DELL Technologies

Man-in-the-Middle (MITM): Cyberbeveiliging en veerkracht versterken met Dell Technologies

De toenemende dreiging van Man-in-the-Middle-aanvallen (MITM)

Man-in-the-Middle-aanvallen (MITM) blijven een van de meest geavanceerde en gevaarlijke uitdagingen op het gebied van cyberbeveiliging. Deze aanvallen, waarbij kwaadwillenden privécommunicatie onderscheppen en wijzigen zonder detectie, richten zich op bedrijven van elke omvang in verschillende sectoren. Geen enkele organisatie is immuun voor dit risico, van e-commerceplatforms tot financiële instellingen. MITM-aanvallen maken vaak de weg vrij voor datadiefstal, financiële fraude en reputatieschade, waardoor ze een enorme tegenstander zijn in een steeds digitaler landschap.

Dell Technologies begrijpt de unieke uitdagingen waarmee bedrijven worden geconfronteerd bij bescherming van zichzelf tegen deze geavanceerde bedreigingen. Door innovatieve, schaalbare beveiligingsoplossingen te leveren, stelt Dell organisaties in staat om MITM-bedreigingen te neutraliseren, assets te beschermen en de bedrijfsintegriteit te behouden.

Wat is een Man-in-the-Middle-aanval (MITM)?

Een Man-in-the-Middle-aanval (MITM) vindt plaats wanneer een cybercrimineel in het geheim communicatie tussen twee partijen onderschept, zoals tussen een werknemer en een bedrijfsserver of een klant en een bedrijfswebsite. Het doel van de aanvaller kan variëren, van het stelen van gevoelige data tot het manipuleren van communicatie voor schadelijke doeleinden, maar het resultaat is hetzelfde: een inbreuk op vertrouwen en beveiliging.

Veelvoorkomende MITM-technieken

Enkele van de meest voorkomende methoden die aanvallers gebruiken, zijn de volgende:

Wi-Fi afluisteren: Cybercriminelen maken gebruik van onbeveiligde of gecompromitteerde openbare Wi-Fi-netwerken om communicatie te onderscheppen.

DNS-spoofing: Aanvallers manipuleren DNS-records om gebruikers om te leiden naar frauduleuze websites, waardoor ze onbewust gevoelige informatie kunnen verzamelen.

Sessie kapen: Door actieve sessiereferenties te stelen, krijgen aanvallers ongeautoriseerde toegang tot privéaccounts.

SSL-stripping: Deze techniek degradeert veilige HTTPS-verbindingen naar kwetsbare HTTP-verbindingen, waardoor gevoelige informatie wordt blootgesteld.

Dit aanpassingsvermogen maakt MITM-aanvallen bijzonder schadelijk, omdat ze gebruikmaken van dagelijkse zakelijke transacties en interacties die op het eerste gezicht legitiem lijken.

De impact op bedrijven

Het rimpeleffect van een MITM-aanval reiken veel verder dan het directe incident. Enkele van de meest schadelijke gevolgen zijn:

Omzetverlies

Gestolen inloggegevens en gecompromitteerde activiteiten leiden vaak tot financiële lasten die zich uitstrekken van directe verliezen tot herstelkosten.

Operationele tegenslagen

De tijd en middelen die worden besteed aan het oplossen van een aanval doen afbreuk aan kritieke bedrijfsfuncties, wat van invloed is op de productiviteit en groei.

Verlies van vertrouwen

Het vertrouwen van klanten kan snel afnemen bij inbreuk op hun persoonlijke gegevens, wat leidt tot reputatieschade op de lange termijn.

Gevolgen op het gebied van regelgeving

Bedrijven die actief zijn in sectoren met strikte nalevingsvereisten kunnen boetes of sancties krijgen na een datalek.

