DELL Technologies

中間人 (MITM)：透過 Dell Technologies 技術強化網路安全和韌性

中間人 (MITM) 攻擊威脅不斷上升

中間人 (MITM) 攻擊仍然是最複雜和最危險的網路安全挑戰之一。在這些攻擊中，惡意行為者攔截和更改私人通訊且未被偵測到，並以各行各業各種規模的企業為目標。從電子商務平台到金融機構，沒有任何組織能夠倖免於此風險。在數位化程度日益提高的環境中，MITM 攻擊通常會為資料竊取、金融詐騙和聲譽損害鋪路，讓這些惡意行為形成棘手攻擊。

Dell Technologies 瞭解企業在保護自己遠離這些進階威脅時，所面臨的獨特挑戰。藉由提供創新、具擴充能力的安全性解決方案，Dell 可讓組織消除 MITM 威脅、保護資產，並維護商業誠信。

什麼是中間人攻擊 (MITM)？

當網路犯罪分子秘密攔截某兩方之間的通訊，例如員工與公司伺服器之間的通訊，或客戶與企業網站之間的通訊，就會發生中間人 (MITM) 攻擊。攻擊者的目標可能不同 (從竊取機密資料到惡意操縱通訊)，但結果卻相同，即破壞信任和安全性。

常見的 MITM 技術

攻擊者使用的一些最普遍的方法包括：

Wi-Fi 竊聽：網路犯罪分子利用不安全或遭入侵的公共 Wi-Fi 網路，來攔截通訊。

DNS 欺騙：攻擊者透過篡改 DNS 記錄，將使用者重新路由到詐騙網站，趁使用者毫無戒心時收集機密資訊。

劫持工作階段：透過獲取使用中的工作階段憑證，攻擊者可以未經授權存取私人帳戶。

SSL 分割：此技術將安全 HTTPS 連線降級為易受攻擊的 HTTP 連線，進而暴露機密資訊。

這種適應性讓 MITM 攻擊變得特別惡劣，因為它們利用了表面上看起來合法的日常業務交易和互動。

對企業的影響

MITM 攻擊的連鎖反應遠遠超出了眼前的事件。一些最有害的後果包括：

營收損失

憑證遭竊和營運遭入侵通常會導致財務負擔，從直接損失擴大到復原成本。

營運受挫

解決攻擊所花費的時間和資源會減損關鍵業務功能，進而影響生產力和成長。

信任崩塌

當客戶的個人資訊遭洩露時，他們的信心會迅速動搖，導致長期的聲譽損害。

法規後果

在具有嚴格法規遵循要求的產業中營運的企業，可能會在資料違規後，面臨罰款或制裁。

現實案例

有個令人震驚的案例，涉及一家全球零售企業，其未加密的線上支付平台淪為 SSL 分割攻擊的受害者。攻擊者在結帳時攔截了客戶的信用卡資訊。該公司透過快速偵測和策略性安全措施 (包括 Dell 的端點保護工具)，得以阻止攻擊並減輕長期損害。這種情況突顯了直接的風險，以及對分層防禦的迫切需求。

359 億

全球已知資料違規事件

資料來源：2024 年 5 月：PureWL 報告

透過 Dell Technologies 對抗 MITM 攻擊

Dell Technologies 可為組織提供全方位的前瞻性工具，以便在 MITM 風險造成損害前，加以防堵。

透過 Dell Trusted Device 保護端點

端點通常是 MITM 威脅的來源，因此是優先保護項目。Dell 的受信任裝置將最先進的安全性功能直接嵌入硬體中。例如：

- **Dell SafeBIOS** 可確保系統完整性受到保護，避免開機順序遭到未經授權的篡改。
- **SafeID** 可保護使用者的驗證資料，建立防止憑證遭竊的堡壘，藉此增加另一層防護。
- **Dell SafeData** 提供端對端加密技術，可保護企業防火牆內外的機密資訊，讓遭攔截的資料變得無法讀取。

一些全球企業已部署這些功能，以強化端點系統的信任。舉例來說，一家跨國製造公司使用 Dell Trusted Device 保護其遠端員工，避免公司筆記型電腦遭到 MITM 針對性攻擊，即使在高風險的旅行中也能確保連線安全。

