

Jeg er blevet hacket-tjeklisten

Få et hurtigt overblik over, hvordan du som udgangspunkt bør handle i de første timer, efter du er blevet hacket. Følg trinnene herunder. Den konkrete håndtering afhænger naturligvis af angrebets karakter og omfang.

#1

Skab overblik.

Hvad er ramt – en enkelt konto, en computer eller flere systemer? Notér, hvad du ser, og hvornår du opdagede det.

#2

Isolér berørte enheder.

Afbryd netværksforbindelsen ved at fjerne netværkskablet eller slå wi-fi fra. Lad som udgangspunkt enheden være tændt, så værdifulde spor ikke går tabt. Kan enheden ikke isoleres på anden måde, kan det være nødvendigt at slukke den for at forhindre yderligere spredning.

#3

Sikr kompromitterede konti fra en ren enhed.

Skift adgangskoder til berørte konti fra en enhed, du har tillid til. Priorité eksempelvis e-mail og administrative konti, og aktivér MFA, hvor det er relevant.

#4

Tilkald hjælp.

Kontakt jeres IT-ansvarlige, sikkerhedsteam eller en professionel Incident Response-partner. Undgå at begynde en større oprydning, før hændelsen er vurderet.

#5

Dokumentér hændelsen.

Notér tidspunkter, fejlmeddelelser og andre observationer, og tag relevante skærbilleder. Dokumentation kan være vigtig både for den tekniske undersøgelse og en eventuel anmeldelse.

#6

Afklar jeres anmeldelsespligt.

Hvis personoplysninger er berørt, skal I vurdere, om hændelsen skal anmeldes til Datatilsynet. Er virksomheden omfattet af f.eks. NIS2, kan der også gælde andre og kortere frister.

#7

Informér de rette personer.

Sørg for, at ledelsen og relevante medarbejdere er orienteret. Koordinér kommunikationen, og hold jer til det, I faktisk ved.

Står du midt i et angreb lige nu?

Vent ikke, kontakt straks vores Incident Response-team:
+45 9195 9595