DELL Technologies

提示/SQL 注入：採用 Dell Technologies 強化網路安全和復原能力

提示/SQL 注入攻擊的威脅升溫

提示和 SQL 注入攻擊屢次經證明是網路犯罪分子發動網路攻擊中最具破壞性也最普遍的方法之一。這些攻擊是利用使用者查詢或資料庫系統中的漏洞，讓惡意行為者能操縱伺服器、竊取資料或中斷工作流程。企業對資料驅動應用程式的依賴度日益增加，也因次擴大了攻擊面，使提示和 SQL 注入攻擊手法在所有產業中成為更值得注意的威脅。

從電子商務平台到金融機構，攻擊者利用這些漏洞對敏感資料進行未經授權存取，這顯示出對於設置進階反制措施的迫切需要。Dell Technologies 認識到這些挑戰的關鍵本質，因此提供可擴充的創新解決方案，以保護企業防範提示和 SQL 注入攻擊。

認識提示/SQL 注入攻擊

它們是什麼？

- **提示注入攻擊**涉及透過惡意輸入來操縱 AI (人工智慧) 或自動化提示。這類攻擊會讓 AI 聊天機器人等系統出現混淆，進而做出意外或有害的行為。
- **SQL 注入攻擊**以線上資料庫系統為目標。攻擊者在輸入欄位 (例如登入或搜尋表單) 插入惡意的 SQL 查詢，以操縱和控制後端資料庫。

這如何運作

提示注入程序：

1. 攻擊者利用語意模糊或設計不佳的指令，操弄提示以產生有害的輸出。
2. 這通常會以用於客戶服務、分析或決策的 AI 系統為目標。

SQL 注入程序：

1. 在有弱點的應用程式輸入欄位中注入惡意 SQL 程式碼。
2. 遭利用的系統執行這些指令，從而遂行未經授權的資料存取、刪除或系統控制。

常見手法

- **聯合式 SQL 注入：**集結多個查詢以從資料庫擷取資訊。
- **錯誤式手法：**使用蓄意構建的查詢來製造錯誤，進而顯露出資料庫結構。
- **提示超載或混淆：**提交惡意指令，意圖覆寫 AI 或規則式輸出。

對企業的影響

提示/SQL 注入攻擊的漣漪效應，遠遠超過眼下的事件本身。最不利的後果包括了：

財務成本

這些攻擊造成的直接損失包括客戶資料和交易記錄遭竊，且往往會招致監管機關罰款。一項對金融機構進行的 SQL 注入攻擊，讓該機構在訴訟、賠償和新安全措施等項目上花費近 4000 萬美元。

營運中斷

針對後端資料庫發動的 SQL 注入攻擊，會讓系統當機、癱瘓工作流程並停止基本服務。受影響企業的平均停機時間估計在 18 到 24 小時之間，導致嚴重的生產力損失。

聲譽損害

對 AI 平台發動的提示注入攻擊，通常會導致錯誤資訊或不當決策。商業秘密遭竊或服務遭波及會損及客戶信任並破壞關係。

真實案例

一家零售公司在其支付平台上遭遇 SQL 注入攻擊，這導致客戶信用卡資料外洩，並停止服務達數天之久。為了收拾殘局，必須要向監管機關報告、耗費近 **300 萬美元**的客戶賠償和訴訟費用。

令人擔憂的統計資料

根據 Akamai 的「網際網路現況」報告 (涵蓋 2017 至 2019)，SQL 注入佔所有 Web 應用程式攻擊數將近**三分之二 (~65%)**。

OWASP 在其 2025 年前 10 大名單中，將提示注入攻擊認定為

#1 LLM

(大型語言模型) 安全風險

資料來源：2025: OWASP Top Security Risks (2025年：OWASP 主要安全風險)

