DELL Technologies

Fortalecimiento de la ciberseguridad y la resiliencia frente a ataques MITM con Dell Technologies

Aumento de las amenazas de ataques MITM

Los ataques MITM (man-in-the-middle, "de intermediario") siguen siendo uno de los retos de ciberseguridad más sofisticados y peligrosos. En ellos, agentes maliciosos interceptan y modifican sin ser detectados comunicaciones privadas de empresas de todos los tamaños y sectores. Desde las plataformas de comercio electrónico hasta las instituciones financieras, ninguna organización está inmune ante este riesgo. Los ataques MITM suelen allanar el camino para el robo de datos, el fraude financiero y el daño a la reputación, lo que los convierte en un gran adversario en un panorama cada vez más digital.

Dell Technologies es consciente de las dificultades únicas a las que se enfrentan las empresas para protegerse contra estas amenazas avanzadas. Gracias a sus soluciones de seguridad innovadoras y ampliables, Dell permite a las organizaciones neutralizar las amenazas de ataques MITM, proteger los activos y mantener la integridad empresarial.

¿Qué es un ataque MITM?

Los ataques MITM (man-in-the-middle, "de intermediario") se producen cuando un ciberdelincuente intercepta, sin ser detectado, las comunicaciones entre dos partes, como entre un empleado y un servidor corporativo o un cliente y un sitio web empresarial. Los objetivos del atacante pueden ser varios, desde robar datos sensibles hasta manipular las comunicaciones con fines malintencionados, pero el resultado es siempre el mismo: una vulneración de la confianza y la seguridad.

Técnicas comunes de los ataques MITM

Estos son algunos de los métodos más frecuentes entre los atacantes:

Interceptación a través de Wi-Fi: los ciberdelincuentes aprovechan las redes Wi-Fi públicas no seguras o comprometidas para interceptar las comunicaciones.

Suplantación de DNS: los atacantes redirigen a los usuarios a sitios web fraudulentos manipulando los registros de DNS para recopilar información confidencial sin sospecha.

Secuestro de sesión: cuando consiguen las credenciales de una sesión activa, los atacantes tienen acceso no autorizado a cuentas privadas.

SSL stripping: esta técnica hace que las conexiones HTTPS seguras sean vulnerables, por lo que se expone información confidencial.

Esta adaptabilidad hace que los ataques MITM sean especialmente malintencionados, ya que aprovechan transacciones e interacciones empresariales cotidianas que a simple vista parecen legítimas.

El impacto en las empresas

El efecto dominó de un ataque MITM se extiende mucho más allá del incidente inmediato. Algunas de las consecuencias más perjudiciales son las siguientes:

Pérdida de ingresos

El robo de credenciales y las operaciones comprometidas suelen tener consecuencias financieras que van desde las pérdidas directas hasta los costes de recuperación.

Contratiempos operativos

El tiempo y los recursos dedicados a resolver un ataque desvían la atención a funciones empresariales críticas, y esto afecta a la productividad y el crecimiento.

Daño a la confianza

La confianza de los clientes puede mermarse rápidamente cuando se vulnera su información personal, lo que provoca daños a largo plazo en la reputación.

Consecuencias normativas

Las empresas que operan en sectores con estrictos requisitos normativos pueden enfrentarse a multas o sanciones tras una vulneración de datos.

Ejemplo real

Una empresa minorista global vivió una situación alarmante cuando su plataforma de pago en línea sin cifrar fue víctima de un ataque con SSL stripping. El atacante interceptó la información de la tarjeta de crédito de los clientes durante el pago. Gracias a la rápida detección y las medidas de seguridad estratégicas, incluidas las herramientas de protección de puntos finales de Dell, la empresa pudo detener el ataque y mitigar los daños a largo plazo. Este caso destaca los riesgos inmediatos y la necesidad crítica de defensas en capas.

35,9 mil millones

de vulneraciones de datos conocidas en todo el mundo

Fuente: informe de PureWl de mayo de 2024

Combatir los ataques MITM con Dell Technologies

Dell Technologies proporciona a las organizaciones herramientas integrales y avanzadas diseñadas para frustrar las amenazas de ataques MITM antes de que causen daños.

Protección de puntos finales con Dell Trusted Devices

Las amenazas de ataques MITM suelen originarse en los puntos finales, por lo que su protección es prioritaria. Los dispositivos de confianza de Dell integran seguridad de vanguardia directamente en el hardware. Por ejemplo:

- **Dell SafeBIOS** garantiza que la integridad del sistema esté protegida contra manipulaciones no autorizadas en la secuencia de arranque.
- **SafeID** añade otra capa de protección que asegura los datos de autenticación de usuarios para evitar el robo de credenciales.
- **Dell SafeData** proporciona un cifrado integral que protege la información confidencial dentro y fuera de los firewalls corporativos, de manera que los datos interceptados sean ilegibles.

Estas funciones se han implementado en empresas globales para garantizar la confianza en los sistemas de punto final. Por ejemplo, una empresa multinacional de fabricación utilizó Dell Trusted Devices para proteger los portátiles corporativos de la plantilla en remoto frente a ataques MITM específicos y garantizar así conexiones seguras incluso en situaciones de viaje de alto riesgo.