Praktijkvoorbeeld

Een alarmerend voorbeeld betreft een wereldwijd retailbedrijf waarvan het onversleutelde online betalingsplatform het slachtoffer werd van een aanval met SSL-stripping. De aanvaller heeft creditcardgegevens van klanten onderschept tijdens het afrekenen. Door snelle detectie en strategische beveiligingsmaatregelen, waaronder de tools voor eindpuntbescherming van Dell, kon het bedrijf de aanval stoppen en schade op de lange termijn beperken. Dit scenario belicht de directe risico's en de dringende behoefte aan gelaagde bescherming.

35,9 miljard

bekende datalekken wereldwijd

Bron: mei 2024: PureWL Report

MITM-aanvallen bestrijden met Dell Technologies

Dell Technologies voorziet organisaties van uitgebreide, vooruitstrevende tools die zijn ontworpen om MITM-risico's te voorkomen voordat ze schade veroorzaken.

Veilige eindpunten met Dell Trusted Devices

Bij eindpunten ontstaan vaak MITM-bedreigingen, waardoor ze een prioriteit zijn in de bescherming. De vertrouwde apparaten van Dell integreren geavanceerde beveiliging rechtstreeks in de hardware. Bijvoorbeeld:

- **Dell SafeBIOS** zorgt ervoor dat de systeemintegriteit wordt beschermd tegen ongeoorloofde sabotage in de opstartvolgorde.
- **SafeID** voegt een extra beschermingslaag toe door data voor gebruikersidentificatie te beveiligen, waardoor een fort wordt gecreëerd tegen diefstal van inloggegevens.
- **Dell SafeData** biedt end-to-endversleuteling die gevoelige informatie binnen en buiten de bedrijfsfirewalls beschermt, waardoor onderschepte data onleesbaar is.

Deze functies zijn geïmplementeerd in wereldwijde ondernemingen om vertrouwen in eindpuntsystemen te creëren. Een multinationaal productiebedrijf gebruikte bijvoorbeeld Dell Trusted Devices om zijn externe werknemers te beschermen tegen gerichte MITM-aanvallen op zakelijke laptops, waardoor veilige verbindingen worden gegarandeerd, zelfs tijdens risicovolle reisscenario's.

Geavanceerde detectie met CrowdStrike

MITM-dreigingen in realtime detecteren en erop reageren is cruciaal. CrowdStrike, geïntegreerd met het ecosysteem van Dell, maakt gebruik van kunstmatige intelligentie en gedragsanalyses om verdachte activiteiten te bewaken en te neutraliseren. Continu toezicht zorgt voor bescherming in hybride omgevingen, waar bedreigingen zich vaak verbergen. Door afwijkingen proactief te identificeren, kunnen bedrijven potentiële MITM-aanvallen elimineren voordat er schade optreedt.

Met behulp van geavanceerde detectie heeft een financiële instelling bijvoorbeeld een inbraak in het klantenportaal gedetecteerd en beperkt. De AI van het platform heeft ongebruikelijke netwerkactiviteit gedetecteerd die wijst op SSL-stripping, waardoor onmiddellijk kon worden ingegrepen.

Versterkte databescherming met Dell PowerProtect

Zelfs organisaties met geavanceerde verdediging kunnen te maken krijgen met inbreuken. Hier maakt Dell PowerProtect het verschil. Met mogelijkheden zoals onveranderlijkheid en air-gapped storage worden essentiële bedrijfsdata beschermd tegen wijzigingen, vernietiging of toegang tijdens een aanval. De PowerProtect Cyber Recovery-kluis biedt extra beveiliging door vertrouwelijke data van primaire netwerken te isoleren, zodat gevoelige informatie zelfs in het ergste geval intact en herstelbaar blijft.

Deze technologie was van cruciaal belang voor een organisatie in de gezondheidszorg die te maken had met een DNS-spoofing-aanval. Door gebruik te maken van de onveranderlijke back-ups en herstelkluis van PowerProtect kon de organisatie snel de activiteiten herstellen zonder dataverlies.

