
TRUSLER
OG TRENDER
2021
NorSIS

Trusler og trender er en årlig NorSIS-rapport som beskriver og forklarer de viktigste truslene små og mellomstore virksomheter vil eller kan regne med å bli rammet av. I tillegg skisserer vi hvordan vi mener trusselbildet vil utvikle seg fremover. Rapporten er basert på henvendelser til NorSIS i tillegg til et utvalg trusselvurderinger, rapporter og undersøkelser fra nasjonale og internasjonale statlige og private virksomheter.

Innhold

Unngå ødeleggende konsekvenser – beskytt din virksomhet NÅ!

Det var natt til 9. januar 2021 Østre Toten kommune ble rammet av et massivt løsepengevirusangrep. Alt fra e-post til utbetaling av sosialhjelp, brannalarmer og medisinutlevering til eldre var med ett satt totalt ut av drift.

Løsepengevirus og andre digitale trusler er i høyeste grad alvor og mer aktuelt enn noensinne for alle norske kommuner og små og mellomstore bedrifter. Med sine nesten 15 000 innbyggere er Østre Toten et eksempel på hvor totalt og nådeløst det kan ramme.

Det aller meste av kommunens systemer og informasjon ble med ett kryptert og gjort utilgjengelig. Noen var på innsiden av kommunens IT-systemer. Nå måtte arbeidet med å finne ut hva annet av skade eller tyveri de kunne ha gjort starte. Selv om kommunen raskt hadde nødprosedyrer på plass for å ivareta de kritiske systemene, som innenfor helse- og omsorgstjenestene, måtte de digitale hjelpemidlene i flere tilfeller byttes ut med penn og papir.

Alle har verdier som kan viderselges, brukes til utpressing eller omsettes på en eller annen måte.

Eldre på sykehjem fikk erstattet alarmklokker med små bjeller for å tilkalle hjelp. Eiendomsskatt eller andre regninger som sendes ut digitalt, ble ikke sendt ut. Kommunen fryktet også at sensitive personopplysninger var på avveier.

Store mørketall tilslører den reelle risikoen

Vi vet at løsepengevirus og andre typer dataangrep rammer og ødelegger for store summer rundt om i Bedrifts-Norge hver eneste dag. Det skjer langt oftere og er mye vanligere enn mange tror. Grunnen til at vi ikke kjenner omfanget av denne typen angrep, er at mange virksomheter ikke prater høyt om dette, men holder det for seg selv når det skjer.

Det gjør at svindlerne kan fortsette å bruke de samme metodene for å svindle norske virksomheter som de har gjort de siste årene. Svindlere og nettkriminelle velger den enkleste veien inn der det er mulig.

Derfor ser vi at en rekke svindler, for eksempel direktørsvindel, fakturasvindel, ulike typer phishing eller SMiShing, nærmest kjøres som kampanjer.

Alle har verdier som er attraktive for noen

Mange tenker at de ikke er et attraktivt mål for nettkriminelle. Det er feil. Alle har verdier som kan videreselges, brukes til utpressing eller omsettes på en eller annen måte. Og kanskje er ikke din virksomhet hovedmålet for angrepet, men en vei inn til en kunde, leverandør eller en annen kontakt dere har. Informasjonssikkerhet er derfor like viktig enten du driver frisørsalong, nettbutikk eller leverer teknologi til oljeindustrien eller kritisk infrastruktur.

Annerledesheten øker risikoen for å bli svindlet

Vi ser også at nettkriminelle er svært gode til å tilpasse angrepene til endring i vår adferd. Nå når svært mange av oss har flyttet virksomheten hjem til de ansatte, har mange en annerledes jobbhverdag. Samtidig vet vi at en av måtene å avsløre svindel på er at en henvendelse på telefon, i en SMS eller en e-post blir oppfattet som annerledes. Når det meste er annerledes med situasjonen svært mange for tiden befinner seg i, er det mye vanskeligere å avsløre svindelforsøk nå enn tidligere.

Kunnskap om digitale trusler og egne sårbarheter er avgjørende

Selv om det finnes teknologi som kan gjøre oss bedre beskyttet mot å bli lurt, kan denne bare beskytte oss til en viss grad. Til syvende og sist er det den enkelte ansattes kunnskap om trusselbildet og egne sårbarheter og hvilke tiltak virksomheten har iverksatt, som avgjør om de unngår lammende dataangrep som i verste fall kan knekke en liten bedrift.
Vi vet at det er alvor. Heldigvis vet vi også at det ikke krever mye å redusere risikoen for at dette skjer. «Trusler og trender 2021» er en kort og enkel gjennomgang av de vanligste digitale truslene som vil ramme mange norske virksomheter. Ved å følge rådene og anbefalingene vi gir, vil du og din virksomhet være godt rustet for å møte de digitale truslene som dukker opp.

