NorSIS

SKADEVARE

Noen i virksomheten mottar en e-post.

Den ser kanskje ut til å være legitim – men med et klikk på en lenke eller åpning av et vedlegg, blir alle stengt ute fra nettverket. Lenken lastet ned programvare som holder datamaskinen din som gissel. Det er utpressing ved hjelp av skadevareangrep.

Angriperen ber om penger eller kryptovaluta, men selv om du betaler, vet du ikke om du får informasjonen din tilbake. Informasjon du behøver for å drive virksomheten din, i tillegg til detaljer om kunder, ansatte og bedriften, er nå i hendene til kriminelle. Skadevare kan ha alvorlige konsekvenser for din virksomhet.

Hvordan skjer det?

Kriminelle kan starte et skadevare-angrep på en rekke måter.

Svindelmail

med lenker og vedlegg som kan ta kontroll over informasjonen og utstyret ditt. Disse phishing-e-postene utgjør den største delen av skadevareangrep.

nettvett.no/phishing/

Sårbarheter

i operativsystem eller programvare som kan bli utnyttet av hackere.

nettvett.no/oppdateringer/

Infiserte nettsider

www som automatisk laster ned skadevare på din datamaskin når du besøker nettsiden.

Digital reklame

som inneholder skadevare – selv på nettsider du kjenner til og stoler på.

nettvett.no/okonomisk-svindel-rettet-bedrifter/

CYBERSIKKERHET FOR
SMÅ VIRKSOMHETER

NorSIS

HVORDAN **BESKYTTE** VIRKSOMHETEN DIN

Ha en beredskapsplan

Hvordan ville du drive din virksomhet etter et skadevareangrep? Skriv tiltakene ned på papir, og del den med alle som trenger å vite om den.

Sikkerhetskopier filene dine

Utfør regelmessig sikkerhetskopiering av viktige dokumenter og filer til en ekstern disk eller server som ikke er på det interne nettverket. Gjør dette til en fast rutine.

nettvett.no/sikkerhetskopiering/

Hold sikkerheten din oppdatert

Installer alltid de nyeste oppdateringene til operativsystem og programvare. Aktiver automatisk oppdatering på bedriftens datamaskiner og andre digitale enheter. På mobile enheter, kan det hende du må gjennomføre oppdateringen manuelt.

nettvett.no/oppdateringer/

Varsle de ansatte

Lær de ansatte hvordan de kan unngå phishing-svindel, og informer de om vanlige måter skadevare infiserer datamaskiner og andre enheter. Inkluder tips for å identifisere og beskytte mot skadevare i virksomhetens regelmessige opplæring.

nettvett.no/falske-e-poster/

Hva bør du gjøre om du blir utsatt for angrep

Begrens skaden

Koble de aktuelle enhetene fra nettverket med en gang. Varsle kunder, ansatte og andre som kan ha blitt påvirket.

Kontakt politiet

Eventuelt varsle de som leverer sikkerhetstjenester til bedriften.

Hold firmaet gående

Nå er det på tide å iverksette beredskapsplanen. Å ha en oppdatert sikkerhetskopi vil være nyttig.

Burde jeg betale?

NorSIS anbefaler aldri noen å betale utpressere, det er ingen garanti for at du får informasjonen din tilbake.