DELL Technologies

Prompt/SQL-Injection: Stärkung der Cybersicherheit und Resilienz mit Dell Technologies

Die zunehmende Bedrohung durch Prompt/SQL-Injection-Angriffe

Prompt- und SQL-Injection-Angriffe haben sich wiederholt als eine der schädlichsten und am weitesten verbreiteten Methoden von Cyberkriminellen erwiesen. Diese Angriffe nutzen Sicherheitslücken in Nutzerabfragen- oder Datenbanksystemen aus und ermöglichen es böswilligen Akteuren, Server zu manipulieren, Daten zu stehlen oder Workflows zu unterbrechen. Die zunehmende Abhängigkeit von datengesteuerten Anwendungen hat die Angriffsfläche vergrößert, sodass Prompt- und SQL-Injection-Techniken in allen Branchen eine immer größere Bedrohung darstellen.

Von E-Commerce-Plattformen bis hin zu Finanzinstituten nutzen Angreifende diese Lücken aus, um unbefugten Zugriff auf sensible Daten zu erhalten, was die dringende Notwendigkeit fortschrittlicher Gegenmaßnahmen demonstriert. Dell Technologies ist sich der kritischen Natur dieser Herausforderungen bewusst und bietet innovative und skalierbare Lösungen zum Schutz von Unternehmen vor Prompt- und SQL-Injection-Angriffen.

Grundlegendes zu Prompt/SQL-Injection-Angriffen

Was genau?

- **Prompt-Injection-Angriffe** umfassen die Manipulation von KI- oder Automatisierungs-Prompts durch böswillige Eingaben. Diese Angriffe verwirren Systeme wie KI-Chatbots und führen zu unerwarteten oder schädlichen Aktionen**.**
- **SQL-Injection-Angriffe** zielen auf Online-Datenbanksysteme ab. Angreifende fügen bösartige SQL-Abfragen in Eingabefelder (z. B. Anmelde- oder Suchformulare) ein, um Back-end-Datenbanken zu manipulieren und zu kontrollieren.

Wie sie funktionieren

Prompt-Injection-Prozesse:

1. Angreifende manipulieren Prompts, um schädliche Ausgaben zu generieren, indem sie mehrdeutige oder schlecht gestaltete Anweisungen ausnutzen.
2. Dies zielt häufig auf KI-Systeme ab, die für den Kundenservice, Analysen oder die Entscheidungsfindung verwendet werden.

SQL-Injection-Prozesse:

1. Ein bösartiger SQL-Code wird in Eingabefelder einer anfälligen Anwendung eingefügt.
2. Das ausgenutzte System führt diese Anweisungen aus und ermöglicht unbefugten Datenzugriff, Löschung oder Systemkontrolle.

Gängige Techniken

- **Verbandsbasierte SQL-Injection:** Kombinieren von Abfragen, um Informationen aus der Datenbank zu extrahieren.
- **Fehlerbasierte Techniken:** Verwendung von absichtlich erstellten Abfragen, um Fehler zu erzeugen, die die Datenbankstruktur aufdecken.
- **Prompt-Überlastung oder -Verwirrung:** Übermittlung bösartiger Anweisungen, die KI- oder regelbasierte Ausgaben überschreiben.

Die Auswirkungen auf Unternehmen

Die Auswirkungen eines Prompt/SQL-Injection-Angriffs reichen weit über den unmittelbaren Incident hinaus. Zu den schädlichsten Folgen zählen:

Finanzielle Kosten

Zu den direkten Verlusten aus diesen Angriffen gehören gestohlene Kundendaten und Transaktionsdatensätze, die häufig zu Geldbußen führen. Ein SQL-Injection-Angriff auf ein Finanzinstitut kostete das Unternehmen fast 40 Millionen USD für Rechtsstreitigkeiten, Rückerstattungen und neue Sicherheitsmaßnahmen.

Betriebsunterbrechungen

SQL-Injection-Angriffe, die auf Back-end-Datenbanken abzielen, können Systeme abstürzen lassen, Workflows lähmen und wesentliche Services anhalten. Die durchschnittliche Ausfallzeit für betroffene Unternehmen wird auf 18 bis 24 Stunden geschätzt, was zu erheblichen Produktivitätsverlusten führt.

Rufschädigung

Prompt-Injection-Angriffe auf KI-Plattformen führen häufig zu Fehlinformationen oder falschen Entscheidungen. Gestohlene Geschäftsgeheimnisse oder kompromittierte Services untergraben das Kundenvertrauen und schaden den Beziehungen.

Praxisbeispiel

Ein Einzelhandelsunternehmen wurde Opfer eines SQL-Injection-Angriffs auf seine Zahlungsplattform, wodurch Kundendaten kompromittiert und Dienste für mehrere Tage unterbrochen wurden. Die Beseitigung des Incidents erforderte behördliche Meldungen, Kundenentschädigungen in Höhe von fast **3 Millionen USD** und Prozesskosten.

Warnmeldungsstatistiken

SQL-Injection macht laut dem „State of the Internet"-Bericht von Akamai (für den Zeitraum 2017–2019) fast **zwei Drittel (ca. 65 %)** aller Angriffe auf Webanwendungen aus.

OWASP hat Prompt-Injection in seiner Top-10-Liste für 2025 als das **größte LLM-Sicherheitsrisiko** eingestuft.

