SANS SECURITY AWARENESS

Det månedlige nyhedsbrev om IT-sikkerhed til dig

Er jeg blevet hacket?

Oversigt

Ligegyldigt hvor sikker du er, kan du, ligesom når du kører bil, før eller senere blive udsat for et uheld. Nedenfor er der metoder til at finde ud af, om du er blevet hacket og i så fald hvad skal du gøre. Jo hurtigere du identificerer noget dårligt, er sket, desto mere sandsynligt er det, at du kan løse problemet.

Spor der tyder på at du er blevet hacket

- **Dit anti-virusprogram giver dig en advarsel om, at dit system er inficeret. Sørg for, at det er dit antivirusprogram, der genererer advarslen, og ikke et pop-op-vindue fra et websted, der forsøger at narre dig til at ringe til et nummer eller installere noget andet. Hvis du ikke er sikker, skal du åbne dit antivirusprogram.**
- **Du får et pop-up-vindue, der siger, at din computer er krypteret, og du skal betale en løsesum for at få dine filer tilbage.**
- **Din browser tager dig til websteder, du ikke ønskede at gå til.**
- **Din computer eller programmer går konstant ned, der er ikoner til ukendte apps eller mærkelige vinduer, der dukker op.**
- **Dit kodeord virker ikke længere, selvom du ved, at dit kodeord er korrekt.**
- **Venner spørger dig, hvorfor du spammer dem med e-mails, som du ved, du aldrig har sendt.**
- **Der er hævninger på dit kreditkort eller udbetalinger fra din bankkonto, du aldrig selv har godkendt.**

Dette skal du gøre

Hvis du har mistanke om at du er blevet hacket, skal du reagere hurtigt. Jo hurtigere du handler des bedre er det. Hvis hacket er arbejdsrelateret, skal du ikke forsøge at løse problemet selv, men rapporter det øjeblikkeligt. Hvis det er et personligt system eller konto, der er blevet hacket, er der her nogle ting du bør gøre.

Du skal ændre dine adgangskoder: Dette omfatter ikke blot at ændre adgangskoderne på dine computere og mobile enheder, men til dine online-konti. Brug ikke den hackede computer til at ændre dine adgangskoder, brug et andet system, som du ved, er sikkert. Hvis du har mange konti, start med de vigtigste først. Kan du ikke holde styr på alle dine adgangskoder, brug en password manager.

Kreditkort: Hvis der er problemer med dit kreditkort eller finansielle konti, skal du ringe til din bank- eller kreditkortselskab med det samme. Brug et betroet telefonnummer til at ringe til dem, f.eks. fra bagsiden af dit bankkort, dit kontobevægelser eller det nummer der vises på deres hjemmeside når du tilgår den fra en betroet computer. Overvej desuden at spærre dine kreditkort.

Antivirus: Hvis dit anti-virussoftware informerer dig om en inficeret fil, skal du blot gøre som den anbefaler. De fleste anti-virus software vil give dig nogle links, som du kan følge for at lære mere om den specifikke infektion.

Geninstallation: Hvis du ikke kan reparere en inficeret computer, eller du vil være mere sikker på, at dit system er sikkert, skal du geninstallere operativsystemet. Geninstaller ikke fra sikkerhedskopier, men i stedet skal sikkerhedskopier kun bruges til at gendanne dine personlige filer. Hvis du er utryg ved at geninstallere, kan du overveje at bruge en professionel til at hjælpe dig. Eller hvis din computer eller enhed er gammel, kan det være lettere at købe en ny. Endelig, når du har genopbygget dit system eller købt en ny, skal du sørge for at den er opdateret og aktivere automatisk opdatering, hvis det er muligt.

Sikkerhedskopier: Et vigtigt skridt til at beskytte dig selv er at forberede dig før der sker noget ved at lave regelmæssige sikkerhedskopier. Mange løsninger sikkerhedskopierer automatisk dine filer dagligt eller endog hver time. Uanset hvilken løsning du bruger regelmæssigt, skal du kontrollere, at du er i stand til at gendanne disse filer. Ofte er genoprettelse af dine data fra backup, den eneste måde du kan gendanne dine data efter du er blevet hacket.

Lovhåndhævelse: Hvis du føler dig på nogen måde truet eller er blevet udsat for identitetstyveri, skal du rapportere hændelsen til Politiet.

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Gæsteredaktør

Dr. Johannes Ullrich *(@johullrich) er dekan for forskning på "SANS Technology Institute", direktøren for "SANS Internet Storm Center" og en "SANS Fellow". Han oprettede DShields og er vært for "Internet Storm Center" daglige podcast.*

Hvis du vil vide mere

Backups:	https://www.sans.org/u/JGP
Passphrases:	https://www.sans.org/u/JGU
Password Managers:	https://www.sans.org/u/JGZ
Hvad er malware:	https://www.sans.org/u/JH4