksomheten eller banktjenester. Det samme tettvevde systemet omfatter også ulike virksomheter og programmer. Vi har allerede sett en vridning der kriminelle i økende grad angriper disse legitime kanalene og systemene, simpelthen fordi det er mindre motstand her enn i de ofte godt sikrede IKT-systemene. Spesielt er SMB-markedet ekstra sårbart. Manglende kompetanse og færre ressurser til å ha oversikt over systemene er hovedårsaken til at de er spesielt utsatte.

Ifølge Europol* har antallet verdikjedeangrep økt med hele 78 prosent innenfor enkelte sektorer i 2018. De tror det vil bli enda mer av denne typen angrep i tiden fremover.

1 av 4 ledere

har opplevd nedetid eller driftsavbrudd som skyldes sikkerhetsbrudd

Kontohacking langt mer risikofylt enn mange tror

Det svakeste leddet i en verdikjede er den korteste veien til mest mulig fortjeneste for de kriminelle. En av de enkleste og vanligste truslene er såkalt kontohacking. Bare i 2019 fikk NorSIS hundrevis av henvendelser fra virksomheter eller personer som mistet kontrollen over en eller flere av sine kontoer i sosiale medier. Det er dessverre slik at bare halvparten av alle nordmenn**** bruker forskjellige passord for de fleste tjenester på nett. Mer enn seks av ti nordmenn bruker heller ikke sikker pålogging, såkalt totrinnsbekreftelse. Dersom noen først får tilgang til Facebook-kontoen din, er veien kort til de andre personlige kontoene der du bruker samme brukernavn og passord.

> «På mange områder ser NorSIS at svindlere og utpressere i økende grad benytter de samme metodene som profesjonelle markedsførere for å få ut sine budskap.»

Mister du tilgangen til en e-postkonto i virksomheten din, kan det være kritisk. Da kan kriminelle få tilgang til sensitive opplysninger ved at andre utgir seg for å være deg på e-post. Det er et perfekt utgangspunkt for direktørsvindel, fakturasvindel eller annen type kriminalitet.

Mange tror at kapring av Facebook-kontoen er en betydningsløs hendelse i en økonomisk sammenheng. Det er ikke nødvendigvis det som står på veggen din som er sensitivt, men all informasjonen uvedkommende får tilgang til gjennom din Messenger. Her deles det ofte opplysninger om alt fra bankkonto til bilder og annet som kan misbrukes av svindlere.

Det er bare én god måte å møte stadig mer profesjonelle kriminelle på – nemlig ved å bli mer profesjonell i din tilnærming til informasjonssikkerhet.

* Internet Organised Crime Threat Assessment (IOCTA), 2019

** Pricing Analysis of Goods in Cybercrime Communities, cybersikkerhetsselskapet Flashpoint 2019

*** Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) 2019, Næringslivets sikkerhetsråd

**** Nordmenn og digital sikkerhetskultur 2019, NorSIS

Absolutt hele kassasystemet til Bakke Maskinservice i Øystre Slidre kommune ble lammet da bedriften i august ble rammet av løsepengevirus. – Det kostet oss vanvittig mye, både i arbeidstimer og datastøtte, sier medeier Kristin Bakke.

Serveren hvor alt som var mottatt og registrert av fakturakjøp var lagret, ble kryptert i angrepet.

I tillegg til butikk, driver familien også et traktorverksted. Her var det gjort mange store ordrer som de ikke lenger hadde tilgang til. Flere hundre tusen kroner i varer som de ennå ikke hadde mottatt penger for, var plutselig utilgjengelig.

> «Vi var uten kassasystem i fjorten dager. Da ble alt ført manuelt med penn og papir. Selv om vi har greid å spore opp mye, tror jeg vi aldri får full oversikt over hva vi har tapt av varer.»
>
> Kristin Bakke, medeier i Bakke Maskinservice AS

– Det var et mareritt som har kostet oss masse, både i tid og penger. Vi la ut en melding til kundene våre på Facebook og ba dem sa ifra om de hadde vært innom og hentet ut noe i det aktuelle tidsrommet. Mange av kundene våre er innom flere ganger i uka, så det var naturlig nok flere som hadde problemer med å huske, sier Bakke.

Sen betaling ville gi høyere løsepengesum

Alt startet en tidlig morgen i august. Kassasystemet virket ikke, og Kristin og samboeren gikk inn på rommet hvor serveren står. Fra skjermen lyste beskjeden mot dem:

«Deres viktige filer er nå kryptert fordi det er et sikkerhetsproblem med deres PC. Nå må du sende en e-post til oss med din personlige informasjon. Denne e-posten er en bekreftelse på at du er klar til å betale for en dekrypteringsnøkkel.»

– Vi hadde hørt om krypteringsvirus før, men man tenker jo alltid at «det skjer ikke oss». Løsepengesummen ville øke etter hvert som vi ventet. Vår dataleverandør rådet oss imidlertid til å ikke betale, sier Bakke.

Leverandøren av økonomisystemet til Bakke Maskinservice fortalte at flere av kundene deres hadde blitt angrepet av løsepengevirus. Dette var imidlertid første gang at krypteringen gikk ut over hele databasen.

Lå i systemet i 12 dager

Ikke bare låste viruset systemet – det hadde også hindret

Løsepengevirus lammet Valdres-butikk i flere uker:

– KOSTET OSS VANVITTIG MYE TID OG PENGER

daglig backup av data fra kassasystemet i hele 12 dager før den faktiske krypteringen.

– Vi brukte vanvittig med tid på å få samlet sammen flere hundre ordrer. Vi gikk også gjennom videoovervåkningssystemet i butikken for å se hvem som hadde vært innom og handlet i denne perioden, sier Bakke.

Løsepengeviruset medførte også at de måtte bruke penger på mange timer med datasupport.

– Vi var uten kassasystem i fjorten dager. Da ble alt ført manuelt med penn og papir. Selv om vi har greid å spore opp mye, tror jeg vi aldri får full oversikt over hva vi har tapt av varer. Samtidig er det selvsagt en lettelse at ikke regnskap og data for flere år ble borte, sier Kristin.

Aldri aktuelt å betale

Å betale løsepengekravet var aldri aktuelt.

– Nei, absolutt ikke. Om det er noen kunder som har fått gratis varer av oss, så tenker vi at det er bedre enn å betale de som står bak viruset, sier Bakke. – Vi trodde jo at vi hadde backup, og var egentlig ganske optimistiske først. Fortvilelsen tok imidlertid over da vi skjønte at backup ikke hadde vært gjort på tolv dager. August er en travel måned for oss, og vi visste da at mange ordrer var borte.

Selv nå, flere måneder etter angrepet, kjenner de imidlertid på usikkerheten angrepet har skapt.

– Vi har skaffet oss cyberforsikring og er enda mer nøye med å kontrollere at backup av dataen vår faktisk skjer. Samtidig vet vi ikke helt sikkert om de har hatt tilgang til andre ting på PC-ene våre. Det kjenner en jo litt på, sier medeier av Bakke Maskinservice, Kristin Bakke.

Tre kjappe tips for bedre sikkerhet

1. Alle bør aktivere såkalt totrinnsbekreftelse for pålogging på sine digitale kontoer.
2. Virksomheter bør benytte DMARC eller tilsvarende for å sikre e-postkontoer. Dersom din virksomhet har implementert dette, sammen med SPF/DKIM, vil andre, når de mottar en e-post som angivelig er fra deg eller din virksomhet, enklere kunne finne ut om avsenderen er ekte eller falsk.
3. Det er viktig med intern åpenhet om sikring av opplysninger og en kultur der alle oppfordres til å melde fra om ting som avviker fra normalen.


Trusler og trender - 2019-2020
16

DETTE ER DE 10 STØRSTE DIGITALE TRUSLENE AKKURAT NÅ

LØSEPENGEVIRUS

ID-TYVERI

FALSKE TRUSLER OG UTPRESSINGSKRAV (SOM PORNOSVINDEL)

PHISHING

EKTE UTPRESSING OG SVINDEL

KONTOHACKING

DATAINNBRUDD

MENNESKELIG FEIL

KRENKELSER

VERDIKJEDEANGREP

LØSEPENGEVIRUS

Løsepengevirus er en av de vanligste truslene mot små og mellomstore bedrifter i Norge og Europa for øvrig, og også en av de som øker mest.

Hva er det?

Løsepengevirus krypterer filene på offerets datamaskin og krever løsepenger for å frigjøre dem. Dette er en stor trussel mot virksomheter som har mange virksomhetskritiske filer lagret i sine datasystemer, og dermed mister tilgang til dem.

Hvordan gjøres det?

Løsepengevirus er en type skadevare som først og fremst spres via vedlegg og linker i e-post, Microsoft Office-filer eller via infiserte nettsider.

Forholdsregler

- Vær kritisk til hva du laster ned og hvilke programmer du installerer på maskinen din. Er det en troverdig avsender?
- Ta jevnlig sikkerhetskopi av filer som er viktige for deg.
- Hold datamaskinens operativsystem og programvare oppdatert.
- Bruk antivirusprogram og sørg for at det er oppdatert.
- Løsepengevirus sprer seg. Unngå derfor å ha andre disker og enheter koblet til datamaskinen til enhver tid.
- Løsepengevirus kan også spre seg til skytjenestene dine, som Dropbox eller OneDrive. Derfor bør du unngå å være tilkoblet disse hele tiden, men heller logge deg på og av etter behov.

Når du er rammet

Betal aldri løsepenger! Det er ingen garanti for at du får tilbake tilgang til innholdet på datamaskinen. Ved å betale, holder du liv i denne typen kriminalitet.

Unngå spredning – koble deg av nettet. Koble alle enheter som har krypterte filer fra nett. Dette gjelder både datamaskinen og eksterne harddisker og USB-minnepinner.

Finn et dekrypteringsverktøy. På nomoreransom.org kan du se om det finnes et dekrypteringsverktøy for løsepengeviruset du er rammet av.

ID-TYVERI

Mer enn 100 000 nordmenn har vært utsatt for ID-tyveri.* Dette blir ofte utført av noen du har en nær relasjon til, men stadig oftere også av kriminelle. ID-tyveri rammer både virksomheter og privatpersoner.