God lesing!

LØSEPENGEVIRUS:

Europas største digitale trussel mot virksomheter i alle størrelser

Med et par klikk og en nedlasting av et ukjent vedlegg i en e-post, en Facebook-post eller en SMS kan hele din virksomhets IT-system bli lammet og kryptert. Løsepengevirus har seilt opp som en av de virkelig store digitale truslene mot både små og store bedrifter over hele Europa.

Alt tyder på at denne utfordringen bare vil øke fremover.

Det ondartede programmet spres gjerne som vedlegg og lenker i e-post, Microsoft-filer eller via infiserte nettsider. Når det lastes ned, får viruset tilgang til systemene slik at det kan kryptere all data i hele virksomheten. Dette kan skje umiddelbart eller når avsender velger å aktivere viruset. Resultatet er at virksomheten din blir fullstendig lammet og du trues med at du ikke får tilgang til å bruke datamaskinen din før løsepenger, gjerne i kryptovaluta, blir betalt til de kriminelle.

Ikke betal løsepengekravet

Når skaden først har skjedd, er vårt klare råd å ikke betale løsepengekravet. Dersom du velger å betale, er du med på å finansiere kriminelle, og det er heller ingen garanti for at de gir deg tilgangen tilbake. Mye tyder på at du ved å betale gjør deg enda mer sårbar for nye dataangrep. De kriminelle har fanget opp at du har betalingsvilje for denne typen kriminalitet.

*«Når skaden først har skjedd, er det NorSIS sitt klare råd **å ikke betale løsepengekravet.**»*

Kan spre seg videre til skytjenester og andre tilknyttede IT-systemer

Løsepengeviruset kan også ligge lenge i systemet til virksomheten din før det slår til. Det kan i tillegg spre seg videre til skytjenestene dine, som Dropbox eller OneDrive. Det finnes flere eksempler på at den ondartede programvaren har spredd seg og satt hele byer, sykehus eller globale virksomheter totalt ut av spill.

Kan ligge lenge i systemet før det slår til

Løsepengeviruset kan også ligge lenge i systemet til virksomheten din før det slår til. Det kan i tillegg spre seg videre til skytjenestene dine, som Dropbox eller OneDrive. Det finnes flere eksempler på at den ondartede programvaren har spredd seg og satt hele byer, sykehus eller globale virksomheter totalt ut av spill.

Det finnes også flere eksempler på løsepengevirus som har ligget sovende i virksomheters IT-systemer i flere måneder før de aktiveres når du minst trenger det, for eksempel i forbindelse med en kontraktsignering, en viktig lansering eller lignende. Dette gjøres for å øke virksomhetens vilje til å betale de kriminelle.

Husk at det ikke bare er på PC-en du kan få løsepengevirus. Mobiltelefoner, produksjonsutstyr, maskineri og annet som er koblet til nett er også sårbart for å bli kryptert og satt ut av spill.

10,1 milliarder euro er ENISAs anslag på hvor mye som ble betalt i løsepenger i 2019

Trenger du mer hjelp?

Flere tips for å unngå løsepengevirus her

Sjekkliste for å unngå løsepengevirus:

Dersom det er noen av disse punktene du ikke forstår eller kan utføre selv, hør med driftsleverandøren din.

Har du sørget for:

- at alle ansatte har fått opplæring i hva de bør tenke over/sjekke ut før de sier ja til å laste ned og installere programmer på maskinen?
- å skille mellom hvilke ansatte som har administrasjonsrettigheter, brukerrettigheter og eventuelle andre rettigheter i systemene ut fra hvilket behov de har i sin jobb?
- at det jevnlig tas sikkerhetskopier av alle viktige filer?
- at sikkerhetskopien er offline eller på et annet nettverk enn det den sikkerhetskopierer?
- at all nødvendig segmentering av nettverk er gjort? Dersom du lurer på om dette gjelder din virksomhet, spør driftsleverandøren din.
- at alle virksomhetens datamaskiner, operativsystem og programvare til enhver tid er oppdatert?
- at alle virksomhetens datamaskiner har og bruker oppdatert antivirusprogram?
- at du og dine ansatte ikke har andre disker og enheter koblet til datamaskinen til enhver tid? Det vil hindre spredning av løsepengevirus til alle.
- at du og dine ansatte ikke er tilkoblet skytjenester hele tiden? Løsepengevirus kan også spre seg til disse når du er logget på.
- at du har en plan for hva du og dine ansatte skal gjøre dersom dere rammes av et løsepengevirus, og at alle ansatte kjenner til denne planen – for eksempel å trekke ut nettverkskablene og koble fra datamaskinene umiddelbart?
- at dere tilbyr og bruker totrinnspålogging på alle kontoer?

