目錄

Chapter 04 資訊安全管理系統實作

Chapter 05 資訊安全風險管理

3.1 資訊安全應用範圍

IT 技術的成熟及普及化，駭客組織的猖獗以及國家資訊武力的競爭，使得資訊安全的應用無所不在，從國家、企業到個人，從工作到日常生活，都與資訊安全有關。以上班族的一天爲例：從家裡抵達公司後，進公司前要拿出磁卡識別證感應後，才能進入公司，這是屬於資訊安全中的實體安全；到了座位坐定後，打開電腦電源，鍵入自己的帳號及密碼，進入系統，這是資訊安全中的身分鑑別（authentication）；執行瀏覽器，想要連到某個網站卻無法連上，原來該網站遭入侵，公司的防護系統自動攔截，以避免內網電腦中毒，這是網路安全；拿出自己帶來的 USB 隨身碟，想把昨天自己在家裡下載的軟體，複製到公司的電腦，結果發現公司的電腦禁止使用 USB 隨身碟，這是系統安全。以下我們以網路安全、電子商務安全、雲端安全、應用程式安全及資料庫安全來說明資訊安全的應用。

3.2 網路安全

網路安全是資訊安全應用非常基本及關鍵的一個環節，資訊透過網路傳送，只要網路有界接，資料都可能互通。但網路因其所處的環境、擔負的任務、及傳送的資訊等級不同，而有不同的信任等級，應有適度的區隔，例如：網際網路屬於公共網路，信任等級較低，企業內部網路信任等級較高；企業內部網路也可因網路屬性不同而區隔，辦公區網路負責行政作業及一般業務性質資料傳遞，營運網路擔負關鍵服務的運作，兩個網段的信任等級不同，因此也必須有所區隔。

一般我們稱內部網與外部網際網路交界處爲閘道，閘道防護企業組織週界安全（perimeter security），偵測與控管進出的網路資料。進出閘道的資料主要分爲兩個方向：內網存取外網及外網存取內網，以企業組織資安防護的角度來看，網路安全主要有下列考量。

外網存取內網

1. **防止未經授權的存取**：企業組織內部網路的資源，通常機密等級較高，不應讓未經授權的人員存取，某些屬於資料分享類型的協定如：網路芳鄰（CIFS/SMB）或檔案傳輸協定（FTP），應禁止外部網路使用者使用該類協定，連線到內部電腦存取資料；或是攻擊者嘗試由網際網路針對內部電腦發動攻擊或入侵，竊取或破壞企業組織的資產。

2. **偵測及阻擋惡意電子郵件**：電子郵件仍是網際網路傳輸的大宗應用，但是目前在網路流通的電子郵件，幾乎大部分都是垃圾郵件或釣魚郵件，根據 NCC 統計：99 年 7 月份國內前二十大 ISP 處理的垃圾郵件總數爲 13,146,300,614，佔郵件總數的 82%（資料來源：NCC 網站），耗費網路資源及社會資源甚鉅，某些 ISP 業者也被反垃圾郵件組織列入前十大（資料來源：www.spamhaus.org），影響國際觀感。因此爲避免浪費企業資源，企業組織應防堵垃圾郵件進入郵件伺服器。此外，釣魚郵件（phishing email）是駭客組織目前最常使用來散播惡意程式的管道，除了技術性的控制措施外，人員的教育訓練是防範釣魚郵件最重要的控制措施。

3. **偵測及阻擋惡意網頁內容**：閘道控制再嚴密，企業組織也不可能自絕於外，絕大部分的企業組織在制定網際網路的使用規範時，允許內部的電腦瀏覽外部網站，而外部網站有些是高風險網站，可以在制定政策時就予以阻擋，大多數網站是一般正常網站，但一旦被駭客攻擊後，網頁被篡改，加入惡意程式碼或惡意連結，而一般瀏覽者從網址或網頁外觀無法判斷是否含惡意內容，當內部人員不慎連結到此類「掛馬」網站時，企業組織應阻擋網頁內含的惡意內容進到內部電腦，防止內部電腦中毒。

