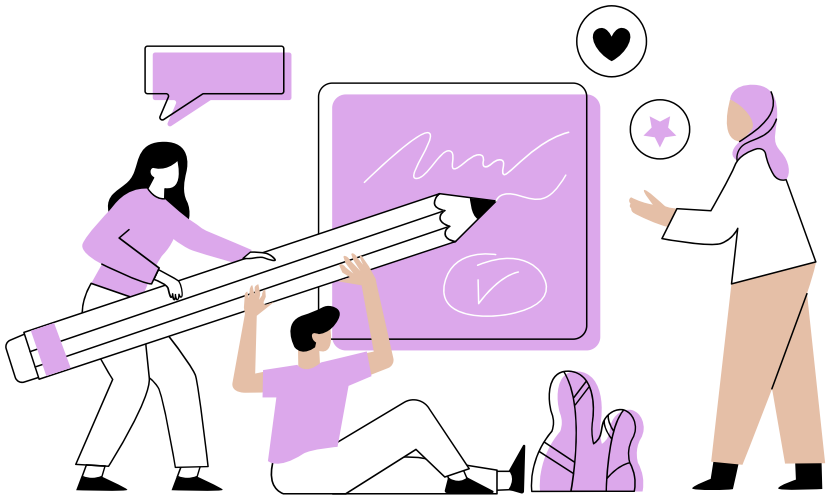
112年8月號

公務機密

# 資訊安全維護



01 資安時事案例

02 個人資料保護法

03 生活中的資安

04 數位學習

https://www.youtube.com/watch?v=nQhOdLGUTTQ

農業部林業及自然保育署臺東分署　政風室

# 【資安日報】6月21日，微軟Azure AD傳出存在OAuth漏洞，可被用於帳號挾持

OAuth身分驗證機制的應用越來越普遍，然而這類機制一旦實作上出現不足之處，有可能造成嚴重的後果。例如，近期資安業者Descope揭露雲端目錄服務Azure AD有個漏洞，取名為nOAuth，並認為攻擊者可輕易利用，將其用於挾持使用者的Azure AD帳號。
駭客鎖定Linux伺服器並透過暴力破解嘗試SSH帳密的攻擊，最近又有一起行動。殭屍網路Tsunami藉由這種手法劫持Linux伺服器，目的綁架這些伺服器用於DDoS攻擊與挖礦。
新的竊資軟體最近也不斷出現，而現在有一支名為RDStealer的這類惡意程式，引起研究人員關注，因為當中外洩資料的手法很特別：他們濫用遠端桌面連線（RDP）向C2傳送檔案。

圖來源: Pixabay

# 小心Wi-Fi遭駭　資安專家「4招」確保連線安全

許多人家中都使用Wi-Fi上網，但要如何保證連線安全無虞，不會遭到駭客入侵，進而導致財務損失？資安專家近日向《太陽報》透露4個關鍵技巧，幫助用戶確保網路安全。

英國網路安全公司SenseOn的技術總監費里曼（Brad Freeman）指出，若駭客駭入Wi-Fi網路，就能監視用戶、釋出惡意軟體並控制設備。使他們能藉機竊取用戶的錢財，或取得私人訊息進行詐騙和敲詐。此外，若Wi-Fi頻寬被他人入侵占用，還會導致網速變慢。為了避免以上情況發生，費里曼建議所有Wi-Fi使用者確認以下4件事。

## 1.　確認設備保持更新

盡可能為手機、平板電腦和電腦安裝安全性修補程式。費里曼指出，設備沒有更新是一個危險訊號。更新往往能修補安全性漏洞，防止設備遭遇網路犯罪。當用戶發現有安全性更新時最好盡快下載，這樣的更新通常免費，且安裝速度快。

## 2. Wi-Fi不要使用預設的登錄訊息

費里曼建議，最好改變家用Wi-Fi網路的預設身份驗證資訊。用戶可以在網路瀏覽器中輸入「http://192.168.1.1」並點擊輸入鍵，即可登入Wi-Fi路由器。進入後就能變更登入資訊。

資安專家指出，必須確保電腦防火牆開啟。（示意圖／shutterstock 達志影像）

## 3.　電腦有無正確安全防護

確認電腦的防火牆開啟，防毒軟體持續啟動。費里曼指出，這是非常簡單的防護方式，可避免常見的網路攻擊。

## 4.　所有設備不要都連接同一個Wi-Fi網路

費里曼建議，如果用戶的家用Wi-Fi支持，可以創建一個訪客用網路。這樣來訪的訪客就能使用訪客網路，而非用戶的私人網路。

# 第 6 條

有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

一、法律明文規定。

二、公務機關執行法定職務或非公務機關履行法定義務必　要範圍內，且事前或事後有適當安全維護措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。

# 扯！中國人民大學畢業生盜全校學生個資設網站 還有「顏值評分表」

即時新聞／綜合報導〕中國今（2）日有網友爆料，一名人民大學碩士畢業的男子盜取校內同學的姓名、照片等個人資訊，甚至還用這些個資設立一個網站製作「顏值評分表」。中國人民大學則回應，目前正配合警方調查。

綜合中媒報導，有網友爆料，中國人民大學高瓴（ㄌㄧㄥˊ）人工智能學院一名碩士畢業生盜取全校學生的個人資訊，包括姓名、照片、學號、生日、出生地等，甚至還製作顏值排行表的網站供人查看。

