公務機密宣導

我政府機關遭駭 近3年1709件

行政院資安處資料顯示，自107年至109年7月底止，中央及地方政府機關共計發生1709件資安事件，其中以「非法入侵」占四成二為最多；且107至108年的資安事件中，逾一成五為中、高風險資安影響等級。

臺灣面臨的資安威脅，主要來自中國。法務部調查局曾揭露，中國駭客組織Blacktech與Taidoor，已長期滲透國內政府機關及其資訊服務供應商，試圖竊取機敏資訊及民眾個人資料。

立法院預算中心評估報告也提及，國內接連發生政府機關、企業個資外洩及勒索病毒等資安事件，顯示國際駭客手法詭譎多變，攻擊行為近期更變本加厲。

另行政院「國家資通安全情勢報告」分析，資安事件通報類型以「非法入侵」與「網頁攻擊」為大宗。資安威脅類型方面，國家資安防護中心據去年彙整情資區分出：系統服務、入侵攻擊、阻斷服務、惡意程式、政策規則、掃描刺探、尚需調查等七大類。

【節錄自自由時報電子報】

公務機密宣導

政府資安漏洞很大！

中國近年不斷駭侵我政府機關竊密，外界常分不清是中共網軍或民間駭客所為。軍方背景人士受訪表示，中共對台網路戰有「軍民通用」特性，往往秘而不宣開戰，對外不會承認其駭客攻擊，國際法上難以界定是戰爭行為，但對國安所構成的威脅不容忽視。

根據行政院「國家資通安全情勢報告」，全球勒索軟體攻擊劇增，該攻擊手法於109年有增無減。在網路釣魚攻擊部分，除藉電子郵件外，今年有更多駭客利用簡訊、社交媒體、遊戲平台發動攻擊。

隨著5G時代來臨，市場上越來越多物聯網裝置，資安風險亦隨之升高，正因為5G資料量暴增，也衍生更多隱私保護與資料外洩風險。

美國聯邦調查局曾呼籲大眾，勿將連網攝影機、遊戲機、智慧喇叭等IoT裝置，與家用電腦連接於同一Wi-Fi網路，因為國際駭客可透過IoT裝置入侵Wi-Fi網路，再經由家用路由器擴散到各連網裝置，包括儲存隱私資訊與密碼的電腦。

【節錄自自由時報電子報】

【貼心提醒】

在網路資通訊產品、設備日新月異的今天，資訊安全與你我都有切身利害關係，小則個人資訊遭不當外洩及利用，以致權益受損；大則公務、國家機密遭人竊取，而影響國家安全，尤其現在公務之進行、文書之擅打非使用電腦不可，一旦不慎即有外洩公務機密之可能，要知道，刑法上的洩密罪是有罰「過失」的，也就是說，執行公務使用網路資訊設備不慎洩漏了「公務機密」的話，仍是有刑責的呦，請大家一定要特別小心！