IT-säkerhet: En investering – inte en utgift

Både privatpersoner, företag och offentliga organisationer är djupt beroende av försörjnings- och energibranschen. Denna nyckelroll i samhället kräver rätt beredskap. Energiförsörjningsföretag måste tillämpa ett smart och holistiskt tillvägagångssätt för säkerhetshantering, där mänskligt beteende, infrastruktur och konsulttjänster tillsammans säkerställer data, försörjningstrygghet och verksamhetens integritet.

De viktigaste hoten förklarade

Främmande ord och jargong har alltid varit en integrerad del av IT, och säkerhetsområdet är inget undantag. Här förklaras några av de viktigaste hoten och varför de är viktiga att förhålla sig till.

Hackerangrepp

När kriminella grupper får obehörig tillgång till företags IT-system i ett "**hackerangrepp**" är det kapabelt att förlama hela organisationer och påverka försörjningstryggheten.

Oavsett om hackarna bara har ekonomiska intressen eller representerar fientliga stater, har oönskad tillgång till data och system stora konsekvenser.

Ransomware och malware

Ransomware är en mjukvara som kriminella använd-er för att låsa åtkomsten till data på det infekterade systemet, så att de kan utpressa företag att betala en lösensumma i utbyte mot att återfå åtkomsten.

Malware betyder malicious (ondsint) software och hit räknas till exempel datavirus, keyloggers, trojanska hästar och spionprogram, som alla på olika sätt gör skadliga eller oönskade saker på de drabbade datorerna.

Phishing

Phishing är när cyberbrottslingar försöker att få personer att göra något de inte borde göra. Det kan tex vara massutskick av e-post som lockar till att klicka på en länk som öppnar en infekterad fil.

Vid **spear phishing** är specifika personer utvalda att få personifierad e-post, som offret är mer benäget att falla för.

Social Engineering

Social Engineering är termen för attacker där kriminella bygger förtroende hos anställda och manipulerar dem till att begå säkerhetsmisstag eller ge bort känslig information.

Datasäkerhetskultur och prevention

Dina data är din största tillgång, och tekniken ensam kan inte skydda dig från alla attacker. Med väldefinierade processer och policyer som stödjer och skapar en stark säkerhetskultur kan dina medarbetare vara det första och bästa försvaret mot angrepp.

Zero Trust-säkerhetsmodell

Det finns ett otal ingångar till företags system, såsom datorer, surfplattor och sensorer. En **Zero Trust**-strategi bygger på att alla åtkomstpunkter utgör en risk och att den externa säkerheten kan vara äventyrad. Alla åtkomster måste verifieras och autentiseras varje gång.

Säkert surfande

Webbläsare är ett av de primära sätten på vilka dina medarbetare interagerar med Internet och är därför ett viktigt mål för kriminella. Det är vitalt att:

- Hålla **webbläsaren** uppdaterad med den senaste versionen.
- Inte upprätta förbindelse till webbplatser när du får en **webbläsarvarning** .
- Endast installera nödvändiga och godkända **webbläsar-plug-ins** eller tillägg.

Lösenord

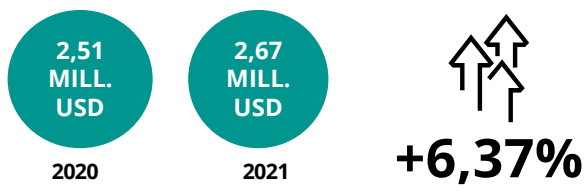
Lösenord är frontlinjen för skydd av personliga system och konton. Där måste du och dina medarbetare:

- Använda olika och komplexa **lösenord** på olika konton och webbplatser.
- Aldrig använda er arbetsrelaterade **användarinformation** för privata göromål.
- Byta **lösenord** regelbundet.
- Aldrig dela **lösenord** med någon, inte ens med chefer eller kollegor.
- Aktivera **multi-factor authentication (MFA)**, om det stöds.

