助產業遠離駭客攻擊

工研院加入FIDO聯盟 共倡五大安全戰略

隨著網路駭客頻繁出現，為了保護產業的資訊安全，工研院積極參與國際標準組織研議產業標準與規範，2月參與「2023 FIDO Taipei Seminar」國際研討會，並與FIDO（Fast IDentity Online）聯盟臺灣分會會員一同展現臺灣零信任資安防護的完整能量。

撰文／編輯部

工研院與FIDO聯盟臺灣分會會員在研討會中一起展示零信任架構的五大關鍵面向，包含保護使用者端的「身分識別」技術、從裝置端登入需多重驗證的「零信任桌面」技術、網路環境端防護的「自動化網路微隔離」機制、伺服器資料端的「隱私強化」技術、在應用程式端只允許經過驗證授權執行的「零信任端點防護」技術，以及最重要的資安風險評級等系統之核心技術。

在展現臺灣零信任資安防護完整能量的同時，更期望協助臺灣產業遠離駭客的攻擊，並在面對駭客攻擊時有其應對能力。

工研院資訊與通訊研究所副所長黃維中表示，數位信任建立在三大基礎上，包含國家身分識別體系、電子簽章法制規範以及資訊安全防護，因此全球各國都必須因應變化快速的數位科技，進一步及時調整相關政策規範，而FIDO標準的推動過程該如何符合當地的法制或規範要求，更是全球化與在地化等齊並重的不二法門。

黃維中進一步分析，對於駭客攻擊，平均必須等待約60天左右，才能發現入侵軌跡，也必須花上約69天時間，才得以修補一個重大漏洞，顯示駭客不僅能輕易的在未修補升級的系統或主機上植入惡意程式，更甚者還能干擾企業營運、影響產品生命週期的秩序。

「駭客入侵、資安防護無疑是搶時間的『攻防競賽』。」黃維中表示，臺灣對此早有應對策略，因我國工業高度發展，製造業產值更超過3成占比，此外如半導體與智慧製造產線，其設備架構變異性小，又是高度機敏性環境，多屬於封閉型設備網路，因此若透過「自動化網路微隔離」機制，再輔以AI人工智慧進一步深度學習端至端的各點路徑，不僅能在網路連結脫離日常路徑時，即時發出警示，還能解決舊系統無法立即更新的風險，完美打造隔離防護網。

工研院與國際共享研發的零信任桌面、自動化網路微隔離、隱私強化技術、零信任端點防護、資安風險評級等系統的核心技術。

工研院除了協助國內產業，在此次研討會中，也大方與國際共享在數位部數位產業署與經濟部技術處支持下所研發的零信任桌面、自動化網路微隔離、隱私強化技術、零信任端點防護、資安風險評級等系統的核心技術。期待在厚植臺灣數位信任與資安防護研發能量之外，更能成為全球供應鏈最得以信賴的合作夥伴。