Förbättra cybersäkerheten – håll koll på dina leverantörer

Varje företag är bara så starkt som sin svagaste länk. Data Breach Investigations Report (DBIR) 2022 påpekar att ”små” organisationer är lika attraktiva för brottslingar som stora.

– Detta beror på att man utnyttjar sårbarheter hos den mindre leverantören och därefter dess förtroende hos det större målföretaget, säger Mattias Nilsson, vd på Softjoy.

Alla har vi lärt oss att vara försiktiga med att öppna bifogade filer från okända avsändare. Men hur är det med filer från dem som vi tror oss känna? Hur vet vi att e-posten vi får faktiskt kommer från rätt avsändare? Detta är ett problem som funnits länge och där det finns lösningar där kontroll och verifiering av avsändare och mottagare nästintill omöjliggör förfalskningar.

– Det finns ett antal framtagna ”best practise” för hur man ska ställa in både sin e-postserver och domän för en säker kommunikation, men då efterlevnaden är undermålig väljer många en mer frikostig inställning bara för att säkerställa att inget kommer bort – eller så vet man helt enkelt inte om sina inställningar och kör strutsteknik, säger Mattias Nilsson, vd på Softjoy.

Måste använda sina funktioner

Många system levereras med funktioner för att försvåra dataintrång; utmaningen är att använda dem. Myndigheter går i dag ut med att vi måste stärka vår cybersäkerhet medan fåtalet av organisationerna egentligen förstår vad som menas eller vart man ska börja.

– En bra och enkel strategi är att skaffa sig en överblick över det man har i dag och säkerställa att det är konfigurerat och inställt på ett säkert sätt – och enligt de rekommendationer som finns.

När man säkerställt att grunden är säker och stabil kan man enligt Jörgen Olofsson, CTO på Softjoy, börja jobba vidare med övriga områden och system.

– Att hålla koll på dina system och dess attackytor och på så sätt se till att ditt första försvar är redo är lika viktigt som antivirus.

”Man litar på sin webbplats”

Dina gränsytor mot internet kan förenklat delas upp i några specifika delar: hur organisationens domännamn hanteras, regelverk för e-post, inställningar för webbserver och andra externa tjänster, samt hur certifikat och krypteringsmetoder hanteras.

– Det är klart att man litar mer på sin leverantörs webbplats än på en organisation som man aldrig hört talas om, menar Mattias.

Det finns redan färdiga betygsskalor för dessa delar och även goda argument till att hålla koll på vilka betyg som partners och leverantörer till din organisation har.

– Nu är det dags att tillsammans förstärka varje länk i kedjan! Genom att öka medvetenheten om din närmaste omvärld tar du ett ytterligare steg i att hålla jämna steg med de föränderliga utmaningar som digital säkerhet innebär.

Läs mer på:
https://lets-secure.eu

SOFTjoy