Hva er det?

Noen benytter seg av ditt ID-bevis, din tilgang til et system eller en konto og utgir seg for å være deg. Misbruket kan være alt fra å bestille en vare eller tjeneste i ditt navn til å påføre deg eller virksomheten din et omdømmetap ved å utgi seg for å være deg.

Hvordan gjøres det?

Personlige opplysninger som påloggingsinformasjon eller finansielle opplysninger og organisasjonsnummeret samles inn. Dette kan gjøres ved hjelp av ondsinnet e-post hvor du blir bedt om å oppgi informasjon (phishing) eller via SMS (smishing). Målrettede kampanjer mot enkeltvirksomheter eller personer (spear fishing) forekommer også langt oftere. Datalekkasjer hos tjenesteleverandører er en informasjonskilde. Også datainnbrudd (hacking) benyttes.

Forholdsregler

- Ikke oppgi personlig informasjon til ukjente over internett, på telefon eller e-post.
- Klikk aldri på lenker i e-poster for å legge inn personinformasjon på siden du kommer til. Skriv heller adressen til nettstedet rett inn i adressefeltet i nettleseren din.
- Sikre dine kontoer for e-post og nettsamfunn med totrinns-bekreftelse.
- Lås postkassen din for å hindre tyveri av personopplysninger.

Når du er rammet

Vær rask. Hva er forsvunnet/misbrukt av informasjon og identitetsdokumenter?

Anmeld forholdet. Da har du dokumentasjon på det faktiske forholdet.

Ta kontakt med banken. Steng umiddelbart rammede kontoer. Be om skriftlig dokumentasjon på at dette er gjort. Påpek urettmessige transaksjoner raskt.

Be om frivillig sperring hos kredittopplysningsbyråene. De fleste som gir kreditt, vil verifisere din kredittverdighet hos selskap som Bisnode, Experian, Creditsafe eller Evry. En sperring hos disse vil kunne verne deg mot ytterligere skade.

Følg nøye med på postgangen – at den kommer som normalt. Vurder å sperre deg mot uønsket adresseendring hos Posten.

Bruk forsikringen. Mange har i dag en ID-tyveriforsikring innbakt i innboforsikringen.

ID-tyveri på nett: Reager umiddelbart dersom du mottar informasjon om at det er opprettet en konto i ditt navn eller at brukerrettighetene for din konto er endret. Les flere tips på nettvett.no.

* Representativ årlig undersøkelse utført for NorSIS og Skatteetaten

FALSKE TRUSLER OG UTPRESSINGSKRAV (som pornosvindel)

E-poster med usanne påstander om at du har blitt hacket har blitt en av de største truslene som rammer både folk flest og små og mellomstore bedrifter.

Hva er det?

Svindelen eller utpressingsforsøket starter gjerne med en e-post hvor du får beskjed om at svindlerne sitter på video eller bildemateriale av deg mens du ser på porno. Dette har de fått ved å hacke seg inn på PC-en din. Det såkalte beviset er ofte at de oppgir passordet ditt. De truer med offentliggjøring hvis du ikke betaler.

Hvordan gjøres det?

De ondsinnede e-postene er svært ofte masseutsendte. Passorddetaljer, brukernavnet og telefonnummeret er ofte det lille de har av personlig preg. Dette er informasjon de kriminelle har fått fra store datalekkasjer og som automatisk settes inn i den masseutsendte e-posten. Du er ikke hacket.

NorSIS har også sett flere eksempler på falske trusler om kidnapping eller bombetrusler dersom du ikke etterkommer kravet om betaling.

Forholdsregler

- Vurder om e-posten kunne ha blitt sendt til mange andre uten at teksten ble endret vesentlig.
- Et fellestrekk ved de falske utpressingskravene er at de kriminelle ber om betaling i kryptovaluta.
- Stemmer alle påstandene i e-posten? Har du ikke webkamera på din PC og de sier at de har filmet med dette, er det et sikkert tegn på at trusselen er falsk.
- De falske truslene blir ofte fremsatt på engelsk, svensk eller dårlig norsk. Samtidig ser NorSIS en tendens til at oversettelsene i de ondsinnede e-postene blir stadig bedre.

Når du er rammet

Bytt passord. Om du får en e-post med et av passordene dine, er det et sikkert tegn på at det er kjent for andre. Da må du umiddelbart bytte passord. Dersom du bruker samme passord på flere tjenester, må du bytte passord til alle tjenestene. Bruk ulike passord til ulike tjenester, og aktiver gjerne totrinnsbekreftelse. Sjekk også på haveibeenpwned.com om flere av passordene dine er offentlig kjent og må byttes.

Betal aldri det falske kravet!

Det er ufarlig å slette e-posten. Det er heller ikke noe risiko forbundet med å ta vare på den.

Phishing er ifølge Europols siste rapport om cybersikkerhet en av de aller største kjernetruslene mot privatpersoner og virksomheter, og danner ofte utgangspunktet for en rekke andre former for kriminalitet.**

Hva er det?

Kriminelle lurer deg til å oppgi sensitiv informasjon om deg selv eller din virksomhet. Dataene brukes til ID-tyveri, utpressing og svindel, eller videreselges til andre kriminelle.

Hvordan gjøres det?

Ved phishing-angrep kontaktes offeret som regel via e-post, og avsenderen fremstår som en reell virksomhet, for eksempel en bank. De kan også benytte seg av «hackede» profiler og kontakte profileiers venner via meldinger eller SMS (såkalt smishing). Offeret lures til å klikke seg inn på en falsk nettside for å «logge seg inn» eller oppgi sensitiv informasjon som fødselsnummer eller organisasjonsnummer. Svindlerne spiller gjerne på fristelse, frykt eller tillit. De kan lokke med at du kan vinne noe i en konkurranse hvis du deler personlig informasjon (fristelse), meldingen kommer fra noen du kjenner (tillit) eller du blir bedt om å installere et program for å stoppe et virus du skal ha fått (frykt). Svindlerne kan også ringe fra falske telefonnummer og be om personopplysninger (såkalt spoofing).

** Internet Organised Crime Threat Assessment (IOCTA) 2019

Forholdsregler

- Sjekk avsenderadressen.
- Send aldri personlig eller finansiell informasjon via e-post.
- Hold musepekeren over adressen og se hvor e-posten egentlig kommer fra. Se også om adressen er feilstavet eller inneholder en .com-ending i stedet for .no, osv.
- Vurder avsender og nettside nøye før du gir fra deg informasjon.
- Selv om det står https:// og hengelåssymbol i adressefeltet, kan siden være upålitelig og brukes til phishing.
- Dersom du får opp en adresse, kan du skrive denne direkte inn i søkefeltet i stedet for å klikke på den.
- Husk at om du klikker på en link, er det ikke krise. Det er først når du oppgir informasjon eller laster ned noe at du kan få problemer.
- Vær på vakt om du mottar en melding fra en bekjent som fremstår som spesielt merkelig. Denne kan være falsk.
- Hold operativsystem og programmer oppdaterte. Benytt også oppdatert antivirusprogram.

Når du er rammet

Kontakt banken eller kredittkortselskapet umiddelbart. Kontroller kontoen nøye for mistenkelige belastninger.

Vurder politianmeldelse.

EKTE UTPRESSING OG SVINDEL

Selv om det er få som blir rammet av dette, er det ofte en ekstremt stor påkjenning for de det gjelder. For privatpersoner er dette ofte knyttet til seksuell utpressing og datingsvindel. For næringslivet er spesielt direktørsvindel og fakturasvindel utfordrende.

Hva er det?

Seksuell utpressing: Et typisk offer kommer i kontakt med unge utenlandske kvinner på en datingside eller chattetjeneste. Samtalen flyttes etter hvert over til en kanal der videosamtale er mulig. Personen som tar kontakt, kler av seg og utfører seksuelle handlinger med seg selv i en videosamtale. Offeret blir oppfordret til å gjøre det samme. Dette blir videofilmet, og så truer svindlerne med å spre videoen dersom offeret ikke betaler penger, gjerne 3000–5000 kroner.

Datingsvindel: Dette starter gjerne med en henvendelse eller venneforespørsel fra en person, gjerne en tidligere amerikansk soldat, en suksessfull forretningsperson eller en flott dame. Tilliten bygges opp gjennom flere måneders dialog på nett. Så oppstår det en «uforutsett hendelse» der vedkommende trenger penger fra offeret for å løse et problem raskt. Svindleren tilbyr gjerne et fysisk møte hvis offeret betaler.

Direktørsvindel: Svindleren sender en e-post eller SMS til en økonomimedarbeider, tilsynelatende fra en direktør eller annen sjef i virksomheten. «Direktøren» ber om en større overføring til et gitt kontonummer eller betaling av en falsk faktura.

Telefonsvindel (wangiri): Offeret blir ringt opp fra et ukjent utenlandsk telefonnummer. Etter at det har ringt et par ganger, blir det lagt på. Ringer man opp igjen til dette telefonnummeret, er det et høytakstnummer der man blir belastet med en svært høy minuttpris.

Fakturasvindel: Spesielt mot slutten av 2019 så NorSIS et oppsving i antall fakturasvindler mot norske små og mellomstore virksomheter. Her sender svindlerne ut fakturaer for reelle tjenester eller produkter mottatt av andre, men med deres eget kontonummer. Den falske fakturaen blir oversendt etter lengre tids sosial manipulering, typisk via e-post, slik at bedriften skal tro at fakturaen er ekte.

Investeringsbedrageri: Du lokkes til å investere pengene dine på nett, ofte i produkter eller tjenester som få har kunnskap om, som kryptovaluta eller valutaspekulasjoner. Svindlerne benytter seg av falske nettsider, som gjerne inneholder grafer med falsk kursutvikling. Svindlerne ringer deg også opp med investeringstips. Ofte blir denne type investeringsbedrageri solgt inn med falske nyheter i sosiale medier, der kjente personer forteller hvor mye de har tjent på dette.