8 %

Andelen nordmenn som oppgir at de har blitt rammet av løsepengevirus på jobb i løpet av det siste året*

45 %

Andelen virksomheter som betalte løsepengekravet i 2019. Halvparten av disse mistet likevel sine data.***

«Løsepengevirus som retter seg mot smarttelefoner vil mulig øke i omfang.» *

* YouGov-undersøkelse for NorSIS, juli, 2020
** Telenor Digital Sikkerhet 2020
*** ENISA Threat Landscape 2020 - Ransomware

KONTOKAPRING:

8 av 10

datainnbrudd i sky- og lagringstjenester er knyttet til kompromitterte passord***

Passordet er nøkkelen til vårt digitale liv

Fremdeles er det slik at et av verdens mest brukte passord er «123456» eller «123456789». Bruker du eller noen andre i din virksomhet enkle passord for å logge inn på jobbtjenester, kan det gjøre dere sårbare for angrep som kan få store økonomiske konsekvenser for hele arbeidsplassen.

*** Securelink/ Verizon Data Breach Report

Når kriminelle på denne måten tar over en e-postkonto eller andre kontoer i bedriften, kan de for eksempel utgi seg for å være en ansatt og be om en pengeoverføring eller opplysninger eller stjele hemmelig informasjon fra bedriften. De kan også plante ondsinnede spionprogrammer eller løsepengevirus i bedriftens IT-system.

Mulighetene er nærmest uendelige for noen som har passord og adgang til en virksomhets e-post, et fagsystem, en Facebook-konto, påloggingsdetaljene til Office 365 eller andre programmer som ligger på nett.

Hvordan kan angripere få tak i de ansattes passord?

En metode som brukes for å «knekke» passord, er det som kalles passord-spraying. Da «pepres» virksomheters IT-systemer og skyløsninger med en strøm av kjente e-postadresser, kombinert med de mest brukte eller vanligste passordene. Ifølge IT-selskapet NordPass var passord som «123456», «111111», «Password» og lignende de klart mest populære å bruke globalt også i fjor.

En annen kjent metode for å få tilgang, er å bruke hackede eller lekkede passord og e-postadresser. Du kan sjekke om ditt brukernavn og passord er på avveier på ***Have I Been Pwned.***

Selv om innbruddene ofte er fra tjenester de ansatte helst bruker privat, er særlig de av oss som bruker samme passord alle steder sårbare for denne typen angrep.

Et mindretall bruker forskjellige passord til ulike nettjenester

Denne utfordringen understrekes av et av funnene i vår nyeste rapport om nordmenns digitale sikkerhetskultur. Kun et mindretall av oss bruker ulike passord til ulike nettjenester. Dersom en av dine ansattes passord er på avveier, kan det gi kriminelle tilgang til vedkommendes jobbkonto.

Nøkkelen til å unngå dette er at alle i bedriften bruker sterke og unike passord både på jobbsystemer og på andre nettjenester. I tillegg bør alle bruke totrinnspålogging der det er mulig. Dere bør sørge for at alle virksomhetens systemer settes opp med mulighet for totrinnspålogging.

Sjekkliste for å unngå kontokapring

Dersom det er noen av disse punktene du ikke forstår eller kan utføre selv, hør med driftsleverandøren din.

Har du sørget for:

- at alle virksomhetens systemer settes opp med totrinnspålogging som standard?
- at alle ansatte bruker totrinnspålogging på alle sine innlogginger i alle systemer?
- at alle brukere av systemet sikrer sin tilgang med et sterkt og unikt passord dersom det ikke er mulig å bruke totrinnspålogging i et system?
- at det er stilt krav til nye leverandører/systemtilbydere eller andre om at innlogging må beskyttes med totrinnspålogging?
- at alle vet at de må gi beskjed dersom de har lagt igjen brukernavn og passord et sted de er usikre på, for eksempel via en lenke?
- at dere har rutiner for gjenoppretting av passord, det vil si at alle vet hvem de skal kontakte for å få et nytt passord og hvor de får passordet sendt?

Blir det mange passord å holde styr på, er det bedre å skrive dem ned på en lapp og legge den et trygt sted enn å bruke enkle passord eller like passord for flere nettjenester.

