DELL Technologies

Man-in-the-Middle (MITM): Stärkung von Cybersicherheit und Resilienz mit Dell Technologies

Die wachsende Bedrohung durch MITM-Angriffe (Man-in-the-Middle)

MITM-Angriffe (Man-in-the-Middle) sind nach wie vor eine der ausgefeiltesten und gefährlichsten Herausforderungen der Cybersicherheit. Diese Angriffe, bei denen böswillige AkteurInnen private Kommunikation unbemerkt abfangen und ändern, zielen auf Unternehmen jeder Größenordnung in allen Branchen ab. Von E-Commerce-Plattformen bis hin zu Finanzinstituten – kein Unternehmen ist gegen dieses Risiko immun. MITM-Angriffe ebnen oft den Weg für Datendiebstahl, Finanzbetrug und Reputationsschäden, sodass sie ein gewaltiger Gegner in einer zunehmend digitalen Landschaft sind.

Dell Technologies versteht die einzigartigen Herausforderungen, mit denen Unternehmen beim Schutz vor diesen fortschrittlichen Bedrohungen konfrontiert sind. Durch die Bereitstellung innovativer, skalierbarer Sicherheitslösungen ermöglicht Dell es Unternehmen, MITM-Bedrohungen zu neutralisieren, Ressourcen zu schützen und die geschäftliche Integrität aufrechtzuerhalten.

Was ist ein MITM-Angriff (Man-in-the-Middle)?

Ein MITM-Angriff (Man-in-the-Middle) findet statt, wenn Cyberkriminelle heimlich die Kommunikation zwischen zwei Parteien abfangen, z. B. zwischen MitarbeiterInnen und einem Unternehmensserver oder Kunden und einer Unternehmenswebsite. Das Ziel der AngreiferInnen kann variieren – vom Diebstahl sensibler Daten bis hin zur Manipulation der Kommunikation für bösartige Zwecke. Das Ergebnis ist jedoch stets dasselbe: ein Verstoß gegen Vertrauen und Sicherheit.

Gängige MITM-Techniken

AngreiferInnen nutzen die folgenden häufigsten Methoden:

Abhören des Wi-Fi-Netzwerks: Cyberkriminelle nutzen ungesicherte oder kompromittierte öffentliche Wi-Fi-Netzwerke aus, um die Kommunikation abzufangen.

DNS-Spoofing: AngreiferInnen leiten NutzerInnen auf betrügerische Websites um, indem sie DNS-Einträge manipulieren und so unbemerkt vertrauliche Informationen sammeln.

Sitzungs-Hijacking: Durch das Abfangen aktiver Sitzungsanmeldedaten verschaffen sich AngreiferInnen unbefugten Zugang zu privaten Konten.

SSL-Stripping: Bei dieser Technik werden sichere HTTPS-Verbindungen zu angreifbaren HTTP-Verbindungen herabgestuft, wodurch vertrauliche Informationen preisgegeben werden.

Diese Anpassungsfähigkeit macht MITM-Angriffe besonders heimtückisch, da sie alltägliche Geschäftsvorgänge und -interaktionen ausnutzen, die auf den ersten Blick legitim erscheinen.

Die Auswirkungen auf Unternehmen

Die Dominoeffekte eines MITM-Angriffs reichen weit über den unmittelbaren Incident hinaus. Zu den schädlichsten Folgen zählen:

Umsatzeinbußen

Gestohlene Zugangsdaten und kompromittierte Betriebsabläufe können zu erheblichen finanziellen Belastungen führen, die sich von direkten Verlusten bis hin zu den Kosten für die Recovery der Systeme erstrecken.

Betriebliche Rückschläge

Der Zeit- und Ressourcenaufwand für die Behebung eines Angriffs beeinträchtigt kritische Geschäftsfunktionen und wirkt sich auf Produktivität und Wachstum aus.

Aushöhlung des Vertrauens

Das Kundenvertrauen kann schnell schwinden, wenn ihre personenbezogenen Daten verletzt werden, was zu langfristigen Rufschädigungen führt.

Regulatorische Auswirkungen

Unternehmen, die in Branchen mit strengen Complianceanforderungen tätig sind, können aufgrund einer Datenschutzverletzung mit Geldstrafen oder Sanktionen belegt werden.