Forholdsregler

Seksuell utpressing på nett

- Ikke svar. Dette er organiserte kriminelle. Om du gjør deg utilgjengelig, er det mulig at de forstår at de kaster bort tiden, og går videre til neste offer.
- Ikke betal. NorSIS sin erfaring er at betaling bare medfører flere og høyere krav.
- Anmeld saken til politiet. Dokumenter mest mulig av hva som har skjedd, og ta skjermbilder.
- Bryt kontakten ved å blokkere utpresseren. Ikke slett kontoer eller installert programvare før politiet har gjort sine undersøkelser.
- Ofte publiserer de kriminelle videoen på tjenester som Flickr, og truer med å dele link til videoen. Ta kontakt med tjenesten selv og be dem fjerne videoen. Guide til dette finner du på Slettmeg.no.

! Forebyggende tiltak mot utpressing er å skjule vennelisten sin på Facebook, skjule profilen sin på søkemotorer og sørge for at din tidslinje bare er tilgjengelig for venner.
Les mer på nettvett.no/seksuell-utpressing-pa-nett/.

Datingsvindel

Vær skeptisk dersom

- den du chatter med ber om penger
- han eller hun er veldig opptatt av å trekke samtalen over på en annen kanal
- vedkommende søker privat informasjon om deg og er veldig opptatt av å bygge tillit hos deg
- han eller hun sender deg store mengder e-post og er pågående
- profilens profilbilde ser profesjonelt ut eller er arrangert med tillitsskapende detaljer som uniformer eller spesielt velkledde personer

! Dersom du oppdager at du er utsatt for datingsvindel: Stopp alle utbetalinger til personen. Saken bør anmeldes til politiet. Kontakt også banken din dersom du har gitt fra deg informasjon som kan gjøre at svindleren kan tappe deg for ytterligere verdier.

Direktørsvindel

- Les e-poster der det anmodes om overføring av penger to ganger.
- Ledelsen bør informere sine økonomimedarbeidere på forhånd hvis de vet at det kan være aktuelt med raske pengeoverføringer i tiden som kommer.
- Hvis du som økonomimedarbeider mottar e-post fra sjefen om å overføre penger, kontakt sjefen på telefon eller SMS for å få en bekreftelse på at overføringen er reell.
- Dersom det står et telefonnummer i e-posten eller du får en SMS-forespørsel om overføring – ikke bruk disse numrene. Der treffer du sannsynligvis svindleren i den andre enden.

! Dersom transaksjonen gjennomføres, må du ringe banken med en gang for å varsle om hendelsen. Anmeld også saken til politiet.

Fakturasvindel

- Sjekk alltid med leverandøren som har byttet kontonummer om dette virkelig stemmer. Dette bør gjøres på telefonen, ikke på e-post.

Investeringsbedrageri

- Gjør et google-søk på firmaet og eventuelt den kjente personen som fronter annonsen. Hvem driver nettsiden? Har andre lagt ut advarsler mot firmaet?
- Blir du kontaktet direkte, så spør deg selv om det er naturlig at de henvender seg til akkurat deg.
- En seriøs aktør vil aldri be deg oppgi passord til nettbank eller annen sensitiv informasjon. Husk at også kopi av pass eller annen legitimasjon er sensitiv informasjon.

! Høres noe for godt ut til å være sant, er det gjerne det.

KONTOHACKING

Hvert år får NorSIS og Slettmeg.no hundrevis av henvendelser fra enkeltpersoner eller virksomheter som har fått sine kontoer på Facebook, Instagram, e-post eller lignende hacket. Dette er en trussel som er lett å forebygge.

Hva er det?

Hackere eller andre personer har tatt over en persons eller virksomhets konto og kan bruke denne.

Hvordan gjøres det?

Innloggingsinformasjonen kan ha blitt gjort tilgjengelig for andre gjennom store datainnbrudd. Brukere kan også ha delt passordet med andre eller blitt fralurt påloggingsinformasjon ved phishing-angrep. For virksomheter kan det å få sin konto hacket og misbrukt få svært store konsekvenser for tusenvis av deres kunder. Det medfører gjerne også et omdømmetap for virksomheten hvis deres kontoer har blitt misbrukt til spredning av svindel og lignende.

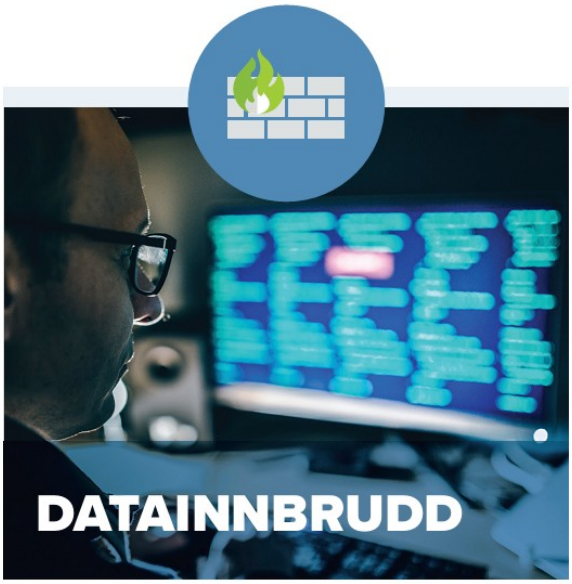
Forholdsregler

- Totrinnsbekreftelse er et enkelt tiltak som bedrer sikkerheten betraktelig. Det fungerer ved at du logger inn med brukernavn og passord slik du pleier, men ved førstegangs pålogging fra en ny enhet må du også oppgi en engangskode. Denne koden får du gjerne tilsendt til din mobil per SMS eller via en app.
- Det er viktigere å bruke unike passord på de ulike tjenestene og systemene man benytter enn å bytte passord ofte. Lag deg en huskeregel for passord som gjør at du kan lage variasjoner over en frase som sikrer unike passord for hver enkelt tjeneste. Ikke del passordene dine med andre. Flere råd om passord finner du på nettvett.no.
- Skriv gjerne passordene ned på et papir som du lagrer på et trygt sted eller benytt passordhåndteringsprogrammer.

Når du blir rammet

Ta kontakt med leverandøren av tjenesten. De må få bekreftet at det er du som er den rettmessige eieren. Dette gjøres som regel ved å sende inn en kopi av gyldig ID, som førerkort, bankkort eller pass.

Bruk Slettmeg.no sine guider. Her har NorSIS samlet en oversikt over fremgangsmåten ved kontohacking for de mest brukte nettjenestene.



Mer enn hver tiende norske virksomhet har vært utsatt for forsøk på datainnbrudd eller hacking.*

Hva er det?

Utenforstående bryter seg inn i et datasystem. Målet kan være alt fra å stjele forretningshemmeligheter, kundelister eller personopplysninger til spionasje og sabotasje. Det kan også være et ledd i et angrep der en mindre virksomhet blir brukt for videre angrep mot en større eller mer attraktiv aktør som disse samarbeider med.

Hvordan gjøres det?

Det kan enten gjøres ved at hackere angriper sårbarheter i et system eller at noen i virksomheten uforvarende laster ned ondsinnet programvare som gir de kriminelle adgang til deres IT-system.

Forholdsregler

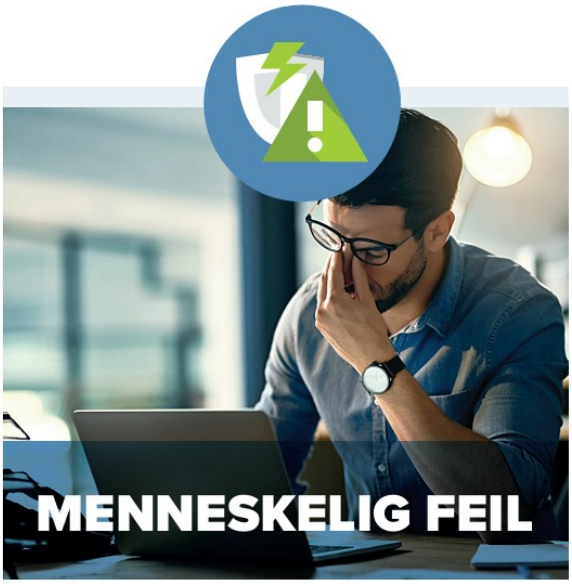
Disse fire tiltakene forhindrer 9 av 10 dataangrep:

1. Oppgrader program- og maskinvare.
2. Vær rask med å installere sikkerhetsoppdateringer.
3. Ikke tildel sluttbrukere administratorrettigheter. De fleste vanlige brukere har ikke behov for å installere programvare på maskinen.
4. Blokker kjøring av ikke-autoriserte programmer. La brukerne kjøre kun godkjente programmer ved å bruke verktøy som Windows AppLocker.

Når du blir rammet

Slå av PC-en, trekk ut nettverkskabelen og kontakt IT-ekspertise med en gang.

*NSR Mørketallsundersøkelsen 2018



Ifølge Mørketallsundersøkelsen 2018 fra Næringslivets sikkerhetsråd skyldes mer enn halvparten av sikkerhetsbruddene i norske virksomheter menneskelig feil.

Hvordan gjøres det?

Med stadig flere tilkoblede enheter, mer komplekse og uoversiktlige systemer, øker faren for at hver og en av oss skal gjøre feil. Det krever stadig mer kunnskap og oppmerksomhet for å redusere faren for at noen av de andre truslene skal ramme oss selv eller virksomheten.

Forholdsregler

Det aller viktigste vi kan gjøre for å unngå menneskelig feil, er å få grunnleggende kunnskap om informasjonssikkerhet og en kultur hvor det er ok å spørre om råd og hjelp.

Når du blir rammet

Vær åpen om feil som begås – og lær av det! Det må være åpenhet på den enkelte arbeidsplass rundt feil som begås. NorSIS ser ofte at denne type feil «feies under teppet» og blir forsøkt glemt.

Ifølge Medietilsynet* har åtte prosent av barn og unge mellom 9 og 18 år i Norge blitt mobbet eller opplevd at noen har vært slemme med dem månedlig eller oftere på nett. Samtidig bruker mange voksne rollemodeller – både kjente personer og den vanlige mannen i gaten – et språk som NorSIS mener ikke bidrar til å redusere utfordringen med hets og krenkelser.**

Hva er det?

Krenkelser er trakassering, mobbing, trusler og hets rettet mot enkeltpersoner, grupper eller virksomheter. Det kan være både direkte og indirekte handlinger og/eller verbale uttrykk. Alt fra politikere og privatpersoner til representanter for forskjellige yrkesgrupper som har tatt del i debatter, har i året som har gått blitt utsatt for uakseptable krenkelser.