Services voor snelle respons en herstel

De services voor databescherming van Dell vullen de technologieën aan door snel, door experts geleid herstel te bieden in het geval van een inbreuk. Van dataherstel op afstand tot incidentrespons, deze oplossingen beperken downtime en minimaliseren operationele onderbrekingen. Wanneer elke seconde telt, zorgt een vertrouwde partner ervoor dat organisaties vol vertrouwen kunnen herstellen.

Geavanceerde netwerkbeveiliging en microsegmentatie met Dell PowerSwitch Networking en SmartFabric OS

Versterkt de bescherming tegen zero-day-aanvallen door geavanceerde netwerksegmentatie, strikte toegangscontroles en realtime verkeersanalyse te leveren in uw hele infrastructuur.

Beveiliging versterken met een meerlaagse aanpak

Om MITM-aanvallen volledig te bestrijden, moeten organisaties een veelzijdige beveiligingsstrategie implementeren. Dell Technologies legt de nadruk op deze praktische stappen:

- **Pas Zero Trust-principes toe:** Verifieer alle activiteiten en gebruikerstoegang op elk punt, ongeacht of ze van binnen of buiten het bedrijfsnetwerk komen.
- **Gebruik geavanceerde versleuteling:** End-to-endversleuteling voor alle communicatie zorgt ervoor dat onderschepte data onbruikbaar worden voor aanvallers.
- **Implementeer meervoudige verificatie (MFA):** MFA voegt verificatielagen toe aan systemen, waardoor kwetsbaarheden voor onbevoegde toegang aanzienlijk worden verminderd.
- **Informeer werknemers:** Creëer een waakzamer personeelsbestand door risico's te markeren zoals phishing, verdacht Wi-Fi-gebruik en niet-geverifieerde koppelingen.
- **Regelmatige systeemtests:** Frequente tests en updates voor indringingsrisico helpen beveiligingslekken te identificeren en ervoor te zorgen dat de beveiliging up-to-date blijft.

Het holistische beveiligingsaanbod van Dell, in combinatie met deze praktijken, zorgt voor een formidabele, aanpasbare verdediging tegen nieuwe bedreigingen.

De waarde van strategische partnerschappen

De samenwerking van Dell Technologies met toonaangevende cyberbeveiligingsbedrijven, zoals CrowdStrike en Secureworks, versterkt het aanbod verder. Door expertise in deze partnerschappen te integreren, kan Dell elke mogelijke aanvalsvector aanpakken. CrowdStrike verbetert bijvoorbeeld de eindpuntbescherming door de platforms van Dell te verrijken met informatie over bedreigingen, terwijl Secureworks uitvoerbare inzichten biedt in veranderende risico's, waardoor continue voorbereiding en aanpassing worden gegarandeerd.

Het voordeel van Dell Technologies

Kiezen voor Dell Technologies betekent samenwerken met een vertrouwde leider op het gebied van innovatie in cyberbeveiliging. Of het nu gaat om eindpuntbescherming, dataherstel of samenwerkingsverbanden, de end-to-end oplossingen van Dell stellen organisaties in staat om aanvallers voor te blijven.

Beveilig uw bedrijf, behoud het vertrouwen van klanten en maak uw activiteiten toekomstbestendig met de uitgebreide MITM-oplossingen van Dell. Neem vandaag nog contact met ons op om te beginnen met het opbouwen van een veerkrachtige, veilige toekomst voor uw bedrijf.

Door samen te werken met Dell Technologies, neemt u een actieve houding aan tegen cyberdreigingen, creëert u blijvend vertrouwen met klanten en belanghebbenden en zorgt u voor operationeel succes in een steeds onveiligere digitale wereld. Een veiligere toekomst begint bij Dell.

Ontdek hoe u enkele van de grootste uitdagingen op het gebied van cyberbeveiliging van dit moment kunt aanpakken op **Dell.com/SecuritySolutions**

Meer informatie over Dell oplossingen

Neem contact op met een Dell Technologies expert

Bekijk meer informatiebronnen

Neem deel aan het gesprek via #HashTag

DELL Technologies