DELL Technologies

Bösartige Insiderangriffe: Stärkung von Cybersicherheit und Resilienz mit Dell Technologies

Die wachsende Bedrohung durch bösartige Insiderangriffe

Bösartige Insiderangriffe sind zu einer der dringendsten Cybersicherheitsbedrohungen in der heutigen Unternehmenslandschaft geworden. Im Gegensatz zu externen Bedrohungen verfügen böswillige InsiderInnen bereits über ein gewisses Maß an Vertrauen und Zugriff innerhalb eines Unternehmens, wodurch ihre Handlungen besonders schädlich und schwieriger zu erkennen sind. Vom Zugriff auf sensible Daten bis hin zur Sabotage von Systemen können Insiderangriffe kritische Vorgänge beeinträchtigen und schwerwiegende finanzielle und Reputationseinbußen verursachen.

Dell Technologies ist sich der wachsenden Gefahr durch diese Angriffe bewusst und entwickelt innovative, skalierbare Lösungen, mit denen Unternehmen die Risiken durch böswillige InsiderInnen erkennen, verhindern und mindern können. Durch die Kombination modernster Technologie mit fachkundigen Services unterstützt Dell Unternehmen dabei, diesen internen Bedrohungen einen Schritt voraus zu sein.

Was sind bösartige Insiderangriffe?

Ein böswilliger Insiderangriff liegt vor, wenn eine Person innerhalb eines Unternehmens ihren Zugriff missbraucht, um Daten zu kompromittieren, Betriebsabläufe zu stören oder sensible Informationen für persönliche, finanzielle oder wettbewerbsbezogene Zwecke zu extrahieren. Bei dieser Person kann es sich um MitarbeiterInnen, AuftragnehmerInnen, PartnerInnen oder Personen mit legitimem Zugriff auf die Systeme und Netzwerke des Unternehmens handeln.

Wie bösartige Insiderangriffe funktionieren

Böswillige InsiderInnen nutzen ihre vertrauenswürdige Position aus, um herkömmliche Sicherheitsabwehrmaßnahmen zu umgehen. Zu den gängigen Techniken gehören:

1. **Datendiebstahl:** Exfiltration von vertraulichen Kundendaten, geistigem Eigentum oder Finanzunterlagen.
2. **Sabotage:** Vorsätzliche Beschädigung von IT-Systemen, um den Geschäftsbetrieb zu stören oder den Ruf zu schädigen.
3. **Missbrauch von Anmeldedaten:** Verwendung gestohlener oder missbräuchlich verwendeter Anmeldedaten, um Zugriffsrechte zu erweitern oder Scheinkonten zu erstellen.
4. **Zusammenarbeit mit externen AngreiferInnen:** Weitergabe von Zugriffsrechten oder sensiblen Informationen an externe Cyberkriminelle im Austausch gegen finanzielle Vorteile.

Dieser doppelte Vorteil von Vertrauen und Insiderwissen macht bösartige InsiderInnen im Vergleich zu externen AngreiferInnen außergewöhnlich gefährlich.

Auswirkungen auf Unternehmen

Bösartige Insiderangriffe führen zu erheblichen Schäden, die weit über finanzielle Verluste hinausgehen. Mit folgenden Folgen können Unternehmen konfrontiert sein:

Finanzielle Verluste

Der Diebstahl sensibler Informationen, Betrug oder Sabotage führen zu Umsatzverlusten und Wiederherstellungskosten, die sich auf mehrere Millionen belaufen können.

Betriebsunterbrechung

Systemsabotage oder Datenvernichtung können den Betrieb anhalten, was zu Verzögerungen, verpassten Verkaufschancen und reduzierter Produktivität führt.

Reputationsschäden

Eine Verletzung oder ein Angriff durch InsiderInnen untergräbt das Kunden- und Stakeholdervertrauen und beeinträchtigt die Kundenbindung und die Wahrnehmung auf dem Markt.

Nichteinhaltung gesetzlicher Vorschriften

Je nach Branche können Insiderangriffe zu hohen Geldstrafen und Strafen führen, wenn es sich um sensible Daten wie Gesundheits- oder Finanzdaten handelt.

Praxisbeispiel

Im Jahr 2020 löschte ein IT-Auftragnehmer, der für ein großes Finanzinstitut arbeitete, absichtlich wichtige Systemkonfigurationen und verursachte damit einen Netzwerkausfall von über **10 Stunden**. Dieser Sabotageakt führte zu finanziellen Verlusten in **Millionenhöhe**, umfangreichen Wiederherstellungskosten und Reputationsschäden. Solche Vorfälle verdeutlichen die zerstörerische Potenz von Insiderbedrohungen und unterstreichen die Dringlichkeit der Einführung robuster Erkennungs- und Präventionsmaßnahmen.

