公務機關資安事件726件！非法入侵佔7成　數發部曝5大威脅

數發部資安署公布，2025年公務機關通報資安事件共726件，其中以非法入侵為大宗，占68.60%，並示警機關須查證以避免安裝偽冒即時通訊程式、網路邊緣設備存在漏洞或組態設定風險等5大威脅。

機關依資通安全事件通報應變及演練辦法規定，依事件機密性、完整性及可用性衝擊嚴重程度，通報的資安事件等級由輕至重區分成1級到4級。

資安署表示，2025年公務機關通報資安事件（不含實兵演練）共726件，較2024年減少29件。其中，1級資安事件占87.33%最多，2級占9.78%居次，3級占2.89%，4級則未發生。

資安署指出，通報資安事件類型以非法入侵居多、占68.60%；其次為設備問題占15.43%；阻斷服務占4.96%；網頁攻擊占2.48%，以及其他資安事件。

資安署根據威脅情勢與2025年政府機關資安事件通報案例，分析駭客入侵常用手法，提出5大資安威脅與防護建議。

第一，使用者在設備汰換或取得新電腦後，不慎自非官方網站下載偽冒通訊軟體，導致電腦遭植入後門程式。機關應建立資通系統變更管理與下載控管機制，要求軟硬體及應用程式安裝須申請與審核。

第二，勒索團體以自帶驅動程式手法入侵並迴避偵測。資安署指出，機關應定期執行網站漏洞掃描與修補，導入網頁應用程式防火牆，阻擋惡意請求，並建立端點防護持續運作機制，更新防護產品與威脅偵測規則。

第三，供應鏈管控疏漏，系統維護廠商於網站主機上安裝遠端桌面軟體，遭駭客暴力破解密碼登入機關網站。資安署表示，機關須訂定供

應商安全管理規範，如存取權限控管、資料保護措施、漏洞管理流程及事件通報等，並定期執行資安稽核與合規檢查。

第四，網路邊緣設備存在漏洞或組態設定風險，導致發生惡意連線行為。資安署建議，機關對外連線應採用白名單策略，封鎖非必要通訊埠，同時盤點網路邊緣設備型號與韌體版本，建立持續更新與驗證流程，確保漏洞及時修補。

第五，社交工程攻擊並結合雲端服務濫用，導致資料外洩風險。資安署指出，機關應導入電子郵件過濾與沙箱檢測機制，攔截惡意附件與連結；另限制雲端硬碟共享權限，啟用檔案上傳掃描機制，對雲端連結進行安全檢測，避免惡意檔案散布。

資安署表示，除持續提供各機關資安防護重點建議外，法規也明定各機關須具備資料備份、備援及復原功能；另需落實營運持續計畫（BCP）演練，確保必要時可迅速切換至備援系統，維持核心功能運作。

此外，數發部推動關鍵民生系統資料加密分持備份機制，將重要資料加密並分持備份至不同公有雲環境，以降低單一節點失效風險，提升整體資安韌性。

（資料來源：TVBS 新聞網 115 年 5 月 24 日報導）

發掘潛在危機因素；改進安全防護缺失