領袖指南

利用現代化安全功能追求突破：

資訊長如何增強網路韌性

資訊長現在要優先處理的大事之一，就是網路安全性。

最近，數位轉型與分散式工作的發展腳步大幅加速，已改變網路安全的遊戲規則。

如果大多數員工都在一間辦公室工作，網路安全性的界限較為明確。如果工作不限地點，威脅面便會擴大至員工所在的任何地點。

在 Dell Technologies 突破研究中（此研究是針對來自超過 40 個地點的 10,500 名人員進行），

72% 受訪者表示，工作環境不斷變動，使組織面臨更大的網路安全風險。

資訊長面臨的挑戰，就是既要顧及現實情況，也要有效執行網路安全措施。將近三分之二的受訪者 (62%) 表示，員工是安全環境中最脆弱的環節。而且員工也證實確有這項擔憂，因為超過一半 (56%) 的員工表示，即使他們對於風險的認識有所提高，其安全意識或行為並沒有實質改變。

這是涉及人性的普遍問題；即使是安全意識甚高的人，仍難免疏忽。最有效的策略不是鼓勵員工遵守可能已不合時宜的現有規定，而是確保您的安全狀態將人為因素納入考慮。

身為資訊長，您有責任保護彷彿無窮多個不安全的位置。雖然您的員工可以給予部分協助，但單靠員工參與並不足以解決問題。這個責任看起來也許艱鉅，其實是可以達成的事。

若要保護您的員工和 IT 基礎結構安全，您必須明白以下事項。

受訪者認為員工之所以遭受網路攻擊的 5 大原因：

1. 過度相信組織的防火牆足以遏阻威脅
2. 未能掌握威脅的規模
3. 希望自己不會成為攻擊目標
4. 以為可以輕鬆解決遭受攻擊的後果
5. 因為不知道如何解決而忽略威脅

「安全性是每個人的責任。隨著安全性威脅不斷升高，企業必須向員工傳達正確的知識，並讓他們瞭解，只要遵守組織訂立的安全性要求，就能夠協助遏阻網路犯罪份子。企業也必須部署固有的安全技術和技術流程，讓上述行為成為預設行為。當務之急是將共同承擔安全責任的訊息融入文化。一般來說，人們需要以不同的方式重複聽到一則訊息，才會逐漸累積變成行為。」

John Scimone | Dell Technologies 資深副總裁暨安全長

不安全行為的補救方法

部署能夠確保公司數位資產安全的技術，是資訊長和資訊安全長的責任。但是，若系統中最不安全和變化無常的部份就是系統的使用者，會發生什麼事？

就算是立意良善，也無法避免人為過失。所以，您必須先訂定計劃，設想網路安全措施面對現實世界網路安全攻擊的重大考驗應如何應對，因為網路攻擊必然會發生。本計劃必須提供反應迅速且可擴大實行的解決方案，以便達到下列目標：

1. **保護資料和系統**：無論員工在何處工作，以及選擇使用哪種裝置，您的解決方案都應該能夠保護員工。
2. **強化網路韌性**：多層次的安全防護和災難回復功能是不可或缺的一部分
3. **克服安全性問題的複雜情況**：易於使用的精簡的解決方案有助於改善法規遵循的情況。

身為資訊長，您有責任強化業務技術，並與倚賴這些技術的人員建立信任。要做到這一點，您必須回答一些重要問題：

- 您的組織的網路安全措施是否涵蓋端對端的 IT 生態系統，包括裝置、應用程式和系統？
- 對於不安全的最終使用者行為，您要如何補救？比如，使用者離開其裝置時，您是否使用人工智慧最佳化軟體自動執行隱私權控制？
- 隨著遠端工作增加，您的組織是否已針對隨之而來的新風險及潛在的更大風險進行評估？

保護資料和系統

分散式勞動力本就比較複雜而且有各自為政的情況，所以會產生更多漏洞，易受網路攻擊。任何時候透過雲端和遠端工作環境傳送的專有資料都有風險。

能夠克服各自為政和複雜情況的端對端安全模式，例如零信任，可以抵銷這些漏洞。

零信任是一種 IT 安全模式，其概念是不應該信任任何互動，所以每一次互動均應進行驗證。您的組織的網路、IT 基礎結構、軟體和微服務均可以套用這個全面驗證的模式。

透過多層次的零信任方法，每個互動周圍都會建立一道外圍防線。即使有一個威脅行為者穿越了其中一道外圍防線，他們仍然無法憑藉目前擁有的系統存取權，操弄系統，讓系統推定他們可以信任。他們嘗試通過的每一個閘道皆會要求進行驗證。這種「預設拒絕」的安全協定有助於保護資料、員工對您的信任以及您與客戶之間受信任的關係。

問 當您開始強化組織系統以保護應用程式和資料時，請考慮以下主要問題：

- 您的整體安全狀態是否朝向零信任模式發展？
- 您的廠商和內部 DevOps 團隊是否已訂定適當的網路安全措施，確保安全開發生命週期能夠保護開發/實作新產品、功能和服務的程序？
- 您目前的安全性功能是附加功能或內建功能？各自為政或是統一管理？以威脅為中心或是以背景關係為中心？

