資通安全網路月報（111年9月）

資通安全網路月報（111年9月）

<近期政策重點>

為強化機關連網安全，再次重申請各政府網際服務網(GSN)使用機關須將DNS快取主機設定指向GSN Cache DNS(210.69.1.1 與 210.69.2.1)，並請務必確認機關已完成相關設定；另為避免機關同仁誤使用其他DNS快取服務，請設定防火牆限制TCP 53 埠及 853 埠的連線對象。

採自建DNS權威主機(Authoritative DNS)提供服務者，請評估其必要性及關閉不必要的DNS開放解析(open DNS resolver)，並請妥為防護以降低該主機遭受攻擊(如DDoS)之影響。

<整體威脅趨勢>

事前聯防監控

本月蒐整政府機關的資安聯防情資共77,108件，統計近1年情資數量分布詳圖1。經分析前揭資安聯防情資，可明確辨識的威脅種類，第1名為掃描刺探類(42%)，主要係外部主機執行掃描探測攻擊；其次為入侵攻擊類(29%)，主要是網頁攻擊行為；以及政策規則類(15%)，主要為單一帳號持續登入失敗。

其中，進一步分析聯防情資彙整資訊，發現近期多起政府機關遠端管理服務暴露於網際網路，包含RDP、VNC及Telnet等遠端管理通訊協定，以及機關架設的智慧居家系統服務(如資訊庫管理系統phpMyAdmin介面等)，前述服務易受大量遠端服務暴力破解與弱點探測，導致機關設備除遭入侵外，亦可能造成內部感染擴散。技服中心已針對開放遠端管理服務之政府機關發布警訊，並透過聯防監控月報提供相關防護建議供各機關參考。

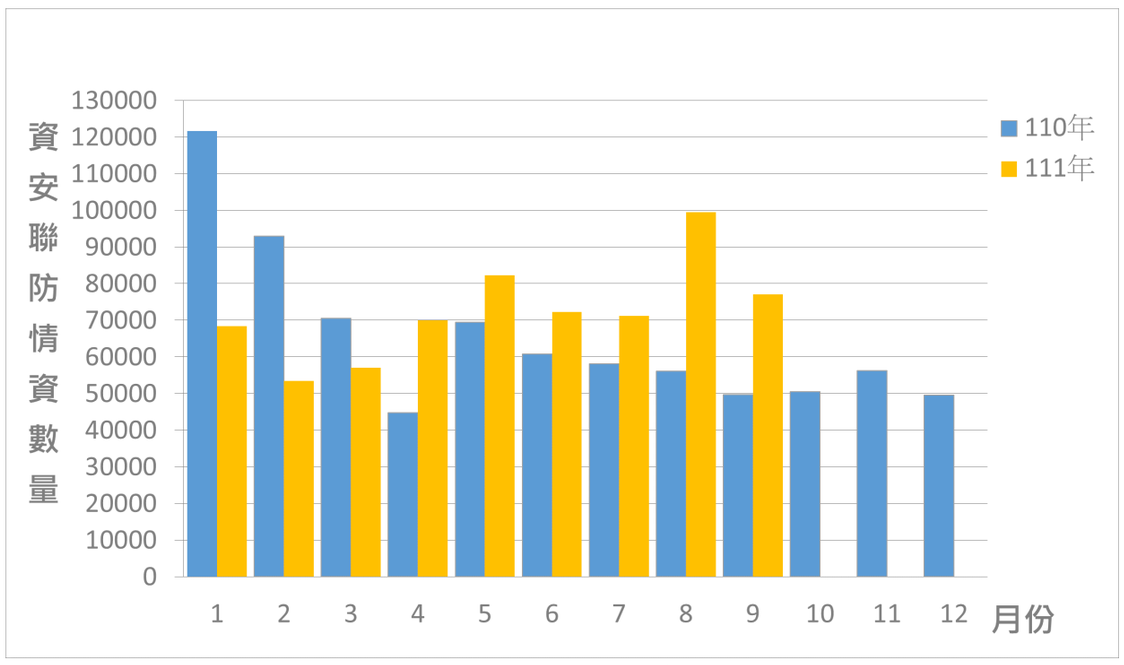

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共124件，近1年資安事件通報統計詳圖2。本月通報事件較去年同期增加45.88%，主要係實兵演練攻擊成功案件較多，為去年同期實兵演練案件之4.36倍，其中多數機關使用第三方應用程式套件CKEditor與CKFinder，因其檔案上傳功能未限制存取，可成功上傳實兵演練圖檔，發現存在不安全組態設定的弱點。

