Schutz vor Cyberangriffen in der Lieferkette mit Dell Technologies

Zusammenfassung

Die zunehmend globale und vernetzte Natur des Geschäftsbetriebs hat Unternehmen einer wachsenden Bedrohung durch Cyberangriffe in der Lieferkette ausgesetzt. Diese ausgeklügelten Angriffe nutzen Sicherheitslücken im Lebenszyklus der Hardware – von der Herstellung bis zur Bereitstellung – sowie Software von Drittanbietern aus, die es böswilligen AkteurInnen ermöglichen, ganze Systeme über vertrauenswürdige Anwendungen oder Updates zu kompromittieren. Solche Vorfälle sind nicht nur finanziell katastrophal, sondern können auch Rufschädigungen und massive Betriebsunterbrechungen zur Folge haben.

Die Auswirkungen dieser Bedrohungen sind tiefgreifend. Angriffe in der Lieferkette bleiben oft unentdeckt, bis erhebliche Schäden entstanden sind. Daher sind proaktive Abwehrstrategien unerlässlich. Mit fortschrittlichem Endpunktschutz, proaktiver Überwachung und umfassenden Lösungen für Server- und Datensicherheit versetzt Dell Unternehmen in die Lage, ihre Lieferketten durchgängig zu sichern. Durch Technologie, Partnerschaften und Fachwissen können Unternehmen Resilienz aufbauen und sich vor Sicherheitslücken in ihren Ökosystemen schützen.

Die wachsende Bedrohung durch Cyberangriffe in der Lieferkette

Angriffe auf die Lieferkette haben in den letzten Jahren erheblich zugenommen. Durch Manipulationen an physischen Geräten während der Produktion, des Versands oder der Bereitstellung oder durch das Auffinden von Schwachstellen bei Softwareanbietern erhalten AngreiferInnen die Möglichkeit, bösartige Komponenten oder Code einzuschleusen, Systeme zu beschädigen oder sensible Daten zu exfiltrieren. Die Opfer reichen von kleinen Unternehmen bis hin zu Weltkonzernen. Die Folgen sind unter anderem schwere finanzielle Verluste, beeinträchtigtes Kundenvertrauen und rechtliche Konsequenzen. Dell Technologies ist sich dieser wachsenden Gefahr bewusst und setzt sich für präventive Maßnahmen ein, um die katastrophalen Auswirkungen solcher Angriffe zu mindern.

Verständnis von Cyberangriffen auf die Lieferkette

So funktionieren Hardwareangriffe in der Lieferkette

1. **Fertigungsphase: AngreiferInnen** führen während der Hardwaremontage bösartige Komponenten ein und nutzen dabei häufig kompromittierte Lieferanten.
2. **Versandphase:** Geräte werden während des Transports abgefangen und so verändert, dass sie schädliche Firmware- oder Hardwaremodifikationen enthalten.
3. **Bereitstellung und Aktivierung:** Sobald die kompromittierte Hardware in das Unternehmensnetzwerk gelangt ist, erhalten AngreiferInnen Zugriff auf sensible Daten oder ermöglichen Backdoor-Vorgänge.

So funktionieren Angriffe auf die Softwarelieferkette

1. **Anfängliche Sicherheitsverletzung:** Ein Drittanbieter von Software wird kompromittiert, oft durch Phishing, ungepatchte Sicherheitslücken oder Insiderbedrohungen.
2. **Codemanipulation:** Böswillige AkteurInnen schleusen schädliche Elemente wie Malware oder Hintertüren in Software ein, um sie dort zu verteilen.

3. **Weitergabe an EndnutzerInnen:** Unternehmen, die kompromittierte Software installieren oder aktualisieren, laden versehentlich schädliche Komponenten herunter.

Gängige Techniken – Hardware

- **Firmwaremanipulation:** Einbettung von bösartigem Code, der nach der Bereitstellung aktiviert wird
- **Hardwareimplantation:** Einbau von versteckten Komponenten zur Überwachung oder Exfiltration von Daten
- **Exploits bei vertrauenswürdigen Lieferanten:** Ausnutzung von Drittanbietern mit weniger sicheren Prozessen

Gängige Techniken – Software

- **Komponenten-Hijacking:** Infizieren von Bibliotheken oder Frameworks von Drittanbietern mit bösartigem Code
- **Injektion in Updates:** Abänderung offizieller Softwareupdates, um Exploits einzuschleusen
- **Abhängigkeitsverwirrung:** Ausnutzung der Abhängigkeit von Unternehmen von unsicheren Paketabhängigkeiten

Die Auswirkungen auf Unternehmen

Finanzielle Konsequenzen

Angriffe auf Lieferketten verursachen häufig Kosten in Form von Bußgeldern, Kosten für die Recovery von Systemen und Entschädigungen für Kunden. Ein aufsehenerregender Vorfall, in den ein weltweit tätiges IT-Managementunternehmen verwickelt war, führte zu Verlusten von über 70 Mio. USD und verdeutlicht die finanziellen Folgen, die solche Angriffe anrichten können.