Hvordan gjøres det?

Det skjer gjerne gjennom sosiale medier eller på andre nettsteder, både i åpne og lukkede grupper. Det er ofte svært vanskelig å kontrollere for gruppen eller enkeltpersonene som blir utsatt for dette, siden det alltid er mer krevende å avlive en løgn eller et rykte enn å starte det. Mange nettsteder og forum fungerer også som «ekkokamre», der en spesiell mening – om det er om ansatte i barnevernet, om en navngitt lege, en lærer eller en virksomhet – er svært fremherskende.

Krenkelser på nett kan skremme både privatpersoner og politikere fra å delta i offentlig debatt, som er helt essensielt i et levende demokrati. Dette er en trussel som derfor bør tas svært alvorlig.

Forholdsregler

- Alle har ansvar for egne ytringer og må forholde seg til eksisterende lovverk. Trusler, sjikane, falske påstander eller brudd på privatlivets fred kan straffes etter straffeloven.
- Ha en åpen dialog med barn og unge om oppførsel på nett og vær gode rollemodeller. Informasjon og kunnskap gir grunnlag for å ta gode valg.
- Virksomheter bør ha retningslinjer for hvordan de håndterer og følger opp sine ansatte som blir utsatt for krenkelser på nett.

Når du blir rammet

- Kontakt vedkommende som har publisert krenkelsene og be om at de blir fjernet. Dersom det ikke hjelper, ta kontakt med tjenesteleverandøren eller eier av nettstedet.
- Slettmeg.no gir råd og veiledning om fjerning

*** Barn og medier-undersøkelsen 2018, Medietilsynet

NorSIS ser en stadig tydeligere tendens til at kriminelle ikke angriper sine mål direkte, men finner det svakeste leddet for å angripe en virksomhet.

Hva er det?

Dette kan være angrep rettet mot en tredjeparts dataprogramvare, en underleverandør eller en usikret IoT-enhet (Internet of Things). De angriper verdikjeden som leder til målet for angrepet, ikke målet selv.

Hvordan gjøres det?

Bare de siste årene har både virksomheter og privatpersoner omgitt seg med stadig flere enheter som er koblet opp mot nett. Etter NorSIS' erfaring er disse sjelden godt nok sikret. I stedet for å angripe nettverket direkte, angriper de kriminelle via de usikrede enhetene. Det kan være langt enklere å angripe en underleverandør eller en kunde med adgang til den store virksomheten og komme seg inn på denne måten. Også programvare som blir lastet ned på PC-er uten å bli godkjent av virksomhetens IT-ledelse, kan infiseres og gi de kriminelle adgang til virksomhetenes system.

Forholdsregler

- Sørg for at alle enheter, inklusive kaffetraktere, vaskemaskiner eller varmeovner som er koblet opp mot nett, er sikret med et godt brukernavn og passord.
- Selv om du oppfatter din virksomhet som mindre interessant for kriminelle, kan dine kunder eller leverandører være av interesse for kriminelle. Et angrep mot kunder eller underleverandører gjennom din virksomhet kan bli svært problematisk for virksomhetens omdømme.
- Sørg for at samarbeidspartnere, kunder og leverandører som har tilgang til dine datasystemer har gode rutiner for IT-sikkerhet.
- Driver du en virksomhet, bør du skaffe deg oversikt over dine dine verdier, verdikjeder og sårbarheter.
- Generelt bør du alltid avinstallere programvare du ikke bruker.

Når du blir rammet

- Finn årsaken.
- Fjern eventuelt enheten som er usikker.
- Gjenopprett fra backup og/eller sikkerhetsoppdater enheten/produktet/løsningen.
- Hvis dette også kan ha rammet din kunde/leverandør, husk å varsle.

Forsøkt utpresset på nett:

– DET KOMPLETTE MARERITT

På få sekunder forandret videosamtalen karakter – fra et opphissende møte til det komplette mareritt. Truslene strømmet over skjermen til den middelaldrende mannen fra Sør-Norge. – Mitt livs største tabbe, oppsummerer han i etterkant.

> «Jeg fikk beskjed om at jeg var filmet, at dette ville bli delt med Facebook-vennelisten min om jeg ikke betalte 9000 kroner. Det var et mareritt.»

– Jeg var på et sjekkenettsted, og kom i kontakt med det jeg trodde var en norsk dame. Vi chattet på norsk, før hun spurte om vi skulle fortsette samtalen med en Skype-videosamtale, forteller han.

NorSIS er kjent med mannens identitet, men av hensyn til familie, venner og bekjente ønsker han å være anonym.

Denne kvelden satt han med mobiltelefonen og la ut en profil på en internasjonal datingside. Noen få timer senere fikk han en chathenvendelse fra en som utga seg for å være en norsk kvinne. Da samtalen ble flyttet over til en videosamtale, uten lyd, men med chat, endret den karakter og ble mer seksualisert.

– Plutselig fikk jeg beskjed på chat om at hun ble borte noen minutter. Da bestemte jeg meg for å kutte.

En knapp halvtime senere begynte Skype-beskjedene å komme

Dette er utdrag fra noen av de mange cyberbeskjedene som ble sendt til mannen.

inn til mannen. Hun ville chatte mer og ba om en videosamtale.

De fortsatte i samme spor som de avsluttet, med en form for videosexlek.

Truet med å dele alt med hans Facebook-venner om de ikke fikk 9000 kroner

– Plutselig reiste hun seg, og det så ut som om hun snakket med noen andre i rommet. Deretter ble alt svart. Kort tid etterpå begynte det å komme inn mengder med chatbeskjeder. Jeg fikk beskjed om at jeg var filmet, at dette ville bli delt med Facebook-vennelisten min om jeg ikke betalte 9000 kroner. Det var et mareritt, sier mannen til NorSIS.

Ettersom mannen nektet å betale utpresserne, ble truslene stadig tøffere. I chatten dukket det opp bilder av kjente og kjære i mannens omgangskrets som skulle motta sexfilmen.

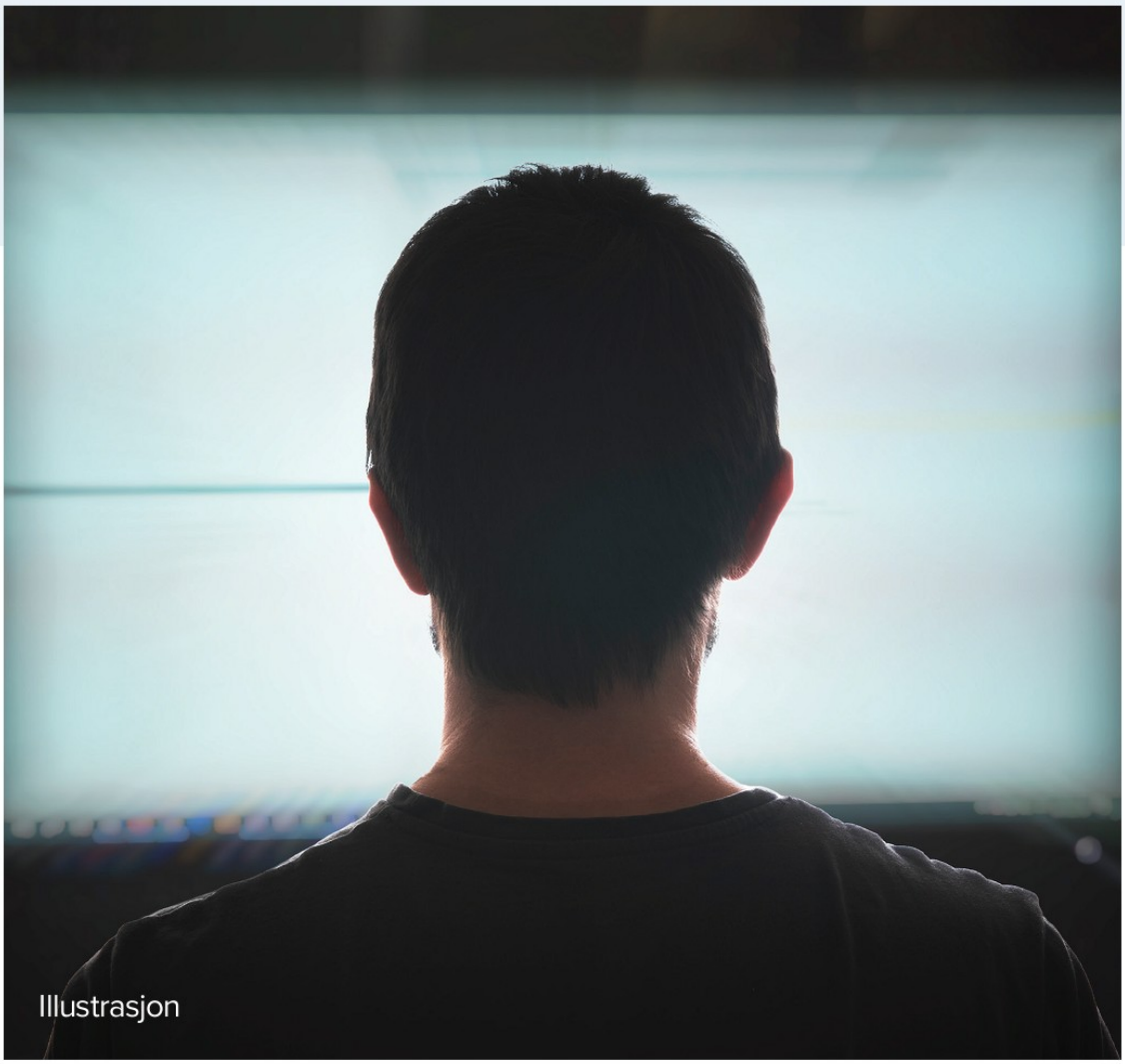
Det ene tok det andre. Truslene ble verre og verre.

– Jeg forsto ikke hva som skjedde, men oppfattet heldigvis at det ikke var noen garanti for at videoen av meg ville bli slettet dersom jeg betalte. Det kunne i neste omgang bare føre til at jeg fikk nye krav. Jeg bestemte meg derfor for å fortsette å nekte, og informerte om at jeg ville politianmelde truslene.

