DELL Technologies

Man-in-the-middle (MITM): Stärk cybersäkerheten och motståndskraften med Dell Technologies

Det ökande hotet från Man-in-the-Middle-attacker (MITM)

MITM-attacker (Man-in-the-Middle) är fortfarande en av de mest sofistikerade och farliga cybersäkerhetsutmaningarna. Dessa attacker, där illvilliga aktörer fångar upp och ändrar privat kommunikation utan att upptäckas, riktar sig mot företag av alla storlekar i olika branscher. Från e-handelsplattformar till finansinstitut – inget företag är skyddat mot denna risk. MITM-attacker banar ofta väg för datastöld, ekonomiska bedrägerier och skador på anseende. Det gör dem till en otäck motståndare i ett alltmer digitalt landskap.

Dell Technologies förstår vilka unika utmaningar som företag står inför när de måste skydda sig mot dessa avancerade hot. Genom att leverera innovativa, skalbara säkerhetslösningar gör Dell det möjligt för företag att neutralisera MITM-hot, skydda tillgångar och upprätthålla affärsintegriteten.

Vad är en Man-in-the-Middle-attack (MITM)?

En Man-in-the-Middle-attack (MITM) inträffar när en cyberbrottsling i hemlighet fångar upp kommunikation mellan två parter, till exempel mellan en anställd och en företagsserver eller en kund och en företagswebbplats. Angriparens mål kan variera – från att stjäla känsliga data till att manipulera kommunikation i skadliga syften. Men resultatet är detsamma: tappat förtroende och säkerhetsbrott.

Vanliga MITM-tekniker

Några av de vanligaste metoderna som angripare använder är följande:

Wi-Fi-avlyssning: Cyberbrottslingar utnyttjar osäkra eller komprometterade offentliga Wi-Fi-nätverk för att fånga upp kommunikation.

DNS-spoofing: Angripare omdirigerar användare till falska webbplatser genom att manipulera DNS-poster och utan att tveka samla in känslig information.

Sessionskapning: Genom att utnyttja aktiva sessionsinloggningsuppgifter får angripare obehörig åtkomst till privata konton.

SSL-strippning: Den här tekniken nedgraderar säkra HTTPS-anslutningar till sårbara HTTP-anslutningar och exponerar känslig information.

Den här anpassningsförmågan gör MITM-attacker särskilt illvilliga, eftersom de utnyttjar vardagliga affärstransaktioner och interaktioner som verkar legitima på ytan.

Påverkan på företag

Dominoeffekterna av en MITM-attack sträcker sig långt bortom den omedelbara incidenten. Några av de mest skadliga konsekvenserna är:

Förlorade intäkter

Stulna inloggningsuppgifter och komprometterade åtgärder leder ofta till ekonomisk börda som sträcker sig från direkta förluster till återställningskostnader.

Operativa problem

Tiden och resurserna som läggs på att lösa en attack minskar kritiska affärsfunktioner, något som i sin tur påverkar produktiviteten och tillväxten.

Urholkning av förtroende

Kundernas förtroende kan snabbt försvinna när deras personliga information kompromitteras, vilket leder till långsiktiga skador på företagets anseende.

Regelmässiga konsekvenser

Företag som är verksamma i branscher med strikta efterlevnadskrav kan drabbas av böter eller sanktioner efter en dataläcka.

Verkliga exempel

Ett oroande fall handlade om ett globalt detaljhandelsföretag vars okrypterade betalningsplattform online föll offer för en SSL-strippningsattack. Angriparen snappade upp kreditkortsinformation från kunder i kassan. Genom snabb detektering och strategiska säkerhetsåtgärder, inklusive Dells slutpunktsskyddsverktyg, kunde företaget stoppa attacken och mildra långsiktiga skador. Det här scenariot belyser de omedelbara riskerna och det kritiska behovet av skiktade försvar.

35,9 miljard

kända dataintrång globalt

Källa: Maj 2024: PureWL Report

Bekämpa MITM-attacker med Dell Technologies

Dell Technologies utrustar företag med omfattande och framtidssäkra verktyg som utformats för att förhindra MITM-risker innan de orsakar skada.

Säkra slutpunkter med Dell Trusted Devices

MITM-hot har ofta sitt ursprung i slutpunkter, något som gör dem till en skyddsprioritet. Dells Trusted Devices bäddar in dem i den senaste säkerheten, direkt i hårdvaran. Till exempel:

- **Dell SafeBIOS** säkerställer att systemets integritet skyddas mot obehörig manipulation i startsekvensen.
- **SafeID** lägger till ytterligare ett skyddslager genom att skydda användarautentiseringsdata. Det skapar en fästning mot stöld av inloggningsuppgifter.
- **Dell SafeData** tillhandahåller heltäckande kryptering som skyddar känslig information inuti och utanför företagets brandväggar, vilket gör att avlästa data blir omöjliga att tyda.

Dessa funktioner har distribuerats i globala företag för att upprätthålla förtroende för slutpunktssystem. Ett multinationellt tillverkningsföretag använde till exempel Dell Trusted Devices för att skydda sina distansmedarbetare mot riktade MITM-attacker på bärbara företagsdatorer, något som säkerställer säkra anslutningar även under högriskresor.

