proofpoint.
Protect people. Defend data.

DATASKYDD I SVERIGE

Sett inifrån:

När jag pratar med kunder om utveckling av säkerhetsstrategier så brukar vi vara överens om att alla strategier måste stödas av data. Cybersäkerhet är en bransch i snabb utveckling där data från olika håll kan ändras hela tiden, samtidigt som kunderna vill ha aktuell information som är relevant för just deras verksamhet.

För att hjälpa kunder och få veta vad de anser om interna risker så intervjuade vi 75 höga svenska chefer. Förutom att analysera orsaker och konsekvenser av dataintrång ville vi veta hur cheferna såg på interna hot vid uppbyggandet av en säkerhetskultur.

Annika Westlund,
Nordenchef, Proofpoint

En tredjedel vet inte ens om att de utsatts för intrång

Vi har publicerat hela undersökningen **här** och slutsatserna är tydliga. Nästan hälften av de organisationer som vi talade med hade utsatts för dataintrång under de senaste 12 månaderna. Det är visserligen många men vad som slog mig mest var att en tredjedel inte ens kände till om de utsatts eller inte.

Det tyder på brister i den interna kommunikationen (inte alla som vi talade med arbetade med säkerhet) eller brist på verktyg och processer för att snabbt kunna identifiera dataintrång.

Stöld av inloggningsuppgifter var ett genomgående tema bland dataintrången. Det var huvuddelen av såväl orsaker som konsekvenser av intrången vilket tyder på att attackerna är återkommande. Angriparna skaffar sig inloggningsdata (t.ex. via darknet) och får tillgång till organisationer och kan stjäla ytterligare inloggningsdata som sedan kan säljas och så fortsätter problemen.

Medvetet eller omedvetet slarv kan bli kostsamt

Våra intervjuer pekar på att kunderna underskattar de interna riskerna för att de inte har en klar bild av interna hot, t.ex. anställda som är missnöjda eller illvilliga och läcker eller stjäl data. Många företag tror inte att någon anställd skulle stjäla data och de har kanske rätt men slarviga användare utgör nästan lika stort hot enligt vår undersökning. Anställda kan slarva genom att inte följa rådande säkerhetsrutiner och det är då som intrången sker.

Distansarbete tycks öka riskerna, 57 % av de chefer vi pratade med säger att anställda inte följer säkerhetsrutinerna lika bra sedan de började arbeta på distans, samtidigt säger 68 % att rutinerna för distansarbete gör att de inte längre har samma insyn i vad de anställda gör.

Skydd mot interna hot är ett tveeggat svärd

För att minska interna risker krävs både utbildning och rätt verktyg. Att hjälpa de anställda förstå riskerna med slarvigt beteende kan sätta deras arbete i ett sammanhang. En andra försvarsåtgärd, men lika viktig, är att ha rätt verktyg på plats som identifierar interna risker innan de blir ett problem.

Det är positivt att fler än hälften (61 %) av cheferna i vår undersökning säger att de utbildar personalen om interna hot. Detta område var sammantaget det som oftast angavs gällande kunskap om cybersäkerhet vilket förekom i 64 % av organisationerna. 64 % utbildade också om lösenordshygien och 61 % om risker med utpressningsprogram.

De flesta (72 %) hade en DLP-lösning som skyddade känslig information från att läcka ut, men avsaknad av specifik teknik mot interna hot är det som bidrar mest till riskerna, 73 % höll med om det.

Moderna lösningar som minskar interna hot gör att organisationer kan minska risker och frekvens för dessa hot, snabbt åtgärda upptäckta incidenter och besvara dessa effektivare.

Glöm inte att läsa hela rapporten från vår undersökning: **Interna säkerhetshot - Utmaningar och prioriteringar bland svenska organisationer.**