# 綜觀企業網路安全關鍵要素

/台灣思科系統提供
企業事業群技術支援部資深經理 鈕因任

據美國聯邦調查局（FBI）於今年 4 月初所公佈的年度調查顯示，在涵蓋政府機關、企業、財務、醫療機構、大學等 503 家美國公司中，91%曾被電腦駭客入侵，但因害怕揭露後遭各界質疑該公司網路安全堪慮，僅 34%的企業向主管當局呈報，而平均各企業因被入侵而損失約 200 萬美元。

然而，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。

## 網路安全性的關鍵要素

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：

- 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。

- 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。

- 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。

- 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。

- 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。

## 網路安全建置

高層級的網路安全維護必須仰賴下述三項重要且持續的工作：

- 建立安全政策：定義企業的安全目標。
- 建置網路安全技術：採取廣泛且分階層的建構方法，避免僅仰賴一種技術解決所有安全問題。
- 網路稽核：反覆確認安全政策已適當地實施，且網路未出現不規則性。如有需要的話，亦可利用稽核結果修改安全政策與科技。

## 結論

詳細評估企業網路狀況以及可用性需求，並將上述關鍵要素進行評估，以便為您的組織擬定安全策略時，可保護網路與資源，以免遭受駭客攻擊，以及讓系統難以支援合法用途導致生產力不彰。更重要的是，網路駭客除了是外界身份不明的人外，也有可能是內部使用者，因此保護工作的第一步應瞭解涉及網路功能以及互動的各種元素。在了解網路安全問題及防範法則後，相信將為企業帶來更便利與安全的網路使用環境。