DELL Technologies

惡意的內部人員：採用 Dell Technologies 強化網路安全和復原能力

惡意內部人員攻擊的威脅加劇

惡意內部人員攻擊已然成為當今商業環境中最迫切的網路安全威脅之一。心懷惡意的內部人員與外來威脅不同，他們在組織內擁有一定程度的信任和存取權限，因此他們的行為格外具破壞性，也更難偵測。從存取敏感資料到破壞系統，內部人員攻擊都可能癱瘓關鍵營運作業，並對財務和聲譽造成嚴重影響。

Dell Technologies 發現這類攻擊帶來的危險日益增加，因此開發出可擴充的創新解決方案，讓企業能夠識別、防範並減輕惡意內部人員帶來的風險。Dell 將最先進技術與專家主導的服務相結合，協助組織搶先一步因應內部威脅。

什麼是惡意內部人員攻擊？

當組織內部人士濫用其存取權限來洩露資料、中斷營運或擷取敏感資訊，以用於私人、財務或競爭目的時，即為惡意內部人員攻擊。此人可以是員工、承包商、合作夥伴，或任何可以合法存取公司系統和網路的人。

惡意內部人員攻擊的運作方式

心懷惡意的內部人員利用其受信任的身分來規避傳統安全防禦機制。常見手法包括：

1. **竊取資料：**洩露機密客戶資料、智慧財產或財務記錄。
2. **破壞：**蓄意破壞 IT 系統，使業務運作中斷或聲譽受損。
3. **濫用認證：**使用遭竊認證或濫用他人認證，以提高存取權限或建立假帳戶。
4. **與外部攻擊者合作：**與外部網路犯罪分子分享存取權限或敏感知識，以換取經濟利益。

信任和內部知識的雙重優勢，使得惡意的內部人員比外部攻擊者更加危險。

對企業的影響

惡意內部人員攻擊帶來的損害相當廣泛，範圍超越財務損失。企業可能面臨以下後果：

財務損失

敏感資訊遭竊、欺詐或破壞導致高達數百萬美元的收益損失和復原費用。

營運中斷

系統破壞或資料毀損致使運作停擺，導致作業延誤、錯失商機並降低生產力。

聲譽受損

內部人員的違規行為或攻擊，會削弱客戶和利害關係人的信任，影響客戶忠誠度和市場觀感。

違反法規

視產業而定，如果涉及醫療保健或財務等敏感資料，內部人員攻擊會導致巨額罰款和懲處。

真實案例

2020 年一家大型金融機構的 IT 承包商刻意刪除關鍵系統組態，導致網路中斷超過 **10 小時**。這種蓄意破壞行為導致**數百萬**美元的財務損失、高昂的復原成本，還有聲譽損害。這類事件說明內部人員威脅暗藏的破壞力，也突顯設置健全偵測和防範措施的迫切性。

估計成本

根據 2024 年 Ponemon Institute 的一項研究，內部人員相關事件帶來的平均成本估計為 **499 萬美元**，占所有違規行為將近 **55%**。這個數字包含偵測、復原和緩解等費用，顯示出組織投資先發制人的防禦措施，以防堵內部人員攻擊風險的迫切需求。

83%

組織在過去一年中通報過至少一次內部人員攻擊

資料來源：2024: Cybersecurity Insiders’ Report (2024 年：網路安全內部人員報告)

採用 Dell Technologies 對抗惡意內部人員攻擊

Dell Technologies 提供完善的工具和服務生態系統以對抗惡意內部人員威脅，確保您的組織能為各種意外情況做好萬全準備。

透過 Dell Trusted Device 保護端點

端點通常是內部人員威脅的進入點。Dell Trusted Device 將尖端安全功能整合至硬體之中，以強化端點並保護敏感資料。

- **Dell SafeBIOS** 可確保韌體完整性，遏止攻擊者意圖從硬體層級操縱系統作業的行為。
- **SafeID** 可保護認證資料，防止未經授權的存取和認證濫用。
- **SafeData** 可對敏感資料進行端到端加密，確保惡意內部人員即便攔截或擷取到資訊也無法讀取。