Därför är säkerhetsintrång allvarliga för din verksamhet

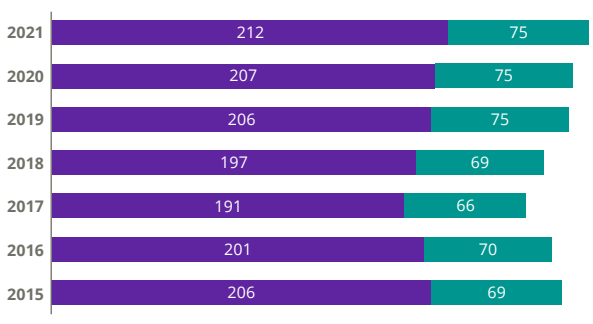
Datasäkerhetsbrott är inte ett flyktigt och övergående problem. Enligt IBM ökade den genomsnittliga kostnaden för säkerhetsintrång i Skandinavien 2021 med 6,37 % till 2,67 miljoner USD. Det är inte bara dyrt, utan också tidskrävande. I genomsnitt tog det hela 287 dagar att upptäcka och få ordning på säkerhetsintrånget.

De genomsnittliga kostnaderna vid säkerhetsintrång i Skandinavien har stigit



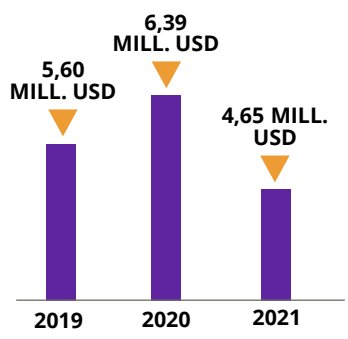
Källa: IBM & Ponemon Institute

Genomsnittliga antal dagar för att identifiera och begränsa ett säkerhetsintrång



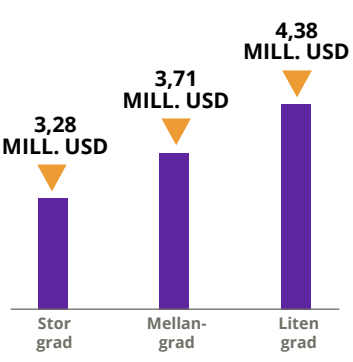
Källa: IBM & Ponemon Institute

Genomsnittliga totala kostnader för ett säkerhetsintrång globalt i energisektorn



Källa: IBM & Ponemon Institute

Genomsnittliga totala kostnader för ett säkerhetsintrång enligt graden av "Zero Trust"-implementering



Källa: IBM & Ponemon Institute

Rusta dig för ett angrepp med DXC:s ransomware-försvarsguide

Följ den här checklistan för att säkra system och data mot ransomware »

Få expertkunskap om Zero Trust från Microsoft

Klicka på ikonen och läs mer om Zero Trust, de sex försvarsområdena och hur produkter från Microsoft kan hjälpa din organisation att begränsa riskerna »

Håll dig uppdaterad med DXC Security Threat Intelligence Report

Skydda ditt företag. Prenumerera på DXC:s månatliga rapport om de senesta hoten, cyberkriminalitet och statsaktiviteter. »

DXC:s bud på ditt företags säkerhet

IDENTIFIERA:
- Fastslå risk- och hotbilden som är relevant för din verksamhet.
- Se till så att policyer och kontroller är på plats för att begränsa risker och hot.

SKYDDA:
- Upprätta skydd (brandväggar), djupförsvar, identitets- och åtkomstkontroll och liknande.

UPPTÄCK:
- Installera anti-malware.
- Registrera (försök till) intrång.
- Konsolidera logg till Security Information and Event Management i enlighet med risk- och hotbilden.

REAGERA:
- Initiera etablerade processer för att reagera på situationen.
- Använd existerande verktyg och resurser.

ÅTERSTÄLL:
- Initiera Disaster Recovery-processer.
- Återställ servrar och data där det är möjligt, använd expertkonsulter för att rengöra system.

DXC Technology Sverige
Gustav III:s Boulevard 36
169 85 Stockholm
Sverige
T +46 (0)10-5201600

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services across the Enterprise Technology Stack to drive new levels of performance, competitiveness, and customer experience. Learn more about how we deliver excellence for our customers and colleagues at www.dxc.com.

ENE-076S. Mars 2022