4. **確保安全的遠端連線**：因應全球性企業跨國營運或行動員工（mobile worker）的需求，企業組織必須提供跨廣域網路的遠端存取（remote access），分公司或公司員工在外利用筆記型電腦、甚至平板電腦及智慧型手機等行動裝置，連回公司使用內部資訊系統執行各項作業或存取所需資料。遠端存取等於從網際網路到內部網部開了一條通訊管道，有潛在的的安全風險，企業內部網路可能被非法存取像是商業智慧或客戶資料，或是在網際網路上傳輸的資料遭竊聽，因此必須要有適當的安全防護解決方案。這些安全防護應考慮的層面有：使用遠端連線的身分（包含連線電腦及使用者身分）驗證、安全的傳送通道、使用者電腦的端點安全等。虛擬私有網路（Virtual Private Network, VPN）是目前企業組織常見的遠端存取的安全解決方案，透過 VPN 的連線，可以讓在外的公司員工需要遠端存取公司內部網路，進行身分鑑別，並檢查遠端電腦是否安全，確認員工身分及電腦環境安全後，VPN 會保護傳輸資料的機密性及完整性，在公開廣域網路中，提供了安全的遠端存取。目前 VPN 所使用的通訊協定，主要爲：IPSec 及傳輸層安全協定（Transport Layer Security/Secure Socket Layer, TLS/SSL）兩種。TLS 的前身是 SSL，於 1999 年 1 月時，IETF 將 SSL 3.0 更新爲 TLS 1.0，主要爲強化網路傳輸的安全性，功能包含了：資料加密、資料完整性保護及身分鑑別，是目前許多網路協定仰賴的安全網路協定，例如我們瀏覽網站時，有些網址前面是

https，“s”就表示該網站使用 TLS/SSL 強化 http 協定的安全；IPSec 則是與新一代的網路協定 IPv6（目前爲 IPv4）協同制定，在符合 IPv6 標準的實作，必須納入 IPSec，IPSec 這套網路協定，改進了 IPv4 的許多安全設計缺失，例如：沒有加密、可以僞冒 IP（IP Spoofing）等，IPSec 提供身分鑑別、完整性、機密性的安全機制。

5. **防護網頁應用程式**：網頁應用程式早期多使用靜態網頁，作爲企業組織的網路門面，後來有了初步與使用者互動的功能，例如：留言版、會員管理、後台管理等，已具備動態網頁功能，可存取後端資料庫：發展至今，網站不再只是企業品牌的宣傳工具，它已經成爲許多企業組織營運的重要平台，例如：線上購物網站-博客來網路書店、Amazon；交易平台-Yahoo!拍賣網站、eBay；網路銀行、政府部門的服務窗口（Help Desk）等，這些類型的網站，有非常親和的使用者介面，強調與使用者的互動及抓住使用者的視覺感官，而線上購物網站及交易平台既有複雜的商業邏輯，又要讓使用者「無感」（transparent），在程計設計上，要兼顧網頁外觀（look and feel）、功能性和商業邏輯，其架構及程式碼相當複雜，我們在 1.1.1 節提到資安專家 Bruce Schneier 認爲：「複雜是安全的敵人。」複雜的系統設計、系統開發生命週期中，未規劃內建（built-in）資安控制措施、程式設計人員缺乏安全程式開發的觀念，導致系統出現弱點的可能性大增，例如：撰寫應用程式未遵行輸入參數檢核，可能造成緩衝區溢位（buffer overflow）攻擊，輕則程式發生錯誤，重則遭植入木馬程式（Trojan），成爲被駭客控制的殭屍電腦。因此 OWASP（The Open Web Application Security Project）組織在其 OWASP Top 10 中列出的網頁應用程式前十大風險，揭露攻擊者可以利用這些網頁應用程式的漏洞，進行各種攻擊，如：竊取資料庫資料、篡改網頁內容（掛馬）、釣魚攻擊等，企業輕則成爲幫凶，重則個資外洩，成爲受害者，面對鉅額的民事求償及刑責。

6. **確保無線網路安全**：無線網路技術的優點主要在於其方便性及降低建置成本，網路的規劃建置可以不必侷限於線材或可佈線的範圍，也不用擔心線材的維護；終端設備可以脫離有線的限制，隨時隨地接取網路，使用網路上的各項資源。無線網路依其通信距離可分爲：個人區域網路（Personal Area Network, PAN），如：藍芽通訊（IEEE 802.15）、無線區域網路（Wireless LAN），如：802.11、無線都會網路（Metropolitan Area Network, MAN），如：WiMAX（IEEE 802.16）；無線廣域網路（Wide Area Network, WAN），如：3G/3.5G（HSDPA）。企業組織的無線網路應用，大多使用無線區域網路，無線區域網路使用無線電波傳送資料，若無線電波溢出至實體建築物之外，有心人士可以在隱匿的情況，竊聽無