83 %

der Unternehmen meldeten im vergangenen Jahr mindestens einen Insiderangriff

Quelle: 2024: Report von Cybersecurity Insiders

Geschätzte Kosten

Laut einer Studie des Ponemon Institute aus dem Jahr 2024 belaufen sich die durchschnittlichen Kosten eines Insidervorfalls auf **4,99 Millionen USD** und machen fast **55 %** aller Sicherheitsverletzungen aus. Diese Zahl berücksichtigt die Kosten für die Erkennung, Recovery und Schadensbegrenzung und zeigt, wie wichtig es für Unternehmen ist, in vorbeugende Maßnahmen zum Schutz vor Insiderrisiken zu investieren.

Bekämpfung bösartiger Insiderangriffe mit Dell Technologies

Dell Technologies bietet ein umfassendes Ökosystem an Tools und Services zur Bekämpfung bösartiger Insiderbedrohungen, damit Ihr Unternehmen auf unerwartete Situationen vorbereitet ist.

Sichere Endpunkte dank Dell Trusted-Devices

Endpunkte dienen oft als Einstiegspunkte für Insiderbedrohungen. Dell Trusted-Devices integrieren modernste Sicherheitsfunktionen in die Hardware, um Endpunkte zu stärken und sensible Daten zu schützen.

- **Dell SafeBIOS** sorgt für die Firmwareintegrität und verhindert Versuche, Systemvorgänge auf Hardwareebene zu manipulieren.
- **SafeID** schützt Zugangsdaten und verhindert unbefugten Zugriff und Missbrauch von Zugangsdaten.
- **SafeData** verschlüsselt sensible Daten von Ende zu Ende, sodass abgefangene oder extrahierte Informationen für bösartiger InsiderInnen unlesbar bleiben.

Durch den Einsatz dieser Lösungen können Unternehmen sicherstellen, dass ihre Endpunkte geschützt sind, unabhängig davon, ob die Bedrohung intern oder extern entsteht.

Proaktive Bedrohungserkennung mit CrowdStrike

Die Identifizierung von Insiderbedrohungen erfordert Transparenz und Monitoring des Nutzerverhaltens. Die in die Lösungen von Dell integrierte CrowdStrike-Software nutzt künstliche Intelligenz und Verhaltensanalysen, um Anomalien zu erkennen, die auf Insiderbedrohungen hindeuten.

Beispielsweise werden ungewöhnliche Datenübertragungen außerhalb der Geschäftszeiten oder unbefugter Zugriff auf kritische Bereiche des Netzwerks sofort markiert, was eine schnelle Reaktion ermöglicht. Ein US-amerikanisches Gesundheitsunternehmen nutzte kürzlich die proaktive Bedrohungserkennung, um den Versuch eines Mitarbeiters, Patientendaten zu exfiltrieren, zu identifizieren und zu unterbinden und so eine kostspielige Datenschutzverletzung zu verhindern.

Verbesserte Data Protection mit Dell PowerProtect

Dell PowerProtect bietet eine robuste Verteidigungslinie durch sichere Backups, Air-gapped-Storage und unveränderliche Kopien kritischer Daten. Indem Sie sicherstellen, dass sensible Informationen vor Änderungen oder Löschungen geschützt sind, machen Sie Insiderangriffe, die auf Datenintegrität abzielen, ineffektiv

Ein Beispiel ist ein Fertigungsunternehmen, das mit einem unzufriedenen Mitarbeiter konfrontiert war, der versuchte, Konstruktionsdateien zu sabotieren. Dank des Recovery Vault von Dell PowerProtect konnte das Unternehmen den Betrieb innerhalb weniger Stunden wiederherstellen, wodurch Störungen vermieden und die Business Continuity aufrechterhalten wurden.

Schnelle Incident-Recovery mit Dell Professional Services

Wenn eine Insiderbedrohung zu einem Incident eskaliert, ist eine schnelle Recovery unerlässlich. Die Dell Professional Services, einschließlich Remote Data Recovery und Incident Response, stellen sicher, dass Unternehmen Daten und Systeme schnell wiederherstellen können. Die ExpertInnen von Dell leiten den Prozess, um Ausfallzeiten zu minimieren und Auswirkungen zu mindern.

Dies sind nur einige Beispiele aus dem Dell Portfolio an Lösungen, die bei bösartigen Insiderbedrohungen helfen können.