Mannen tok en rekke bilder av dialogen med utpresserne.

16 %

Andelen nordmenn som mottok pornosvindel-e-post og betalte kravet



Illustrasjon

3 av 4
mener de utsetter seg selv for risiko når de er på nett

Den foregikk på dårlig norsk. NorSIS har sett denne dokumentasjonen på hendelsen.

– Det er som å gå på nåler

– Jeg trodde først at de bare skulle gi opp da jeg nektet, og gå videre til neste offer. Senere fikk jeg imidlertid en e-post som etter sigende skulle stamme fra YouTube. De gjorde meg oppmerksom på at videoen av meg var for drøy til å bli lastet opp hos dem og brøt med amerikansk straffelov. De ba meg fjerne videoen, uten å si noe mer om hvor den lå, fortsetter mannen.

NorSIS har sett denne e-posten. Den er falsk, og stammer ikke fra YouTube.

– Følelsen jeg har kan ikke beskrives. Det er som å gå på nåler. Ja, jeg har gjort mitt livs største tabbe. Jeg er heldigvis en mann som er stabil, men tør ikke tenke på hvordan andre takler dette ekstreme presset. Det er uutholdelig skamfullt og vondt. Jeg vil likevel fortelle om det, slik at ingen andre setter seg selv i en lignende situasjon. Ikke videochatt med fremmede på nettet. Da skal du i så fall holde deg til en videosamtale som både naboen og arbeidskollegaene dine kan se på uten at det føles veldig feil, understreker han til NorSIS.

Kripos:

KAN ANTA AT DET ER BETYDELIGE MØRKETALL

Kripos tror seksuell utpressing er en type kriminalitet hvor det er betydelige mørketall. Ofrene kan være både unge og voksne menn. Fremgangsmåten er ifølge dem ofte tydelig profesjonalisert, og sporene går gjerne til land utenfor Europa.

– Det som beskrives i dette intervjuet er svært likt det vi har sett. Vi har også fått beskrevet likelydende modus fra politimyndigheter i andre land. Vi ser videre at de aktuelle gjerningspersonene innenfor denne formen for seksuell utpressing i stor grad har et økonomisk motiv bak ugjerningen, og at ofrene kan være både unge og voksne menn, sier påtaleansvarlig og politiadvokat hos Kripos, Ole Kristian Bjørge.

«Dette er en kriminalitetstype med betydelige mørketall.»

Politiadvokat, Kripos, Ole Kristian Bjørge

De startet en omfattende etterforskning kalt «Operasjon Malstrøm» etter at en ung mann tok livet av seg i forbindelse med seksuell utpressing i 2017.

– I løpet av etterforskningen hadde vi kontakt med flere personer som var utsatt for denne typen seksuell utpressing. Et av likhetstrekkene var at disse i all hovedsak ikke hadde meldt fra om dette, verken til politiet eller andre. Dette underbygger antagelsen om at dette er en kriminalitetstype med betydelige mørketall, og vi håper at et sterkere fokus vil bidra til å bedre denne statistikken, sier Bjørge.

De har tidligere trukket frem chattetjenester som for eksempel Chatroulette, Omegle og C-date som steder der seksuell utpressing har skjedd.

Mange føler skamfølelse og press

Kripos kjenner også igjen belastningen intervjuobjektet beskriver for en slik type utpressing.

– Skamfølelse og press er gjerne ord som fornærmede benytter i sine beskrivelser av situasjonen de befant seg eller befinner seg i.

Politiadvokat i Kripos, Ole Kristian Bjørge

– Ikke betal utpresserne

Kripos råder de som blir utsatt for dette å ikke betale utpresserne og bryte kontakten med en gang man opplever å befinne seg i en slik situasjon.

– Vår erfaring tilsier at innfrielse av et krav ofte blir fulgt opp av nye krav. Da vet gjerningspersonene at det er penger å hente, sier den erfarne Kripos-advokaten.

Vær varsom med å dele personlig informasjon med ukjente

De ønsker også å understreke viktigheten av å forebygge at denne typen hendelser oppstår.

– Det er viktig at alle er varsomme med å dele personlig eller sensitiv informasjon på nett dersom man ikke er sikker på hvem man kommuniserer med, og således ikke kan vite om dette er personer man kan ha tillit til ikke på noen måte kan komme til å misbruke informasjonen, sier påtaleansvarlig og politiadvokat hos Kripos, Ole Kristian Bjørge.

Kripos oppfordrer også alle som blir utsatt for denne typen kriminalitet til å dokumentere mest mulig av korrespondansen, melde fra til politiet så raskt som mulig og ikke slette noe.

Bare i løpet av de siste to årene har antallet norske virksomheter utsatt for phishing og andre typer sosial manipulasjon mer enn doblet seg. Når maskinene blir stadig bedre beskyttet, er mennesket angrepsvektoren som de kriminelle i økende grad vil benytte seg av.

Ifølge Mørketallsundersøkelsen til Næringslivets sikkerhetsråd har andelen norske virksomheter som sier de har vært utsatt for en eller annen form for sosial manipulasjon økt fra 8 prosent i 2016 til 18 prosent i 2018-undersøkelsen. Sosial manipulasjon er et psykologisk angrep hvor en angriper forleder deg til å gjøre noe de vil du skal gjøre.

«NorSIS ser en klar trend der de kriminelle i økende grad lurer sensitiv informasjon ut av mennesker. Dette er mer effektivt og verdifullt enn å få tilgang til informasjonen gjennom mer klassiske datainnbrudd.»

NorSIS ser en klar trend der de kriminelle i økende grad lurer sensitiv informasjon ut av mennesker. Dette er mer effektivt og verdifullt enn å få tilgang til informasjonen gjennom mer klassiske datainnbrudd.

Kan stå foran en bølge av svindel med BankID

BankID er et eksempel på noe vi frykter kan bli en av de neste store svindelbølgene. Mer enn fire millioner nordmenn har i dag BankID. Denne brukes som autentiseringsmetode for alt fra netthandel til banktjenester og justering av virksomhetsinformasjon i Altinn. Den siste tiden har vi avdekket flere saker hvor sosial manipulasjon har blitt brukt for å fralure enkeltpersoner deres BankID.

Ved hjelp av en målrettet og svært profesjonelt utformet phishing-e-post eller SMS lurer svindlerne deg først til å klikke på en lenke som tilsynelatende fører deg til banken din. Her blir du møtt av det etter hvert kjente BankID-vinduet, men dette er en falsk side hvor svindlerne kan følge hver eneste inntasting du foretar deg.

Timingen fra et kriminelt ståsted er svært bra. Nordmenn bruker BankID på stadig flere steder. Vi senker trolig skuldrene for hver gang vi gjør det, og tenker mindre og mindre over hvor sensitiv informasjonen vi deler er.

Denne type svindel, hvor nettopp det som er der for å gjøre oss tryggere, som BankID eller for den saks skyld totrinnsbekreftelse, blir overvåket og utnyttet av svindlere, gjør oss ekstra sårbare.

Bruker innsikt om den enkelte for mer målrettede svindler

NorSIS mener svindel rettet mot denne type identifisering kan bli en stor fremtidig trussel. I prinsippet kan kriminelle på denne måten manipulere alt fra adresseendringer til kontonumre penger skal overføres til, samt gjennomføre regelrette utbetalinger.

> «I dag har både cyberkriminaliteten og den teknologiske utviklingen tatt en retning som fordrer at hver og en av oss har mer kunnskap om informasjonssikkerhet.»

Dette er også et godt eksempel på fremtidig bruk av sosial manipulasjon. De kriminelle må skaffe seg kunnskap om ofrene i forkant og være klare til å utføre den faktiske svindelen der og da.

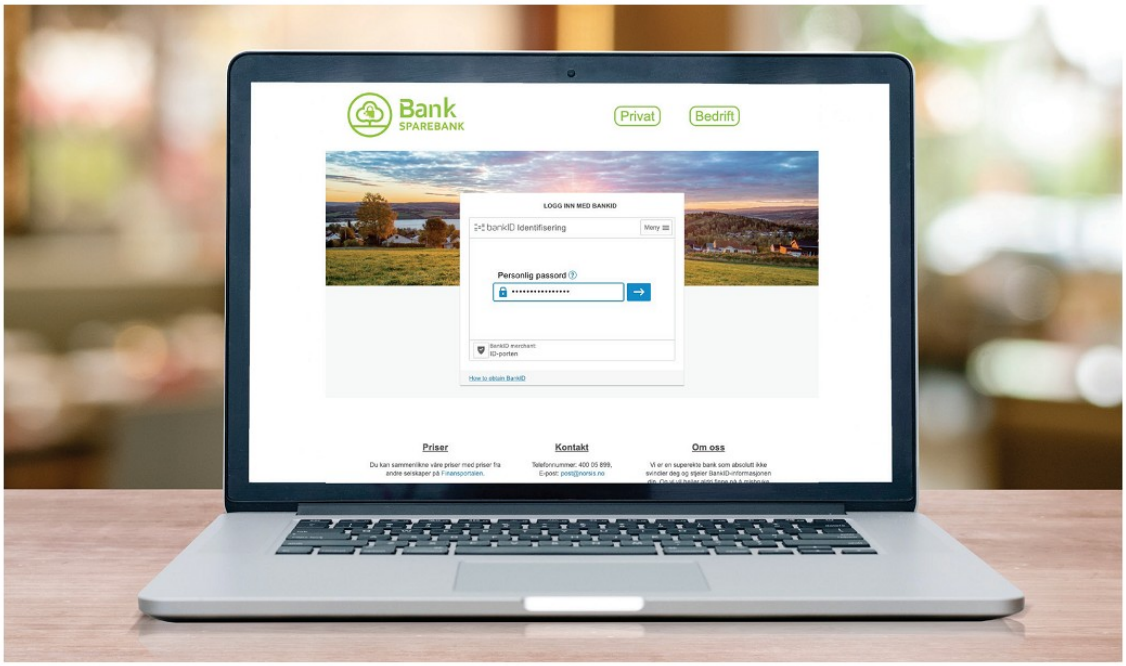
Kunstig intelligens tas i bruk av de kriminelle

Kunstig intelligens og stordata kan gjøre cyberkriminaliteten enda vanskeligere å avsløre, enten den skjer via e-post, sosiale medier eller på telefonen. Angrepene blir vanskeligere å stoppe med tradisjonell sikkerhetsprogramvare, de blir langt mer persontilpassede og følgelig mye mer effektive. Allerede i dag bruker kriminelle Google Analytics for å følge med på hvor godt deres phishing-angrep gjør det. I de neste årene kan dette bli enda mer profesjonalisert.

