資通安全網路月報（111年8月）

資通安全網路月報（111年8月）

<近期政策重點>

一、配合數位發展部及其所屬資通安全署於本(111)年8月27日成立，資通安全管理法及其子法條文涉及各該新機關掌理事項者，業經行政院111年8月24日院臺規字第1110184307號公告變更(可至行政院公報資訊網查詢第28卷第160期公報)。

二、為協助各機關辦理資安稽核作業，已開辦「111年資安稽核實務訓練說明」之職能訓練課程，並於111年9月6日上午10時起開放網路報名(網址：https://ctts.nccst.nat. gov.tw)，歡迎踴躍報名參訓。

三、為協助政府機關於建置或使用雲端服務時，可依據雲端資安相關標準要求，檢視及降低使用雲端服務可能帶來的風險，已於行政院國家資通安全會報技術服務中心(下稱技服中心)網站共通規範專區，公布「政府機關雲端服務應用資安參考指引」提供各機關參考。

<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99,451件，統計近一年情資數量分布詳見圖1。經分析上述資安聯防情資，可明確辨識的威脅種類，第1名為掃描刺探類(56%)，主要係外部主機執行掃描探測攻擊；其次為入侵攻擊類(21%)，主要為網頁攻擊行為；以及政策規則類(11%)，主要是單一帳號持續登入失敗。

其中，依聯防情資彙整資訊進一步分析，近期發現駭客藉「年度防疫獎勵實施計畫」之郵件主旨，大規模對多個政府機關發動魚叉式社交工程電子郵件攻擊，以提供防疫獎勵為由，誘騙目標收件人開啟惡意郵件附檔，使駭客可竊取受駭主機資訊並遠端操控受駭主機，技服中心已透過聯防監控月報提供相關防護建議予各機關參考。

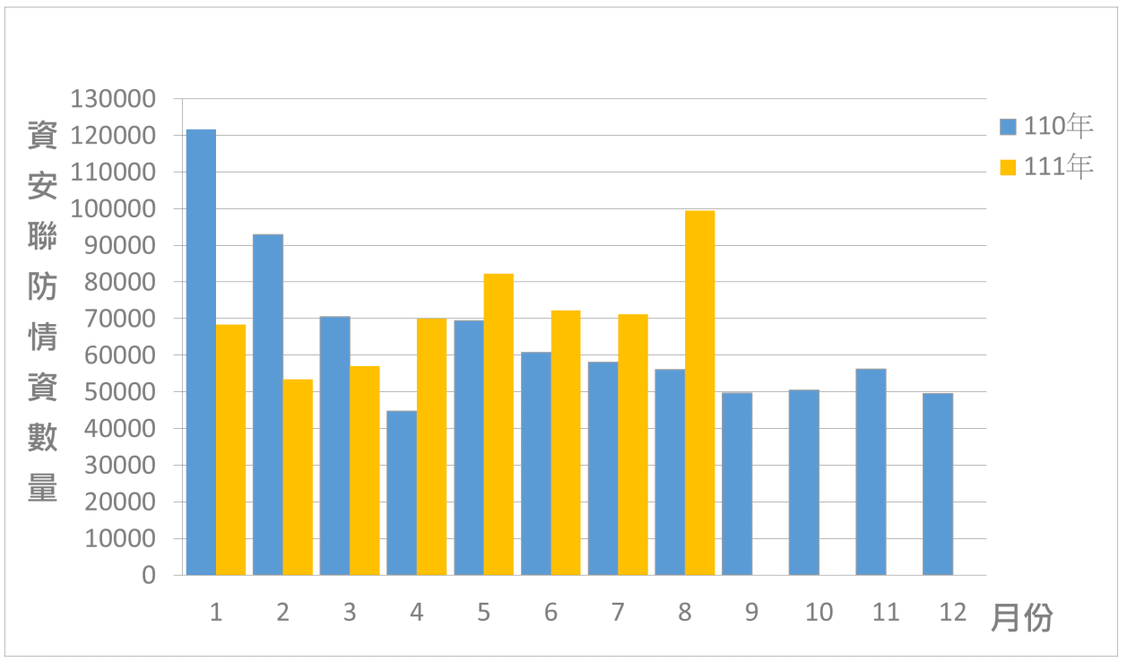

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共224件，近一年資安事件通報統計詳見圖2。本月通報事件為去年同期通報件數2.49倍，主要是本月實兵演練攻擊成功案件較多，占本月通報件數57.14%，多數係因網站存在無效的存取管制措施，致能取得網站的非機敏但非公開資料。

