Detaljhandeln är ett av de cyberkriminellas favoritmål

Detaljhandlare som på rätt sätt hanterar en ökande mängd data får både effektivitetsvinster och större kunskap om sina kunder. Samtidigt har ransomware och andra typer av angrepp på IT-system blivit en allt vanligare och kostsammare företeelse. När säkerheten är dålig, cyberattacken är ett faktum och kundernas data är på vift eller butikernas kassor inte fungerar, skjuts den goda kundupplevelsen i sank. Här får du insikt i hoten och hur du skyddar din detaljhandel.

Vilka är de största hoten inom retail?

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

Hackerangrepp

När kriminella grupper får obehörig tillgång till företags IT-system i ett "**hackerangrepp**" kan det förlama hela organisationer och påverka säkerheten. Oavsett om hackarna enbart har ekonomiska intressen eller representerar fientliga stater, får oönskad tillgång till data och system stora konsekvenser.

Ransomware, Malware & Phishing

Ransomware är en mjukvara som kriminella använder för att låsa data på infekterade system. Därefter utpressar de drabbade 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, vilka alla på olika sätt gör skadliga eller oönskade saker på de drabbade datorerna.

Phishing innebär att skurkar skickar e-post som efterliknar mejl från legitima avsändare. Om mottagaren klickar på den skadliga länken eller bilagan i mejlet kan angriparen stjäla information eller installera skadlig programvara för att orsaka ytterligare skada.

Vid **spear phishing** är specifika personer utvalda att få individuellt anpassad e-post som den drabbade är mer benägen att falla för.

Skimming & POS-attacker

Kreditkortsdata är hårdvaluta för cyberbrottslingar och därför är kortbedrägerier ett stort hot inom detaljhandeln. **Skimming** är en vanlig metod och innebär att bovarna insticker kod i din e-handelslösning. Det kan göras genom att säkerheten hos en pålitlig extern tredje part vars kod är legitimt inkluderad i lösningen, såsom en extern databas, chatbot eller annonsleverantör, äventyras.

POS-attacker är en form av kreditkortsbedrägeri som riktar sig mot fysiska transaktionsenheter. Cyberbrottslingar distribuerar malware på POS-enheter, t.ex. kortbetalningsmaskiner i butik, för att fånga upp data. Sedan ansluter de till enheten på distans för att komma över kortinformationen.

Inventory Hoarding & -Grabbing

Inventory hoarding är när mjukvarurobotar riktar in sig på onlinebutiker och lägger varor i kundvagnen utan att slutföra köpet. Detta gör produkterna otillgängliga för riktiga kunder och hindrar verksamheten att sälja. Vid **inventory grabbing** är effekten den samma, med tillägget att avsikten för de cyberkriminella är att sälja varorna till högre pris.

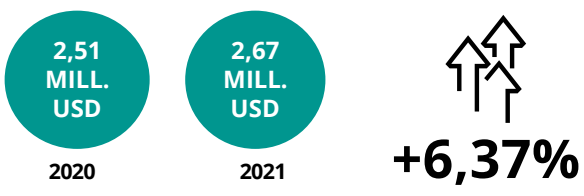
Social Engineering

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

Därför är säkerhetsintrång allvarliga för din verksamhet

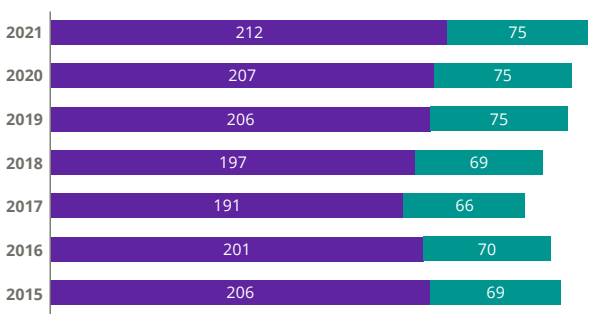
Datasäkerhetsbrott är inte ett flyktigt och övergående problem. Enligt IBM ökade den genomsnittliga kostnaden för säkerhetsintrång i Skandinavien 2021 med 6,37 % till 2,67 miljoner USD. Det är inte bara dyrt, utan också tidskrävande. I genomsnitt tog det hela 287 dagar att upptäcka och få ordning på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

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

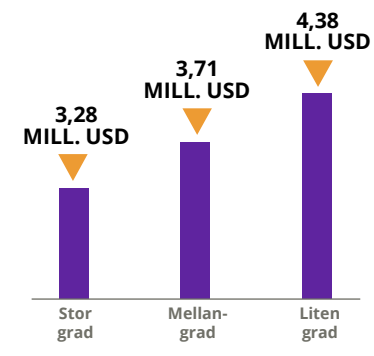
Hur attackeras företag inom detaljhandeln?

41% av alla cyberattacker utförs genom att kriminella tillämpar phising för att få åtkomst.

E-postintrång, serveråtkomst, datastöld och insamling av betalningssuppgifter är de **vanligaste** typerna av cyberattacker inom retail.

Källa: Återtryckt med tillåtelse från IBM Corporation © 2022

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



Källa: IBM & Ponemon Institute

Datasäkerhetskultur och prevention

Dina data är din största tillgång, och tekniken ensam kan inte skydda dig mot 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.

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.

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.

Minimera riskerna

Som återförsäljare i dag måste du ta de potentiella hoten på allvar och skydda din verksamhet och dina kunder genom att:

- **Kryptera** alla känsliga data
- Utföra regelbundna **säkerhetskopieringar** av data
- Använda **skydd** mot POS-malware
- Hänga med i den **digitala utvecklingen**

Säkert surfande

Webbläsare är ett av de primära verktygen som dina medarbetare använder för att komma ut på nätet 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.

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. »

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

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

Håll dig uppdaterad med DXC Security Threat Intelligence Report

Skydda din verksamhet genom att prenumerera på DXC:s månatliga rapport om de senaste 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-077S. Augusti 2022