張貼日期：2022/08/02

【資安訊息】請各單位加強網站安全檢查，並加強資安維運暨系統之防護

- 主旨說明：請各單位加強網站安全檢查，並加強資安維運暨系統之防護

- 內容說明：
  - 國際政經情勢動盪，國家級網軍活動頻繁，除行政院國家資通安全會報技術服務中心已發布近日可能有大規模網路攻擊行為預警。建議各級機關應提高警覺，加強檢視網頁個資狀況，監控網站異常流量，檢視例行性排程設定與派送機制，如相關日誌發現異常連線或警示，應深入釐清事件原因與影響範圍，避免錯失調查時機。
- 影響平台：無
- 建議措施：
  1. 確認網站服務不中斷，若遭受DDoS攻擊應循「臺灣學術網路 (TANet) 分散式阻斷服務 (DDoS) 通報應變作業指引」申請作業DDoS清洗服務。
  2. 依資安法相關規定，定期審查所保留資通系統產生之日誌(Log)□包含作業系統日誌(OS event log)□網站日誌(web log)□應用程式日誌(AP log)□登入日誌(logon log)□並建議至少保留半年。
  3. 檢視有無異常登入、存取及操作行為。加強監控不尋常或未授權之活動（例如:網站被竄改□log有異常登入、存取及操作行為等）。
  4. 不定期檢視資通訊系統帳號使用情況，並定期變更帳號密碼，確保密碼設定符合複雜性原則，避免字符轉換情況發生。
  5. 針對保有個人資料之網站，強化個資安全防護措施，檢視網站上之公開資訊及公告附件檔案，是否有未經授權之個資檔案放置網站上。建立並落實網站公告內容之審查機制(例如:單位主管審核流程)，若需要公告相關個資請進行遮罩方式處理，以避免造成個資外洩風險。
  6. 確認作業系統、防毒軟體及應用程式(如Chrome□Java)更新情況，並定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為。
  7. 請使用者留意相關電子郵件，注意郵件之來源的正確性，不要開啟不明來源信件的附檔或連結，以防被植入後門程式。
- 參考資料：
  1. 106年Web應用程式安全參考指引(修訂)v2.1_1101231.rar https://download.nccst.nat.gov.tw/attachfilecomm/106%E5%B9%B4Web%E6%87%89%E7%94%A8%E7%A8%8B%E5%BC%8F%E5%AE%89%E5%85%A8%E5%8F%83%E8%80%83%E6%8C%87%E5%BC%95(%E4%BF%AE%E8%A8%82)v2.1_1101231.rar
  2. 臺灣學術網路個資外洩事件之預防與應變指南https://portal.cert.tanet.edu.tw/docs/pdf/2021062504061515474561388386374.pdf
  3. 個人資料保護法 https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20220802_01

Last update: **2022/08/02 15:25**