Detaljhandel er ett av favoritt-målene for nettkriminelle

Forhandlere som forvalter en økende mengde data på riktig måte får både effektivitetsgevinster og større kunnskap om kundene sine. Samtidig har ransomware og andre typer angrep på IT-systemer blitt et stadig mer vanlig og kostbart fenomen. Når sikkerheten er dårlig, cyberangrepet er et faktum, kundens data er i fare eller butikkens kasseapparater ikke fungerer, undergraves den gode kundeopplevelsen. Her får du innsikt i truslene og hvordan du kan beskytte din detaljhandel.

Hva er de største truslene innen detaljhandel?

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, Malware & Phishing

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 innebærer at svindlere sender e-poster som etterligner e-poster fra legitime avsendere. Hvis mottakeren klikker på den skadelige lenken eller vedlegget i e-posten, kan angriperen stjele informasjon eller installere skadelig programvare for å forårsake ytterligere skade.

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

Skimming & POS-attacker

Kredittkortdata er hard valuta for nettkriminelle, kortsvindel er derfor en stor trussel i detaljhandelen. **Skimming** er en vanlig metode og innebærer at bakmennene setter en kode inn i e-handelsløsningen din. Dette kan gjøres ved å true sikkerheten til en pålitelig ekstern tredjepart, hvis kode er legitimt inkludert i løsningen, for eksempel i en ekstern database, chatbot eller annonseleverandør.

POS-attacker er en form for kredittkortbedrageri som retter seg mot fysiske transaksjonsenheter. Nettkriminelle distribuerer skadelig programvare på POS-enheter, f.eks. kortbetalingsautomater i butikken, for å fange data. Deretter kobler de til enheten eksternt for å få tilgang til kortinformasjonen.

Inventory Hoarding & -Grabbing

Inventory hoarding er når programvareroboter retter seg mot nettbutikker og legger varer i handlekurven uten å fullføre kjøpet. Dette gjør produktene utilgjengelige for ekte kunder og hindrer virksomheten i å selge. Ved **inventory grabbing** er effekten den samme, med tillegg til at intensjonen for de nettkriminelle er å selge varene til en høyere pris.

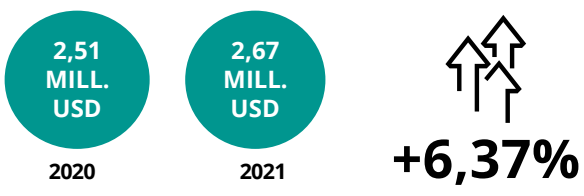
Social Engineering

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

Derfor er sikkerhetsbrudd alvorlige for din forretning

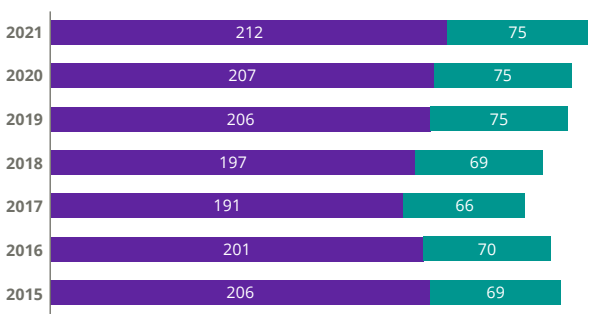
Brudd på datasikkerheten er ikke et flyktig og forbigående problem. Ifølge IBM steg de gjennomsnittlige kostnadene ved sikkerhetsbrudd i Skandinavia i 2021 med 6,37 % til 2,67 millioner US Dollars. Det er ikke bare dyrt, det er også tidskrevende. I gjennomsnitt tok det hele 287 dager å oppdage og få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

Gjennomsnittlige omkostninger ved sikkerhetsbrudd i Skandinavia har økt:



Kilde: IBM & Ponemon Institute

Gjennomsnittlig antall dager for å identifisere og begrense et sikkerhetsbrudd:



Kilde: IBM & Ponemon Institute

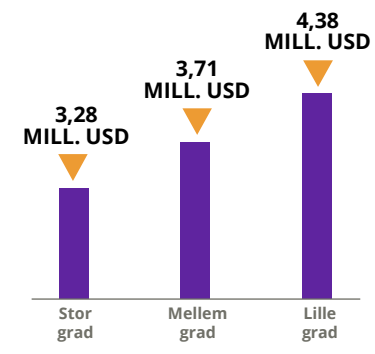
Hvordan blir forhandlere angrepet?

41% av alle nettangrep utføres av kriminelle bruker phishing for tilgang

E-posthacking, servertilgang, datatyveri og innsamling av betalingsdata er de **vanligste** typene cyberangrep i detaljhandelen.

Kilde: Gjengitt med tillatelse fra IBM Corporation © 2022

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



Kilde: IBM & Ponemon Institute

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.

Passord

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

- Bruke ulike 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.

Zero Trust sikkerhetsmodell

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

Minimer risikoen

Som forhandler i dag må du ta de potensielle truslene på alvor og beskytte virksomheten din og kundene dine ved å:

- **Krypter** all sensitiv data
- Utfør regelmessig **sikkerhetskopiering** av data
- Bruk **beskyttelse** mot POS-malware
- Følg med på den **digitale utviklingen**

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.

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. »

Forbered deg på et angrep med DXC sin ransomware-forsvarsguide

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

Hold deg oppdatert med DXC Security Threat Intelligence Report

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

DXC sin tilnærming til din virksomhets sikkerhet

IDENTIFISER:
- Fastslå risikobildet og trusselsbildet som er relevant for din virksomhet.
- Sørg for,at politikker 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-077N. August 2022