Quelle: 2025: OWASP Top Security Risks

Lösungen von Dell Technologies zum Schutz vor Prompt/SQL-Injection

Dell Technologies stattet Unternehmen mit einem Ökosystem aus Tools und Schutzmechanismen aus, die speziell auf die Abwehr komplexer Angriffe wie Prompt- und SQL-Injection zugeschnitten sind.

Endpunktsicherheit mit Dell Trusted-Devices

Endpunkte sind die Gateways zu Unternehmensnetzwerken. Dell Trusted-Devices integrieren Sicherheit auf Hardwareebene für robusten, kompromisslosen Schutz.

- **Dell SafeID** schützt Nutzerzugangsdaten mit verbesserter hardwarebasierter Authentifizierung.
- **SafeData** verschlüsselt sensible Daten sowohl während der Übertragung als auch im Ruhezustand und schützt so vor Kompromittierung durch SQL-Injection-Exploits.

Proaktive Bedrohungserkennung mit CrowdStrike

Die proaktiven Erkennungstools von Dell unterstützt von CrowdStrike nutzen KI, um ungewöhnliches Verhalten zu identifizieren und zu neutralisieren.

- **Echtzeitmonitoring:** Stellt sicher, dass Prompt- oder SQL-Anomalien in hybriden Umgebungen sofort gemeldet werden.
- **Bedrohungseindämmung:** KI-basierte Algorithmen isolieren betroffene Nodes im Netzwerk, um eine vollständige Kompromittierung zu verhindern.

Ein multinationales Fertigungsunternehmen, das proaktive Bedrohungserkennung nutzt, hat SQL-Injection-Abfragen seiner industriellen Datenbanken präventiv gestoppt und so potenzielle Ausfallzeiten in Millionenhöhe vermieden.

Server- und Storage-Sicherheit von Dell

- **Vertrauenswürdige Server:** Schützen Sie Datenbankanwendungen, indem Sie Server gegen Angriffsversuche absichern.
- **Adaptive Workload-Sicherheit:** Verhindert die unbefugte Ausführung von bösartigem Code oder Injektionen.

Dell PowerProtect für Datenintegrität

- **Unveränderliche Backups:** Verbesserte Resilienz gewährleistet die Recovery auch dann, wenn Datenbanken oder Prompts beschädigt sind.
- **Air-Gap-Storage:** Isoliert Recovery-Punkte physisch und logisch und mindert so die Manipulation durch SQL-Injection-Fallbacks.

Beispielsweise stellte ein Telekommunikationsanbieter während eines SQL-Injection-basierten Ransomwareangriffs den Betrieb mithilfe der Backupisolationen von Dell PowerProtect in weniger als 48 Stunden wieder her und vermied so kritische Verluste.

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.

Strategische Nutzung von Partnerschaften

- **Microsoft:** Integrierte Abwehrmaßnahmen gegen abfragebasierte Injektionen auf weit verbreiteten Plattformen wie Azure und SQL Server**.**
- **CrowdStrike und Secureworks:** Erweiterte Threat Intelligence und maßgeschneiderte Reaktionen auf Vorfälle stärken die allgemeine Resilienz in Kombination mit der Infrastruktur von Dell.

Entwicklung einer mehrschichtigen Sicherheitsstrategie

Wichtige Maßnahmen, die Unternehmen ergreifen sollten

- **Zero-Trust-Framework:** Implementieren Sie eine umfassende Validierung für alle Nutzer und Systembefehle.
- **Sichere Programmierverfahren:** EntwicklerInnen sollten Nutzereingaben bereinigen und coderesistente SQL-Injections bereitstellen.
- **Verschlüsselungsprotokolle:** Schützen Sie Datenübertragungen und -Storage mit fortschrittlichen Verschlüsselungsalgorithmen.
- **Mitarbeiterschulung:** Schulen Sie Ihre MitarbeiterInnen darin, Eingabeanomalien, Phishing-Versuche und böswillige Eingabeaufforderungen zu erkennen.
- **Systemaudits und -tests:** Regelmäßige Schwachstellenprüfungen stellen sicher, dass die Abwehrmaßnahmen gegen Prompt- und SQL-Injections auf dem neuesten Stand bleiben.

Die Architektur von Dell wendet all diese Prinzipien gleichzeitig an und schafft einzigartige sichere Plattformen für seine Kunden.

Nutzung von Dell Professional Services

Von der Reaktion auf Incidents bis hin zum täglichen Monitoring unterstützen Dell Professional Services Unternehmen mit einem personalisierten Ansatz. Qualifizierte Teams bewerten Risiken, implementieren robuste Abwehrmaßnahmen und bieten schnelle Abhilfemaßnahmen bei Bedrohungen.

Sicherheit für das, was am wichtigsten ist – mit Dell Technologies

Die Bekämpfung der ausgeklügelten Prompt- und SQL-Injection-Cybersicherheitsangriffe erfordert einen proaktiven Ansatz. Dell Technologies ist Ihr Partner und bietet hochmoderne Tools, strategische Partnerschaften und Expertenservices.

Die Zukunft der betrieblichen Integrität und des Kundenvertrauens beginnt mit präventiven Lösungen. Wenden Sie sich noch heute an Dell Technologies, um Ihre Daten zu schützen, Ausfallsicherheit zu schaffen und in der digitalen Welt erfolgreich zu sein.

Gemeinsam schützen wir das, 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