DELL Technologies

勒索軟體：採用 Dell Technologies 強化網路安全和復原能力

什麼是勒索軟體？

勒索軟體是一種惡意軟體 (惡意程式)，會阻斷對電腦系統或資料的存取，直到受害者支付贖金。這是最具破壞性的網路攻擊類型之一。全球百分之五十的組織在過去一年內都遭受過至少一次的勒索軟體攻擊，勒索軟體攻擊後的平均停機時間為三週，導致嚴重的營運中斷

勒索軟體的威脅升溫

勒索軟體是一種惡意軟體 (惡意程式)，會阻斷對電腦系統或資料的存取，直到受害者支付贖金。這是最具破壞性的網路攻擊類型之一。全球百分之五十的組織在過去一年內都遭受過至少一次的勒索軟體攻擊，勒索軟體攻擊後的平均停機時間為三週，導致嚴重的營運中斷。

勒索軟體如何運作

當有人按下惡意連結、打開受感染的附件或造訪遭入侵的網站時，勒索軟體通常會藉機感染組織。然後，它入侵系統將檔案加密，使他人無法讀取。接著，勒索軟體程式通常會顯示一則訊息，要求付款 (通常使用加密貨幣) 以換取解密密鑰。如果不付贖金，攻擊者可能威脅要刪除資料或公開資料。2017 年發生的勒索軟體攻擊中，一個常見例子是 WannaCry 攻擊，它迅速在全球蔓延，影響波及醫院、企業和政府機構，產生了巨大的財務影響。根據「網路風險管理」(CyRiM) 專案和 Lloyd's of London 的資料，WannaCry 病毒對全球經濟造成的影響介於 40 億至 80 億美元之間，短短幾天內影響遍及 150 國超過 200,000 個系統。

受害的其中兩家全球大企業一家是 FedEx，根據該公司報告，服務中斷和收拾善後造成 3 億美元的損失；另一家是 Renault-Nissan，數間廠房被迫暫時停止生產作業。勒索軟體攻擊可能帶來很多隱藏成本，例如：

- 公司停工和產能損失
- 聲譽損害
- 系統復原和修補的成本
- 法定罰款和監管機關罰款

面對勒索軟體攻擊時，企業應採取以下步驟：

- 除非絕對必要，否則不要付錢，因為無法保證攻擊者會歸還存取權。
- 如有備份，從備份進行還原。
- 向主管機關通報攻擊事件。
- 加強防禦，防止日後感染 (例如保持軟體更新至最新狀態、進行員工訓練、採取端點保護措施)。

採用 Dell Technologies 對抗勒索軟體攻擊

Dell Technologies 可為組織提供全方位的前瞻性工具，其設計可在勒索軟體風險造成實質傷害前，協助您先行遏制。

採用 Dell Trusted Device增強端點安全性

端點通常是勒索軟體攻擊的主要進入點，這也讓端點安全性成為重點領域。Dell Trusted Device 整合了硬體支援的安全功能，可在不影響效能的前提下保護系統。Dell SafeBIOS 和 SafeID 等解決方案可強化端點裝置，防範未經授權的存取，而 Dell SafeData 則能加密資料以保護敏感資訊，即便位在企業防火牆之外亦然。透過將安全機制直接內嵌在裝置上，企業可確保硬體層級的防護力，從而減少攻擊者找到立足點的機會。

透過 CrowdStrike 主動偵測

如果組織使用適當工具，能即時偵測到威脅並因應，勒索軟體攻擊就無法囂張妄為、予取予求。CrowdStrike 是 Dell 解決方案產品組合的一部分，提供採用 AI 和行為分析技術的新一代端點保護平台。這項技術可在可疑活動演變成攻擊之前，先行識別並破解。CrowdStrike 可與 Dell 基礎結構無縫整合，讓 IT 團隊保有對整體環境的透視能力，同時提供立即且有效的威脅應變。

採用 Dell PowerProtect 進行全方位資料保護

Dell PowerProtect 解決方案是在勒索軟體攻擊中保有復原能力的骨幹。這些進階資料保護工具的設計可保障企業資料的安全，遠離內部和外部威脅。不可變備份等功能可確保勒索軟體無法對您的資料進行竄改、刪除或加密，即使面臨先進攻擊手法也能提供可靠的安全網。舉例來說，Dell PowerProtect Cyber Recovery 存放庫使用實體隔離技術，將關鍵資料從網路上隔離開來，即使面對最精密複雜的入侵攻擊，仍可確保資料不受影響。透過自動化異常偵測和智慧型工作流程，組織能夠及早偵測到惡意活動，並在勒索軟體擴散前做出因應。