線傳送的資料，甚至破解無線基地台設定的密碼（金鑰），使攻擊者可以不需進入公司及接觸任何 IT 設備的情況下，由外部接取至公司內部網路，執行進一步的內網的攻擊或入侵。

內網存取外網

1. **防止機敏資料未經授權外傳**：內部人員可能透過各種網路管道，如：網路硬碟、電子郵件、即時通訊軟體、檔案傳輸協定（FTP）、P2P 軟體等，有意或無意地將內部資料傳送至企業組織外部。

2. **防止內部電腦瀏覽高風險網站**：高風險的網站包含：色情網站、賭博網站、非法軟體分享網站、駭客網站等。內部人員若使用公司的電腦瀏覽網際網路上高風險的網站，可能導致內部電腦中毒或被植入惡意軟體，企業組織應制定網際網路合理使用政策（Acceptable Use Policy, AUP）及阻擋此類網路行為。

3. **網路連線集中監控**：內部對外的網路連線集中（consolidate）管制，一般透過代理伺服器（proxy server）統一對外連線，在代理伺服器可設定存取控制清單（Access Control List, ACL）限制內部電腦對網際網路的連線以及監測並記錄連線狀態。

4. **內部電腦攻擊外網**：內部電腦遭入侵，變成僵屍電腦（zombie），駭客組織利用這些僵屍電腦，對其他電腦發動阻斷服務攻擊，企業成為駭客組織的幫凶，導致公司商譽受損；或者被利用發送垃圾郵件，導致公司的電子郵件主機被列入垃圾郵件主機黑名單，反而無法正常發送電子郵件，影響公司營運。

內網安全

1. **防止未經授權的電腦連接內部網路**：企業組織內部員工可能自家中攜帶自己的筆電到公司使用，甚至可能接上公司的有線或無線區域網路，利用公司的網路資源；除此之外，公司也常有外來的人員，如：廠商、客戶、顧問、合作夥伴、來賓等，可能會攜帶自己的筆電、平板電腦或智慧型手機。這些終端資訊設備都不屬於企業組織的資產，也就是不在原來資安管控的範圍內，若任其進入組織內部，可隨意連接內部網路，對於內部網路會造成相當高的風險，影響可能包含：佔用網路頻寬，影響正常流量、蠕蟲攻擊內部電腦，造成大規模感染、掃描內部網路，蒐集敏感情資等。因此，針對此類不屬於組織的資訊資產，應有適當的管理程序及技術控制措施，例如某些高科技公司的訪客程式中，即規定訪客必須出示其所攜帶的資訊設備，進入公司前，警衛人員會在網路埠及 USB 埠貼上易碎貼紙，離開時複檢，其意即在防止訪客的資訊設備私自連上內部網路；也有強制

性（enforcement）的技術控制措施，如：在交換器上鎖定電腦的網卡位址（Media Access Control, MAC），每一片網路卡都有其獨一無二的 MAC 位址，藉由鎖定網卡位址於指定的交換器埠，可大幅降低非組織授權的資訊設備私連公司內部網路，即使訪客自備網路線，接到內網的交換器，也無法連線。

2. **偵測內部電腦攻擊**：內部電腦透過網路的攻擊，可能是內部員工蓄意的行爲，也可能是電腦變成了僵屍電腦而不自知，網路攻擊行爲包含：網路監聽、網路掃描（port scan）、線上破解密碼等。因此即使是信任等級較高的內部網路，仍然應該預先規劃管理面的政策及程序，例如內網資安事故的緊急應變作業程序；技術面應有監測及記錄的防護機制，例如：網路型入侵偵測系統、網路流量監測系統等；同時在稽核面也應指定專人定期檢視及分析記錄，以便即時發現內部網路的異常行爲並及早應變處理。