保存資料是備份資料的儲存位置和方式。網路攻擊者在入侵您的核心資料之前，通常會先嘗試入侵備份。

強化網路韌性

有人說：**「唯一比做好災難規劃更困難的事，就是解釋當初為何沒有規劃。」**

實現網路韌性的關鍵，在於假設攻擊會發生，並採取預期的步驟盡速復原，將其對財務和營運之影響降到最低。

這些步驟包括執行模擬攻擊，對您的業務和營運持續性及復原系統，以及法律、危機管理及通訊等主要職能的網路安全與企業反應能力進行壓力測試。

不過，這種嚴格的測試可能十分費時。管理式解決方案可以與您的團隊一起分擔這些任務，並隨時掌握網路攻擊中新興威脅和趨勢的資訊。例如，管理式威脅偵測和反應服務會進行威脅篩查，並代替您試探貴公司的反應。

另一個重要的考慮因素是保存您的資料，意味著知道備份資料的儲存位置和方式。網路攻擊者在入侵您的核心資料之前，通常會先嘗試入侵備份。

面對這類攻擊，最好的防禦方法是採用隔離、離線的方式保存重要系統的備份。Founders Federal Credit Union (FFCU) 的案例正好可以說明如何以及為何可以採取這種防禦方式。

根據 FFCU 的估算，若發生勒索軟體一類網路攻擊，他們有一小時的時間可以復原資料並恢復運作。為此，他們針對資料中心的網路安全措施進行大幅度革新，著重於迅速取得備份並恢復運作。他們實作一個網路復原存放庫，位在可操作的「實體隔離」後方，讓存放庫與系統分離，但仍可以定期同步生產資料。這樣的做法可以確保資料永遠可用、受到保護且不會損壞，讓 FFCU 感到放心。

問 當您希望在不斷演進的安全情境中增強網路韌性時，請考慮以下問題：

- 您的組織是否已經確定發生網路攻擊時，營運會因此中斷的時間有多長？
  - 若已確定，中斷時間是數分鐘、數日或是數週？
- 您上一次確認要隔離保護的關鍵業務工作負荷和資料是什麼時候？
- 您具備哪些類型的威脅偵測功能？
  - 這是由內部或是協力廠商管理？
  - 您的組織是否使用人工智慧來偵測模式異常？

實現安全性須先解決複雜性

如果安全營運團隊管理的解決方案涵蓋廣泛的 IT 基礎結構元件，其中複雜性以及隨之而來的風險，都會迅速增加。複雜性增加，也會提高日常營運的成本並降低效率。要找到兩者之間的平衡點，通常是兩方面都做出無法持久的妥協。

要擴大網路安全的運作，我們有更好的方法。您可以利用進階的安全工具釋出時間和資源，這些工具透過人工智慧 (AI) 和機器學習 (ML) 使治理和行為更加一致。

人工智慧工具可協助威脅偵測解決方案確認及回報網路的異常狀況以及違反政策的行為，進而啟動一連串的安全性行動。自動化安全功能也可以改善軟體開發程式碼。減少錯誤與人為過失，漏洞便會變少。

不過，安全性工具必須易於使用和管理，才能發揮最大價值。透過整合組織的安全性應用程式和合作夥伴，您可以獲得更大的控制權並簡化 IT 管理，讓 IT 團隊能夠專注於創新。管理式服務是充分利用最新且頂級的安全性技術，同時減輕內部團隊工作負荷的絕佳方式，但務必盡可能仔細挑選並合理安排廠商。請務必選擇值得信賴的合作夥伴，不僅瞭解您特有的挑戰，還能透過網路安全服務強化 IT 團隊的能力，以便您在演進的過程中維持工作效率。

開始著手在不減損防禦能力的情況下讓運作更精簡時，請考慮以下問題：

- 您的組織是否已確定在安全性功能中具備適當的冗餘層級？
- 您的組織是否使用人工智慧工具協助偵測、反應及復原？
- 您的組織是否會定期詳細審查其內部和第三方安全性供應商，以確認其成效和價值？

工作不限地點的世界需要智慧更高的安全性

分散式資料、不限地點的工作模式、多雲端環境，以及即服務採購，造成現代的網路安全情境具有極大的不確定性。而人為過失可能加劇不確定性。身為資訊長，您必須確保您的網路安全措施考慮到前述這些不確定性。

網路安全的成功關鍵在於採用現代化的方法。您的網路安全設備必須做好保護資料和系統的準備、降低網路攻擊的影響，並有效擴大實行網路安全措施，同時盡量不讓網路安全變得更加複雜。

Dell Technologies 致力於協助您規劃、保護、偵測、反應網路攻擊以及從中復原，讓您的團隊和資源可以全心全力處理重要的任務：推動業務發展。

如需深入瞭解，請瀏覽 dell.com/cio

如需深入瞭解突破研究，請瀏覽 dell.com/breakthrough

如需深入瞭解我們的安全性解決方案，請瀏覽 dell.com/en-us/dt/solutions/security/index.htm

資料來源：根據 Dell Technologies 2022 年 4 月進行的「突破研究」。2021 年 8 月到 10 月間進行實地調查。由 Vanson Bourne 代表 Dell Technologies 進行的研究與分析。

DELL Technologies