採用 Dell Technologies 解決方案防禦提示/SQL 注入攻擊

Dell Technologies 為企業提供一套工具生態系統和量身打造的防護機制，以對抗提示和 SQL 注入等精密複雜的攻擊形式。

以 Dell Trusted Device 保護端點安全

端點是進入公司網路的閘道。Dell Trusted Device 於硬體層級嵌入安全機制，提供毫不妥協的強健防護。

- **Dell SafeID** 以經過強化的硬體式驗證功能保護使用者認證。
- **SafeData** 可對傳輸中和靜態的敏感資料進行加密，防範在 SQL 注入攻擊期間遭到入侵。

透過 CrowdStrike 主動偵測威脅

Dell 的主動偵測工具採用 CrowdStrike 技術，運用 AI 來識別並破解異常行為。

- **即時監視：**確保能在混合環境中立即標記提示或 SQL 異常狀況。
- **威脅遏制：**以 AI 為基礎的演算法可將網路上受影響的節點進行隔離，以防堵手法純熟的入侵行為。

一家跨國製造公司使用主動威脅偵測功能，先發制人阻止了攻擊者針對其產業資料庫發動的 SQL 注入查詢嘗試，從而保住數百萬美元的潛在停機時間損失。

Dell 的伺服器和儲存安全性

- **受信任的伺服器：**透過強化伺服器抵禦入侵嘗試的能力，保護資料庫應用程式。
- **適應性工作負載安全：**防止未經授權執行惡意程式碼或注入。

Dell PowerProtect 保障資料完整性

- **不可變備份：**增強的復原能力可確保即使資料庫或提示毀損也能進行復原。
- **實體隔離儲存裝置：**在實體上和邏輯上隔離復原點，緩解攻擊者改採 SQL 注入備用操縱計畫的風險。

例如，在 SQL 注入式勒索軟體攻擊期間，電信供應商使用 Dell PowerProtect 的備份隔離，在不到 48 小時內即恢復運作，避免了重大損失。

透過 Dell PowerSwitch Networking 和 SmartFabric OS 提供的進階網路安全和微切分

透過在整個基礎結構中提供進階網路切分、嚴格的存取控制和即時流量分析，增強對零時差攻擊的防禦。

夥伴關係的策略性運用

- **Microsoft**：在 Azure 和 SQL Server 等廣為使用的平台上，納入對於查詢式注入的整合防禦機制。
- **CrowdStrike 和 Secureworks**：先進的威脅情報與量身打造的事件回應，結合上 Dell 基礎結構，可強化整體復原能力。

打造多層式安全策略

企業應採取的關鍵行動

- **零信任架構：**對所有使用者和系統命令實施全面驗證。
- **安全編碼實務：**開發人員應清除使用者輸入，並部署防程式碼 SQL 注入。
- **加密通訊協定：**使用進階加密演算法，保護資料傳輸和儲存。
- **員工訓練：**教育人員識別輸入異常狀況、網路釣魚嘗試和惡意提示操縱。
- **系統稽核和測試：**例行漏洞檢查可確保提示和 SQL 注入防禦措施保持最新狀態。

Dell 的架構可同時套用這所有原則，為客戶打造極度安全的平台。

運用 Dell Professional Services

Dell Professional Services 以個人化方式協助企業，從事件回應到日常監控全程涵蓋。技術熟練的團隊評估風險，建置強大的防禦機制，並在面臨威脅時快速提供補救措施。

採用 Dell Technologies 保護最重要的資產

要對抗提示和 SQL 注入網路安全攻擊的精密複雜性質，需要採取積極主動的策略。Dell Technologies 是您的合作夥伴，提供尖端工具、策略合作關係及專家服務。

營運穩健和客戶信任的未來前景，始於預防性的解決方案。現在就與 Dell Technologies 聯絡，保護您的資料安全、建立復原能力，並在數位世界中蓬勃發展。

我們攜手合作，保護您最重要的資產。

請造訪 **Dell.com/SecuritySolutions**，瞭解如何解決當今主要的網路安全挑戰

深入瞭解 Dell 解決方案

聯絡 Dell Technologies 專家

檢視更多資源

使用 #HashTag 加入對話

DELL Technologies