Trenger du mer hjelp?

[Slik aktiver du totrinnspålogging]

[Slik sletter du en profil]

Bruk totrinnspålogging!

Tiltaket som vil øke sikkerheten i din virksomhet mest, er å bruke totrinnspålogging alle steder det tilbys. Dette 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.

10 %

av alle nordmenn oppgir at de i løpet av det siste året har mistet full kontroll over en eller flere av sine sosiale medier- eller e-postkontoer. Dette kan bli et problem dersom de bruker samme påloggingsinformasjon på jobbsystemer.*

4 av 10

nordmenn bruker forskjellige passord til sine nettjenester, og omtrent like mange legger vekt på å lage sikre passord**

50 PROSENT

av sikkerhetsbruddene i norske virksomheter skyldes blant annet menneskelige feil**

10 593 285 880

Antall stjålne brukernavn og passord til e-postkontoer, sosiale medier og en rekke andre tjenester i den gigantiske data-basen «Have I Been Pwned» i januar 2021

* Yougov-undersøkelse for NorSIS, juli 2020

** Mørketallsundersøkelsen 2020, Næringslivets Sikkerhetsråd

**** NorSIS-rapporten "Nordmenn og digital sikkerhetskultur 2020

VERDIKJEDEANGREP:

Virksomheten din er en brikke i et puslespill!

Det kan få ødeleggende konsekvenser for din virksomhetens omdømme dersom den brukes i et angrep mot kunder, leverandører eller andre samarbeidspartnere.

Teknologien knytter oss stadig tettere til våre samarbeidspartnere, kunder og leverandører og gjør oss gjensidig avhengige av hverandre. Det betyr at dersom en av dine samarbeidspartnere er dårlig sikret, kan angripere nå deg gjennom deres systemer. Eller omvendt.

Dette komplekse bildet krever også at du virkelig forstår og analyserer hvilke utfordringer og risikoer din egen virksomhet kan utsettes for. Det kan være at du bør stille krav til sikkerheten hos de du samarbeider med.

I et verdikjedeangrep angripes noen i verdikjeden som kan lede angriperen til målet for angrepet, istedenfor at selve målet angripes. I Europa har det de siste årene blitt stadig vanligere at angrep på store virksomheter skjer gjennom angrep rettet mot virksomheter i deres verdikjede. Et angrep mot en liten, lokal underleverandør kan i ytterste konsekvens medføre at systemer i store, globale konsern settes ut av spill. Fordi data utveksles mellom disse aktørene i verdikjeden, kan også virus utveksles og forplante seg.

Gratisprogrammer og usikrede hjemmekontor gjør bedriften sårbar for angrep

Når så å si alle komponenter vi bruker og deler i vårt verdikjedenettverk er koblet til nett, er det viktig å se hele bildet for å kunne sikre virksomhetens verdier og omdømme. Både det at Sharepoint og lignende ikke er sikret i skyen, at ansatte bruker nettbaserte gratisprogram som ikke er godkjent i bedriftens IT-system eller at noen bruker barnas PC til å koble seg på VPN kan gjøre bedriften sårbar for verdikjedeangrep.

Et angrep mot en liten, lokal leverandør kan i ytterste konsekvens sette et globalt konsern ut av spill.

Samtidig som dere må ha kontroll over systemer og utstyr, bør utstyret være så godt sikret at det ikke spiller noen rolle hvilket nettverk den enkelte bruker. Dette kan være krevende å få til. I så fall må virksomheten søke hjelp hos sin driftsleverandør.

Noen eksempler på verdikjedeangrep:

- Det store SolarWinds Orion-angrepet som ble avslørt i midten av desember i fjor, kan illustrere fremgangsmåten. Her ble et populært program som brukes av tusenvis av virksomheter over hele verden, inklusiv USAs sikkerhetsdepartement, Visa, Microsoft og flere norske virksomheter, kompromittert. Når kundene oppgraderte programmet, ble systemene deres infisert, og det ble mulig for kriminelle å spionere på eller sabotere for selskapene.

- Skadevare, som løsepengevirus eller tjenestenektangrep (DDoS-angrep), kan brukes i målrettede angrep mot tredjeparter i verdikjeden. Dersom deres systemer «tas ned», kan det få store konsekvenser for kundene eller leverandørene deres. Et sykehus kan stå uten tilgang til pasientjournaler, frisøren får ikke brukt timeavtalesystemet sitt eller en snekker får ikke registrert eller fakturert kundene sine.

«NSM ser det som sannsynlig at angrep på leverandør-kjeder vil øke.»*

Trenger du mer hjelp?

