DELL Technologies

Zero Day: Stärkung von Cybersicherheit und Resilienz mit Dell Technologies

Die wachsende Bedrohung durch Zero-Day-Angriffe

Zero-Day-Angriffe haben sich schnell zu einer der größten Herausforderungen in der heutigen Cybersicherheitslandschaft entwickelt. Diese Angriffe nutzen Sicherheitslücken aus, die den Softwareanbietern und SicherheitsexpertInnen unbekannt sind, sodass Unternehmen unvorbereitet und gefährdet bleiben. Unternehmen in allen Branchen, vom Gesundheitswesen bis zur Finanzbranche, sind anfällig für solche Sicherheitsverletzungen, die oft schwerwiegende finanzielle und betriebliche Folgen haben.

Das Tempo der digitalen Transformation beschleunigt sich und Zero-Day-Angriffe werden immer häufiger und raffinierter. Noch nie war der Bedarf an robusten Schutzmaßnahmen so groß wie heute. Dell Technologies ist sich der kritischen Natur dieser Bedrohung bewusst und bietet Unternehmen innovative, skalierbare Abwehrmaßnahmen, um Zero-Day-Angriffe effektiv zu bekämpfen und ihren Betrieb wiederherzustellen.

Was sind Zero-Day-Angriffe?

Bei einem Zero-Day-Angriff wird eine nicht offengelegte Sicherheitslücke in Software oder Hardware ausgenutzt, bevor ein Patch oder eine Korrektur verfügbar ist. AngreiferInnen nutzen dieses Zeitfenster und verursachen oft weitreichende Unterbrechungen, bevor die Sicherheitslücke entdeckt und behoben wird.

So funktionieren Zero-Day-Angriffe

1. **Erkennung von Sicherheitslücken:** Hacker identifizieren Codierungsfehler oder verborgene Hintertüren in Softwareanwendungen oder Systemen.
2. **Entwicklung von Exploits:** Malware wird entwickelt, um die Sicherheitslücke auszunutzen. AngreiferInnen können gezielte Phishingkampagnen oder Websites mit Malware nutzen, um den Exploit einzuschleusen.
3. **Ausführung des Angriffs:** Der Exploit wird bereitgestellt, wodurch das System kompromittiert wird und Datendiebstahl oder Betriebsunterbrechungen möglich werden.

Gängige Techniken

- Drive-by-Downloads verleiten NutzerInnen dazu, unwissentlich Malware zu installieren.
- Phishing-E-Mails verbreiten bösartige Links oder Payloads, um Sicherheitslücken auszunutzen.
- Dateilose Angriffe umgehen die Erkennung, indem sie Vorgänge vollständig im Arbeitsspeicher eines Systems ausführen.

Diese hochmodernen Angriffsvektoren machen Zero-Day-Angriffe besonders gefährlich, da sie von herkömmlichen signaturbasierten Erkennungstools oft nicht erkannt werden.

Die Auswirkungen auf Unternehmen

Zero-Day-Angriffe bergen aufgrund ihrer Unvorhersehbarkeit und der Verzögerung bei der Erkennung erhebliche Risiken. Die Folgen können an mehreren Fronten katastrophal sein.

Finanzielle Verluste

Ein erfolgreicher Zero-Day-Angriff kann zu hohen Kosten führen, von Bußgeldern bis hin zu Umsatzeinbußen während der Ausfallzeit. Beispielsweise könnte eine nicht identifizierte Sicherheitslücke, die in einer E-Commerce-Plattform ausgenutzt wird, den Kaufprozess deaktivieren und sich direkt auf den Vertrieb auswirken.

Reputationsfolgen

Die öffentliche Wahrnehmung eines Unternehmens kann irreparabel beeinträchtigt werden. Kunden verlieren das Vertrauen, wenn vertrauliche Informationen offengelegt werden oder Services ausfallen.

Betriebsunterbrechung

Nicht behobene Sicherheitslücken lähmen Systeme oft, was zu einer geringeren Produktivität, verzögerten Projekten und verpassten Geschäftschancen führt.

Praxisbeispiel

Ein großer Anbieter im Gesundheitswesen wurde Opfer eines Zero-Day-Angriffs, der auf ungepatchte Software für medizinische Geräte abzielte. Der Angriff unterbrach wichtige Betriebsabläufe, enthüllte Patientendaten und kostete das Unternehmen **Millionen** an Wiederherstellungskosten, während das Vertrauen der PatientInnen untergraben wurde.

Warnmeldungsstatistiken

Laut einer Studie von Ponemon aus dem Jahr 2023 liegt der Prozentsatz der Sicherheitsverletzungen im Zusammenhang mit Zero-Day-Angriffen bei etwa 80 %.

Zero-Day-Angriffe machen durchgehend mehr als **70 %** der ausgenutzten Sicherheitslücken aus.

Quelle: IMandiant „M-Trends“, 2024

Bekämpfung von Zero-Day-Angriffen mit Dell Technologies

Dell Technologies bietet branchenführende Lösungen, die Unternehmen dabei helfen, sich aktiv vor Zero-Day-Angriffen zu schützen und gleichzeitig eine schnelle Recovery nach solchen Verstößen zu ermöglichen.

Server- und Storage-Sicherheitslösungen

Die Server- und Storage-Sicherheitslösungen von Dell bieten zusätzliche Schutzebenen:

- Sichere Server überwachen und blockieren unbefugte Zugriffsversuche.
- Datenbackup- und -Recovery-Systeme sorgen dafür, dass kritische Informationen auch im schlimmsten Fall zugänglich und intakt bleiben.

Verstärkte Endpunkte mit Dell Trusted-Devices

Endpunkte sind ein wichtiger Einstiegspunkt für AngreiferInnen. Dell Trusted-Devices umfassen erweiterte Sicherheitsmaßnahmen, um sicherzustellen, dass Endpunkte vor nicht erkannten Bedrohungen geschützt bleiben.