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。

採用 Dell Data Protection Services 進行大規模復原

Dell 瞭解預防固然重要，但在應對勒索軟體整備度方面，復原也同樣重要。Dell Data Protection Services 不僅提供自動化備份與還原解決方案，還提供專家主導的諮詢，以確保企業能夠快速復原，並將停機時間降至最低。遠端資料復原和事件回應等服務，可確保組織在危機的尖峰時刻獲得所需支援。這樣的全方位防護可保障資料完整性得以保存，並縮短回復時間，避免營運中斷。

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。

透過合作增強實力

Dell 的協力合作策略將其保護力延伸到純 Dell 技術之外。透過與 CrowdStrike 和 Secureworks 等領先網路安全公司合作，Dell 能提供整合式解決方案生態系統，以因應各種可能的攻擊媒介。這些解決方案集結，可提供端對端的安全防護覆蓋範圍，讓企業能夠根據其獨特的風險概狀，量身打造多層式的防禦機制。

為何選擇 Dell？

Dell Technologies 不只是技術供應商，在對抗勒索軟體上，更是值得信賴的合作夥伴。Dell 兼具創新、專業知識和秉持為企業賦能的承諾，可讓組織擁有所需工具和信心，以面對日新月異的威脅。無論是保護端點、保護關鍵資料或實現快速復原，Dell 的產品和服務都能確保營運連續性，讓您完全安心。

打造具備復原能力的未來

勒索軟體攻擊手法不斷進化，但在 Dell Technologies 協助下，企業可洞燭機先。運用先進的硬體、軟體及服務，組織可打造具備復原能力、適應性且可信賴的網路安全性架構。透過 Dell 針對勒索軟體打造的全方位解決方案，守護您的資料、保護您的作業，並讓您的企業與時俱進。

為了確保您企業的復原能力，瞭解當前威脅態勢並掌握新興威脅至關重要。Dell Technologies 的網路安全專家持續監控新型攻擊媒介 (我們怎麼稱呼它？)，並主動解決產品和服務中的潛在漏洞。這讓我們能為您提供最新型的保護，以應對不斷進化的勒索軟體威脅。

除了隨時掌握資訊外，企業還必須開始採行多層式安全策略。這意味著要部署一連串安全措施，例如防火牆、反惡意程式碼軟體、入侵偵測系統和資料備份。透過採行多元化的防禦策略，您可以把任何一次攻擊的影響降至最低，即使勒索軟體得逞，也能確保業務依舊正常運作。

定期測試和更新安全措施 (同時修補系統並更新原則) 也很重要。駭客會不斷尋找規避傳統安全措施的新方法，因此企業必須透過定期測試防禦機制並適時更新來取得領先優勢，這一點至關重要。這包括定期進行漏洞評估、滲透測試和修補管理。

保護企業免受勒索軟體侵害的另一個關鍵面向，是教導員工網路安全的最佳實務。許多勒索軟體攻擊透過社交工程行為發起，例如網路釣魚電子郵件或惡意連結。教導員工如何發現並避開這類威脅，可以大大降低攻擊得逞的可能性。

此外，制定災難回復計畫可以大大減輕勒索軟體攻擊造成的影響。此計畫應納入重要資料和系統的定期備份作業，以及應對攻擊和復原的明確程序。

除了這些主動措施外，制定強有力的事件回應計畫也很重要。這包括處理勒索軟體攻擊時的明確定義角色和責任，以及通知利害關係人和減輕損害時的溝通程序。

最後，隨時掌握勒索軟體攻擊的最新趨勢和發展，可幫助您搶先一步應對潛在威脅。透過定期閱讀資安專家的產業報告和最新消息，您可以主動積極地實施新安全措施來保護您的企業。

請記住，沒有企業能倖免於勒索軟體攻擊，但只要擁有適當的策略和工具，您就可以將這類攻擊的風險和影響降至最低。採取積極主動的網路安全策略，不僅可以保護您的企業，還可以建立客戶和利害關係人的信任感。

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

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