10 anbefalte tiltak for å øke virksomhetens egenevne til digital sikkerhet

* NSM-rapporten «Helhetlig digitalt risikobilde 2020»

Sjekkliste for å unngå verdikjedeangrep.

Dersom det er noen av disse punktene du ikke forstår eller kan utføre selv, hør med driftsleverandøren din.

Har du sørget for:

- at alle enheter, inkludert kaffetraktere og varmeovner som er koblet opp mot nett, er sikret med et godt brukernavn og passord, ikke standardpassordet som fulgte med?
- at alle samarbeidspartnere, kunder og leverandører som har tilgang til dine datasystemer har gode rutiner for IT-sikkerhet?
- å ha oversikt over dine verdier, verdikjeder og sårbarheter?
- at dere har rutiner for å avinstallere programvare som ikke brukes?
- at alle enheter er sikkerhetsoppdatert?
- at dere har sørget for logging og monitorering av systemene, slik at uregelmessigheter kan oppdages?
- at de ansatte har dedikert utstyr å jobbe på?

52 %

av sikkerhetshetsbruddene i små virksomheter oppdages ved en ren tilfeldighet**

6 AV 10 LEDERE

tillater ansatte å bruke privat datautstyr***

32 % av ledere

tillater de ansatte å laste ned programvare på jobb-PC eller mobil uten at det foreligger en godkjenning fra virksomheten***

** Mørketallsundersøkelsen 2020, Næringslivets Sikkerhetsråd

*** YouGov, lederundersøkelse for NorSIS, 2019

SVINDEL:

Angripere velger alltid den letteste veien inn i virksom-heten din

Nettsvindel fortsetter å være en stor trussel for små og mellom-store bedrifter. Dette er en type angrep der lav innsats kan gi angriperne stor uttelling.

18 prosent

har lagt igjen sensitiv informasjon som personnummer og kontonummer på en nettside uten å vite hvem som eier den**

** YouGov-undersøkelse for Buypass, november 2020

Svindel handler som regel om sosial manipulering, og spiller på frykt, fristelse eller tillit. Frykt for å skremme deg til å raskt – uten å tenke deg om – klikke på en lenke, laste ned et vedlegg eller gjøre hva avsenderen ber deg om. Fristelse ved at du raskt og lettvint kan vinne en mobil eller noe annet. Tillit fordi avsenderen av f.eks. en e-post utgir seg for å være en du kjenner til, og derfor blir budskapet i e-posten viktig og riktig.

1 av 20

hadde ifølge politiets Innbyggerundersøkelse 2019 i løpet av det siste året personlig opplevd svindel eller bedrageri på internett

De 3 vanligste svindlertriksene!

TILLIT - Avsender er tilsynelatende noen du kjenner eller stoler på. Da er vi ofte mindre skeptiske. Kjente merkenavn blir også utnyttet i svindler eller konkurranser.

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.

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 følger sesonger, trender og store hendelser, og tilpasser seg adferden vår

Våren 2020 opplevde en rekke virksomheter både å få fakturaer for smittevernutstyr de ikke hadde bestilt og falske tilbud om å kjøpe smittevernutstyr. Ut over våren opplevde en rekke sektorer som tradisjonelt ikke har jobbet mye hjemmefra at svært mange ble utsatt for en svindel med falske oppdateringer av systemer de brukte. Målet var å hente ut brukernavnet og passordet deres.

Ettersom nordmenns handlemønster har endret seg til å først og fremst foregå på nett, samtidig som vi tilbringer stadig mer tid i digitale kanaler, har en rekke virksomheter opplevd å få merkevaren sin misbrukt – både til å selge falske produkter eller å gjennomføre falske nettarrangement, konkurranser eller julekalendere.

PHISHING

Phishing er elektronisk kommunikasjon (e-post/SMS) der avsenderen prøver å lure deg til å oppgi informasjon du ellers ikke ville gitt fra deg. Det er typisk, finansielle opplysninger, som kredittkort og annen betalingsinformasjon eller brukernavn og passord.

Sjekkliste for å unngå å gå på phishing-forsøk:

Dersom det er noen av disse punktene du ikke forstår eller kan utføre selv, hør med driftsleverandøren din.

Har du sørget for:

- at dere har en kultur der alle ansatte tør å si ifra hvis de gjør noe galt, og at du er et godt eksempel på dette ved å rose de som sier ifra om feil?
- at dere har gode rutiner for at ingen betaler med kredittkort eller gir fra seg kredittkortinformasjon på steder der virksomheten ikke har en profil eller innlogging?
- at virksomheten ikke tillater at noen kjører kode eller installerer programmer fra en lenke eller et vedlegg de har fått tilsendt?

