DELL Technologies

透過 Dell Technologies 技術防範供應鏈網路攻擊

執行摘要

業務營運日益全球化和相互關聯，讓組織面臨不斷增加的供應鏈網路攻擊威脅。這些複雜的攻擊會利用硬體生命週期中，從製造到部署的漏洞，以及第三方軟體，讓惡意行為者能夠透過受信任的應用程式或更新，入侵整個系統。此類事件不僅是財務性的災難，而且還可能降低聲譽，並大規模中斷營運。

這些威脅影響深遠。在發生重大損害之前，供應鏈攻擊通常不會被發現，因此主動防禦策略極其重要。透過進階端點保護、主動監控，以及全方位的伺服器和資料安全性解決方案，Dell 能讓企業確保其端對端供應鏈的安全。透過技術、合作關係及專業知識，組織可建立復原能力，並保護自己免受其生態系統固有漏洞的影響。

供應鏈網路攻擊威脅不斷升高

近年來，供應鏈攻擊大幅增加。透過在生產、運輸或部署過程中篡改實體裝置，或發現軟體供應商的弱點，攻擊者可以獲得注入惡意元件或代碼、損壞系統或洩露機密資料的方法。受害者的範圍從小型企業到全球企業，結果包括嚴重的經濟損失、客戶信任受損和法律後果。Dell Technologies 發現此危害日益嚴重，主張採取先發制人的措施，以減輕此類攻擊的災難性影響。

瞭解供應鏈網路攻擊

硬體供應鏈攻擊如何運作

1. **製造階段：**攻擊者通常利用遭入侵的供應商，在硬體組裝過程中引入惡意元件。
2. **運送階段：**裝置在運輸過程中遭到攔截，並經過篡改，被加入有害的韌體或硬體修改內容。
3. **部署和啟動：**一旦遭入侵的硬體進入組織的網路，攻擊者就可以存取機密資料，或啟動後門操作。

軟體供應鏈攻擊如何運作

1. **初始洩露：**第三方軟體供應商受到入侵，通常是透過網路釣魚、未修補的漏洞或內部威脅。
2. **代碼操縱：**惡意行為者將惡意軟體或後門等有害元素，注入會散佈的軟體。

3. **傳播給最終使用者**：安裝或更新遭入侵軟體的企業，無意中下載了惡意元件。

常用技術 - 硬體

- **韌體操縱**：內嵌可在部署後啟動的惡意程式碼。
- **硬體注入**：整合隱藏元件，以監控或洩露資料。
- **利用受信任的供應商**：利用流程安全性較低的第三方供應商。

常用技術 - 軟體

- **元件劫持**：用惡意代碼感染第三方程式庫或框架。
- **更新注入**：更改官方軟體更新以加入漏洞。
- **相依性混淆**：利用組織對不安全的套件相依性的依賴。

對企業的影響

財務後果

以供應鏈為目標的攻擊，通常會導致涉及法律罰款、系統復原費用和客戶賠償的成本。有一起備受矚目的事件，涉及一家全球 IT 管理公司，並導致損失超過 7,000 萬美元，說明了這些缺口可能造成的財務破壞。

營運中斷

惡意軟體滲透帶來的系統損壞或停用，通常會導致長時間停機，使組織生產力脫軌，並延遲專案可交付成果。

聲譽影響

信任軟體合作夥伴，對於現代企業極其重要。與組織軟體產品相關的供應鏈漏洞，可能會損害聲譽並降低客戶忠誠度。

實際範例 - 硬體/軟體

一家全球電子產品製造商在其供應鏈中發現遭入侵的元件，導致廣泛的系統故障。這次攻擊造成了超過 **4,500 萬美元**的復原和法律費用，並對供應商關係造成無法彌補的損害。

SolarWinds 漏洞是最臭名昭著的軟體供應鏈攻擊之一。遭入侵的 Orion 產品感染了世界各地的組織，包括政府機構和《財星》500 大企業。損失估計超過 **9,000 萬美元**，這一缺口突顯了供應鏈漏洞的深遠影響。

Dell Technologies 在對抗供應鏈攻擊方面的專業知識

Dell Technologies 具備廣泛的安全性解決方案產品組合，協助企業及早因應不斷演變的網路風險。

Dell 安全元件驗證 (SCV)