Praxisbeispiel

Ein alarmierender Fall betraf ein globales Einzelhandelsunternehmen, dessen unverschlüsselte Onlinezahlungsplattform einem SSL-Stripping-Angriff zum Opfer fiel. AngreiferInnen haben Kreditkarteninformationen von Kunden während der Kaufabwicklung abgefangen. Durch schnelle Erkennung und strategische Sicherheitsmaßnahmen, einschließlich der Endpunktschutztools von Dell, konnte das Unternehmen den Angriff stoppen und den langfristigen Schaden begrenzen. In diesem Szenario werden die unmittelbaren Risiken und die kritische Notwendigkeit mehrschichtiger Abwehrmaßnahmen betont.

35,9 Mrd.

bekannte Datenschutzverletzungen weltweit

Quelle: PureWL Report, Mai 2024

Bekämpfung von MITM-Angriffen mit Dell Technologies

Dell Technologies stattet Unternehmen mit umfassenden, zukunftsorientierten Tools aus, die MITM-Risiken abwehren, bevor sie Schaden anrichten.

Sichere Endpunkte dank Dell Trusted-Devices

Endpunkte sind oft der Ursprung von MITM-Bedrohungen, weshalb sie besonders geschützt werden müssen. Bei Dell Trusted-Devices ist hochmoderne Sicherheit direkt in die Hardware integriert. Beispiel:

- **Dell SafeBIOS** sorgt dafür, dass die Systemintegrität vor unbefugten Manipulationen in der Startreihenfolge geschützt wird.
- **SafeID** fügt eine weitere Schutzebene hinzu, indem Nutzerauthentifizierungsdaten gesichert werden und so eine Festung gegen den Diebstahl von Zugangsdaten geschaffen wird.
- **Dell SafeData** bietet End-to-End-Verschlüsselung, die vertrauliche Informationen innerhalb und außerhalb von Unternehmensfirewalls schützt und abgefangene Daten unlesbar macht.

Diese Funktionen wurden in globalen Unternehmen eingesetzt, um das Vertrauen in Endpunktsysteme zu stärken. So hat beispielsweise ein multinationales Fertigungsunternehmen Dell Trusted-Devices eingesetzt, um seine AußendienstmitarbeiterInnen vor gezielten MITM-Angriffen auf Firmenlaptops zu schützen und selbst bei risikoreichen Reisen sichere Verbindungen zu gewährleisten.

Erweiterte Erkennung mit CrowdStrike

Die Erkennung und Reaktion auf MITM-Bedrohungen in Echtzeit ist entscheidend. CrowdStrike-Lösungen sind in das Dell Ökosystem integriert. Sie nutzen künstliche Intelligenz und Verhaltensanalysen, um verdächtige Aktivitäten zu überwachen und zu neutralisieren. Kontinuierliches Monitoring gewährleistet den Schutz in hybriden Umgebungen, in denen sich Bedrohungen oft verbergen. Durch die proaktive Erkennung von Anomalien können Unternehmen potenzielle MITM-Versuche eliminieren, bevor Schaden entsteht.

Beispielsweise konnte ein Finanzinstitut mithilfe der erweiterten Erkennung einen Angriff auf sein kundenorientiertes Portal erfolgreich erkennen und abwehren. Die KI der Plattform identifizierte ungewöhnliche Netzwerkaktivitäten, die auf SSL-Stripping hindeuteten, und ermöglichte eine sofortige Korrektur.

Verstärkte Data Protection mit Dell PowerProtect

Selbst in Unternehmen mit erweiterten Abwehrmaßnahmen kann es zu Sicherheitsverletzungen kommen. Hier kommt Dell PowerProtect ins Spiel. Mit Funktionen wie Unveränderlichkeit und Air-Gapped-Storage schützt die Lösung geschäftskritische Daten davor, dass sie bei einem Angriff verändert, zerstört oder zugänglich gemacht werden. Der PowerProtect Cyber Recovery Vault bietet zusätzliche Sicherheit, indem er vertrauliche Daten von den primären Netzwerken isoliert und so sicherstellt, dass selbst im schlimmsten Fall sensible Informationen intakt und wiederherstellbar bleiben.

Diese Technologie war entscheidend für ein Gesundheitsunternehmen, das einen DNS-Spoofing-Angriff bewältigen musste. Durch den Einsatz der unveränderlichen Backups und des Recovery Vault von PowerProtect konnte das Unternehmen den Betrieb schnell und ohne Datenverlust wiederherstellen.

Schnelle Reaktions- und Wiederherstellungsservices

Die Data-Protection-Services von Dell ergänzen die Technologien von Dell, indem sie eine schnelle, von ExpertInnen geleitete Recovery im Falle einer Sicherheitsverletzung bieten. Von Remote Data Recovery bis hin zu Incident Response reduzieren diese Lösungen Ausfallzeiten und minimieren Betriebsunterbrechungen. Wenn jede Sekunde zählt, sorgt ein vertrauenswürdiger Partner für eine zuverlässige Recovery von Unternehmen.

