苗栗縣政府政風處

公務機密與機關安全維護宣導

中華民國 114年9月

CONTENTS

1 公務機密宣導案例

2 機關安全維護宣導案例

1 公務機密宣導-駭客假冒資安院發動社交工程攻擊

據資通安全署（簡稱資安署）最新發布的1月資通安全網路月報，114年1月資安聯防情資共蒐整7萬9,566件，較上月減少3,539件。值得注意的是，近期發現駭客偽冒資安院，以「資安攻擊預警」為名對臺灣學術機構發動針對性社交工程攻擊。

資安署分析指出，本月政府機關資安聯防情資中，威脅種類排名第一的是資訊蒐集類，占比達40%，主要是透過掃描、探測及社交工程等攻擊手法取得資訊。其次為惡意內容類，占24%，多透過文字、照片、影片等形式散播不當內容。入侵嘗試類則占16%，主要係嘗試入侵未經授權的主機。

1 公務機密宣導-駭客假冒資安院發動社交工程攻擊

在資安事件通報方面，1月共有47件通報，較上月增加7件，為去年同期的0.61倍。其中，部分機關遭受阻斷服務攻擊，造成網站服務緩慢或中斷的情況，占本月通報件數的12.77%。

值得警覺的是，**監測發現駭客偽冒資安院身分，對臺灣學術機構發動針對性社交工程電子郵件攻擊。這些攻擊以「資安攻擊預警」為名義，要求收件人執行所謂的勒索軟體偵測工具，實則誘騙使用者下載與執行惡意附檔。**相關情資已提供各機關作為聯防監控防護參考。

1 公務機密宣導-駭客假冒資安院發動社交工程攻擊

本次報告也分享了一起值得借鏡的個資外洩案例。某政府機關在辦理活動期間，將活動簡章存放於Google雲端空間供民眾下載，但承攬廠商也將包含個人資料的報名者資訊上傳至同一雲端空間，且存取權限設定不完善，導致未授權使用者能夠存取這些資料，造成民眾個人資料外洩。

針對雲端資料管理，資安署建議政府機關應確保公開文件與涉及個人資料的檔案存放於不同雲端目錄或獨立儲存空間，並設定適當存取權限。委託廠商辦理活動時，應於合約中明訂個人資料保護責任，包含資料存放方式、存取限制、保存期限及刪除機制等。活動結束後應即辦理個人資料移除或歸檔作業，不得將個資存放於雲端儲存空間，以降低個人資料外洩風險。

2 機關安全維護宣導-災害與關鍵基礎設施之關係

美國FEMA在關鍵基礎設施保護(Critical Infrastructure Protection,CIP)計畫中，將關鍵基礎設施分為18類，而台灣則分為8類(運輸、水資源、警急救援與醫療、能源、資通訊、中央政府、高科技園區、銀行金融)，各政府部門或國營事業體管轄之CI，目前正逐步進行各類型CI受災後之災損境況模擬，以提前進行保護與災害應變機制建立。

如1999年9月21日集集大地震，南投縣中寮超高壓變電所遭震損，加上高壓輸配電塔倒塌、造成全台大停電，使得北部供電吃緊，尤其新竹科學園區損失最為慘重，甚至影響全球科技產業零組件之正常供應。

2 機關安全維護宣導-災害與關鍵基礎設施之關係

此外，2011年3月11日東日本大地震，因核電廠受到海嘯影響破壞，除了造成核災之外，亦使得電力無法正常供應，導致日本關東區域輪流限電，影響災後緊急救助以及全日本的經濟成長率，甚至是全球關鍵零組件的產業供應鍊。

易言之，水源、電力、電信與天然氣等維生線系統與各種交通路網系統等，為現今都市甚或國家社會整體運作之基石，不論是恐怖攻擊或是天然災害，將可能導致CI無法正常運作，並致使國家社會造成重大影響及巨大的損失。

祝平安喜樂

苗栗縣政府政風處廉政專線

037-356639

《宣導資料取自網路編製》