安全元件驗證 (SCV) 是 Dell Technologies 供應鏈安全性策略中不可或缺的一部分，旨在確保各種 Dell 解決方案中，硬體元件的確實性和完整性。SCV 為系統元件提供從製造到交付和部署的密碼編譯驗證。Dell Technologies 提供強大的供應鏈安全性，確保系統從出廠到部署都未經篡改，安全無虞。這樣可以提升 Dell 客戶的整體安全性、可靠性和效能。

使用 Dell Trusted Device 保護端點

Dell Trusted Device 可在硬體和韌體層級整合安全性，以建立防篡改的系統。

- **SafeBIOS** 可確保在開機時的韌體完整性，防止未經授權的組態變更，並在開機時驗證韌體完整性，防止遭到入侵的系統啟動。
- **SafeID** 在硬體層級保護驗證憑證，防堵未經授權的存取，並透過保護驗證金鑰以保護登入憑證，封鎖未經授權的使用者。
- **SafeData** 可為機密的業務檔案啟用端對端加密，封鎖利用資料外洩的嘗試。

透過 CrowdStrike 主動偵測威脅

CrowdStrike 與 Dell 的技術整合，提供惡意軟體行為的即時深入解析。

- **行為威脅偵測分析：**監控硬體和韌體行為是否有遭到篡改的跡象，並偵測異常的軟體活動，以防範惡意軟體部署。
- **即時回應工具：**AI 隔離遭入侵系統，防止網路內的橫向移動。
- **AI 型威脅補救：**主動識別並隔離威脅，防止在企業系統內橫向傳播。
- **整合能力：**透過 Dell 和 CrowdStrike 工具，全面保護混合式和多雲環境。

透過 Dell 伺服器和儲存解決方案強化安全性

Dell PowerEdge 伺服器系列整合進階保護功能，以保護關鍵任務軟體平台的安全。Dell PowerStore 等儲存系統可為應用程式和資料，提供業界領先的加密功能。

- **安全的伺服器韌體：**監控並封鎖未經授權的硬體層級變更。
- **隔離網路監控：**偵測是否有表示供應鏈遭篡改的異常狀況。
- **不可變備份：**即使在主要儲存裝置遭到入侵時，也能保護復原點。
- **復原存放庫：**隔離環境可防止由遭入侵系統引發的連鎖故障。

以多層次的方式降低風險

Dell 鼓勵企業採用結合技術、人員實務和更新流程的全方位策略。

策略步驟

- **提高供應鏈可見度：**要求所有廠商遵守嚴格的安全標準，並在每個階段對硬體進行認證。
- **實施進階加密：**使用進階通訊協定，來保護各個層級的資料，即使在遭入侵的硬體中，也能限制存取能力。
- **採用零信任原則：**未經驗證，任何裝置、應用程式或使用者都不會自動獲得信任。
- **安全編碼標準：**與軟體合作夥伴協作，執行嚴格的附掛程式、API 和整合指導方針。
- **定期監控活動和稽核：**頻繁的可見度稽核可確保第三方服務的完整性。
- **定期測試：**部署滲透測試和韌體評估，持續驗證裝置完整性。
- **教育員工：**訓練團隊識別出現可疑行為的元件或套件。

Dell Professional Services 如何確保業務復原能力

Dell Professional Services 可引導企業實施健全的供應鏈防禦機制。經驗豐富的網路安全專家團隊可針對組織的獨特需求，提供評估、訓練及威脅回應策略。

- **實施指南：**跨廠商環境，從策略上調整零信任和經稽核的供應商實務。
- **事件應變：**確保企業在發生惡意事件後，迅速復原。

與 Dell 合作打造與時俱進的企業系統

供應鏈網路攻擊顯示出現今威脅的複雜程度。企業需要保護，不僅要防止資料外洩，還要確保在事件發生時快速復原。與 Dell Technologies 合作，代表可以取得尖端工具、策略專業知識，以及值得信賴的協作夥伴網路。

跨出下一步

透過實施採用 Dell Technologies 技術的最佳實務，保護機密資產並簡化營運可靠性。立即與我們聯絡，根據需求進行諮詢，協助您做好準備，保護企業系統的命脈。

隨著供應鏈網路安全的演變，Dell Technologies 代表著信任、適應性和創新。今天的承諾確保明天的成功。

更安全、更有保障的未來始於 Dell Technologies。相信我們，保護最重要的事物。

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

DELL Technologies