Erweiterte Netzwerksicherheit und Mikrosegmentierung mit Dell PowerSwitch-Netzwerklösungen und SmartFabric OS

Profitieren Sie von einer verstärkten Abwehr von Zero-Day-Angriffen durch erweiterte Netzwerksegmentierung, strenge Zugriffskontrollen und Echtzeitanalysen des Datenverkehrs in Ihrer gesamten Infrastruktur.

Mehr Sicherheit mit einem mehrschichtigen Ansatz

Um MITM-Angriffe vollständig zu bekämpfen, müssen Unternehmen eine vielseitige Sicherheitsstrategie implementieren. Dell Technologies empfiehlt diese umsetzbaren Schritte:

- **Einführung von Zero-Trust-Prinzipien:** Überprüfen Sie alle Aktivitäten und den Nutzerzugriff an jedem Punkt, unabhängig davon, ob sie innerhalb oder außerhalb des Unternehmensnetzwerks stattfinden.
- **Nutzung einer erweiterten Verschlüsselung:** Die End-to-End-Verschlüsselung für die gesamte Kommunikation sorgt dafür, dass abgefangene Daten für AngreiferInnen unbrauchbar werden.
- **Implementierung der Multi-Faktor-Authentifizierung (MFA):** MFA fügt zusätzliche Authentifizierungsebenen zu den Systemen hinzu und reduziert so die Anfälligkeit für unbefugten Zugriff erheblich.
- **Schulung von MitarbeiterInnen:** Schaffen Sie eine wachsamere Belegschaft, indem Sie auf Risiken wie Phishing, verdächtige Wi-Fi-Nutzung und ungeprüfte Links hinweisen.
- **Regelmäßige Systemtests:** Häufige Penetrationstests und Updates helfen dabei, Sicherheitslücken zu identifizieren und sicherzustellen, dass die Abwehrmaßnahmen auf dem neuesten Stand bleiben.

Die ganzheitlichen Sicherheitsangebote von Dell schaffen in Kombination mit diesen Praktiken eine beeindruckende, anpassbare Abwehr vor sich entwickelnden Bedrohungen.

Der Wert strategischer Partnerschaften

Durch die Zusammenarbeit mit führenden Cybersicherheitsunternehmen wie CrowdStrike und Secureworks stärkt Dell Technologies sein Angebot weiter. Dank der Integration des Fachwissens in diese Partnerschaften kann Dell jeden möglichen Angriffsvektor angehen. CrowdStrike beispielsweise verbessert den Endpunktschutz, indem es die Plattformen von Dell mit Bedrohungsdaten anreichert, während Secureworks verwertbare Erkenntnisse über sich entwickelnde Risiken liefert und so eine kontinuierliche Vorbereitung und Anpassung gewährleistet.

Der Dell Technologies Advantage

Wenn Sie sich für Dell Technologies entscheiden, gehen Sie eine Partnerschaft mit einem zuverlässigen Marktführer im Bereich der Cybersicherheit ein. Ob durch Endpunktschutz, Daten-Recovery oder Kooperationspartnerschaften – mit den End-to-End-Lösungen von Dell bleiben Unternehmen AngreiferInnen einen Schritt voraus zu sein.

Mit den umfassenden MITM-Lösungen von Dell sichern Sie Ihr Unternehmen, halten das Vertrauen Ihrer Kunden aufrecht und sorgen für zukunftssichere Betriebsabläufe. Kontaktieren Sie uns noch heute, um eine ausfallsichere Zukunft für Ihr Unternehmen zu schaffen.

Durch die Partnerschaft mit Dell Technologies setzen Sie sich aktiv gegen Cyberbedrohungen ein, schaffen dauerhaftes Vertrauen bei Kunden und StakeholderInnen und sorgen für betrieblichen Erfolg in einer zunehmend unsicheren digitalen Welt. Eine sicherere Zukunft beginnt mit Dell.

Erfahren Sie unter **Dell.com/SecuritySolutions**, wie Sie einige der größten Herausforderungen von heute im Bereich der Cybersicherheit bewältigen können.

Weitere Informationen zu den Lösungen von Dell

Kontakt zu Dell Technologies ExpertInnen

Weitere Ressourcen anzeigen

Kommen Sie ins Gespräch über #HashTag

DELL Technologies