Kjenner du trikset med tullebrukernavn og tullepassord?

Dette er et godt triks for å sjekke om innloggingslenken du har fått på e-post eller SMS er ekte eller ikke. Dersom du kommer inn, så vet du at det er phishing.

Her forklarer Hans Marius dette

DIREKTØR- OG FAKTURASVINDEL:

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

Fakturasvindel dreier seg ofte om en falsk henvendelse for en reell tjeneste der en leverandør skal ha byttet kontonummer, for eksempel en faktura for kontorrekvisita som virksomheten ikke har bestilt.

«Svindlene er gjerne sesongbetont eller knyttet opp mot større hendelser.»

Sjekkliste for å unngå direktør- og fakturasvindel:

Dersom det er noen av disse punktene du ikke forstår eller kan utføre selv, hør med driftsleverandøren din.

Har du sørget for:

- at henvendelser der det anmodes om pengeoverføringer alltid dobbeltsjekkes? Kommer den på e-post, les den to ganger og kontakt den som ber om overføringen på telefon, det vil si i en annen kanal enn den dere mottok henvendelsen gjennom, for å få bekreftet at den er ekte.
- at dere har en rutine for at ledelsen informerer sine økonomimedarbeidere på forhånd dersom de vet at det kan bli aktuelt med eller behov for kjappe overføringer?
- at rutinene for pengeoverføringer er risikovurdert, det vil si at dere blant annet har gjort en grundig gjennomgang av om rutinene kan «stå imot» et svindelforsøk eller muligheter for menneskelige feil?
- at dere alltid dobbeltsjekker med leverandøren når dere har mottatt meldinger om endring av kontonummer? Her er det viktig å sjekke via en annen kanal enn der dere fikk henvendelsen om endringen. Dere må for eksempel ikke bruke telefonnummeret som står i e-posten dere mottok om kontonummerskifte.
- å sikre e-postkontoene med totrinnspålogging for å unngå kontoovertagelse?

BARE 4 AV 10

undersøker alltid om lenker og vedlegg er trygge før de åpner dem***

*** NorSIS-rapporten «Nordmenn og digital sikkerhetskultur 2020»

FALSKE NETTBUTIKKER, NETTSIDER OG PROFILER

Ved å misbruke kjente og ofte etablerte virksomheters navn på falske nettsider, nettbutikker, konkurranser eller profiler på sosiale medier, tiltrekker svindlerne seg både kunder av virksomheten den etterligner og andre som kjenner til navnet.

Når kundene blir svindlet og lurt, går det ikke bare ut over dem, men også den misbrukte virksomhetens omdømme. Denne typen svindel er ofte vanskelig å avdekke før man får et tips om det.

8 %

av alle nordmenn har blitt utsatt for svindel som har fått økonomiske konsekvenser for dem i løpet av det siste året*

«En seriøs aktør vil aldri be deg oppgi passord til nettbank eller annen sensitiv informasjon.»

Sjekkliste for å oppdage og håndtere falske nettsider, profiler eller annet i din virksomhets navn:

Dersom det er noen av disse punktene du ikke forstår eller kan utføre selv, hør med driftsleverandøren din.

Har du sørget for:

- å ha oversikt over hvor virksomhetens navn blir nevnt, for eksempel et Google Alerts-søk som vil gi deg beskjed når det publiseres noe som inneholder navnet på virksomheten din?
- å ta alle henvendelser fra kunder om dårlig behandling på alvor og sjekke ut hvor de faktisk stammer fra? Det kan stamme fra en falsk profil, nettsted eller lignende.
- å ha rutiner for å si ifra til kunder og andre brukere, for eksempel på nettsiden deres og i sosiale medier, dersom noen har laget en falsk nettside, konkurranse eller profil og utgir seg for å være virksomheten din?

Trenger du mer hjelp?

Her er 10 enkle tips som hjelper din virksomhet å avsløre svindel

* YouGov-undersøkelse for NorSIS, juni 2020

Her er de tre viktigste tiltak-ene som gjør virksomheten din langt sikrere!

Det skal mindre til enn du tror å gjøre virksomheten din langt bedre rustet mot stadig mer kyniske og profesjonelle cyberkriminelle.

