ERP 與資訊安全

中央大學資訊管理系　陳奕明
cym@mgt.ncu.edu.tw

近來『十餘家銀行網路破功　被盜千萬』、『郵局遭到電腦病毒：三分之一郵局改採人工作業』的新聞，總是吸引了社會大眾的注意。在高度資訊化的社會裡，這些危害資訊安全的事件，不可避免地會影響每一個人的生活。同樣地，當愈來愈多的企業依賴 ERP 來維繫公司的每日營運時，ERP 系統的安全問題，自然格外受到重視。試想某家年營業額數千億元的跨國電子公司的 ERP 系統在上班日受到病毒攻擊而無法正常運作超過三小時，或 ERP 資料庫遭到病毒影響，取出來的資料時對時錯時會造成怎樣的後果呢？

一般來說，ERP 強調的安全目標有：(1)秘密性、(2)完整性、(3)可用性、(4)可認證性(Authentication)與(4)存取控制，在達成這些安全目標的做法上，通常會涵蓋下列幾個面向：(1)實體安全、(2)人員安全、(3)作業系統安全、(4)軟體安全、(5)資料安全、與(6)網路安全。本文僅針對有關 ERP 系統安全問題的來源以及如何降低 ERP 系統的資訊安全風險，提出討論。

ERP 系統安全問題的來源

ERP 系統的安全問題主要來自於下列幾方面：

(1).ERP 的複雜性

ERP 系統比大多數資訊系統涵蓋更多的公司業務，處裡的事務複雜，使用了成百上千個各式各樣的電子表格，其中許多表格代表複雜的業務流程，牽一髮而動全身，對一個 ERP 模組進行修改，可能會對其他模組造成不可預期的影響。目前 ERP 系統大多仰賴嚴密的帳號管理加上嚴格的授權來控制使用者的權限，以減少這些意外的發生。但是頻繁的人員異動，或員工臨時調整工作內容時，往往使原有的權限設定無法契合實際的需要，此時若無法即時調整權限，將給 ERP 系統帶來很大的安全漏洞。

(2).ERP 建立在既有的作業系統上

意指所有作業系統的安全漏洞，都可能影響到 ERP 系統的安全，例如 2003 年 8 月針對微軟視窗作業系統 RPC 模組中的緩衝區溢位漏洞的疾風病毒，便會造成微軟 Windows NT、2000、與 XP 等作業系統自動重開機，使得執行的 ERP 系統也連帶遭到影響。若深入探究，這又可以分成兩個方面的問題：首先是對 ERP 系統的資料庫與核心程式所在的電腦伺服器來說，因爲有這些程式必須保持開機運作，以致於這些伺服器端的電腦無法關機或離線來進行安全修補(security patch)，而且有些安全修補程式執行後可能會造成應用程式運作不順暢。其次在 ERP 系統的用戶端，因爲和一般用戶程式(如 e-mail、瀏覽器等)共用電腦，所以其他用戶程式引進的惡意程式(如電子郵件帶來的病毒)仍可能造成 ERP 系統的用戶端癱瘓而無法正常運作。

(3).ERP 系統仍依存於現有的網路基礎設施

基於成本與管理的考量，大部分公司都不會爲 ERP 系統建置一套獨立的網路。如此，當網路受到 CodeRed 或 Slammer 等網蟲的癱瘓服務(Denial of Service)攻擊時，ERP 系統一樣無法倖免。另外，當有駭客在內部網路安裝網路竊聽程式以攔截 e-mail、ftp 等使用者帳號密碼時，在相同網路上傳輸的機密 ERP

資料同樣無法免於被竊聽的風險。

(4).ERP 系統仍欠缺一套嚴謹的安全查核方法

雖然許多 ERP 系統不允許用戶自行修改核心程式，而只能用調整參數的方式來適應個別公司的需要；但問題是，誰來保證 ERP 核心程式百分之百正確無誤，不會像微軟作業系統一樣，經常被人發現存在安全漏洞？此外許多 ERP 系統都允許以外掛程式的方式來增強原有 ERP 系統的功能。當外掛程式愈來愈多時，如何保證這些外掛程式和核心程式相容，並且都達到 ERP 核心程式原設計的安全標準呢？

如何降低 ERP 系統的安全風險

因爲成本或管理等原因，任何資訊系統都難以做到百分之百的安全，但是盡可能降低資訊安全風險卻是每一個資訊管理人員必須面對的重要課題。以下我們列出幾個可以降低 ERP 系統安全風險的途徑：

(1).縱深防禦

意指由外而內，利用各種安全工具來建立防禦機制。例如在公司對外網路的進出點設置防火牆與病毒過濾器、在 ERP 主機端安裝入侵偵測系統並定期進行弱點掃瞄、對敏感的資料採取加密後再存入資料庫、對 ERP 主機進行異地備援等。在縱深防禦下，即使某一環節遭駭客或惡意程式突破，仍有下一道防線可守，不至於讓駭客長驅直入，一發不可收拾。

(2).遵循基本安全原則

在資訊安全領域上，存在幾個普遍適用的基本安全原則，同樣地也可用於 ERP 系統的設計、開發與管理上。例如『最小權限原則』，指的是一個程式若只需要最初級權限就可以達到功能的話，就沒有必要以中級權限去執行，以免此程式意外出錯後，造成較大的損害。又例如『分權原則』，指的是某些工作流程必須分開由兩人分別執行。舉例來說，批准帳號新增修改的工作就應和實際執行帳號新增修改的工作由不同的人來擔任，且分別留下工作紀錄，這樣就不會發生有人擅自新增帳號，做非法動作後再消除帳號以掩飾非法行爲的弊端發生。

(3).建立可以遵循的資訊安全政策與管理制度

這是最基本也是最重要的工作。資訊安全政策是用來指導一個公司的資訊系統應該如何運作才足以保證資訊安全，上至是否允許公司的 ERP 系統與上下游夥伴廠商的 ERP 連接交換資料，下至 ERP 用戶密碼多久必須更換一次等，都包含在資訊安全政策之內。但徒法不足以自行，必須要有一套管理方法與規章協助資安政策的落實，近年來熱門的 ISO17799 資訊安全管理規範就是用來協助這方面的工作。

結語

導入 ERP 系統雖然給企業帶來極大的方便，但 ERP 系統本身先天上具有的複雜性，加上建立在既有的作業系統與網路基礎架構上，在網路安全威脅日增的今日，ERP 系統的安全是必須嚴肅面對的課題。

本文提出的『深度防禦』、『遵循基本安全原則』以及『建立可以遵循的資訊安全政策與管理制度』等途徑，雖然能降低 ERP 的資訊安全風險，但是由於下列原因：(1).Web-based ERP 的盛行，使得駭客多了一個利用 Web 爲途徑(包括經由 ERP 用戶端的 Web 瀏覽器以及與 ERP 系統相連的 Web 伺服器)來入侵 ERP 系統，(2).愈來愈多 ERP 系統整合了供應鏈管理(SCM)系統，使得 ERP 的安全管理不再僅限於公司內部，還包括的上下游廠商，甚至包括上下游廠商的伙伴廠商，新的資訊安全挑戰也不斷湧現。所以未來如何進行 ERP 系統的安全規則正規化驗證(Formal validation)，以及如何做好內部交易控管(經由異常行爲偵測技術)等都是值得繼續研究的課題。