SANS SECURITY AWARENESS

Ditt månedlige nyhetsbrev om sikkerhetsbevissthet

Har jeg blitt hacket?

Oversikt

Akkurat som med bil, uansett hvor sikker du er kan du før eller siden bli utsatt for en ulykke. Under finner du noen kjennetegn på at du har blitt hacket, samt hva du kan gjøre om det er tilfellet. Jo fortere du blir klar over at noe har skjedd, jo mer sannsynlig er det at du kan rette opp i det.

Tegn på at du har blitt hacket

Du får et varsel fra antivirus-programmet ditt om at systemet ditt er infisert. Sørg for at varselet faktisk kommer fra antivirus-programmet ditt, og ikke fra et pop-up-vindu i en nettside som prøver å lure deg til å ringe et nummer eller installere noe. Om du er usikker kan du åpne antivirus-programmet ditt.

Det åpnes et vindu hvor du får beskjed om at filer på maskinen har blitt kryptert, og du må betale løsepenger for å få dem tilbake.

Nettleseren din åpner forskjellige nettsider som du ikke ønsker å besøke.

Maskinen eller programmer på den krasjer ofte, det dukker opp ikoner for ukjente programmer eller apper, og underlige vinduer åpner seg.

Passordet ditt virker ikke lenger, selv om du er helt sikker på at det er korrekt.

Vennene dine spør deg hvorfor du sender dem spam selv om du vet at du ikke har sendt noe slikt.

Kontoutskriften din viser trekk fra kortet ditt som du vet at du ikke står bak.

Hva burde du gjøre?

Om du mistenker at du har blitt hacket er det lurt å handle raskt. Om det er snakk om noe som har skjedd i jobbsammenheng må du ikke prøve å fikse problemet selv, istedenfor burde du si fra til IT-/sikkerhetsansvarlig med en gang. Men dersom det er snakk om et personlig system eller brukerkonto, kan du ta noen grep:

Endre passord: Dette inkluderer ikke bare endring av passord på datamaskin og mobil, men også på brukerkontoer på nett. Ikke bruk den hackede maskinen for å endre passord, bruk istedenfor et annet system som du vet er sikkert. Dersom du har mange brukerkontoer, begynn med de viktigste først. Om du ikke kan holde oversikt over alle passordene kan du bruke et passordhåndteringsprogram, også kjent som passordhvelv.

Økonomi: Dersom det gjelder bank- eller kredittkort, eller kontoer knyttet til bank eller økonomi, burde du ringe banken eller kredittselskapet med en gang. Ring dem på et telefonnummer du vet går til dem, dette finner du gjerne på bankkortet eller på brev fra banken. Eventuelt kan du besøke nettsiden deres fra en sikker datamaskin. Vurder eventuelt sperring av kort eller frivillig kredittsperre.

Antivirus: Dersom antivirus-programmet ditt informerer deg om virus eller infiserte filer bør du gjøre det den foreslår, for eksempel sette de aktuelle filene i karantene. De fleste antivirus-programmer har også lenker til nettsidene deres dersom du vil lese mer om den aktuelle typen skadevare.

Reinstallering: Dersom du ikke klarer å fikse en infisert maskin, eller du ikke er sikker på at den er sikret, kan du reinstallere operativsystemet. Ikke reinstaller fra sikkerhetskopier, sikkerhetskopi burde kun brukes for å gjenopprette personlige filer. Dersom du ikke er komfortabel med reinstallering kan du vurdere å betale et profesjonelt firma for å gjøre det. Eventuelt, dersom maskinen er veldig gammel, er det kanskje enklere og greiere å bare kjøpe ny. Til slutt, etter reinstallering eller kjøp av ny maskin, sørg for å oppdatere programvare og operativsystem, og sørg for at automatisk oppdatering er aktivert.

Sikkerhetskopi: Et nøkkelgrep for å sikre seg er å ta sikkerhetskopi med jevne mellomrom. Mange løsninger eksisterer som gjør dette automatisk. Uansett hvordan du løser det, burde du også teste at du får gjenopprettet fra sikkerhetskopien. I mange tilfeller er gjenoppretting fra sikkerhetskopi den eneste måten du kan komme deg etter et hackerangrep.

Politi: Om du føler deg truet på noen måte, meld fra til politiet. I Norge kan man finne ressurser for anmelding av datakriminalitet på https://www.politiet.no/rad/datakriminalitet/, du kan også sende tips til politiet på https://www.politiet.no/tjenester/tips-politiet/.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Gjesteredaktør

Dr. Johannes Ullrich *(@johullrich) er dekan for forskning ved SANS Technology Institute, direktør for SANS Internet Storm Center og er en SANS Fellow. Han skapte det samarbeidsbaserte sensornettverket DShield, og er programleder for Internet Storm Center's daglige podcast om nettverkssikkerhet.*

Ressurser

Sikkerhetskopiering og gjenoppretting:	https://www.sans.org/u/JGP
Passordsetninger:	https://www.sans.org/u/JGU
Passordhvelv:	https://www.sans.org/u/JGZ
Hva er skadevare?:	https://www.sans.org/u/JH4
Nettvett.no ID-tyveri:	https://nettvett.no/id-tyveri/