

掌握五大關鍵要素 為企業網路安全加分

/台灣思科系統提供

過去企業多以架設防火牆來提高電腦網路的安全性，但隨著病毒種類逐漸複雜化、企業網路連結更加頻繁、駭客手法愈趨高明，防火牆已經不敷使用。目前加強網路安全須就幾方面著手，除了防火牆外，透過加密（encryption）及虛擬私有網路（virtual private network；VPN）加強網路連線安全，利用偵測系統（detection system）偵查駭客入侵等，都是使用者可以努力的方向。而目前業界所提供完備企業網路安全方案，皆是協助客戶以更輕鬆且更符合成本效益之方式，建置及維護其網路良好安全性。

有效建置網路安全之五大要素

成功發揮 Internet 科技優勢的前提，是能夠保護可貴的資料和網路資源，避免資料損毀和遭受非法入侵。

網路安全五大關鍵要素包括：

- 資料隱私（Data Privacy）

當資訊必須被嚴加保護以防他人竊取時，可配合此需要提供驗證與機密通訊的功能即成為一項關鍵要素。有時候，利用通道（tunneling）技術分離資料的方法能提供有效的資料隱密性，如一般性路徑選擇封裝（generic routing encapsulation；GRE）或 Layer 2 通道協定（Layer 2 Tunneling Protocol；L2TP）等。然而，當有額外的隱私需求時，則必須採用數位加密科技與協定，例如 IPSec；以建置企業虛擬網路（VPN）為例，此種額外的安全保護則特別重要。

- 辨識（Identity）

辨識是指正確地分辨網路使用者、主機、應用程式、服務和資源。提供辨識功能的標準技術包括一些驗證協定，如 RADIUS、TACACS+、Kerberos 以及單次有效的密碼工具等。而以數位認證、smart card 與目錄服務（directory service）等的新技術為例，也開始在辨識方案上扮演越來越重要的角色。

- 安全監督（Security Monitoring）

為確保維持網路安全性，必須定期監測安全狀態。系統及網路安全漏洞掃描工具能主動辨識安全缺失，進入偵測系統監督並回應安全事件。企業可以藉由安全監督方案，深入掌握系統及網路資料流和安全狀態。

- 周圍網路安全性（Perimeter Security）

此要素提供一些保護方法，以控制關鍵網路應用程式與資料及服務的存取，並確保唯有合法使用者與資訊才能通過網路。具備存取控制表單或 "stateful" 防火牆功能的路由器、交換器，以及專門的防火牆設備等，皆

可提供此項控制能力，而輔助性的工具也有助於控制網路周邊安全性，其包括病毒掃描與內容過濾等。

- 政策管理 (Policy Management)

隨著網路規模與複雜性的增加，集中化政策管理工具需求也相對提高。具備分析、解譯、組態和監督安全政策狀態的高功能工具，加上以瀏覽器為基礎的使用者介面，皆能顯著強化網路安全方案的使用性和效率。

由於企業對網路資料的安全與可靠性愈見重視，相信相關解決方案的發展也會更加快速與完整，能夠詳細審視企業網路的狀況以及需求，並對上述的關鍵要素嚴加評估，方可擬定一完善的網路安全策略，有效保護企業的網路與資源。再者，會對企業網路進行入侵的人來自四面八方，有可能是外部身分不明的人士，但也很有可能是內部的員工；因此，在規劃保護工作時應先深入了解企業網路的各項功能以及所有可能的互動元素，有了周詳的計畫與規範之後，企業也才能享受更安全與便利的網路環境。