- **SafeBIOS** schützt die Firmware vor Manipulationen und stellt so die Systemintegrität von Grund auf sicher.
- **SafeID** schützt Nutzerzugangsdaten durch Sichern von Authentifizierungsprozessen.
- **SafeData** verschlüsselt sensible Daten im Ruhezustand und während der Übertragung und macht sie unbrauchbar, falls sie abgefangen oder ausgenutzt werden.

Proaktive Bedrohungserkennung mit CrowdStrike

CrowdStrike nutzt erweiterte Analysen und KI, um die Endpunktaktivität zu überwachen und ungewöhnliches Verhalten zu erkennen, das auf Zero-Day-Exploits hinweisen könnte. Die proaktive Bedrohungserkennung sorgt für eine schnelle Reaktion, bevor Sicherheitslücken zu weitreichenden Schäden führen können.

Beispielsweise konnte ein Telekommunikationsanbieter, der CrowdStrike verwendet, Anomalien im Netzwerkverkehr frühzeitig erkennen und so einen potenziellen Zero-Day-Exploit auf Kundenservern entschärfen.

Dell PowerProtect-Lösungen

Dell PowerProtect bietet robuste, unveränderliche Backups und isolierte Recovery-Optionen. Unternehmen können den Betrieb nach einem Zero-Day-Angriff schnell und effizient wiederherstellen, die Business Continuity aufrechterhalten und wichtige Kundendaten schützen.

Beispielsweise nutzte eine große Einzelhandelskette PowerProtect, um verschlüsselte Dateien wiederherzustellen, die durch einen Ransomwareangriff aufgrund einer Zero-Day-Sicherheitslücke kompromittiert wurden, wodurch längere Ausfallzeiten vermieden wurden.

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

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

Die Bedeutung eines mehrschichtigen Sicherheitsansatzes

Echte Sicherheit erfordert mehr als eine Lösung. Eine mehrschichtige Strategie kombiniert Technologie, Prozesse und MitarbeiterInnen zu einem umfassenden Framework für Abwehrmaßnahmen.

Wichtige Maßnahmen zur Stärkung der Abwehr

- **Einführung von Zero-Trust-Prinzipien:** Überprüfen Sie alle Personen und Geräte, die versuchen, auf das Netzwerk zuzugreifen.
- **Implementierung einer erweiterten Verschlüsselung:** Nutzen Sie Verschlüsselungsprotokolle, um Daten sowohl während der Übertragung als auch im Ruhezustand zu schützen.
- **Schulung von MitarbeiterInnen:** Bieten Sie detaillierte Schulungssitzungen an, in denen MitarbeiterInnen erfahren, wie sie Phishingversuche und Social-Engineering-Taktiken erkennen können.
- **Regelmäßige Tests von Systemen:** Führen Sie regelmäßig Penetrationstests und Sicherheitslückenscans durch, um sicherzustellen, dass sich die Abwehrsysteme an neue Bedrohungen anpassen.

Dell Technologies kombiniert diese Praktiken mit seinen fortschrittlichen Sicherheitslösungen und stellt so sicher, dass Unternehmen bereit sind, Zero-Day-Sicherheitslücken effektiv zu bekämpfen.

Partnerschaften zur Stärkung der Cybersicherheit

Die Zusammenarbeit von Dell mit den Branchenführern **Microsoft**, **CrowdStrike** und **Secureworks** bietet Kunden Zugang zu modernsten Sicherheitsinformationen und -tools.

- **Microsoft**-Technologie ist nahtlos in Dell Lösungen integriert, um systemweite Kompatibilität und proaktive Schutzmechanismen sicherzustellen.
- **CrowdStrike** bietet erweiterte Threat Intelligence am Endpunkt, um potenzielle Zero-Day-Exploits zu erkennen.
- **Secureworks** stellt fortlaufendes Monitoring und fachkundige Korrekturmaßnahmen für die Echtzeitreaktion auf Angriffe bereit.

Nutzung von Dell Professional Services

Dell Professional Services bieten ein umfassendes Angebot an Beratungs-, Implementierungs- und Wiederherstellungsleistungen, um Unternehmen bei der Bewältigung und Minderung der mit Zero-Day-Bedrohungen verbundenen Risiken zu unterstützen. Von der Reaktion auf Incidents bis zur Planung einer Roadmap für die Cybersicherheit unterstützt Dell Unternehmen dabei, langfristige Resilienz zu erreichen.

Zusammen für eine krisenfeste Zukunft

Investitionen in Dell Technologies bedeuten, einen Partner zu haben, der nicht nur überlegene Technologie, sondern auch die Gewissheit bietet, dass alles reibungslos und sorgenfrei funktioniert. Durch hochmoderne Lösungen, strategische Partnerschaften und beispielloses Fachwissen versetzt Dell Unternehmen in die Lage, selbst die fortschrittlichsten Zero-Day-Angriffe vorherzusehen, zu erkennen und zu bewältigen.

Wenden Sie sich noch heute an Dell Technologies, um Ihr Unternehmen zu sichern, Ihren Ruf zu schützen und in einer unvorhersehbaren digitalen Landschaft erfolgreich zu sein. Vertrauen Sie auf Dell, um Ihre Zukunft gegen die Bedrohungen von morgen zu schützen.

Dell Technologies schafft Vertrauen und ermöglicht es Unternehmen, mit seinen Sicherheitslösungen und -services den Herausforderungen von Zero-Day-Angriffen immer einen Schritt voraus zu sein und das zu schützen, was am wichtigsten ist.

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

Kommen Sie ins Gespräch über #HashTag

DELL Technologies