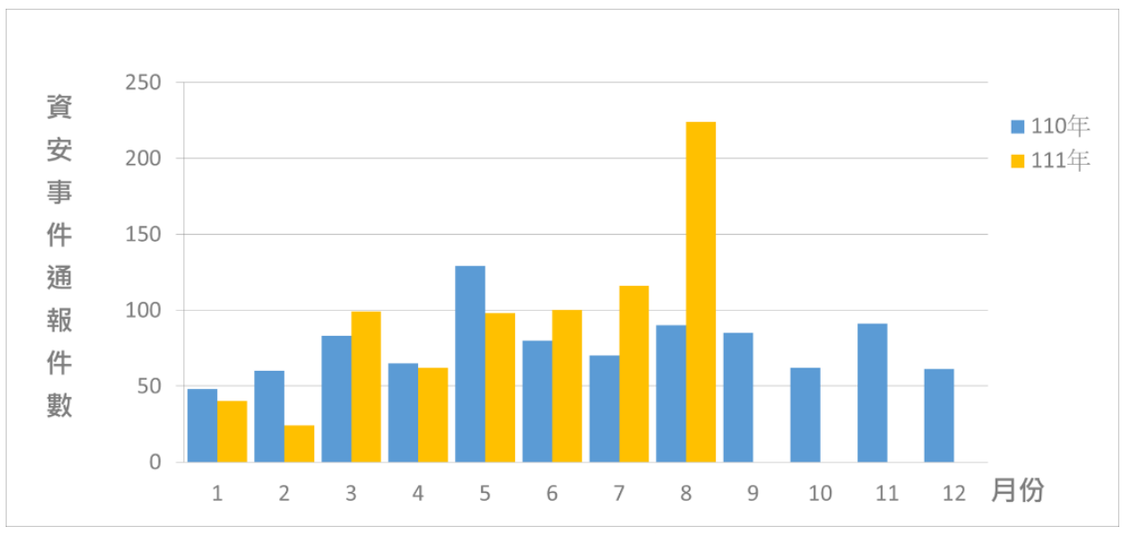

圖2 資安事件通報統計

事後資訊分享

某機關發現其官方網站之外部單位網址疑似遭竄改，導向色情網站，進一步調查發現該網址屬外部單位舊網域，因業務需求更換新域名，而其舊網域租約到期未辦理續約，遭有心人士註冊使用該舊域名，並架設為色情網站，因機關未接獲更新資料，亦未定期檢視網站資料有效性，導致官網存在色情網站連結。

足資借鏡：機關網站除自身內容外，亦常提供相關外部網站連結予民眾參考，惟外部網站非機關所管理維運，故須仰賴機關人員定時檢視網址有效性與內容正確性，避免提供錯誤資訊。

<國內外重點資安新聞>

一、我國數位發展部111年8月27日正式成立，112年將成立資安研究院

經過2年多籌備的數位發展部(moda)在今年8月27日舉行揭牌儀式，該部主要職責為推動國家數位政策的創新和變革，未來政策重點將涵蓋電信、資訊、資安、網路和傳播等5大領域，並統籌國家基礎建設、環境整備和資源運用等業務。

數位發展部設有6司2署，6司為數位策略司、韌性建設司、資源管理司、數位政府司、民主網絡司與多元創新司；2署為數位產業署和資通安全署，前者推動數位科技應用與數位經濟產業發展政策；後者規劃國家資安政策、計畫核議與督導考核，以及辦理國家資安防護演練與基礎設施防護等。

(資料來源：IThome、自由財經、中央通訊社)

二、臺灣推動零信任戰略，優先推動A級公務機關導入

技服中心於7月中旬揭露，將依第六期「國家資通安全發展方案(110年至113年)」推動導入零信任網路，以國內A級政府機關為優先導入對象。

政府推動零信任網路將包括政府機關及商用產品兩大面向，在政府機關面向，將以逐年導入方式，在111年至113年間建立起零信任網路中屬決策引擎的「身分鑑別」、「設備鑑別」與「信任推斷」等3大核心機制，並以A級機關為優先導入對象；在商用產品面向，技服中心於網站推出「零信任網路專區」，使國內廠商可預做準備，提出相應的解決方案。技服中心並於8月16日發布「政府零信任網路身分鑑別機制導入建議_V1.0版」，提供政府機關導入零信任身分鑑別機制之參考建議。

(資料來源：行政院國家資通安全會報技術服務中心、IThome)

三、資安團隊與事件應變論壇FIRST公布新版TLP 2.0協議

資安團隊與事件應變論壇(Forum of Incident Response and Security Teams, FIRST)於8月5日公布情資分享協議Traffic Light Protocol (TLP)2.0版本，此協議規範資安情資分享範圍，最初由英國國家基礎設施安全協調中心(National Infrastructure Security Co-ordination Center, NISCC)擬定，FIRST於2015年進行統一規範，以4種顏色區分訊息之保密程度與分享範圍，今年釋出TLP 2.0版本，預計2023年受到廣泛採用。

TLP 2.0與前一版本差異包含：新增對社群、組織及客戶之定義；原TLP:WHITE更改為TLP:CLEAR；新增TLP:AMBER+STRICT，要求不得與組織外之任何人分享。

(資料來源：HelpNetSecurity、FIRST、IThome)

<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、國家通訊傳播委員會資安長自111年8月1日起，原由孫雅麗委員兼任，現由翁柏宗副主任委員兼任。

二、數位發展部資安長自111年8月27日起，由闕河鳴政務次長兼任。

三、臺北市政府資安長自111年8月31日起，原由黃珊珊副市長兼任，現由陳志銘秘書長兼任。

四、教育部資訊及科技教育司司長自111月8月15日起，原由郭伯臣司長擔任，現由李政軒司長擔任。

五、數位發展部資訊處處長自111年8月27日起，由吳英俊處長擔任。

發布單位：資通安全署　　建立日期：2022-09-15　　更新日期：2022-09-15