Avancerad detektering med CrowdStrike

Det är avgörande att upptäcka och reagera på MITM-hot i realtid. CrowdStrike är integrerat med Dells ekosystem och utnyttjar artificiell intelligens och beteendeanalys för att övervaka och neutralisera misstänkt aktivitet. Kontinuerlig övervakning säkerställer skydd i hybridmiljöer, där hot ofta döljs. Genom att proaktivt identifiera avvikelser kan företag eliminera potentiella MITM-försök innan skador uppstår.

Med hjälp av avancerad detektering kunde ett finansbolag till exempel upptäcka och mildra ett intrång på sin kundriktade portal. Plattformens AI identifierade ovanlig nätverksaktivitet som tyder på SSL-borttagning, vilket möjliggör omedelbara åtgärder.

Förstärkt dataskydd med Dell PowerProtect

Även företag med avancerade försvar kan drabbas av intrång. Det är där Dell PowerProtect kommer in. Med funktioner som oföränderlighet och lagring med luftgap skyddar mjukvaran mot att kritiska affärsdata ändras, förstörs eller nås under en attack. PowerProtect Cyber Recovery Vault erbjuder ytterligare säkerhet genom att isolera konfidentiella data från primära nätverk. Det säkerställer att känslig information förblir intakt och kan återställas även i värsta fall.

Den här tekniken var avgörande för en hälso- och sjukvårdsorganisation som stod inför en DNS-spoofingattack. Genom att utnyttja PowerProtect oföränderliga säkerhetskopierings- och återställningsvalv återställde organisationen driften snabbt utan dataförlust.

Rapid Response och Recovery Services

Dells dataskyddstjänster kompletterar sin teknik genom att erbjuda snabb återställning av experter i händelse av intrång. Dessa lösningar minskar driftavbrott och minimerar driftstörningar, från fjärrdataåterställning till incidentsvar. När varje sekund räknas säkerställer en betrodd partner att företag kan återhämta sig tryggt.

Avancerad nätverkssäkerhet och mikrosegmentering med Dell PowerSwitch Networking och SmartFabric OS

Stärker försvaret mot nolldagsattacker genom att leverera avancerad nätverkssegmentering, strikta åtkomstkontroller och trafikanalys i realtid i hela infrastrukturen.

Stärk säkerheten med en heltäckande lösning i flera lager

För att kunna bekämpa MITM-attacker till fullo måste företag implementera en mångsidig säkerhetsstrategi. Dell Technologies understryker dessa åtgärder:

- **Anta nollförtroendeprinciper:** Verifiera alla aktiviteter och användaråtkomst vid varje punkt, oavsett om de har sitt ursprung i eller utanför företagets nätverk.
- **Använd avancerad kryptering:** Heltäckande kryptering för all kommunikation säkerställer att avlästa data blir oanvändbara för angripare.
- **Implementera MFA (flerfaktorautentisering):** MFA lägger till autentiseringslager i system, något som avsevärt minskar sårbarheter för obehörig åtkomst.
- **Utbilda personalen:** Skapa en mer vaksam arbetsstyrka genom att lyfta fram risker som nätfiske, misstänkt användning av Wi-Fi och okontrollerade länkar.
- **Regelbundna systemtester:** Frekventa intrångstester och uppdateringar hjälper till att identifiera sårbarheter och säkerställa att försvaret förblir aktuellt.

Dells omfattande säkerhetserbjudanden i kombination med dessa metoder skapar ett enastående och anpassningsbart försvar mot föränderliga hot.

Värdet av strategiska partnerskap

Dell Technologies samarbete med ledande cybersäkerhetsföretag, som CrowdStrike och Secureworks, gör det här till ett ännu bättre alternativ. Genom att integrera expertis i dessa partnerskap kan Dell hantera alla möjliga attackvektorer. CrowdStrike förbättrar till exempel slutpunktsskyddet genom att berika Dells plattformar med hotinformation, medan Secureworks ger värdefulla insikter om föränderliga risker. Det här säkerställer kontinuerlig förberedelse och anpassning.

Dell Technologies-fördelen

Väljer du Dell Technologies samarbetar du med en betrodd ledare inom cybersäkerhetsinnovation. Dells heltäckande lösningar gör det möjligt för företag att ligga steget före angripare, oavsett om det gäller slutpunktsskydd, dataåterställning eller samarbetspartnerskap.

Skydda ditt företag, upprätthåll kundernas förtroende och framtidssäkra din verksamhet med Dells omfattande MITM-lösningar. Kontakta oss idag för att skapa en motståndskraftig och säker framtid för ditt företag.

Genom att samarbeta med Dell Technologies tar du en aktiv ställning mot cyberhot, skapar ett bestående förtroende hos kunder och intressenter och säkerställer driftframgång i en alltmer osäker digital värld. En säkrare morgondag börjar med Dell.

Lär dig att hantera några av dagens främsta cybersäkerhetsutmaningar på **Dell.com/SecuritySolutions**

Mer information om Dells lösningar

Kontakta en av Dell Technologies experter

Visa fler resurser

Delta i samtalet med #HashTag

DELL Technologies