評估與維護系統安全

- 評估系統安全性可分為六大部份，簡稱 6P
  - 更新程式 (Patch)
  - 通訊埠 (Ports)
  - 防護機制 (Protect)
  - 安全性政策 (Policies)
  - 探測 (Probe)
  - 實體安全 (Physical)

評估與維護系統安全 (Cont.)

- 更新程式 (Patch)
  - 修復程式錯誤
  - Windows 工具可以掃描系統以找到更新程式
  - 其它作業系統的使用者應該排定一個周期性的更新程式檢查
- 通訊埠 (Ports)
  - 不需要的服務所使用的通訊埠都應該關閉
  - Netcop 可以讓你偵測開啟的通訊埠
  - 在網站上搜尋“通訊埠掃描器（ port scanner ）”

評估與維護系統安全 (Cont.)

- 防護機制 (Protect)
  - 採用了所有合理的防禦軟體和裝置
  - 在主機 / 網路和外面的世界之間架設防火牆
  - 考慮 IDS入侵偵測系統
  - 加入病毒掃描器
- 安全性政策 (Policies)
  - 撰寫明確且清楚的電腦安全性政策
  - 各單位應依安全性政策徹底執行
  - 函蓋範圍應包括電腦、網際網路、電子郵件

評估與維護系統安全 (Cont.)

- 安全性政策的建議
  - 不要開啟可疑的電子郵件附件
  - 明確界定
    - 資料的存取權限及使用範圍
    - 資料備份的進行
    - 遇災後的復原計畫訂定
- 密碼政策
  - 密碼最短長度
  - 密碼之生命週期

評估與維護系統安全 (Cont.)

  - 密碼歷史記錄 (避免重覆使用)
  - 明確說明不安全的密碼樣式
- 人力資源政策
  - 員工離職後公司的安全機制調整
- 探測 (Probe)
  - 利用各式工具測試系統漏洞
  - 定期檢測與掃瞄
- 實體安全 (Physical)
  - 安全的電腦必須放在獨立且被監控的地方

評估與維護系統安全 (Cont.)

- 安全性政策必須包含
  - 上鎖的機房
  - 處理移動式裝置的方法
  - 存放備份磁帶的位置
  - 銷毀過期的資料
- 伺服器機房
  - 防火
  - 堅固的門鎖

評估與維護系統安全 (Cont.)

  - 只有真正必要進入此房間的人才有鑰匙
  - 使用日誌來記錄任何人在何時進入或離開
  - 電子鎖
- 工作站應該
  - 有實體的識別記號
  - 定期盤點

維護電腦系統安全

- 維護家用電腦的安全性
  - 只需要防護個人電腦安全性
- 維護網路上工作站的安全性
  - 利用階層式安全方法來防護個人電腦與網路週圍的安全性
  - 隨時更新
  - 限制程式安裝或變更系統設定的權限
  - 只有網管與支援人員具有較大的權限

維護電腦系統安全 (Cont.)

- 工作站的安全性維護
  - 避免使用者下載惡意程式
  - 避免使用者修改系統設定
  - 避免使用者安裝未經授權或違法的軟體
  - 每一部電腦均要有防毒軟體及反間諜軟體
  - 要定期更新或設定並啟動自動。
  - 啟動系統內建之防火牆
  - 讓使用者遵守密碼政策

維護電腦系統安全 (Cont.)

- 伺服器的安全維護
  - 伺服器提供各項服務，因此存放各種重要資料
  - 應與維護工作站的安全性一樣謹慎
  - 一般而言，伺服器上不會有『實體使用者』
  - 額外的管理措施並不會影響到一般使用者
  - 開啟日誌功能，並定期檢查日誌上的各種事件
  - 資料的備份，如備份的機制，備份資料的存放及保存

維護電腦系統安全 (Cont.)

- 伺服器的安全維護
  - 關閉不需要的服務
  - 移除不需要的軟體及元件
    - 例：遊戲、辦公軟體套件
  - 不要用可以反應權限等級的帳號 Ex. root, administrator
  - 建立一個一般使用者帳號，停用管理者帳號，該使用者帳號具管理權限
  - 例 : 在 Linux 下 建立 jack 帳號 , jack 帳號登入後可用 sudo XXXX 指令執行管理者的工作

維護電腦系統安全 (Cont.)

- 註冊檔設定
  - 設定不顯示最後登入者之使用者名稱
  - 連三次登入錯誤則鎖帳號
  - 移除預設的共享裝置及資料夾
  - 以登入標題嚇阻未經授權的使用

安全的瀏覽網頁

- 防毒軟體及反間諜軟體是必要的
- 避免進入盜版軟體網站
- 拒絕違法及不道德的網站
- 任何從網站上下載的東西都可能是特洛伊木馬