DELL Technologies

Man-in-the-middle (MITM) : renforcer la cybersécurité et la résilience avec Dell Technologies

L'essor des attaques man-in-the-middle (MITM)

Les attaques man-in-the-middle (MITM) ont toujours été l'un des défis de cybersécurité les plus sophistiqués et les plus dangereux. Ces attaques, qui consistent à intercepter et à altérer des communications privées en toute discrétion, ciblent les entreprises de toutes tailles et de tous secteurs. Des plateformes d'e-commerce aux institutions financières, aucune organisation n'est épargnée. Les attaques MITM entraînent généralement le vol de données, des fraudes financières et une atteinte à la réputation de l'entreprise touchée, ce qui en fait un adversaire redoutable dans un paysage toujours plus numérique.

Dell Technologies est conscient des défis uniques que rencontrent les entreprises lorsqu'elles tentent de se protéger contre ces menaces avancées. En proposant des solutions de sécurité innovantes et évolutives, Dell permet aux entreprises de neutraliser les menaces MITM, de protéger leurs actifs et de préserver l'intégrité de l'entreprise.

Qu'est-ce qu'une attaque man-in-the-middle (MITM) ?

Une attaque man-in-the-middle (MITM) se produit lorsqu'un cybercriminel intercepte secrètement les communications entre deux parties, par exemple entre un employé et un serveur d'entreprise ou entre un client et un site Web. L'objectif du pirate n'est pas toujours le même : s'il cherche parfois à voler des données sensibles, il peut préférer manipuler les communications à des fins malveillantes. Le résultat, lui, ne change pas : c'est un abus de confiance et une violation de la sécurité.

Les techniques MITM les plus courantes

Les pirates utilisent certaines méthodes plus que d'autres, dont voici une liste non exhaustive :

Écoute Wi-Fi : les cybercriminels exploitent les réseaux Wi-Fi publics non sécurisés ou compromis pour intercepter les communications.

Usurpation DNS : les pirates renvoient les utilisateurs vers des sites Web frauduleux en falsifiant les enregistrements DNS et récupèrent des informations sensibles ni vu ni connu.

Détournement de session : en récupérant les informations d'identification des session actives, les pirates accèdent à des comptes privés sans autorisation.

SSL stripping : cette technique rétrograde les connexions HTTPS sécurisées vers des connexions HTTP vulnérables, exposant ainsi les informations sensibles.

Cette polyvalence rend les attaques MITM particulièrement néfastes, car elles exploitent des transactions et des interactions professionnelles quotidiennes qui passent pour légitimes à première vue.

Impact sur les entreprises

Les répercussions d'une attaque MITM vont bien au-delà de l'incident qui survient sur le moment. Certaines conséquences peuvent aller extrêmement loin :

Pertes de revenus

Le vol d'informations d'identification et la compromission des opérations entraînent souvent de lourdes conséquences financières, qu'il s'agisse de pertes directes ou de coûts de récupération.

Retards opérationnels

Le temps et les ressources affectés à la résolution d'une attaque nuisent aux fonctions stratégiques de l'entreprise, faisant inévitablement chuter la productivité et la croissance.

Perte de confiance

La confiance des clients peut rapidement s'envoler lorsque leurs informations personnelles sont piratées, entraînant des conséquences réputationnelles à long terme.

Retombées juridiques

Les entreprises qui travaillent dans des secteurs soumis à des exigences de conformité strictes peuvent être passibles d'amendes ou de sanctions suite à une violation de données.

Exemple concret

Une entreprise de vente au détail internationale a été impliquée dans une affaire de ce type. Au moment des faits, sa plateforme de paiement en ligne non chiffrée venait de subir une attaque par SSL stripping. Le pirate a intercepté les informations de carte de crédit des clients au moment du paiement. En détectant rapidement le problème et en mettant en place des mesures de sécurité stratégiques, notamment les outils de protection des points de terminaison de Dell, l'entreprise a pu mettre un terme à l'attaque et limiter les dégâts à long terme. Ce scénario met en évidence les risques immédiats et l'impératif absolu d'instaurer des défenses à plusieurs niveaux.

35,9 milliard

de violations de données enregistrées dans le monde entier

Source : Mai 2024, rapport PureWL

Lutter contre les attaques MITM avec Dell Technologies

Dell Technologies met entre les mains des entreprises des outils complets et avant-gardistes conçus pour déjouer les risques MITM avant qu'ils ne causent préjudice.

Sécurisez les points de terminaison avec Dell Trusted Devices

Les points de terminaison sont souvent le point de départ des menaces MITM. Les protéger doit donc être votre priorité. Les Trusted Devices de Dell intègrent une sécurité de pointe directement au matériel. Par exemple :

- **Dell SafeBIOS** garantit la protection de l'intégrité du système face aux altérations non autorisées dans la séquence de démarrage.
- **SafeID** ajoute une autre couche de protection en sécurisant les données d'authentification des utilisateurs, créant ainsi une forteresse contre le vol d'identifiants.
- **Dell SafeData** fournit un chiffrement de bout en bout qui protège les informations sensibles à l'intérieur et à l'extérieur des pare-feu de l'entreprise, rendant ainsi les données interceptées illisibles.

Ces fonctionnalités ont été déployées dans des entreprises internationales pour renforcer la confiance dans les systèmes de points de terminaison. Par exemple, une société de fabrication industrielle multinationale a utilisé Dell Trusted Devices pour protéger ses télétravailleurs contre les attaques MITM ciblant les ordinateurs portables de l'entreprise, garantissant ainsi des connexions sécurisées même lors de déplacements à haut risque.