4 AV 10
legger vekt på å bruke sikre passord*

42
PROSENT
bruker forskjellige passord for de fleste tjenestene på nett*

47 %
sikkerhetskopierer data som er viktig for dem i privat sammenheng sjeldnere enn hver måned*

* NorSIS-rapporten «Nordmenn og digital sikkerhetskultur 2020»

1 AV 5
har ingen rutiner for å oppdatere*

Dette er de tre viktigste tiltakene alle virksomheter bør innføre:

Sikkerhetskopier så ofte som mulig!

Hvorfor? Skulle virksomheten bli rammet av et løsepengevirus som låser dine mest verdifulle data eller at ondsinnet skadevare ødelegger eller sletter dem, er det å ha en skikkelig sikkerhetskopi helt avgjørende. Alt som er digitalt lagret, enten det er kassasystemet ditt, dine viktigste kontrakter, kundelister eller lignende, kan bli ødelagt ved et angrep. Samtidig kan også menneskelige feil, som skjer hver dag, ramme virksomheten.

Hvordan? Eksempler på data som er viktig å sikkerhetskopiere er data for produksjons-systemer, kundeinformasjon, e-post, kalendre og kontakter. Prioriter det som ikke lett kan reddes ved et tap. Husk at kritiske data også kan finnes på minnepinner og mobiltelefoner. Sørg alltid for å teste at dataene lar seg gjenopprette. Hvis du ikke kan gjenopprette data, vil det ikke være noe vits å sikkerhetskopiere. Velger du en skyløsning må du også sørge for å stille krav til leverandøren slik at du kan stole på at sikkerhetskopien fungerer. Sikkerhetskopien bør lagres offline eller på et annet nettverk enn det dere bruker for å ikke bli omfattet i et potensielt dataangrep. Husk å ta høyde for dette. Kontakt din driftsleverandør dersom du er usikker på hvor og hvordan sikkerhetskopien lagres. Daglige eller ukentlige sikkerhetskopieringer er å anbefale.

Les mer om sikkerhetskopiering her

Oppdater alle systemer og programmer jevnlig!

Hvorfor? Leverandører av operativsystemer, dataprogrammer og mobilapper finner hele tiden sikkerhetshull i sine programmer. For å tette disse lager de oppdateringer som retter feil. Dersom du ikke oppdaterer, er angriperne lynraske til å utnytte og finne hullene i systemet. De kan da ta seg inn i ditt system og stjele verdifull informasjon eller plante virus som spionerer på deg eller lammer hele systemet. Oppdateringer er med andre ord noe langt mer enn nye funksjoner!

Hvordan? Aktiver automatisk oppdatering alle steder du kan. Oppdateringer av selve systemet går også i stor grad automatisk hvis du installerer dem. For mobil gjøres dette enkelt i Google Play (Android) eller Apple App Store. Andre programmer må du sette deg inn i hvordan fungerer.

Les mer om oppdatering her

35 %
av årsakene til sikkerhetshendelser er avvik i nettverk og apper, viser Orange Cyber Defense' analyse av mer enn 50 milliarder IT-sikkerhetshendelser. Blant de vanligste er manglende oppdatering av systemer og programmer med kjente sikkerhetshull.

Bruk totrinnspålogging alle steder du kan!

Hvorfor? For å forhindre at noen tar over en av dine brukerkontoer til e-post, fagsystemer, skyløsninger eller sosiale medier, må du gjøre alt som er mulig for å holde passordet ditt for deg selv. Det er selve nøkkelen til ditt digitale liv. Den klart beste måten å gjøre dette på er å bruke totrinnspålogging. Det er det aller viktigste enkeltsikkerhetstiltaket både i enhver virksomhet og for enhver privatperson. Det fungerer slik at når du logger deg på med en ny enhet, må du i tillegg til passordet bekrefte hvem du er med en engangskode fra SMS eller via en app på telefonen. Det hindrer at uvedkommende kan logge seg på en konto selv om de kjenner brukernavnet og passordet til kontoen.

53 %
bruker totrinns-pålogging der det er mulig*

Hvordan? Hvordan du aktiverer totrinnspålogging varierer fra tjeneste til tjeneste. Felles for alle er at det ofte er svært enkelt og kjapt å gjennomføre.

Her er en detaljert beskrivelse av hvordan du aktiverer totrinns-pålogging på de mest populære e-posttjenestene og sosiale mediene

* NorSIS-rapporten «Nordmenn og digital sikkerhetskultur 2020»

Flere angrep mot mennesker enn maskiner:

Om du gjør enkle tiltak, utgjør det en stor forskjell

Teknologien gjør stadig oftere mennesker til mål for digitale angrep. Samtidig er mange av de digitale truslene mot norske virksomheter de samme som før, selv om de blir mer raffinerte. Slik vil det trolig også være i 2021.