Erweiterte Netzwerksicherheit und Mikrosegmentierung mit Dell PowerSwitch Networking und SmartFabric OS

Stärkung der Abwehr von Zero-Day-Angriffen durch erweiterte Netzwerksegmentierung, strenge Zugriffskontrollen und Echtzeit-Analysen des Datenverkehrs in Ihrer gesamten Infrastruktur

Die Bedeutung eines mehrschichtigen Sicherheitsansatzes

Eine effektive Abwehr von Insiderrisiken erfordert mehr als nur eine Schutzebene. Durch die Implementierung einer mehrschichtigen Sicherheitsstrategie wird sichergestellt, dass keine Sicherheitslücke zu einem Schwachpunkt wird. Die wichtigsten Schritte:

Wichtige Schritte zur Verbesserung der Verteidigung

- **Zero-Trust-Prinzipien:** Überprüfen Sie kontinuierlich alle Zugriffsanfragen und gehen Sie davon aus, dass keine Entität von Natur aus vertrauenswürdig ist, auch nicht innerhalb des Perimeters.
- **Rollenbasierte Zugriffskontrollen (Role-Based Access Controls, RBAC):** Beschränken Sie den Zugriff Ihrer MitarbeiterInnen auf die Systeme und Daten, die für ihre Aufgaben erforderlich sind.
- **Erweiterte Verschlüsselungslösungen:** Verschlüsseln Sie Daten im Ruhezustand und während der Übertragung, um Datendiebstahl effektiv zu verhindern.
- **Sensibilisierung und Schulung von MitarbeiterInnen:** Führen Sie regelmäßige Programme zur Sensibilisierung für Sicherheitsfragen durch, um eine versehentliche Beteiligung an böswilligen Aktivitäten zu verhindern.
- **Regelmäßige Systemtests:** Führen Sie Penetrationstests und Schwachstellenscans durch, um sicherzustellen, dass die Abwehrmaßnahmen zuverlässig bleiben.

Diese Praktiken, die durch die Lösungen von Dell verstärkt werden, schaffen ein beeindruckendes, ganzheitliches Schutzkonzept gegen böswillige Insider.

Stärkung der Abwehrmaßnahmen durch strategische Partnerschaften

Dell arbeitet mit branchenführenden Cybersicherheitsanbietern zusammen, darunter **CrowdStrike** und **SecureWorks**, um die Sicherheitslösungen weiter zu stärken. CrowdStrike verbessert die Endpunktsicherheit und bietet wertvolle Threat Intelligence zu Kompromittierungsindikatoren, während Secureworks Services für Advanced Threat Detection and Response bereitstellt. Diese Zusammenarbeit stellt sicher, dass die Kunden von Dell von einem Ökosystem integrierter und hochmoderner Technologien profitieren.

Gründe für Dell Technologies für Cybersicherheit

Dell Technologies setzt weiterhin den Goldstandard für mehrschichtige Cybersicherheitslösungen. Unternehmen profitieren von der branchenführenden Expertise, den engen Partnerschaften und der innovativen Produktpalette von Dell, die sich an die sich ständig weiterentwickelnde Bedrohungslandschaft von heute anpassen. Von der Endpunktsicherheit über die Erkennung von Insiderbedrohungen bis hin zur Incident Recovery bietet Dell ein umfassendes Resilienz-Framework, das Vertrauen schafft und Wachstum ermöglicht.

Schaffen Sie eine resiliente Zukunft mit Dell Technologies

Schützen Sie Ihr Unternehmen mit den umfassenden, skalierbaren Lösungen von Dell Technologies vor bösartigen Insiderbedrohungen. Indem Sie mit Dell zusammenarbeiten, sichern Sie nicht nur Ihre Betriebsvorgängen, sondern stellen auch die Geschäftskontinuität sicher, fördern das Vertrauen der Kunden und machen Ihr Unternehmen zukunftssicher. Kontaktieren Sie uns, um mehr über die Implementierung proaktiver Abwehrmaßnahmen zu erfahren.

Dell Technologies ist Ihr zuverlässiger Partner im Kampf gegen Insiderbedrohungen, beim Schutz Ihrer kritischen Ressourcen und bei der Stärkung Ihres Unternehmens, damit es in einer dynamischen digitalen Umgebung erfolgreich sein kann. Eine Zukunft der Sicherheit ist eine Zukunft des Erfolgs – und sie beginnt mit Dell.

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

Weitere Informationen zu den Lösungen von Dell

Kontakt zu Dell Technologies ExpertInnen

Weitere Ressourcen anzeigen

Diskutieren Sie mit: #HashTag

DELL Technologies