37 prosent
bruker totrinnsverifisering der det er mulig

Ved hjelp av kunstig intelligens kan cyberkriminelle utvikle leveringsmetoder for ondsinnet programvare som unngår sikkerhetssystemene. Programvaren vil kontinuerlig jobbe for å bli bedre til å skjule seg. Ved et phishing-angrep kan kunstig intelligens, ved å forbedre innholdet i en e-post, gjøre den umulig for sikkerhetssystemet å skille fra en e-post skrevet av et menneske.

Kunstig intelligens kan raskt samle personopplysninger om en gitt person ved bruk av såkalt sosial manipulasjon. Den kan gjøre den kriminelle prosessen enda mer effektiv ved å skrive personlig tilpassede svindel-e-poster eller ringe opp potensielle ofre.



I dag brukes stordata av politiet, Google og en rekke andre aktører for å bekjempe kriminalitet ved å forutse den. På samme måte kan kriminelle også raffinere sine metoder ytterligere. Ved svindel og utpressingsforsøk øker troverdigheten til en falsk trussel når de kriminelle presenterer personlig informasjon. Med tilgang til flere opplysninger er det lettere å forutse hvor stor muligheten er for at noen lar seg lure, hvor mye de er villig til å betale og hva slags trussel som treffer best akkurat på dem.

Angriper mennesker i stedet for maskiner

De store trendlinjene i det digitale trusselbildet er at våre IT-systemer blir sikrere, stadig flere enheter kobles på nett og vi jobber og lever stadig mer i skyen. Det er fleksibelt, enkelt og tilgjengelig. Det betyr også at tilgangskontroll er viktigere enn noensinne. Det er selve nøkkelen til vårt digitale liv, enten det er på jobb eller privat. De stadig lengre verdikjedene gjør oss sårbare for at noen finner det svake leddet, enten det er den smarte vaskemaskinen, styringssystemet eller den private, usikre mobilen vi logger på jobbskyen for å lese e-post med.

De nye utfordringene betyr også at vi må tenke annerledes rundt sikkerhet enn vi har gjort før. Når mer enn halvparten av norske virksomheter ifølge SSB har hele eller deler av sine systemer i skyen, er det helt avgjørende at tilgangen til disse systemene blir sikret. Sikkerhetsutfordringen ligger ikke primært i selve skylagringen – den ligger i tilgangen til skyen og fra hvilke enheter dette skjer.

8 av 10 datainnbrudd skyldes identitetstap

Ifølge Microsoft Norge skyldes hele 80 prosent av datainnbrudd i sky- og andre lagringsløsninger tap av identitet. Ved hjelp av sosial manipulasjon, som phishing, overtar de kriminelle identiteten til en ansatt og kommer seg inn i skyløsningen til virksomheten. Det er derfor så avgjørende viktig at alle enheter som er koblet opp mot skyløsningen er godt nok sikret. Det kan gjøres ved hjelp av ulike former for totrinnsbekreftelse.

> «Hvis en privat mobiltelefon eller en PC har blitt kompromittert med ondsinnet programvare, kan denne hente informasjon om pålogging og deretter gi adgang til virksomhetens dokumenter og filer som ligger lagret i skyløsningen.»

Må sikre enheter og regulere brukertilganger bedre

En undersøkelse NorSIS gjennomførte i 2019 viste også at hele seks av ti norske virksomheter tillater de ansatte å bruke privat datautstyr for å ha tilgang til jobbens systemer for skylagring og e-post. Den store utfordringen med dette er at arbeidsplassen ikke har kontroll på sikkerheten på de enhetene som kan koble seg på jobbens sky. Hvis en privat mobiltelefon eller en PC har blitt kompromittert med ondsinnet programvare, kan denne hente informasjon om pålogging og deretter gi adgang til virksomhetens dokumenter og filer som ligger lagret i skyløsningen.

1 av 2

bruker forskjellige passord til sine nettjenester

Et annet, men vel så viktig punkt, er brukerrettigheter og tilgangsstyring. Ifølge Microsoft har altfor få norske små og mellomstore bedrifter et skille mellom forskjellige brukere og tilgangene hver enkelt har til informasjonen i skyen. Det er ingen grunn til at alle i en virksomhet skal ha tilgang til alt. Det betyr at inngangene for en angriper er langt flere, og de kan fritt finne det svakeste leddet for å komme seg inn i systemene.

Utbyggingen av 5G-nettet vil forsterke IoT-revolusjonen

Utbyggingen av 5G-nettet vil tilrettelegge ytterligere for IoT-revolusjonen og sannsynligvis øke denne sårbarheten.

Det største problemet med IoT-enheter er at mange av selskapene som lager dem ikke har erfaring med sikkerhet, kun med produksjon av husholdningsgjenstander. Som et resultat av dette har mange IoT-enheter i dag liten eller ingen innebygd sikkerhet. De kan derfor raskt bli utdaterte og ha kjente sårbarheter som ikke lar seg fikse. Konsekvensen er at hjemmenettverket ditt havner i en permanent sårbar tilstand gjennom de tilkoblede smarttingene.

Ifølge en undersøkelse Forbrukerrådet la frem våren 2019 er tre av fire nordmenn bekymret for sikkerhet og personvern i smarte produkter.

Digital kompetanse viktigere enn noensinne

Tingenes internett representerer også en utfordring fordi verdikjedene våre vokser seg stadig lengre og mer uoversiktlige. Spesielt for virksomheter er dette det første punktet på listen for å være sikret mot cyberkriminalitet. Du må først og fremst ha oversikt over verdiene og verdikjedene dine. Først da kan du sikre deg.

Akkurat som for skylagring og utviklingen innenfor kunstig intelligens, representerer IoT svært mange positive muligheter både for enkeltpersoner og virksomheter. Trenden er imidlertid klar. Kampen mot cyberkriminalitet i årene fremover handler vel så mye om kompetansen og sikkerhetskulturen hver og en av oss besitter. Tidligere omga vi oss med en vollgrav av sikkerhet, med antivirus og brannmurer som stort sett gjorde sikkerhetsjobben for oss. I dag har både cyberkriminaliteten og den teknologiske utviklingen tatt en retning som fordrer at hver og en av oss har mer kunnskap om informasjonssikkerhet.

Slik beskytter du dine IoT-enheter

- Vurder hvilke enheter du kobler på nett: Om du ikke har behov for det, ikke koble enheten på nett.
- Bytt standard passord med et nytt, sterkt passord: Endre passordet på IoT-enheten. Du finner en veiledning på hvordan du lager sterke passord på nettvett.no.
- Husk å oppdaterte hvis mulig: Å holde IoT-enhetene sine oppdatert er like viktig som med PC-er og mobile enheter. Skru på automatisk oppdatering hvis det er mulig.
- Bytt ut enheten dersom den ikke kan oppdateres: Etter hvert kan det være at IoT-enheten din har for mange kjente sårbarheter som ikke kan fikses, eller det kan ha kommet ut nye enheter som har mye mer sikkerhet innebygd.
- Tenk over hvilke data som samles inn: Om det er mulig å konfigurere personverninnstillinger på IoT-enheten, bør du benytte deg av det til å begrense hvor mye informasjon den deler.
- Separert Wi-Fi-nettverk: På mange Wi-Fi-aksesspunkter har du mulighet til å opprette ekstra nettverk, som et gjestenettverk. En annen løsning er å kjøpe et nytt aksesspunkt til bruk kun for IoT-enhetene. Les mer om trådløse hjemmenettverk.

Gode råd for sikker BankID-bruk

- Hvis noen ber deg oppgi BankID-passord og -koder over telefon - legg på!
- Ingen banker eller legitime institusjoner vil be deg oppgi dine BankID-hemmeligheter på telefon, SMS eller e-post.
- Ikke del BankID-passord og -koder med noen, heller ikke med bankansatte, familie, venner eller andre.
- Har du en dårlig magefølelse eller oppdager at du er svindlet, ta kontakt med banken umiddelbart for å sperre BankID og begrense svindelen.

Kilde: Bankid.no

MER SOSIAL MANIPULASJON OG MÅLRETTEDE, PERSONALISERTE ANGREP

Hver andre norske virksomhet opplevde forsøk på såkalt sosial manipulasjon i 2019.* Her var det snakk om å utnytte menneskelig kontakt og sosiale evner for å få tak i eller påvirke informasjon. NorSIS ser en trend hvor trusselbildet fremover vil få et enda klarere innslag av dette. Også langt mer spissede og mer personaliserte angrep vil sannsynligvis bli vanligere.

3 av 10
bedrifter har vært utsatt for svindel-forsøk det siste året

Sosial manipulasjon

Hva er det?

Sosial manipulasjon handler i bunn og grunn om å spille på dine følelser og lure deg til å klikke på en ondsinnet e-postlenke for å fiske etter personlige opplysninger. Et annet alternativ er å ringe deg og forlede deg til å tro at det er fra banken din og at du må oppgi BankID. Det handler om å bruke triks for å lure deg til å utlevere informasjon som kan gi tilgang til penger, andre personer eller annen verdifull informasjon.

> «Mange IoT-enheter, som lysstyring, kameraer, sensorer eller vaskemaskiner, har ofte dårlig nettsikkerhet sammenlignet med tradisjonelt IT-utstyr.»

Det er også langt enklere å oppnå det man vil med en svindel eller et utpressingsforsøk dersom de kriminelle vet hvem du er og hvor smerteterskelen din går – både rent økonomisk og menneskelig. NorSIS ser at målrettede angrep i økende grad benytter seg av innsikt om deg som person eller om virksomheten din, noe som kan øke sannsynligheten for at angrepet lykkes. Dersom de kriminelle har funnet navn og bilder av familien til den de truer med kidnappingsforsøk, er det større sjanse for at de lykkes. Det samme gjelder en virksomhet. Vet de hvor mye virksomheten tjener, at økonomisjefen lett godkjenner fakturaer på e-post eller at selskapet akkurat har landet en stor avtale, kan dette benyttes i videre kriminelle fremstøt.