Betriebsunterbrechung

Beschädigte oder deaktivierte Systeme, die durch Infiltrationen von Malware verursacht werden, führen häufig zu langen Ausfallzeiten, die die Produktivität des Unternehmens beeinträchtigen und die Projektleistungen verzögern.

Reputationsfolgen

Vertrauen in Softwarepartner ist für moderne Unternehmen von entscheidender Bedeutung. Eine Sicherheitsverletzung in der Lieferkette im Zusammenhang mit den Softwareangeboten eines Unternehmens kann den Ruf schädigen und die Kundentreue untergraben.

Beispiele aus der Praxis – Hardware/Software

Ein globaler Elektronikhersteller hat kompromittierte Komponenten in seiner Lieferkette entdeckt, was zu weit verbreiteten Systemausfällen führte. Der Angriff kostete über **45 Mio. USD** an Recovery- und Anwaltskosten sowie irreparable Schäden an den Beziehungen zu den Lieferanten.

Die SolarWinds-Sicherheitsverletzung gehört zu den berüchtigtsten Angriffen auf die Softwarelieferkette. Die Kompromittierung ihrer Orion-Produkte infizierten Unternehmen auf der ganzen Welt, einschließlich Regierungsbehörden und Fortune 500-Unternehmen. Der geschätzte Schaden lag bei mehr als **90 Mio. USD** und die Sicherheitsverletzung verdeutlichte die weitreichenden Folgen von Sicherheitslücken in der Lieferkette.

Das Fachwissen von Dell Technologies bei der Bekämpfung von Angriffen in der Lieferkette

Das umfassende Portfolio an Sicherheitslösungen von Dell Technologies versetzt Unternehmen in die Lage, sich weiterentwickelnden Cyberrisiken einen Schritt voraus zu sein.

Dell Secured Component Verification (SCV)

Secure Component Verification (SCV) ist ein integraler Bestandteil der Lieferkettensicherheitsstrategie von Dell Technologies, die darauf ausgelegt ist, die Authentizität und Integrität von Hardwarekomponenten in verschiedenen Dell Lösungen sicherzustellen. SCV bietet eine kryptografische Validierung von Systemkomponenten vom Zeitpunkt der Herstellung bis zur Lieferung und Bereitstellung. Dell Technologies bietet eine robuste Lieferkettensicherheit, die sicherstellt, dass die Systeme vom Werk bis zur Bereitstellung manipulationsfrei und sicher sind. Dies verbessert die allgemeine Sicherheit, Zuverlässigkeit und Leistung für Dell Kunden.

Sichere Endpunkte mit Dell Trusted-Devices

Bei Dell Trusted-Devices ist Sicherheit auf der Hardware- und Firmwareebene integriert, um manipulationssichere Systeme zu schaffen.

- **SafeBIOS** sorgt für Firmwareintegrität beim Start, verhindert unbefugte Konfigurationsänderungen und überprüft die Firmwareintegrität beim Starten, sodass kompromittierte Systeme nicht gestartet werden können.
- **SafeID** schützt Authentifizierungszugangsdaten auf Hardwareebene, verhindert unbefugten Zugriff und schützt Anmeldedaten, indem Authentifizierungsschlüssel gesichert und unbefugte NutzerInnen gesperrt werden.
- **SafeData** ermöglicht die End-to-End-Verschlüsselung für sensible Geschäftsdateien und blockiert so Versuche zur ausbeuterischen Datenexfiltration.

Proaktive Bedrohungserkennung mit CrowdStrike

CrowdStrike-Lösungen sind in die Technologien von Dell integriert, um Echtzeiteinblicke in das Verhalten bösartiger Software zu erhalten.

- **Verhaltensanalysen zur Bedrohungserkennung:** Überwacht das Hardware- und Firmwareverhalten auf Anzeichen von Manipulationen und erkennt ungewöhnliche Softwareaktivitäten, um die Verbreitung von Malware zu verhindern.
- **Tools für sofortige Reaktion:** KI isoliert kompromittierte Systeme und verhindert laterale Bewegungen innerhalb des Netzwerks.
- **KI-gestützte Bedrohungskorrektur:** Identifiziert und isoliert Bedrohungen aktiv und verhindert so eine laterale Ausbreitung innerhalb der Unternehmenssysteme.
- **Integrationsfunktionen:** Hybrid- und Multi-Cloud-Umgebungen werden mit Dell und CrowdStrike-Tools ganzheitlich abgesichert.

