勒索軟體威脅防護指南

1. 事前 - 勒索軟體威脅預防措施

1.1 事前預防措施 - 保護系統

(1) 使用防毒軟體，並及時更新系統、軟體和應用程序：攻擊者通常利用未修補的漏洞來訪問未經授權的系統和網路，以執行後續惡意活動。

- 應安裝防毒/防惡意軟體並保持其病毒碼/惡意特徵碼更新。每周至少對系統和網路執行一次掃描，並掃描所有收到的文件。
- 當移動儲存設備(如隨身碟)連接時應執行防毒掃描。
- 將系統、應用軟體與韌體更新到最新版本，並下載最新的安全更新檔。

(2) 強化具派送功能伺服器安全：防毒軟體中控、AD 伺服器、資產管理系統等因具有軟體派送功能，更需注意安全更新，並密切觀察其群組原則或工作排程不正常異動狀況。

(3) 僅在需要時啟用 Microsoft Office 巨集：勒索軟體可能將惡意 Marco 植入 Microsoft Office 檔案中，當受害者開啟 Office 後就會執行巨集，導致感染惡意程式。

(4) 最小化開放埠的設置：勒索軟體可能會利用對外曝露的服務和開放埠（例如 RDP 埠 3389 和 SMB 埠 445）在網路中傳播，除了確認其開放的必要性外，還應確認使用這些服務的對象為可信任。

(5) 設置防火牆，阻止任何與已知惡意 IP、URL 的網路連線行為，禁止使用允許任何連線的規則，只允許與對外服務的 IP、DN 進行連線。

(6) 人員的最小使用權限：為了減少攻擊者獲得管理權限的機會，應該：

- 控制和限制存取權限，為所有的使用者提供工作所需的最低權限，特別是需要遠端登入的帳號，例如:RDP。
- 定期檢視所有帳號的使用情況，並停用非活動帳號。
- 實施多因子身份驗證。

(7) 提高資安意識：應定期對員工進行培訓，建立良好資安意識及網路使用習慣，例如識別可疑電子郵件，不要隨意點擊連結，不打開未知或不受信任來源的電子郵件的附件，並進行社交工程演練，提高訓練成效。

(8) 系統備援：應針對重要服務系統規劃系統備援機制，確保系統發生異常時，能夠保持服務正常運行。

(9) 啟用系統事件紀錄檔（Event logs）功能，紀錄系統故障或異常狀況。

1.2 事前預防措施 - 保護資料

(1) 加密重要或敏感資料：應對重要或敏感資料進行加密，如果資料被竊取，可以使攻擊者難以處理這些資料，另外，某些勒索軟體僅對常用文件類型（例如圖檔和文檔）起作用，則加密還可以防止它們檢測到文件。

(2) 依資料重要性、任務等區分不同的權限管控。

(3) 維護更新的備份並保持離線：定期執行資料備份有助於在發生勒索軟體攻擊時恢復資料，而備份資料儲存且不能連接到既有企業網路中，可防止勒索軟體透過網路影響備份資料。

- 3-2-1 備份原則：3 份備份、2 種儲存媒體、1 個不同的存放地點。

(4) 定期維護重要系統的映像檔(image file)：虛擬機或服務器的映像檔包括預先配置的作業系統和相關的應用軟體，當發生攻擊，而需要重建系統，可以利用這些映像檔達到快速部署恢復。

1.3 企業組織事前預防措施 - 準備事件應變計畫

(1) 在事件發生之前，制定事件應變計畫並進行演練，以測試計畫是否可行是非常重要的。在受到攻擊時難以即時判斷正確作法，透過已制定好的計畫並實施，將有助於員工了解要採取的行動，並確定各項系統與環境的恢復優先等級。

(2) 準備資安事件發生時，可尋求協助的外部資安單位、警調之清單與連絡方式。

(3) 加入資安情資分享組織(如：所屬產業的資安資訊分享與分析中心(ISAC)、臺灣電腦網路危機處理暨協調中心(TWCERT/CC)等)，取得資安預警、資安威脅與資安弱點等情資。

參考資料

[1]https://jenner.com/system/assets/assets/11480/original/memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware.pdf
[2]https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf
[3] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks