Detailhandlen er et af de cyber-kriminelles foretrukne mål

Detailhandlere, der korrekt administrerer en stigende mængde data, opnår både effektivitetsgevinster og større viden om deres kunder. Samtidig er ransomware og andre former for angreb på it-systemer blevet et stadig mere almindeligt og omkostningsfuldt fænomen. Når sikkerheden er dårlig, cyberangrebet er en kendsgerning og kundernes data er i fare eller butikkernes kasseapparater ikke virker, undermineres den gode kundeoplevelse. Her får du indsigt i truslerne, og hvordan du beskytter din detailforretning.

Hvad er de største trusler inden for detailhandlen?

Fremmedord og fagjargon har altid været en integreret del af IT, og sikkerhedsområdet er ingen undtagelse. Her forklares nogle af de vigtigste trusler, og hvorfor de er afgørende at forholde sig til.

Hackerangreb

Når kriminelle grupper får uautoriseret adgang til virksomheders IT-systemer i et "**hackerangreb**", er det i stand til at lamme hele organisationer og påvirke forsyningssikkerheden. Uanset om hackerne blot har økonomiske interesser eller repræsenterer fjendtlige stater, har uønsket adgang til data og systemer store konsekvenser.

Ransomware, Malware & Phishing

Ransomware er et stykke software, som kriminelle bruger til at låse adgangen til data på det inficerede system, så de kan afpresse virksomheder til at betale løsepenge til gengæld for at få adgangen tilbage.

Malware betyder malicious (ondsindet) software og dækker fx over computervira, keyloggers, trojanske heste og spyware, der alle på forskellig vis gør skadelige eller uønskede ting på de ramte computere

Phishing involverer at kriminelle sender e-mails, der efterligner e-mails fra legitime afsendere. Hvis modtageren klikker på det ondsindede link eller den vedhæftede fil i e-mailen, kan angriberen stjæle oplysninger eller installere malware for at forårsage yderligere skade.

Ved **spear phishing** er bestemte personer målrettet og får en personliggjort email, som offeret er mere tilbøjelig til at falde for.

Skimming & POS-angreb

Kreditkortdata er hård valuta for cyberkriminelle, hvorfor kortsvindel er en stor trussel imod detailhandlen.

Skimming er en udbredt metode og går ud på, at de kriminelle indsætter kode i din e-handelsløsning. Det kan gøres ved at kompromittere sikkerheden hos en betroet ekstern tredjepart, hvis kode er lovligt inkluderet i løsningen, såsom en ekstern database, chatbot eller annonceudbyder.

POS-angreb er en form for kreditkortsvindel, der retter sig mod fysiske transaktionsenheder. Cyberkriminelle distribuerer malware på POS-enheder, f.eks. kortbetalingsautomater i butikker, til at fange data. Så opretter de fjernforbindelse til enheden for at få adgang til kortoplysningerne.

Inventory Hoarding & Grabbing

Inventory hoarding er, når softwarebots målrettes mod onlinebutikker og tilføjer varer til indkøbskurven uden at gennemføre købet. Dette gør produkterne utilgængelige for rigtige kunder og forhindrer virksomheden i at sælge. Ved **inventory grabbing** er effekten den samme, med den tilføjelse, at de cyberkriminelles hensigt er at sælge varerne til en højere pris.

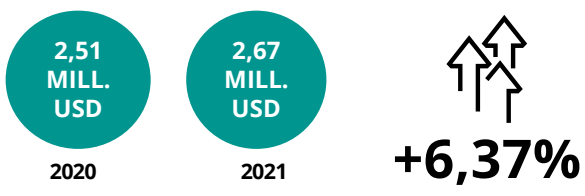
Social Engineering

Social Engineering er betegnelsen for angreb, hvor kriminelle skaber tillid hos medarbejdere og manipulerer dem til at lave sikkerhedsfejl eller at give følsomme oplysninger væk.

Derfor er sikkerhedsbrud alvorlige for din forretning

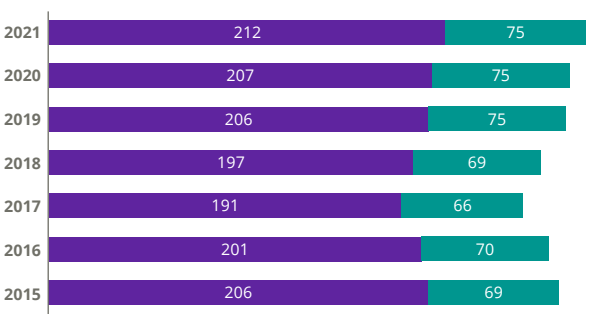
Brud på datasikkerheden er ikke et flygtigt og forbigående problem. Ifølge IBM steg de gennemsnitlige omkostninger ved sikkerhedsbrud i Skandinavien i 2021 med 6,37 % til 2,67 millioner US Dollars. Det er ikke bare dyrt, det er også tidskrævende. I gennemsnit tog det hele 287 dage at opdage og få styr på sikkerhedsbruddet.