使用 CrowdStrike 進行進階偵測

即時偵測和回應 MITM 威脅極其重要。CrowdStrike 與 Dell 生態系統整合，利用人工智慧和行為分析，來監控並消除可疑活動。由於威脅通常是隱藏在混合環境中，因此持續監控可確保跨混合環境提供保護。透過主動識別異常，企業可以在損害發生之前，消除潛在的 MITM 嘗試。

例如，某金融機構使用進階偵測，成功偵測並緩解了針對其客戶入口網站的入侵。該平台的 AI 識別出表示有 SSL 分割的異常網路活動，因此得以立即修復。

透過 Dell PowerProtect 強化資料保護

即使是擁有進階防禦能力的組織，也可能遭到入侵。這就是 Dell PowerProtect 出場的時機。透過不變性和實體隔離儲存裝置等功能，它可以在攻擊期間保護關鍵業務資料，避免遭更改、破壞或存取。PowerProtect Cyber Recovery 存放庫可將機密資料與主要網路隔離，提供額外的安全性，確保即使在最糟的情況下，機密資訊仍維持完整且可復原。

這項技術對於面臨 DNS 欺騙攻擊的醫療保健組織來說極其重要。藉由 PowerProtect 不可變的備份與復原存放庫，組織可快速復原作業，避免資料遺失。

快速回應與復原服務

Dell 的資料保護服務可在資料洩露時，透過提供由專家主導的迅速復原，來補強其技術。從遠端資料復原到事件回應，這些解決方案可減少停機時間，並將營運中斷時間降至最低。必須把握每一秒時，擁有值得信賴的合作夥伴，可確保組織能安心地復原。

使用 Dell PowerSwitch 網路與 SmartFabric OS 的進階網路安全性和微區段

透過在整個基礎架構中，提供進階網路切分、嚴格的存取控制和即時流量分析，增強對零日攻擊的防禦。

透過多層式方法強化安全性

為了全面抵禦 MITM 攻擊，組織必須實施多面向的安全策略。Dell Technologies 著重以下可行的步驟：

- **採用零信任原則：**在每個點驗證所有活動和使用者存取，無論其來源在企業網路內部或外部。
- **使用進階加密：**對所有通訊進行端對端加密，可確保攻擊者無法使用攔截的資料。
- **實施多重因素驗證 (MFA)：**MFA 為系統增加驗證層，顯著減少未經授權的存取漏洞。
- **教育員工：**透過強調網路釣魚機制、使用可疑 Wi-Fi 和未經驗證的連結等風險，建立警覺性更高的工作團隊。
- **定期系統測試：**頻繁的滲透測試和更新有助於識別漏洞，並確保防禦措施保持最新狀態。

Dell 的全方位安全性產品結合這些實務，打造強大且適應性強的防禦機制，來應對不斷演變的威脅。

策略性合作關係的價值

Dell Technologies 與 CrowdStrike 和 Secureworks 等業界領先的網路安全性公司的合作，進一步強化了其產品。跨合作關係整合的專業知識，讓 Dell 能夠因應各種可能的攻擊媒介。舉例來說，CrowdStrike 利用威脅情報充實 Dell 平台，強化端點保護能力，而 Secureworks 則針對不斷演變的風險提供可行的深入解析，確保持續做好準備和適應。

Dell Technologies 優勢

選擇 Dell Technologies，代表與值得信賴的網路安全創新領導者合作。無論是透過端點保護、資料復原或協同合作關係，Dell 的端對端解決方案都能讓組織領先攻擊者一步。

使用 Dell 的全方位 MITM 解決方案，確保您的業務安全、維護客戶信任，以及讓您的營運經得起未來考驗。立即聯絡我們，開始為貴企業打造彈性且安全的未來。

透過與 Dell Technologies 合作，您可以採取積極立場來對抗網路威脅，與客戶和利害關係人建立長久的信任，並確保在越來越不安全的數位世界中能順利營運。從 Dell 開始，打造更安全的明天。

造訪 **Dell.com/SecuritySolutions**，瞭解如何解決現今一些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