臺中市政府經濟發展局政風室

公務機密宣導專欄

政府機關網站實兵演練揭三大弱點，VPN 安全成焦點

據資通安全署（簡稱資安署）最新發布的 12 月資通安全網路月報，**透過 113 年對政府機關網站的實兵演練，發現三大主要資安弱點，其中以加密機制失效、注入攻擊及無效存取控管最為常見。**

資安署指出，部分機關在處理敏感資料時，僅使用 PDF 軟體的遮罩功能進行保護，這種做法容易遭到破解。建議機關在遮蔽敏感資料後，應進一步將文件轉換為圖片格式，以確保資料安全。

在注入攻擊方面，許多政府網站的輸入功能仍存在安全漏洞，未能有效過濾特殊字元如引號、尖括號等符號，致使駭客有機可趁。針對此問題，資安署建議機關應強化輸入驗證機制，並確實過濾所有潛在危險字元。

資安監控數據顯示，12 月份共計蒐整 8 萬 3,105 件資安聯防情資，較 11 月減少 1 萬 3,070 件。其中，**資訊蒐集類攻擊佔 52%，主要透過掃描、探測及社交工程手法進行；入侵攻擊類次之，佔 21%；入侵嘗試類則佔 16%。**

值得關注的是，近期發現駭客以行政陳情為幌子，運用第三方郵件服務針對特定機關發動魚叉式攻擊。駭客通過夾帶看似正常的陳情文件，實則植入惡意程式，藉此竊取機敏資料。

在資安事件通報方面，12 月共接獲 40 件通報，較上月減少 13 件。其中，近半數（47.50%）與惡意中繼站連線或惡意程式下載有關。特別案例中，某機關遭駭客利用先前外洩的 VPN 帳密成功入侵，並竊取內部資料。該事件突顯了 VPN 存取控管的重要性。

針對 VPN 安全議題，資安署特別建議各機關採取「**原則禁止、例外允許**」的嚴格管理方針，並建議啟用多因子驗證機制，定期稽核使用紀錄，同時建立即時警示系統，及時發現並處理異常狀況。此外，機關在處理資安事件時，應全面清查可能外洩的資訊，並確實執行受影響帳號的停用或密碼變更作業。

【資料來源】

☞ 臺中市政府政風處

臺中市政府經濟發展局
TAICHUNG CITY GOVERNMENT
ECONOMIC DEVELOPMENT BUREAU

創新 Innovation　服務 Service　活力 Dynamics