IT-sikkerhet: En investering – ikke en utgift

Både privatpersoner, virksomheter og offentlige organisasjoner er veldig avhengige av forsynings- og energibransjen. Denne nøkkelrollen i samfunnet krever det riktige beredskapet. Forsyningsselskaper bør bruke en smart og holistisk tilnærming til sikkerhetsstyring, hvor menneskelig atferd, infrastruktur og konsulentytelser tilsammen sikrer data, forsyningssikkerhet og forretningens integritet.

De viktigste truslene forklart

Fremmedord og faguttrykk har alltid vært en integrert del av IT, og sikkerhetsområdet er intet unntak. Her forklares noen av de viktigste truslene, og hvorfor de er avgjørende å forholde seg til.

Hackeangrep

Når kriminelle grupper får uautorisert tilgang til virksomheters IT-systemer i et "**hackeangrep**", er det i stand til å lamme hele organisasjoner og påvirke forsyningssikkerheten.

Uansett om hackerne bare har økonomiske interesser eller representerer fiendtlige stater, har uønsket tilgang til data og systemer store konsekvenser.

Ransomware og malware

Ransomware er en programvare som kriminelle bruker til å låse tilgangen til data på det infiserte systemet, slik at de kan presse virksomheter til å betale løspenger for å få tilgangen tilbake.

Malware betyr malicious (ondsinnet) programvare og inkluderer f eks computervira, keyloggers, trojanske hester og spyware, som alle på forskjellig vis gjør skadelige eller uønskede ting på datamaskinene de angriper.

Phishing

Phishing er når onlinekriminelle prøver å få personer til å gjøre noe de ikke bør gjøre. Det kan f eks være masseutsendte mailer som lokker en til å klikke på en link som åpner en infisert fil.

Ved **spear-phishing** er bestemte personer målrettet og får en personliggjort mail, som offeret er mer tilbøyelig til å falle for.

Social Engineering

Social Engineering er betegnelsen for angrep hvor kriminelle skaper tillit hos medarbeidere og manipulerer dem til å gjøre sikkerhetsfeil eller gi bort sensitive opplysninger.

Datasikkerhetskultur og forebyggelse

Dataene dine er din største ressurs, og teknologi alene kan ikke beskytte deg mot alle angrep. Med veldefinerte prosesser og politikk som understøtter og skaper en sterk sikkerhetskultur, kan dine medarbeidere være det første og beste forsvaret mot angrep.

Zero Trust sikkerhetsmodell

Det finnes uttallige tilnærminger til virksomhetens systemer, som datamaskiner, nettbrett og sensorer. En **Zero Trust** tilnærming er basert på at alle tilgangspunkter utgjør en risiko og den ytre sikkerheten kan være kompromittert. Der bør enhver tilgang verifiseres og autentifiseres hver eneste gang.

Sikker browsing

Browsere er en av de primære måtene dine medarbeidere dere samhandler med internettet på og er derfor et viktig mål for kriminelle. Det er viktig å:

- Holde **browseren** oppdatert med den nyeste versjonen.
- Ikke opprette forbindelse til websteder når du mottar en **browseradvarsel** .
- Kun installere nødvendige og godkjente browser **plug-ins** eller **tilføyelser.**

Passord

Passord er frontlinjen for beskyttelse av personlige systemer og kontoer. Der bør du og dine medarbeidere:

- Bruge forskjellige og komplekse **passord** på forskjellige kontoer og nettsteder.
- Aldri bruke deres jobbrelaterte **brukeropplysninger** til private formål.
- Skifte **passord** regelmessig.
- Aldri dele **passord** med noen, ikke engang ledere eller kolleger.
- Aktivere **multi-factor authentication (MFA)**, hvis det understøttes.

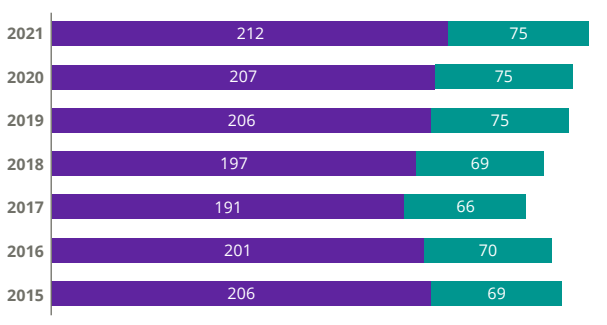
Derfor er sikkerhetsbrudd alvorlige for din forretning

Brudd på datasikkerheten er ikke et flyktig og forbigående problem. Ifølge IBM steg de gjennomsnittlige kostnadene ved sikkerhetsbrudd i Skandinavia i 2021 med 6,37 % til 2,67 millioner US Dollars. Det er ikke bare dyrt, det er også tidskrevende. I gjennomsnitt tok det hele 287 dager å oppdage og få styr på sikkerhetsbruddet.

Gennemsnitlige omkostninger ved sikkerhedsbrud i Skandinavien er steget

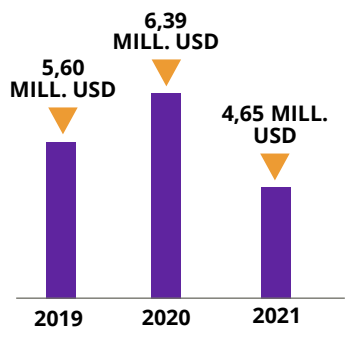
Kilde: IBM & Ponemon Institute

Gjennomsnittlig antall dager for å identifisere og begrense et sikkerhetsbrudd



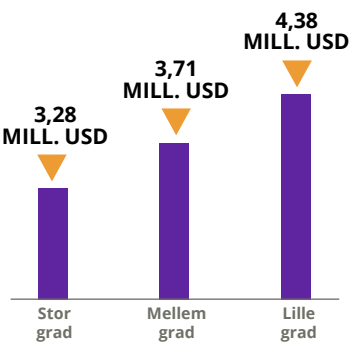
Kilde: IBM & Ponemon Institute

Gjennomsnittlige samlede kostnader for et sikkerhetsbrudd globalt i energi-industrien



Kilde: IBM & Ponemon Institute

Gjennomsnittlige samlede kostnader for et sikkerhetsbrudd etter graden av "Zero Trust"-implementering



Kilde: IBM & Ponemon Institute

Forbered deg på et angrep med DXCs ransomware-forsvarsguide

Følg denne sjekklisten for å sikre systemer og data mot ransomware »

Få ekspertkunnskap om Zero Trust fra Microsoft

Klikk på ikonet og lær mer om Zero Trust, de seks forsvarsområdene, og hvordan Microsoft-produkter kan hjelpe din organisasjon med å begrense risiko »

Hold deg oppdatert med DXC Security Threat Intelligence Report

Beskytt din virksomhet. Abonner på DXCs månedlige rapport om de siste truslene, cyberkriminalitet og nasjonalstatsaktiviteter »

DXCs tilnærming til din virksomhets sikkerhet

IDENTIFISER:
- Fastslå risikobildet og trusselsbildet som er relevant for din virksomhet.
- Sørg for, at retningslinjer og kontroller er på plass for å minske risiko og trusler.

BESKYTT:
- Etabler beskyttelse (firewalls), dybde-forsvar, identitets- og tilgangsstyring og lignende.

OPPDAG:
- Installer anti-malware.
- Registrer (prøv) inntrengeren.
- Konsolider logg til Security Information and Event Management i henhold til risiko- og trusselbildet.

REAGÉR:
- Sett i gang etablerte prosesser for å reagere på situasjonen.
- Bruk eksisterende verktøy og ressurser.

GJENOPPRETT
- Sett i gang Disaster Recovery-prosesser.
- Gjenopprett servere og data der det er mulig, bruk ekspertkonsulenter til å rense systemer.

DXC Technology Norge
Hoffsveien 4
0275 Oslo
Norge
T +47 21634000

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-076N. Mars 2022