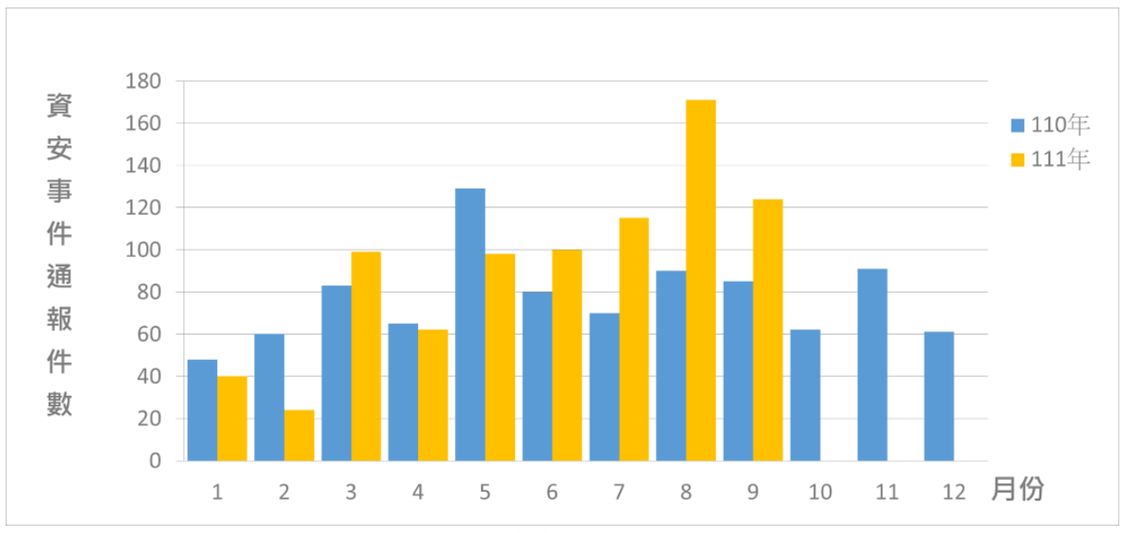

圖2 資安事件通報統計

事後資訊分享

本月偵測發現某機關設備疑似連線至駭客中繼站，嘗試下載殭屍網路相關網路工具，經查發現受駭設備於本年7月曾遭駭客暴力破解遠端桌面登入密碼進而植入惡意程式，因設備老舊已規劃報廢，故未採取進一步處置作為，惟同仁執行網路維護測試時，誤將待報廢設備接上網際網路，導致設備再次連線至駭客中繼站，後續已將受駭電腦重灌並逕行報廢。

個案借鏡：機關應訂定資通訊設備報廢處理相關作業程序，並落實報廢設備管理，統由主責單位進行資料清除或銷毀處理，以避免待報廢設備衍生資安問題之疑慮。

<國內外重點資安新聞>

一、2022資訊服務產業白皮書發表暨資安長聯誼會成立，加速發展產業資安聯防

中華軟協集結理監事與外部資訊專家顧問意見，以數位技術建立經濟、科技、淨零、人文俱進的臺灣為願景，於9月7日發表「2022資訊服務產業白皮書」，提出從國家到產業需涵蓋的五項戰略目標，包括：建立數位強國、促進數位平權、加速數位轉型、強化資安防護與兆元數位服務。

金管會為強化上市櫃公司資安監管機制，明訂2022年底前，依新版「公開發行公司建立內部控制制度處理準則」，需設立資安長與專責單位。有鑑於此，中華軟協亦成立「資安長聯誼會」，協助推動產業資安主管交流、媒合及推廣服務等相關工作，落實資安防護基準。

(資料來源：中華民國資訊軟體協會、經濟日報、工商時報)

二、臺灣資安大會以「數位轉型，資安升級」匯集資安品牌與各界專家

於9月20日到9月22日假南港展覽館二館舉辦第八屆臺灣資安大會，為期三天的活動進行250場以上關於資安的議程與座談，且多達300以上的國內外資安業者參與，共同探討資安動向。

數位發展部部長唐鳳出席大會，就第六期國家資通安全方案（110年至113年），說明將透過數位產業署與資通安全署進行「培植自主創研能量」、「提升關鍵設施韌性」、「主動抵禦潛在威脅」及「提升民間防護能量」等四大推動策略，以建立全民數位韌性。

(資料來源：IThome、中央通訊社)

三、歐盟網路韌性法案草案(Cyber Resilience Act)公布，將智慧裝置納入列管範圍

歐盟執行委員會於9月15日公布網路韌性法案草案(Cyber Resilience Act)，規定從筆記型電腦、行動應用程式到智慧家電，可連結網路的智慧裝置與設備供應業者都必須評估其資訊安全風險，若有網路安全問題產生，需在 24 小時內通報歐盟網路安全局(The European Union Agency for Cybersecurity，ENISA)並採取解決措施，防範歐盟境內網路駭客攻擊。

網路韌性法案草案顯示，違反此法案的相關規定，製造商、經銷商、代理商等供應業者擬將被處最高1,500萬歐元(約1,500萬美元)或年營業額2.5%的罰款，同時歐盟當局可禁止或限制特定產品在其國內市場上市銷售。

(資料來源：European Commission、REUTERS、IThome)

<近期重要資安會議及活動>

為提升機關人員資通安全管理與技術認知，「111年第1次政府資通安全防護巡迴研討會」數位課程已上架於「e等公務園+學習平臺」，歡迎踴躍學習。

<資通安全長及資訊主管異動情形>

無

發布單位：資通安全署　　建立日期：2022-10-14　　更新日期：2022-10-14