Løsepengevirus, svindel, kontokapring og andre former for svindel vil fortsette å prege trussel-landskapet. Dette er alle svindler der sosial manipulering av den enkelte ansatte er en viktig ingrediens. I tillegg er dette svindeltyper som gir de kriminelle god avkastning selv med relativt lav innsats. Det er også slik at det er lav risiko for at de som står bak blir tatt.

Den ansattes kunnskap og kompetanse stadig viktigere

Dreiningen til angrep mot mennesker fremfor virksomhetens IT-systemer gjør det enda viktigere at den enkelte ansatte har kompetanse om hvordan svindlere jobber og hva de skal være på vakt mot. Det er de som blir angrepsvektoren, ikke systemet.

Angrepene med sosial manipulering blir stadig mer utspekulerte. Det blir vanskeligere å skille ekte fra falsk. Bruken av kunstig intelligens til å lage enda bedre norske tekster i svindel-e-poster forekommer allerede, noe som gjør svindelen vanskeligere å avsløre.

En måte vi har sett dette skje på, er at særlig falske utpressings-trusler blir mer avanserte. Vi kaller det dobbel utpressing. Ofte skjer dette knyttet til e-posthenvendelser som truer med å utlevere noe om deg, alt fra pornovaner, utroskap eller noe annet svindlerne oppgir å ha videobevis for at du har gjort. Den første henvendelsen følges deretter opp med en e-post som tilsynelatende kommer fra en sikkerhetsansvarlig hos YouTube, Vimeo eller en annen videoplattform med spørsmål om du vil ha hjelp til å fjerne filmen. Dobbel utpressing har også skjedd i tilfeller med løsepengevirus. Da trues det med at skadevaren brukes både til kryptering av data og tyveri av sensitive data, med påfølgende trussel om publisering eller salg av opplysninger til andre kriminelle.

Informasjon om din virksomhet eller dine ansatte kan også gjøre et svindelforsøk mer troverdig med relativt lav innsats fra de kriminelle.

Samtidig jobber også teknologiselskapene for fullt med å gjøre nettaktivitetene våre enda tryggere. Bruk av BankID på alt fra nettbutikker til sjekketjenester gjør det tryggere å handle (eller sjekke) på nett.

Denne typen løsninger styrker vår digitale sikkerhet. Samtidig er det også en angrepsvektor. Ved å oppgi passord og brukernavn stadig oftere, er det en fare for at vi senker skuldrene og blir mer ukritiske. Dersom de er raske, kan svindlere også utnytte vår BankID i realtid, for eksempel ved å bruke en falsk nettside. Teknologien er på mange måter bra, men ved å manipulere brukeren kan også dette misbrukes.

Det jobbes også stadig med utviklingen av nye tekniske løsninger som kan hjelpe norske virksomheter. Et eksempel er passordfri innlogging. Foreløpig må imidlertid dette testes i stor skala før det kan rulles ut. Det vil ta tid.

Lengre verdikjeder øker sårbarheten for angrep

Det stadig større omfanget av tilkoblingsmuligheter til nett øker også sårbarheten vår. Dette skaper et økt behov for at enkeltpersoner må logge seg på for å kunne benytte seg av de nye tjenestene. Dørene og tilhørende nøkler inn til våre verdier blir flere, slik at de kriminelles muligheter vokser.

Samtidig blir verdikjedene lengre og mer uoversiktlige. Risikoen for et digitalt angrep mot din virksomhets internettilkoblede varmeovn eller skriver øker. Får uvedkommende tilgang til en ansatts brukernavn og passord, kan veien videre til virksomhetens verdier være kort.

Økende utfordringer kan bekjempes med enkle løsninger

Heldigvis er ikke løsningen så komplisert. Med grunnleggende kunnskap blant dine ansatte om svindel, utbredt bruk av totrinnspålogging, sterke passord, regelmessig oppdatering og sikkerhetskopiering, reduserer du sjansen for lammende dataangrep betraktelig.

Virksomheter må derfor ta i bruk de tekniske tiltakene som er tilgjengelige for å beskytte sine verdier. I tillegg må de sørge for at de ansatte har god nok kunnskap, forståelse og åpenhet om feil til å bidra til å sikre virksomheten mot angrep.

Situasjonen her og nå er at konsekvensene av digitale angrep kan være enorme. Samtidig er tiltakene for å unngå mange av de største trusseltrendene absolutt oppnåelige for de aller fleste.

Så ikke utsett det – start nå!

Teknologiveien 22
2815 Gjøvik
Org.nr. 995195003

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