Détection avancée avec CrowdStrike

Détecter les menaces MITM et y répondre en temps réel est essentiel. CrowdStrike est intégré à l'écosystème Dell et exploite l'intelligence artificielle et l'analytique comportementale pour surveiller et neutraliser les activités suspectes. La surveillance continue garantit la protection des environnements hybrides, où les menaces se cachent parfois. En détectant proactivement les anomalies, les entreprises peuvent limiter les éventuelles tentatives de MITM avant qu'elles n'en pâtissent réellement.

Par exemple, grâce à la détection avancée, une institution financière a réussi à détecter et à atténuer une intrusion sur son portail client. L'IA de la plateforme a identifié une activité réseau inhabituelle révélatrice d'un SSL stripping, ce qui a permis d'y remédier immédiatement.

Protection renforcée des données avec Dell PowerProtect

Même les entreprises disposant de défenses avancées sont parfois confrontées à des failles de sécurité. C'est là que Dell PowerProtect intervient. Grâce à des fonctionnalités telles que l'immuabilité et le stockage isolé, il protège les données stratégiques de l'entreprise contre toute altération, toute destruction ou tout accès lors d'une attaque. Le coffre-fort PowerProtect Cyber Recovery offre une sécurité supplémentaire en isolant les données confidentielles des réseaux principaux, garantissant ainsi que même dans le pire des scénarios, les informations sensibles restent intactes et récupérables.

Cette technologie a joué un rôle déterminant pour un établissement de santé faisant l'objet d'une attaque par usurpation DNS. En tirant parti des sauvegardes immuables et du coffre-fort de récupération de PowerProtect, l'entreprise a repris ses opérations rapidement sans perte de données.

Services de récupération et de réponse rapide

Les services de protection des données de Dell complètent ses technologies en proposant une récupération rapide et assurée par des experts en cas de violation de sécurité. De la récupération des données à distance à la réponse aux incidents, ces solutions atténuent les temps d'arrêt et limitent les interruptions opérationnelles. Lorsque chaque seconde compte, un partenaire de confiance permet aux entreprises de reprendre leurs activités en toute confiance.

Sécurité réseau avancée et microsegmentation avec Dell PowerSwitch Networking et SmartFabric OS

Protège contre les attaques zero-day en fournissant une segmentation avancée du réseau, des contrôles d'accès stricts et une analyse du trafic en temps réel sur l'ensemble de votre infrastructure.

Renforcer la sécurité grâce à une approche sur plusieurs niveaux

Pour lutter efficacement contre les attaques MITM, les entreprises doivent mettre en œuvre une stratégie de sécurité à plusieurs facettes. Dell Technologies met l'accent sur ces actions :

- **Adoption des principes Zero-Trust :** vérifiez toutes les activités et l'accès des utilisateurs à chaque point d'entrée, qu'ils proviennent ou non du réseau de l'entreprise.
- **Chiffrement avancé :** le chiffrement de bout en bout de toutes les communications garantit que les données interceptées ne sont pas exploitables par les pirates.
- **Mise en œuvre de l'authentification multifacteur (MFA) :** l'authentification multifacteur ajoute plusieurs niveaux d'authentification aux systèmes, ce qui réduit considérablement les vulnérabilités liées aux accès non autorisés.
- **Sensibilisation des employés :** renforcez la vigilance des employés en soulignant les risques auxquels ils sont confrontés : tentatives de phishing, utilisation suspecte du Wi-Fi et liens non vérifiés.
- **Tests réguliers du système :** des tests de pénétration et des mises à jour fréquents permettent d'identifier les vulnérabilités et de garantir que les défenses restent à jour.

Associées à ces pratiques, les offres de sécurité globales de Dell créent une protection redoutable, qui s'adapte aux menaces en constante évolution.

Valeur des partenariats stratégiques

La collaboration de Dell Technologies avec des entreprises de cybersécurité leaders, telles que CrowdStrike et Secureworks, renforce la valeur de ses offres. L'intégration de son expertise à ces partenariats permet à Dell de mettre à mal tous les vecteurs d'attaque possibles. CrowdStrike, par exemple, améliore la protection des points de terminaison en enrichissant les plateformes Dell avec des renseignements sur les menaces, tandis que Secureworks fournit des informations exploitables sur l'évolution des risques, garantissant une préparation et une adaptation continues.

Le Dell Technologies Advantage

En choisissant Dell Technologies, vous vous associez à un leader de confiance de l'innovation en matière de cybersécurité. Que ce soit à travers la protection des points de terminaison, la récupération des données ou des partenariats collaboratifs, les solutions de bout en bout de Dell permettent aux entreprises de garder une longueur d'avance sur les pirates.

Sécurisez votre entreprise, préservez la confiance de vos clients et pérennisez vos opérations grâce aux solutions MITM complètes de Dell. Contactez-nous dès aujourd'hui pour commencer à forger un avenir solide et sûr pour votre entreprise.

En collaborant avec Dell Technologies, vous adoptez une position proactive face aux cybermenaces, vous instaurez un climat de confiance durable auprès de vos clients et de vos parties prenantes, et vous assurez le succès de vos opérations dans un monde numérique de plus en plus précaire. L'avenir en toute sécurité commence avec Dell.

Découvrez comment relever certains des défis actuels majeurs en matière de cybersécurité sur **Dell.com/SecuritySolutions**

En savoir plus sur les solutions Dell

Contacter un expert Dell Technologies

Consulter d'autres ressources

Prenez part à la discussion avec #hashtag

DELL Technologies