Detección avanzada con CrowdStrike

Detectar y responder a las amenazas de ataques MITM en tiempo real es clave. CrowdStrike, un software integrado con el ecosistema de Dell, aprovecha la inteligencia artificial y el análisis del comportamiento para supervisar y neutralizar actividades sospechosas. La supervisión continua garantiza la protección en entornos híbridos, donde suelen esconderse las amenazas. Gracias a la identificación proactiva de anomalías, las empresas pueden neutralizar posibles intentos de ataques MITM antes de que se produzcan daños.

Por ejemplo, mediante la detección avanzada, una institución financiera detectó y mitigó con éxito una intrusión en su portal para clientes. La IA de la plataforma identificó una actividad de red inusual que indicaba SSL stripping, lo que permitió actuar de inmediato.

Protección de datos reforzada con Dell PowerProtect

Incluso las organizaciones con defensas avanzadas pueden sufrir vulneraciones. Aquí es donde entra en juego Dell PowerProtect. Con características como la inmutabilidad y el almacenamiento con sistema de cámara de aire, protege los datos empresariales críticos para que no puedan ser alterados, destruidos o accedidos durante un ataque. PowerProtect Cyber Recovery Vault aumenta la seguridad al aislar los datos confidenciales de las redes principales para que, incluso en el peor de los casos, la información confidencial se mantenga intacta y se pueda recuperar.

Esta tecnología fue fundamental para una organización sanitaria que sufrió un ataque con suplantación de DNS. Gracias al vault de recuperación y las copias de seguridad inmutables de PowerProtect, la organización restauró las operaciones rápidamente sin perder datos.

Servicios rápidos de respuesta y recuperación

Los servicios de protección de datos de Dell complementan sus tecnologías al permitir una recuperación rápida y dirigida por expertos en caso de vulneración. Desde la recuperación remota de datos hasta la respuesta ante incidentes, estas soluciones reducen el tiempo de inactividad y minimizan las interrupciones operativas. Cuando cada segundo cuenta, tener un socio de confianza garantiza que las organizaciones puedan recuperarse con confianza.

Seguridad de red avanzada y microsegmentación con Dell PowerSwitch Networking y SmartFabric OS

La segmentación de red avanzada, los controles de acceso estrictos y los análisis de tráfico en tiempo real en toda la infraestructura fortalecen las defensas contra ataques de día cero.

Refuerzo de la seguridad con un enfoque multicapa

Para combatir completamente los ataques MITM, las organizaciones deben implementar una estrategia de seguridad multidimensional. Dell Technologies hace hincapié en estas medidas:

- **Adopte principios de confianza cero:** verifique las actividades y el acceso de los usuarios en cada punto, independientemente de si suceden dentro o fuera de la red corporativa.
- **Utilice el cifrado avanzado:** el cifrado integral de todas las comunicaciones garantiza que los datos interceptados sean inutilizables para los atacantes.
- **Implemente la autenticación multifactor (MFA):** la MFA añade capas de autenticación a los sistemas, lo que reduce significativamente las vulnerabilidades de acceso no autorizado.
- **Forme al personal:** destaque riesgos como los esquemas de phishing, el uso sospechoso de Wi-Fi y los enlaces no verificados entre su plantilla para que esté más alerta.
- **Haga pruebas periódicas del sistema:** las pruebas de penetración y las actualizaciones frecuentes ayudan a identificar las vulnerabilidades y a garantizar que las defensas están al día.

Las ofertas integrales de seguridad de Dell, combinadas con estas prácticas, crean una defensa magnífica y adaptable contra las amenazas en constante evolución.

El valor de las colaboraciones estratégicas

La colaboración de Dell Technologies con las principales empresas de ciberseguridad, como CrowdStrike y Secureworks, refuerza aún más sus ofertas. La integración de la experiencia en estas colaboraciones permite a Dell abordar todos los posibles vectores de ataque. CrowdStrike, por ejemplo, mejora la protección de puntos finales al dotar a las plataformas de Dell de inteligencia contra amenazas, mientras que Secureworks ofrece información procesable sobre los riesgos en evolución, lo que garantiza una preparación y una adaptación continuas.

La ventaja de Dell Technologies

Elegir Dell Technologies significa trabajar con un líder fiable en la innovación en ciberseguridad. Ya sea a través de la protección de puntos finales, la recuperación de datos o las colaboraciones con partners, las soluciones integrales de Dell permiten a las organizaciones adelantarse a los atacantes.

Proteja su empresa, cuide la confianza de sus clientes y prepare sus operaciones para el futuro con las soluciones integrales de ataques MITM de Dell. Póngase en contacto con nosotros hoy mismo para empezar a forjar un futuro seguro y resiliente para su empresa.

Al asociarse con Dell Technologies, adopta una postura activa contra las ciberamenazas, crea una confianza duradera en clientes y partes interesadas, y garantiza el éxito operativo en un mundo digital cada vez más inseguro. Un futuro más seguro empieza con Dell.

Descubra cómo afrontar algunos de los principales retos de ciberseguridad actuales en **Dell.com/SecuritySolutions**

Más información acerca de las soluciones Dell

Póngase en contacto con un experto de Dell Technologies

Consulte más recursos.

Únase a la conversación con #HashTag.

DELL Technologies