透過部署這些解決方案，無論威脅來自內部或外部，組織都可確保其端點受到妥善保護。

透過 CrowdStrike 主動偵測威脅

要識別內部人員威脅，需要具備透視和監視使用者行為的能力。整合於 Dell 解決方案內的 CrowdStrike，利用人工智慧和行為分析來偵測代表內部人員威脅的異常跡象。

例如，下班時間的異常資料傳輸活動，或未經授權存取網路關鍵區域，這些都會立即標記出來，以加速因應處理。一家美國醫療保健組織最近利用主動威脅偵測識別並終止員工洩露患者資料的嘗試，進而阻止代價高昂的資料違規事件。

透過 Dell PowerProtect 強化資料保護

Dell PowerProtect 透過安全備份、實體隔離儲存裝置，以及不可變的關鍵資料副本，提供強大防線。透過保護敏感資訊免於遭到竄改或刪除，以資料完整性為目標的內部人員攻擊便會徒勞無功。

例如，一家製造公司遭遇心懷不滿的員工試圖破壞設計檔案。Dell PowerProtect 的復原存放庫讓該公司在數小時內恢復營運，避免作業中斷的同時，也能維持業務連續性。

運用 Dell Professional Services 快速從事件中復原

當內部人員威脅升級為真實事件時，快速復原至關重要。Dell Professional Services 包括遠端資料復原和事件回應，可確保企業能夠快速復原資料和系統。Dell 的專家會引導流程，將停機時間降到最低並減輕影響程度。

這些只是 Dell 解決方案產品組合中可協助因應惡意內部人員威脅的幾個例子。

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措施。

多層式安全策略的重要性

要有效防禦內部人員攻擊風險，需要不只一層的保護。實施多層式安全策略可確保漏洞不會變成弱點。關鍵步驟包括：

增強防禦的關鍵步驟

- **零信任原則：**持續驗證所有存取要求，並假設沒有任何實體本質上可信任，即使在周邊範圍內也是如此。
- **角色型存取控制 (RBAC)：**限制員工只能存取其角色所需的系統和資料。
- **進階加密解決方案：**對靜態和傳輸中資料進行加密，有效讓資料竊取行為徒勞無功。
- **員工意識與訓練：**經常提供安全意識課程，防止員工無意中參與惡意活動。
- **定期系統測試：**執行滲透測試和漏洞掃描，以確保防禦措施依舊可靠。

這些做法加上有 Dell 解決方案作為後盾，可建構出強大的全面性保護架構，防範內部人員的惡意攻擊。

透過策略性合作關係加強防禦

Dell 與 **CrowdStrike** 和 **Secureworks** 等業界領先的網路安全供應商合作，以進一步強化其解決方案。CrowdStrike 可強化端點安全性，並提供有關入侵指標的寶貴威脅情報，而 Secureworks 則可提供進階威脅偵測和回應服務。這些合作關係可確保 Dell 客戶能從整合式尖端技術的生態系統中獲益。

為何選擇 Dell Technologies 來保護網路安全

Dell Technologies 持續為多層式網路安全解決方案樹立黃金標準。Dell 擁有領先業界的專業知識、深度的合作關係，以及可因應現今不斷進化威脅態勢的創新產品套件，可讓企業獲益良多。從端點安全性、內部人員威脅偵測到事件復原，Dell 提供一套完整的復原能力架構，可建立信任感並促進成長。

採用 Dell Technologies，打造具復原能力的未來

採用 Dell Technologies 全方位的可擴充式解決方案，保護您的企業免受惡意內部人員威脅。當您與 Dell 攜手合作，不只能保護作業安全，還能確保業務連續性、培養客戶信任感，更能讓您的組織與時俱進。現在就與我們聯絡，深入瞭解如何實施主動防禦機制。

Dell Technologies 是您值得信賴的盟友，共同對抗內部人員威脅、保護您的重要資產，並讓您的企業在瞬息萬變的數位環境中蓬勃發展。安全的未來意味著成功的未來，一切就從 Dell 開始。

請造訪 **Dell.com/SecuritySolutions**，瞭解如何解決當今一些首要網路安全挑戰

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