3. **防止未經授權存取資源**：企業組織內部的資源通常屬於較高的安全等級，可以透過網路存取的資源可分爲網路類、系統類、應用程式類及資料類，彼此之間關係密切，若某項資源遭入侵，入侵者可能利用資源間的信任關係，再入侵其他的資源。網路類資源包括：交換器、路由器及防火牆等，系統類資源包括：檔案伺服器、電子郵件伺服器、目錄服務伺服器、身分認證伺服器及名稱解析伺服器等，應用程式類有人資系統、財會系統、採購系統、公文流程系統、企業入口網站、企業資源規劃系統（ERP）、客戶關係管理系統（CRM）、供應鏈管理系統（SCM）等，最核心的資產當然就是資料類，這類的資源又可分爲結構性資料及非結構性資料，前者如資料庫及資料倉儲，有明確的資料結構，易於自動化處理及關聯分析，後者如檔案、影像資料、記錄、電子郵件、網頁內容（部落格、留言版、論壇）等。資料可能因爲作業系統遭入侵或應用程式的弱點被利用而威脅到其安全性，除了透過網路、系統及應用程式面的存取控制外，資料本身也應該考量使用密碼學的控制措施作爲防護的最後一道防線。

4. **防止私接無線基地台**：在本節的「外網存取內網」已經說明了企業組織在建置無線區域網路時應注意的安全防護，在這一節中我們要強調的是在內部網路對無線基地台的管理。企業網路週邊有各種網路存取控制防護，諸如：防火牆、入侵防禦系統、網頁內容過濾、代理伺服器等，如果有遠端連線的作業需求，也會使用雙因子身分認證（two-factor authentication）及傳輸加密（如 VPN）防護，其目的都在於防護內部網路的安全。如果內部員工爲了個人一時的方便，私自在企業內網架設了無線基地台，並且連接到內部網路，便形同在企業網路週邊開了一道後門（如圖 3-1 所示），攻擊者不需進入企業內部，便可能藉由此一私接的無線基地台作爲進入點，連進企業的內部網路；甚至內部員工可以透過私自架設的無

線區域網路，繞過網路週邊的防護機制，將公司內的機密資料傳送至公司外，造成機密外洩。因此企業組織對於無線區域網路的使用，應有明確的政策，並告知所有員工，也可以定期稽核內部網路，是否有未經許可，私自架設的網路設備，或是使用無線偵測工具檢測是否有異常的無線網路訊號。

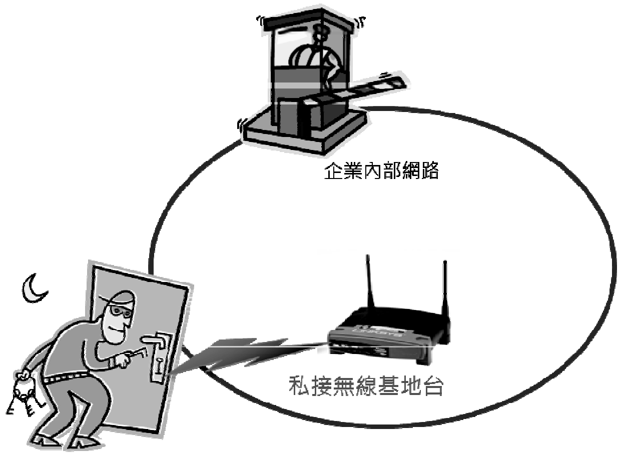

圖 3-1　內部員工私接無線基地台，如同開了一道後門

3.3 電子商務安全

維基百科對電子商務的定義：「電子商務或 EC（E-Commerce）是指在網際網路（Internet）、企業網路（Intranet）和增值網（Value Added Network, VAN）上以電子交易方式進行交易活動和相關服務活動，是傳統商業活動各環節的電子化、網路化。電子商務包括電子貨幣交換、供應鏈管理、電子交易市場、網路行銷、線上事務處理、電子資料交換（EDI）、存貨管理和自動資料收集系統。在此過程中，利用到的資訊科技包括：網際網路、外聯網、電子郵件、資料庫、電子目錄和行動電話。」（資料來源：維基百科/電子商務）

因此事實上電子商務是將傳統的商業活動，利用網際網路及資訊技術，轉換成以電子交易方式進行。電子商務的應用包含：供應鏈管理、電子資料交換（Electronic Data Interchange）、企業資源規劃（ERP）、資料探勘（data mining）、資料倉儲（data warehouse）、線上購物、線上拍賣平台等；以營運模式而言，可分為：B2B（整合產業上中下游的供應鏈）、B2C（線上購物網站）、C2B（團購網）、C2C（銷售競標交易平台）。B2B 常應用於 Extranet；B2C、C2B 和 C2C 則常見於 Internet；Intranet 中則多為企業內部的資訊服務系統（資料來源：[1]）。