Verbesserte Sicherheit durch die Server- und Storage-Lösungen von Dell

Die Dell PowerEdge-Serverproduktreihe bietet erweiterten Schutz für die Sicherung erfolgskritischer Softwareplattformen. Storage-Systeme wie Dell PowerStore bieten eine branchenführende Verschlüsselung für Anwendungen und Daten.

- **Sichere Serverfirmware:** Überwacht und blockiert unbefugte Änderungen auf Hardwareebene.
- **Isoliertes Netzwerkmonitoring:** Erkennt Anomalien, die auf Manipulationen in der Lieferkette hindeuten.
- **Unveränderliche Backups:** Schützen Recovery-Punkte, selbst wenn der primäre Storage kompromittiert ist.
- **Recovery Vaults:** Isolierte Umgebungen schützen vor kaskadierenden Ausfällen, die von kompromittierten Systemen ausgehen.

Mehrschichtige Ansätze zur Risikominderung

Dell ermutigt Unternehmen, umfassende Strategien einzuführen, die Technologie, Mitarbeiterpraktiken und aktualisierte Prozesse kombinieren.

Strategische Schritte

- **Bessere Transparenz in der Lieferkette:** Fordern Sie von allen Anbietern, strenge Sicherheitsstandards einzuhalten und Hardware in jeder Phase zu zertifizieren.
- **Implementierung einer fortschrittlichen Verschlüsselung:** Sichern Sie Daten auf jeder Ebene mit fortschrittlichen Protokollen und begrenzen Sie die Zugänglichkeit selbst bei kompromittierter Hardware.
- **Einführung von Zero-Trust-Richtlinien:** Geräte, Anwendungen und NutzerInnen wird ohne Verifizierung niemals automatisch vertraut.
- **Sichere Codierungsstandards:** Arbeiten Sie mit Softwarepartnern zusammen, um strenge Richtlinien für Plug-ins, APIs und Integrationen durchzusetzen.
- **Regelmäßige Überwachung von Aktivitäten und Audits:** Häufige Sichtbarkeitsprüfungen gewährleisten die Integrität der Services von Drittanbietern.
- **Durchführung regelmäßiger Tests:** Führen Sie Penetrationstests und Firmwarebewertungen durch, um die Geräteintegrität kontinuierlich zu überprüfen.
- **Schulung von MitarbeiterInnen:** Schulen Sie Teams, damit sie Komponenten oder Pakete mit verdächtigem Verhalten erkennen können.

Wie Dell Professional Services die geschäftliche Ausfallsicherheit von Unternehmen sicherstellen

Dell Professional Services unterstützen Unternehmen bei der Implementierung robuster Abwehrmaßnahmen für die Lieferkette. Teams aus erfahrenen CybersicherheitsexpertInnen bieten Bewertungen, Schulungen und Strategien zur Bedrohungsabwehr, die auf die individuellen Bedürfnisse des Unternehmens zugeschnitten sind.

- **Implementierungsleitfaden:** Richten Sie Zero-Trust- und geprüften Anbieterpraktiken in allen Anbieterumgebungen strategisch aus.
- **Reaktion auf Incidents:** Stellen Sie sicher, dass sich Unternehmen nach bösartigen Vorfällen schnell erholen.

Zukunftssicherheit für Unternehmenssysteme mit Dell

Cyberangriffe in der Lieferkette sind ein Beispiel für die Raffinesse moderner Bedrohungen. Unternehmen benötigen einen Schutz, der nicht nur Sicherheitsverletzungen verhindert, sondern auch eine schnelle und effektive Recovery, wenn es zu Incidents kommt. Eine Partnerschaft mit Dell Technologies bedeutet, Zugang zu hochmodernen Tools, strategischem Fachwissen und einem Netzwerk vertrauenswürdiger MitarbeiterInnen zu erhalten.

Unternehmen Sie den nächsten Schritt

Schützen Sie sensible Daten und optimieren Sie die betriebliche Zuverlässigkeit durch die Implementierung von Best Practices auf der Grundlage von Dell Technologies. Nehmen Sie noch heute Kontakt mit uns auf und lassen Sie sich individuell beraten, wie Sie die Lebensader Ihrer Unternehmenssysteme sichern können.

Dell Technologies steht für Vertrauen, Anpassungsfähigkeit und Innovationen, wenn sich die Cybersicherheit in der Lieferkette weiterentwickelt. Ihr heutiges Engagement sichert den Erfolg von morgen.

Eine sichere Zukunft beginnt mit Dell Technologies. Vertrauen Sie darauf, dass wir das 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 über die Lösungen von Dell

Kontakt zu Dell Technologies ExpertInnen

Weitere Ressourcen anzeigen

Kommen Sie ins Gespräch über #HashTag

DELL Technologies