Hvordan gjøres det?

Både sosial manipulasjon og mer personaliserte trusler benytter seg av den store usikkerheten som fremdeles hersker blant mange nordmenn når det gjelder informasjonssikkerhet. Hvis du eller dine ansatte blir truet, fristet eller på annen måte forsøkt forledet på telefonen eller via e-post, er det blant annet deres digitale kompetanse og forståelse som avgjør om dere går på eller ikke.

Personalisering av truslene handler mer enn noe annet om hvilken informasjon det er mulig å innhente om deg eller din virksomhet. Svært ofte er alt fra åpne vennelister på Facebook til informasjon du har delt uforvarende i phishing-e-poster (som e-postadresse, passord, personnummer og lignende) med på å øke risikoen for at en falsk trussel oppfattes som reell. Inntektsnivået ditt kan også si noe om hvor de kriminelle kan legge listen i en utpressingssak. Det er med andre ord et tett samspill mellom hvor godt vi passer på våre egne personopplysninger og risikoen for å bli utsatt for mer målrettet kriminalitet.

Trusselsituasjonen fremover

Etter som teknologien og datasystemene til både virksomheter og enkeltpersoner blir bedre sikret, er det enklere for de kriminelle å gå veien om mennesker, ofte omtalt som det svakeste leddet, fordi disse kan manipuleres.

Ny teknologi som kunstig intelligens og maskinlæring brukes ikke bare aktivt av de som bekjemper cyberkriminalitet, men også av de cyberkriminelle selv. Maskinlæring er selvlærende datateknologi hvor systemet selv blir bedre og bedre til oppgavene det er satt til å utføre. Det kan gjøre phishing-angrep mer effektive ved å gjøre svindel-e-post likere en unik e-post skrevet av et menneske. Maskinlæring kan også brukes til å samle inn stordata, og til å raskt samle sammen personopplysninger om en person.

Kriminelle bruker allerede Google Analytics for å følge med på hvor godt phishing-angrepene deres gjør det. I de neste årene kan dette bli enda mer profesjonalisert.

> «Spesielt i SMB-markedet er det mange som ved skylagring verken sikrer klient (PC, mobil o.l.), bruker sikker totrinnsbekreftelse eller regulerer den enkelte ansattes tilgang til dataene og programmene de har behov for.»

Økt sårbarhet for angrep mot skytjenester

Etter som flere og flere selskaper og privatpersoner benytter seg av skytjeneste for lagring og som arbeidsområder med skybasert programvare, øker også sårbarheten for angrep mot disse.

Hva er det?

En skytjeneste er en databasert tjeneste, for eksempel for lagring av bilder og dokumenter, som blir utført på et helt annet sted enn der du befinner deg – på servere og datamaskiner med enorm kapasitet. At ting er lagret i skyen betyr at det ikke ligger lokalt på telefonen eller maskinen, men at det lagres på en server du kan logge deg på via nett.

> «NorSIS ser at målrettede angrep i økende grad benytter seg av innsikt om deg som person eller om virksomheten din, noe som kan øke sannsynligheten for at angrepet lykkes.»

I dag er ekstreme mengder data lagret i skyløsninger. De mest brukte skyløsningene er ofte sikre og krypterte. Utfordringen er god nok sikring av tilgangen til disse – både datamaskinen eller mobiltelefonen som brukes for å logge seg på samt selve tilgangskontrollen.

3 av 10

har ikke tillit til at myndighetene sikrer deres personopplysninger på en skikkelig måte

Hvordan gjøres det?

Selv om dataene i skyløsninger generelt ofte er bedre sikret enn det som ligger på egne servere, kan spesielt dårlig tilgangskontroll være en stor trussel. Kommer passord på avveie, kan andre få tilgang til alt fra e-post til annen sensitiv data i skyen. Det er derfor ekstra viktig å bruke skytjenester som tilbyr totrinnsbekreftelse til skyen.

Bruk av private enheter til å logge på jobbens skyløsninger for å lese e-post eller andre dokumenter, er også potensielt en stor risiko. Android-brukere må være bevisst på å ikke installere

apper utenfor Google Play-butikken. Slike apper kan inneholde ondsinnet programvare som igjen kan ende opp med å gi andre tilgang til virksomhetens skyløsning. Det samme er tilfelle med programvare som lastes ned på PC og som ikke er godkjent av virksomhetens IT-avdeling.

Trusselsituasjonen fremover

Mer enn halvparten av norske virksomheter benytter ifølge Statistisk sentralbyrås siste statistikk en eller flere nettskyløsninger. For SMB-markedet er den klart vanligste løsningen såkalte SaaS-løsninger (Software as a Service). Her er det skybaserte programmer til alt fra fakturering til reiseregninger som er blant de vanligste bruksområdene.

Spesielt i SMB-markedet er det ifølge Microsoft – som er en av de store innenfor skylagring – mange som verken sikrer klient (PC, mobil o.l.), bruker sikker totrinnsbekreftelse eller regulerer den enkelte ansattes tilgang til dataene og programmene de har behov for.

Her kan kriminelle få tilgang til store mengder data fra flere selskap på ett sted. Europol trekker i sin siste cyberkriminalitetsrapport frem dette som en potensiell fremtidig trussel.

> «Ny teknologi som kunstig intelligens og maskinlæring brukes ikke bare aktivt av de som bekjemper cyberkriminalitet, men også av de cyberkriminelle selv.»

Økende antall nettilkoblede enheter

Antallet enheter som er koblet opp mot våre egne nettverk kan også utgjøre en økende trussel etter som de blir flere.

Hva er det?

Internet of Things (IoT) er betegnelsen på at hverdagslige gjenstander kobles til og styres fra internett og kommuniserer med andre ting, datamaskiner eller oss mennesker. Eksempler på smarte ting er robotstøvsugere, termostater, TV-er og kameraer som kan styres via apper på telefonen.

Hvordan gjøres det?

Mange av enhetene, som lysstyring, kameraer, sensorer eller vaskemaskiner, har ofte dårlig nettsikkerhet sammenlignet med tradisjonelt IT-utstyr. Disse kan da være bakdører inn i virksomheter og privatpersoners IT-system.

1 av 3 ledere

For dyrt og tidkrevende å sikre seg mot dataangrep

Trusselsituasjonen fremover

Ved utgangen av 2019 var det ifølge statistikknettstedet Statista mer enn 26 milliarder tilkoblede IoT-enheter globalt. Allerede i løpet av 2020 kan det komme ytterligere fire milliarder nye IoT-enheter. De blir stadig smartere og mindre. Med utbyggingen av 5G-nettet blir de også enda mer anvendelige. Veksten skjer primært innenfor smarte produkter som brukes hjemme og i virksomheter, men også moderne biler kobles i økende grad opp mot skyen. De mange enhetene som fungerer som sensorer og fanger opp data, kan i tillegg til å være en sikkerhetsrisiko også representere en utfordring med hensyn til personvernet. Det er per i dag ingen minstekrav for IKT-sikkerhet i tilkoblede forbruksprodukter.

3 vanlige triks for sosial manipulering

NorSIS erfarer at sosial manipulasjon ofte benytter seg av disse grepene:

Tillit

Avsender er tilsynelatende noen du kjenner eller stoler på. Da forsvinner ofte skepsisen. Kjente merkenavn blir også utnyttet i svindler eller konkurranser. Husk at avsenderne ikke alltid er den de utgir seg for å være.

Fristelser

Dette er typisk tilfeller hvor du får tilbud om gratis programvare eller spill eller en e-post om at du har vunnet en konkurranse. Husk at dette kan være rent lureri, hvor dine personopplysninger eller lignende ofte er målet for fremstøtet.

Frykt

Å skremme noen til å utføre en handling, for eksempel å laste ned et program for å bli kvitt et påstått virus, er også en vanlig metode.

! Svindlerne vil i alle disse tilfellene ofte gi deg følelsen av at det haster med å foreta seg noe.

* PwC Cybercrime survey, 2019

NSMs fagdirektør om falske nyheter:

– Du skal ikke tro på noe av det du hører og bare halvparten av det du ser

Med falske profiler for norske rikspolitikere, har falske nyheter blitt spredd på sosiale medier. En kopi av TV 2s nyhetsnettside har de også funnet. Fagdirektør i Nasjonal sikkerhetsmyndighet (NSM), Roar Thon, er bekymret over konsekvensene falske nyheter kan ha for samfunnstryggheten.

– Vår aller største bekymring er at man skal komme i en situasjon hvor vi har en samfunnskrise der nordmenn tror at de lytter på myndighetenes råd, mens det de får er det stikk motsatte av hva myndighetene forsøker å komme ut med, sier fagdirektøren i NSM.

Han mener de mystiske hundedødsfallene som rammet Norge tidligere i høst kan illustrere utfordringen på en god måte.

– De ryktene som spredde seg rundt årsaken til dette, etablerte seg i flere miljøer som en slags vedtatt sannhet. Det er litt slik at alle er bekymret for falske nyheter, samtidig som mange ubevisst bidrar til spredning av dette selv, sier Thon.

Fra «tull og tøys» til kynisk påvirkning

NSM startet å følge spesielt nøye med på spredningen av falske nyheter foran stortingsvalget i 2017. Da avdekket de falske sosiale medier-kontoer i navnet til noen av våre mest fremtredende politikere. Dette skjer ifølge ham fremdeles. Selv om NSM får fjernet kontoene, får de raskt mange følgere før de blir avslørt som falske. De aller fleste ekte sosiale medier-kontoene til profilerte politikere er også i dag verifisert og merket med en blå stjerne.

– De farlige falske nyhetene er ikke slik som de hackingen av Dagbladet tidligere i år ga, som var mest tull og tøys på innhold. TV 2-kopisiden var en eksakt kopi. Denne kunne vært en langt større trussel mot samfunnssikkerheten om den hadde blitt misbrukt til falske nyheter, sier NSMs fagdirektør.

