Ch11 : IT security threat mitigation

間諜軟體(Spyware)：指在未經使用者許可下蒐集使用者個人資訊的電腦程式。

間諜軟體除了蒐集你瀏覽過的網站記錄外，還有可能進行鍵盤側錄(Keylogger)，蒐集例如信用卡號的資訊。

勒索軟體(Ransomware)：是一種特殊的惡意軟體，又被歸類為「阻斷存取式攻擊」，其與其他病毒最大的不同在於手法以及中毒方式，其中一種勒索軟體僅是單純地將受害者的電腦鎖起來，而另一種則系統性的加密受害者硬碟上的檔案，所有勒索軟體都會要求受害者繳納贖金以取回對電腦的控制權。

惡意程式阻擋軟體(Anti-malware software)是一種保護電腦的軟體，可以即時偵測並移除惡意軟體。

防毒軟體(Anti-virus programs)

從惡意軟體攻擊中恢復五步驟：

1. 識別(Recognize)：識別出惡意軟體
2. 隔離(Quarantine)：將網路通訊斷開連接
3. 搜索並銷毀(Search and destroy)：銷毀所有可能的為惡意軟體檔案
4. 補救(Remediate)：嘗試救回被刪除會被影響的檔案
5. 教育(Educate)

當使用用戶明及密碼登入時，將進行身分驗證(Authentication)

身分驗證原則

身分驗證是確保用戶身份的過程，以防止未經授權的用戶訪問系統或資料。這是安全管理中的一個基本原則，確保只有合法的用戶能夠進入系統或網絡。身分驗證通常基於以下幾個原則：

1. 唯一性 (Uniqueness)：每個使用者必須有唯一的身份標識，以便系統能夠區分不同的用戶。
2. 保密性 (Confidentiality)：用戶的身份驗證信息（如密碼、指紋等）必須保密，不能被其他人獲取或使用。
3. 完整性 (Integrity)：身分驗證信息不能被篡改或偽造，確保驗證信息的正確性。
4. 可用性 (Availability)：合法用戶應隨時能夠進行身份驗證，而不會因系統問題或限制而無法進入系統。
5. 多重因素驗證 (Multi-Factor Authentication, MFA)：使用多種方式進行身份驗證，確保更高的安全性。多重因素驗證至少需要兩種以上不同類型的驗證方式。

常見的身分驗證方法

1. 知識因素 (Something You Know)
   * 密碼 (Password)：最常見的身份驗證方法，要求用戶輸入一組字母、數字和符號組成的密碼。
   * PIN 碼 (Personal Identification Number)：通常是數字組成的簡短密碼，用於快速驗證，如銀行卡的取款密碼。
2. 擁有因素 (Something You Have)
   * 安全令牌 (Security Token)：硬體設備或軟件應用程式，用於生成一次性驗證碼（如 RSA SecurID）。
   * 智慧卡 (Smart Card)：內建芯片的卡片，必須插入讀卡器或貼近讀卡設備，通常用於公司或政府機構。
   * 移動設備驗證 (Mobile Authentication)：通過手機收到一次性驗證碼（SMS OTP）或使用手機應用程序（如 Google Authenticator）進行驗證。
3. 繼承因素 (Something You Are)
   * 指紋識別 (Fingerprint Recognition)：通過掃描用戶的指紋進行身份驗證。
   * 臉部識別 (Facial Recognition)：使用攝像頭掃描用戶的臉部特徵進行驗證。
   * 虹膜識別 (Iris Recognition)：掃描眼睛的虹膜特徵，這是一種高安全性的生物識別技術。
4. 位置因素 (Somewhere You Are)
   * 地理位置 (Geolocation)：根據用戶的地理位置進行驗證，通常通過 IP 地址或 GPS 數據來確定位置。
   * 時間因素 (Temporal Information)：檢查用戶何時試圖訪問系統，例如，設定時間段限制來提高安全性。
5. 行為因素 (Something You Do)
   * 打字模式識別 (Keystroke Dynamics)：通過分析用戶打字的速度和模式來驗證身份。
   * 行走方式識別 (Gait Analysis)：基於用戶的行走方式特徵進行身份識別，通常使用攝像頭和傳感器來收集數據。

單因子驗證 (Single-Factor Authentication, SFA)

單因子驗證是最基本的身分驗證方法，只依賴於一種驗證因素來確認用戶的身份。這種方法通常容易實施，但安全性相對較低。

* 例子：
  + 密碼 (Password)：要求用戶輸入一組預先設定的密碼。
  + PIN 碼 (Personal Identification Number)：使用數字組成的簡短密碼來驗證身份。
  + 指紋識別 (Fingerprint Recognition)：通過掃描用戶的指紋進行身份驗證。

單因子驗證因其實施簡單和用戶友好而廣泛使用，但如果唯一的驗證因素（如密碼）被泄露或破解，系統的安全性就會受到嚴重威脅。

多因子驗證 (Multi-Factor Authentication, MFA)

多因子驗證是一種使用兩種或兩種以上不同類型的驗證因素來確認用戶身份的安全策略。多因子驗證提高了安全性，因為即使其中一個驗證因素被泄露或破解，攻擊者仍然需要其他額外因素才能進行未授權的訪問。

* 例子：
  + 雙重因素驗證 (Two-Factor Authentication, 2FA)：
    - 知識因素 + 擁有因素：例如，用戶輸入密碼（知識因素），然後再輸入發送到其手機的 SMS 驗證碼（擁有因素）。
    - 擁有因素 + 繼承因素：例如，使用安全令牌（擁有因素）生成一次性密碼，並通過指紋掃描（繼承因素）進行確認。
  + 三重因素驗證 (Three-Factor Authentication)：
    - 使用三種不同類型的驗證因素，例如密碼（知識因素）、安全令牌（擁有因素）、和指紋識別（繼承因素）。

單因子驗證與多因子驗證的比較

| 特點 | 單因子驗證 (SFA) | 多因子驗證 (MFA) |
| --- | --- | --- |
| 安全性 | 低 - 如果唯一的因素被破解，則訪問將被授予 | 高 - 需要多個驗證因素，單一因素被破解不會影響整體安全性 |
| 用戶友好性 | 高 - 用戶只需記住或提供一個驗證因素 | 中等 - 需要額外的步驟，但安全性提高了 |
| 實施成本 | 低 - 技術要求較低 | 高 - 可能需要額外的硬件或軟件 |
| 使用範圍 | 常見於低風險應用或內部系統 | 常見於高風險應用、金融交易、機密信息保護等場景 |

結論

多因子驗證比單因子驗證更安全，是目前保護敏感信息和防止未授權訪問的最佳實踐。它利用多種不同類型的驗證方法來提供額外的安全層，特別是在處理金融交易、醫療數據、企業網絡訪問等高風險場景中。

Alt+F4(Windows) = Command+Q(MAC) : 關閉當前視窗

不同類型的商業軟體可以儲存各種的密碼，如：

Apple使用Keychain紀錄裝置的各項密碼

瀏覽器記憶密碼(Web browsers store passwords)

這些紀錄密碼的方式的安全性是安全的，建立在使用者是此裝置為唯一的使用者，如果不能保證的話，記得登出

加密(Encryption)：獲取文件或文件夾並以一種方式對其進行轉換，要有正確的加密密鑰才能使用