資通安全網路月報（112年1月）

資通安全網路月報（112年1月）

<近期政策重點>

依資通安全責任等級分級辦法第3條規定，各機關應每2年提交自身、所屬、所管、所監督及所轄之資通安全管理法納管對象之資通安全責任等級，提報主管機關核定(或備查)，本次作業將於近期啟動，請各機關預為準備。

近期清查A、B級公務機關資通安全威脅偵測管理機制(SOC)回傳情形，發現有部分機關未落實回傳情資，已通知改善，請各機關確實依法遵規定落實辦理。

另A、B級公務機關應於本(112)年8月23日前完成端點偵測及應變機制(EDR)導入作業，併同資通安全威脅偵測管理機制(SOC)回傳監控管理資料，請機關掌握法遵辦理時效。

<整體威脅趨勢>

事前聯防監控

本月蒐整政府機關資安聯防情資共47,574件，分析可明確辨識的威脅種類，第1名為資訊蒐集類(67%)，係外對內大量連線阻擋事件；其次是入侵嘗試類(16%)，主要是目錄遍歷(Direct Path Traversal)攻擊行為；以及入侵攻擊類(10%)，主要為惡意中繼站成功連線偵測。另統計近1年情資數量分布詳圖1。

進一步彙整分析聯防情資資訊，研究人員發現駭客利用Google雲端硬碟進行社交工程郵件攻擊，駭客將惡意檔案存放Google雲端硬碟並開啟分享，接著將下載網址內嵌在社交工程電子郵件附檔並寄給政府機關人員，誘導收件人透過附檔文件，下載藏有惡意程式檔案。相關情資亦於聯防監控月報提供防護建議，提供政府機關參考。

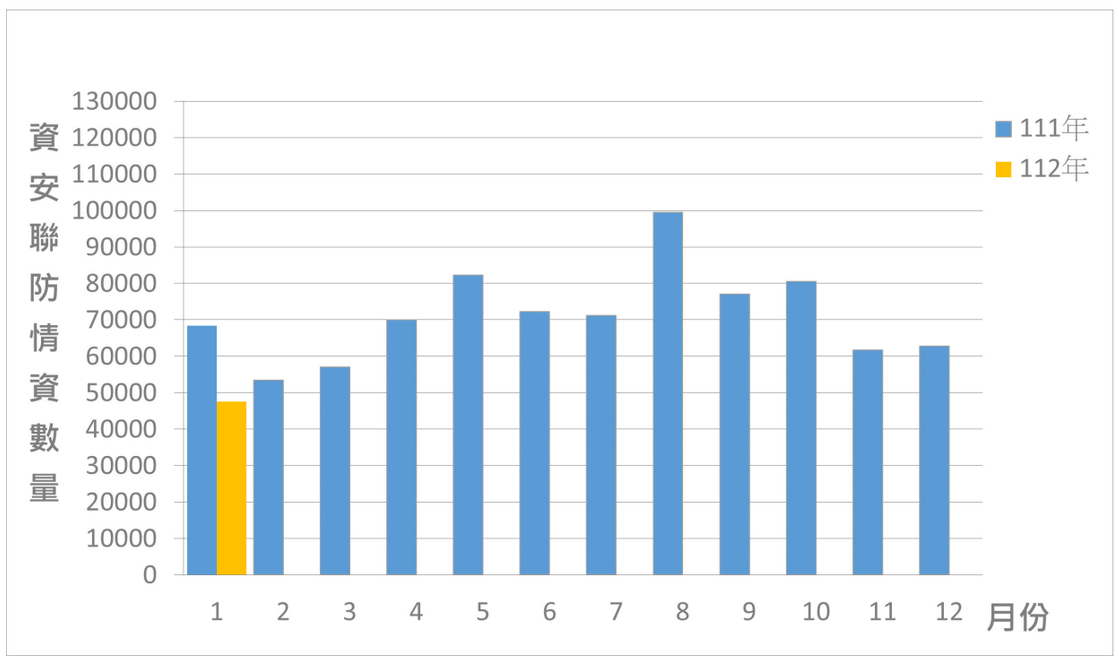

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共33件，與去年同期通報無明顯差異，惟發現多個機關帳號密碼外洩，較上個月增加2.5倍。近1年資安事件通報統計詳見圖2。