De eldre sliter mest med falske nyheter

Ifølge en undersøkelse som Medietilsynet* foretok i vår, er det spesielt de over 60 år som sliter med å skille falske nyheter fra de ekte. Over halvparten klarte ikke dette. Blant de under 30 år hadde også en av tre problemer med å avdekke om en nyhetssak var ekte eller falsk.

– Spesielt det at de eldre sliter med dette, overrasker meg ikke. Det var mer slik før at vi hadde en felles oppfatning av virkelighetens tilstand, og så hadde forskjellige meninger om hvordan ting skulle løses. I dag har det blitt langt mer fragmentert. Vi er ikke lenger i samme grad enige om fakta, sier den erfarne cybersikkerhetseksperten.

Algoritmer og Deep Fake gjør det vanskeligere

Ifølge Thon kan den teknologiske utviklingen i nær fremtid føre til at det blir enda vanskeligere å skille falskt fra ekte.

– Sosiale medier som Facebook har i dag algoritmer som prioriterer video fremfor tekst og bilder. Tradisjonelt har video blitt sett på som et slags sannhetsbevis. Såkalt Deep Fake, det vil si videoer der fjeset til de som snakker på film er manipulert til å si det som avsenderen måtte ønske, vil gjøre det svært vanskelig å skille ekte fra falsk, sier NSMs fagdirektør.

Ifølge Thon er utfordringen også at Facebooks egne algoritmer prioriterer de enkle, sjokkerende og bildesterke postene. Det gjør at en falsk nyhet, som gjerne er enkel, tabloid og oppsiktsvekkende, vil få bedre spredning enn den sanne, som gjerne er mer nyansert.

– Det fører også til at debatten blir forflatet og ført på feil premisser. Nyansene forsvinner og de forskjellige meningsleirene står enda sterkere mot hverandre, ofte basert på feil fakta. Flere og flere blir gående i sine egne ekkokamre, der de stort sett bare får bekreftet sine holdninger via sosiale medier. Det er et svært dårlig utgangspunkt i et demokrati, sier Thon.

Doblet antall land hvor organisert sosial manipulasjon er påvist

Ifølge rapporten «The Global Disinformation Order»**, utgitt av Oxford Internet Institute ved University of Oxford, har organisert sosial manipulasjon fra myndigheter eller politiske partier av en befolknings meninger gjennom bruk av sosiale medier funnet sted i hele 70 land, inkludert Sverige, Storbritannia og Tyskland. Det er mer enn en dobling siden 2017.

Facebook er den klart mest foretrukne kanalen. Deretter følger Twitter, men både YouTube og Instagram blir i økende grad brukt. Dette er gjort ved å bruke sosiale medier-kontoer med falsk identitet, kontoer styrt av såkalte bots (små programmer som genererer automatiske svar på egen hånd) eller deling av manipulert innhold.

– Det trenger ikke være noen stor kunst å gjøre dette. Folkeopplysningen på NRK viste med all tydelighet hvor enkelt det kunne gjøres. De hadde seks–syv falske kontoer som til sammen styrte et stort nok antall elever til at det fikk en betydning. Det viser at det er behov for å øke bevisstheten rundt falsk og ekte.

Pengeinteresser kan ha interesse av å påvirke

Denne type kampanjer kan ifølge Thon også skje innenfor det private næringsliv.

– Det er selvsagt områder hvor også store pengeinteresser har interesse i å påvirke hele eller deler av folkeopinionen. Når vi ser hvor lite som skal til av ressurser, er det all grunn til å følge med også på denne utviklingen.

Selv følger han læresetningen «du skal ikke tro på noe av det du hører og bare halvparten av det du ser».

– Det er mer enn noensinne viktig å ha en sunn skepsis til alt du leser, hører eller ser. Alt er ikke som det utgir seg for å være, sier fagdirektør i NSM, Roar Thon.

* Kritisk Medieforståelse, Medietilsynet, mai 2019

** The Global Disinformation Order, University of Oxford 2019

Slik avslører du falske nyheter

1. Vær skeptisk til fengende eller utrolige overskrifter.
2. Er du i tvil om hvem som står bak artikkelen – undersøk kilden.
3. Sjekk om saken har en forfatter.
4. En ekte nyhet spres fort – sjekk flere kilder for å se om saken er sann.
5. Vær ekstra oppmerksom på saker som vekker sterke følelser.
6. Et bilde kan også lyve – gjør et bildesøk i Google.

(Kilde: Medietilsynet)

Rapporten Trusler og trender er en del av kjernevirksomheten til NorSIS, som jobber med å fremme kunnskap rundt og bevissthet om digitale sårbarheter og trusler samt å bidra til en trygg digital hverdag.

NorSIS er en uavhengig organisasjon som arbeider for å styrke norsk informasjonssikkerhet, med hovedvekt på å bevisstgjøre og bistå enkeltindivider og mindre private og offentlige virksomheter. Disse er blant de mest sårbare fordi de ofte har færre ressurser å sette inn for å beskytte seg.

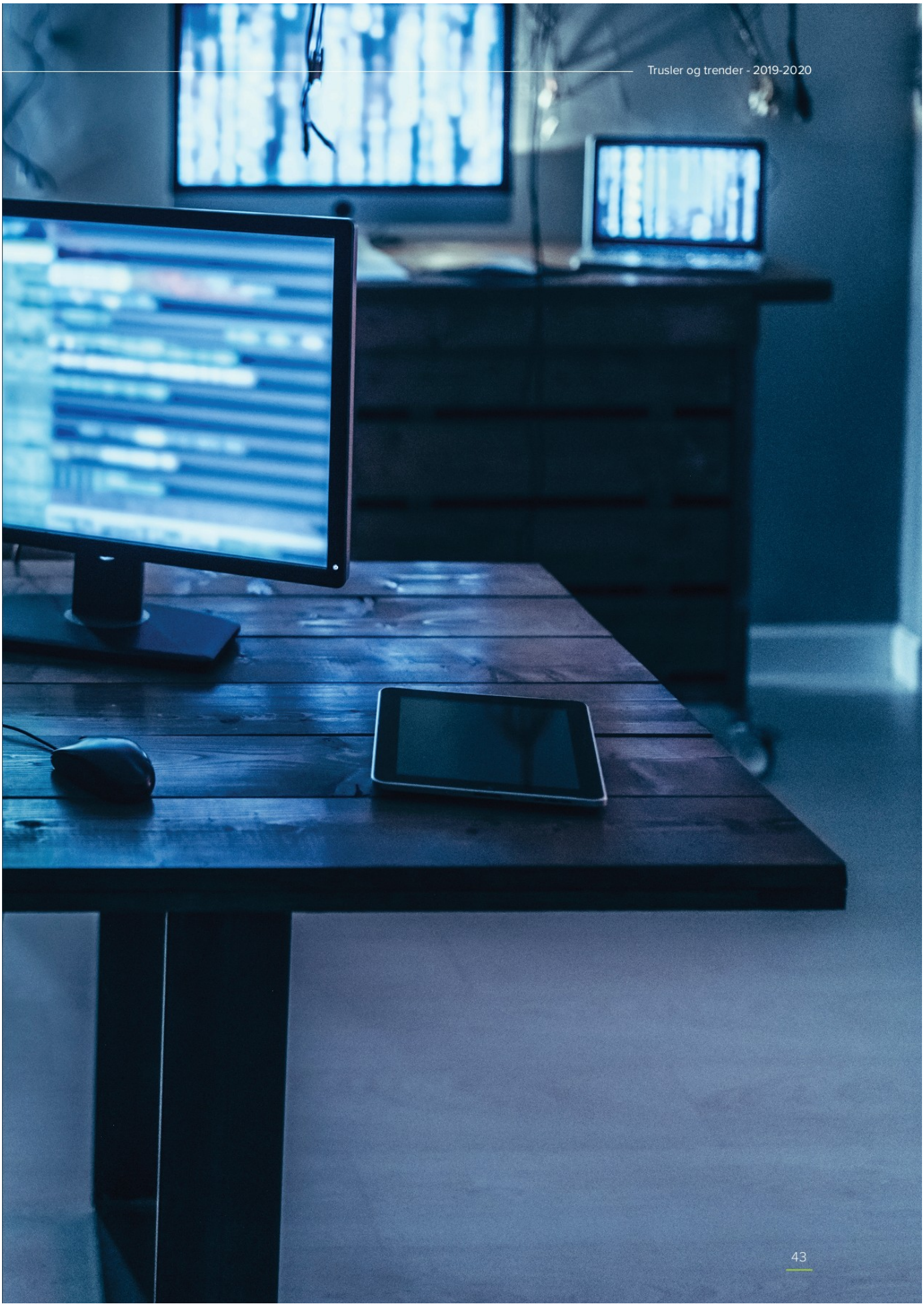
Bevissthet om hvilke verdier som står på spill og egen sårbarhet, er det beste utgangspunktet for å treffe forebyggende tiltak.

NorSIS arbeider bredt for å spre kunnskap, skape bevissthet og gi veiledning. Blant våre viktigste tiltak og tilbud er disse:

- **Nasjonal sikkerhetsmåned** er en nasjonal dugnad med vekt på informasjon og opplæring. NorSIS er nasjonal tilrettelegger og koordinator av Sikkerhetsmåneden, som arrangeres hvert år i oktober.
  www.norsis.no

- **Nettvett** er en nasjonal veiledningstjeneste med grunnleggende råd om styrket sikkerhet og oppdatert rettledning om håndtering av trusler. NorSIS er redaktør av Nettvett, som drives i et samarbeid med NSM og Nkom.
  www.nettvett.no

- **Slettmeg** er en nasjonal tjeneste med grunnleggende råd og personlig veiledning for de som opplever krenkelser på nett. NorSIS har utviklet og bemanner Slettmeg, som består av både et nettsted og en rådgivningstjeneste.
  www.slettmeg.no


Trusler og trender - 2019-2020
43

Du bruker ikke samme børste overalt, hvorfor bruke samme passord?

NorSIS

Teknologiveien 22
2815 Gjøvik
Org.nr. 995195003

Telefon: 40 00 58 99
www.norsis.no
post@norsis.no