Gennemsnitlige omkostninger ved sikkerhedsbrud i Skandinavien er steget:



Kilde: IBM & Ponemon Institute

Gennemsnitlig antal dage om at identificere og begrænse et sikkerhedsbrud:



Kilde: IBM & Ponemon Institute

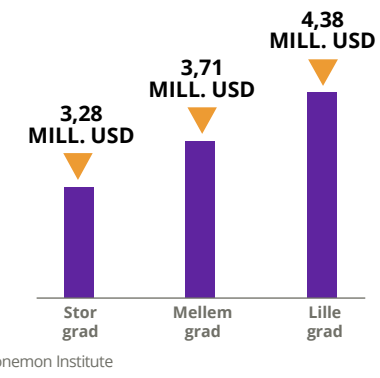
Sådan angribes detailhandelsvirksomheder

41% af alle cyberangreb udføres af kriminelle, der bruger phishing for at få adgang.

E-mail-indtrængen, serveradgang, datatyveri og indsamling af betalingsoplysninger er de mest **almindelige** typer cyberangreb i detailhandlen.

Kilde: Genoptrykt med tilladelse fra IBM Corporation © 2022

Gennemsnitlige samlede omkostninger for et sikkerhedsbrud efter graden af "Zero Trust"-implementering:



Kilde: IBM & Ponemon Institute

Datasikkerhedskultur og forebyggelse

Dine data er dit største aktiv, og teknologi alene kan ikke beskytte dig mod alle angreb. Med veldefinerede processer og politikker, som understøtter og skaber en stærk sikkerhedskultur, kan dine medarbejdere være det første og bedste forsvar mod angreb.

Adgangskoder

Adgangskoder er frontlinjen for beskyttelse af personlige systemer og konti. Der skal du og dine medarbejdere:

- Bruge forskellige og komplekse **adgangskoder** på forskellige konti og websteder
- Aldrig bruge jeres arbejdsrelaterede **brugeroplysninger** til private gøremål
- Skifte **adgangskoder** regelmæssigt
- Aldrig dele **adgangskoder** med nogen, ikke engang ledere eller kolleger
- Aktivere **multi-factor authentication (MFA)**, hvis det understøttes.

Zero Trust sikkerhedsmodel

Der findes et utal af indgange til virksomhedens systemer, såsom computere, tablets, og sensorer. En **Zero Trust** tilgang er baseret på, at alle adgangspunkter udgør en risiko og den ydre sikkerhed kan være kompromitteret. Der skal enhver adgang verificeres og autentificeres hver eneste gang.

Minimér risici

Som forhandler i dag skal du tage de potentielle trusler alvorligt og beskytte din virksomhed og dine kunder ved at:

- **Kryptere** alle følsomme data
- Udføre regelmæssig **sikkerhedskopiering** af data
- Bruge **beskyttelse** mod POS-malware
- Følge med i den **digitale udvikling**

Sikker browsing

Browsere er en af de primære måder, dine medarbejdere interagerer med internettet på og er derfor et vigtigt mål for kriminelle. Det er vigtigt at:

- Holde **browseren** opdateret med den nyeste version
- Ikke oprette forbindelse til websteder, når du modtager en **browseradvarsel**
- Kun installere nødvendige og godkendte **browser plug-ins** eller tilføjelser.

Få ekspertviden om Zero Trust fra Microsoft

Klik på ikonet og lær mere om Zero Trust, de seks forsvarsområder, og hvordan Microsoft-produkter kan hjælpe din organisation med at begrænse risici. »

Forbered dig på et angreb med DXC's ransomware-forsvarsguide

Følg denne tjekliste for at sikre systemer og data mod ransomware. »

Hold dig opdateret med DXC Security Threat Intelligence Report

Beskyt din virksomhed. Abonner på DXC's månedlige rapport om de seneste trusler, cyberkriminalitet og nationalstatsaktiviteter. »

DXC's tilgang til din virksomheds sikkerhed

IDENTIFICER:
- Fastslå risikobilledet og trusselsbilledet, der er relevant for din virksomhed.
- Sørg for, at politikker og kontroller er på plads for at mindske risici og trusler.

BESKYT:
- Etabler beskyttelse (firewalls), dybdeforsvar, identitets- og adgangsstyring og lignende.

OPDAG:
- Installer anti-malware.
- Registrer (forsøg på) indtrængen.
- Konsolider log til Security Information and Event Management i henhold til risiko- og trusselsbilledet.

REAGÉR:
- Sæt gang i etablerede processer for at reagere på situationen.
- Gør brug af allerede eksisterende værktøjer og ressourcer.

GENDAN:
- Sæt gang i Disaster Recovery-processer.
- Gendan servere og data, hvor det er muligt, brug ekspertkonsulenter til at rense systemer.

DXC Technology Danmark
Retortvej 8
2500 Valby
Danmark
T +45 8874 4100

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-077D. August 2022