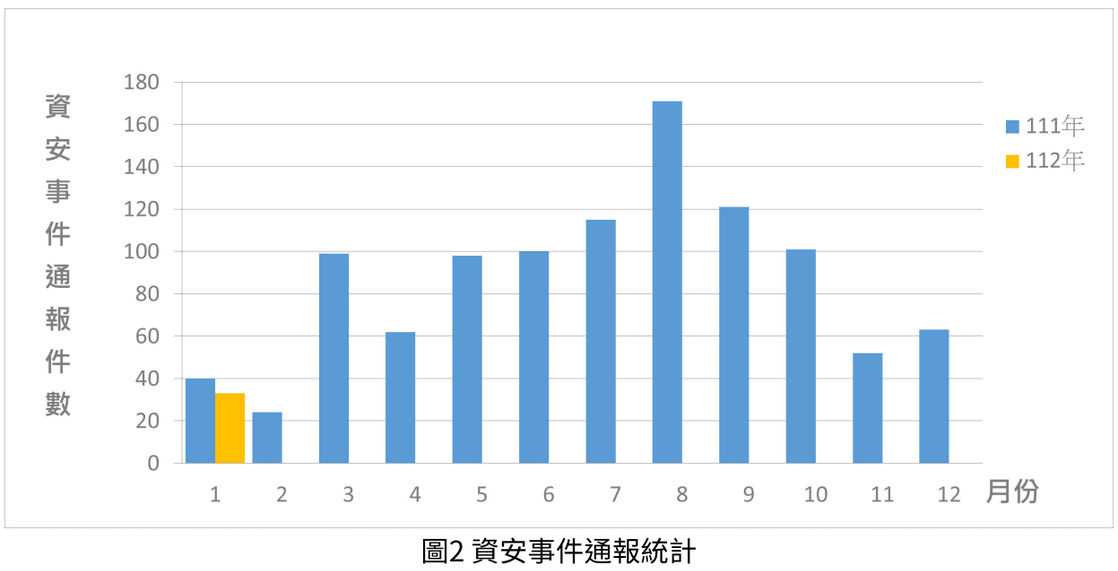

圖2 資安事件通報統計

事後資訊分享

本月某機關端點偵測機制(EDR)發出警示，發現其所屬網站疑似遭SQL Injection攻擊並成功上傳可疑檔案，該機關已修補相關漏洞。經瞭解，該機關資安政策規定每年需對服務網站進行2次弱點掃描，本次受駭網站曾因111年12月資安事件進行弱點掃描，惟仍未能有效杜絕網站漏洞，後再輔以源碼檢測並完成相關弱點修補。

足資借鏡：弱點掃描係利用自動化工具檢測網站是否存在安全性弱點，因應不同廠牌與檢測規則，檢測結果可能產生差異，建議可利用不同廠牌弱點掃描工具交叉比對掃描結果，亦可搭配不同檢測方式，例如滲透測試或源碼檢測，以確保網站安全性。

<國內外重點資安新聞>

一、華航會員資料外洩及iRent的顧客資料庫曝險

華航表示，該公司接獲匿名網路勒贖信件後，已立即報警及依法通報主管機關，並在第一時間有效採取防禦應變措施，確認各項資通系統作業正常，也配合警方追查事件及釐清原因，亦已全面性檢視系統安全，確保資安防護並持續嚴格落實個資保護，強化資訊安全。

和泰汽車旗下iRent雲端資料庫未落實加密，導致個資外洩事件，經公路總局派員稽查結果，因未依「個人資料保護法」與「汽車運輸業個人資料檔案安全維護計畫及處理辦法」採行適當安全維護措施，致個人資料洩漏，已依個人資料保護法規定開罰。

(資料來源：工商時報、鏡周刊)

二、永豐銀行信用卡疑3D Secure驗證碼被竊取遭盜刷

永豐銀行信用卡用戶於春節期間遭盜刷事件，金管會初步分析，係因永豐銀行海外刷卡機制之3D驗證機制(OTP密碼)，透過郵件發送驗證碼，在電子郵件接收驗證碼時被竊取盜刷。該行相關處置作法包含：停止刷卡OTP密碼傳送到EMAIL、將遭盜刷的信用卡先停卡和換卡、針對盜刷的商店作控管、同時於聯合信用卡中心系統將盜刷交易之IP列入黑名單及被盜刷金額列入爭議款項，客戶不需要繳盜刷金額。

(資料來源：iThome、今周刊、聯合新聞網)

三、金管會發布《金融資安行動方案2.0》：3年為期，9大重點

金管會於109年8月6日發布金融資安行動方案1.0版，執行迄今已逾2年，主要推動成果包含設置資安長、導入國際資安標準、辦理資安攻防演練與競賽、建立金融資安事件應變體系等項。

為因應業務發展與科技進步，持續提升金融機構資安防護能量，金管會研訂金融資安行動方案2.0版。重點如下：一、擴大資安長設置，定期召開資安長聯繫會議；二、因應數位轉型及及網路服務開放，增修訂自律規範；三、深化核心資料保全及營運持續演練；四、擴大導入國際資安管理標準及建置資安監控機制；五、鼓勵資安監控與防護之有效性評估；六、鼓勵零信任網路部署，強化連線驗證與授權管控；七、鼓勵配置多元專長資安人才，擴大攻防演訓量能；八、提升資安情資分享動能，增進資安聯防運作效能；九、辦理資安攻防演練，規劃重大資安事件支援演訓。

(資料來源：資安人、金融監督管理委員會官網)

<近期重要資安會議及活動>

無

<資通安全長及資訊主管異動情形>

一、臺北市政府資通安全長自112年1月3日起，原由陳志銘秘書長兼任，改由李四川副市長兼任。

二、桃園市政府資通安全長自112年1月4日起，原由高安邦副市長兼任，改由王明鉅副市長兼任。

發布單位：資通安全署　　建立日期：2023-02-15　　更新日期：2023-02-15