該網站為公開網站，且已存在3年，網站所提供的資訊包括學生屆數、身高區間、星座、籍貫、科系。甚至還能透過搜尋姓名或學號的方式，看到當事人的顏值分數。製作網站的畢業生曾在2020年發文說「今年和志同道合之士完成了這件我大二就想做的壞事，本來想發朋友圈但人多眼雜怕被打拳還是發微博吧。」但目前他的帳號內容已全數清空。

據稱，該名畢業生曾獲選為「三好學生」、「優秀團幹部」，並且曾以高瓴畢業生代表進行求職分享，而他目前任職於騰訊公司的搜索算法部門。

對此，中國人民大學則回應，已第一時間連絡警方，目前正積極配合警方等相關部門調查，校方也強烈譴責侵犯個人隱私等行為。消息曝光後後，許多網友也紛紛抨擊，「今天敢洩漏人大的，明天就敢洩漏騰訊的」、「沒有一點法律意識，侵犯別人隱私以後還可能會洩漏國家隱私」。

# 台灣製造業供應鏈 被當肥羊 專家：加強員工的資安意識

〔記者徐子苓／台北報導〕根據統計，製造業是勒索軟體攻擊的重點目標，且台灣受攻擊量在全球榜上有名，供應鏈資安也逐漸受到重視；資安專家建議，企業應加強對員工的培訓和資安意識，以防範勒索軟體威脅。

根據資安大廠Fortinet全球報告，去年製造業淪為勒索軟體攻擊的重點目標，更有四分之一的製造業廠商表示，遭索取金額超過一百萬美元。

一名資安專家表示，台灣勒索軟體攻擊多，可能與擁有重要製造業供應鏈有關，且製造業產值高、較難承受營運中斷的損失，因此成為駭客眼中的「肥羊」；但其實像台積電這類大型企業資安防護佳，駭客較難攻破，往往從供應鏈脆弱的環節著手，竊取供應商資料後向企業勒索。

Fortinet資深技術顧問楊光明說，勒索軟體不是新手法，近年對企業的威脅也持續成長中，且攻擊方式越來越多元，包含惡意網站、釣魚郵件誘發企業點擊，導致一些惡意程式被下載到電腦裡，接著探索內部資料或橫向感染等；駭客竊取到重要資訊後，開始「擄物勒贖」，將檔案或系統加密，可能先在暗網販賣賺一票，接著要求受害企業支付贖金，扒第二層皮。

至於是否該支付贖金，專家看法不一。台大電機系教授林宗男表示，美國官方文件不建議受害企業支付贖金，原因是無法保證資料能夠拿回來，且可能讓駭客更囂張；但實務上，企業不付贖金，駭客恐怕就會公布資料，導致競爭對手買下受害企業的機密，所以是很兩難的問題。

企業該如何防範勒索軟體威脅？楊光明說，資安體系中，人員的培訓和資安意識非常重要，企業可建立一些SOP，例如打開郵件時，不要隨意點選連結，或員工發現可疑活動時，即應聯絡公司IT部門來探查，安全地使用公司的資產來對外連線。

# 駭客攻擊全球醫療機構 調查局、長庚醫院聯手抵禦

〔記者吳政峰／台北報導〕近來全球醫療機構遭受駭客惡意網路攻擊越趨頻繁，為防範資安攻擊、避免個資外洩，政府定調「資安及國安」，調查局桃園市調查處日前與林口長庚醫院簽訂「資安合作備忘錄」，未來雙方將透過資安交流、協防應變及經驗分享等方式，建立資安聯防機制，共同守護醫療資訊安全。

林口長庚醫院院長陳建宗表示，長庚醫院自創院以來，即重視醫療資訊的推動，近年為提升醫療照護與服務效能，亦逐步更新醫療資訊系統及各項醫療資訊設備，推行包括OT、IOT資料傳輸、智慧醫療、AI、大數據等數位化應用。但網路的高度聯結需求，同時也可能會面臨駭客及惡意程式入侵的威脅，嚴重的話並有可能影響病人安全，讓資通安全成為醫療場域不得不面對的重大挑戰。

陳建宗指出，林口長庚醫院不遺餘力努力維護資通安全領域，2009年起，為確保電子病歷資料安全，建置安全的醫療資訊環境，開始導入國際ISO 27001資訊安全驗證，迄今每年皆持續接受此國際標準的追查驗證。我國「資通安全管理法」於2019年正式實施後，林口長庚醫院即被指定為A級關鍵基礎設施醫院（即CI（critical infrastructure）醫院）。

陳建宗說明，現狀資安防護範圍除了原有的醫療資訊（IT）部門外，亦涵蓋了醫療儀器（OT）部門，及總務工控（IOT）等系統，因資安防護成效卓越，在2022年獲衛福部遴選為全國首次進行醫療資安攻防演練的示範基地，目前也是衛福部認可的資通安全A級機構。

陳建宗表示，現進一步與桃園市調處簽立資安合作備忘錄，相信未來可藉由桃園市調處的專業協助，提供事件鑑識、溯源查處與資安防護建議，共創公私協作資安防護網並保障民眾就醫權益。

桃園市調查處處長李文義指出，林口長庚醫院是全國最大醫學中心、全國醫學教育與醫學研究的重鎮，為全球通過JCI國際醫院認證的最大單一量體醫療機構，同時也是衛福部核定的國家關鍵基礎設施資通安全Ａ級機構。

李文義認為，本次藉由「資安合作備忘錄」的簽署，以建立即時通報、迅速處置的資安聯防機制，有效強化資安防護措施，以達早期預警，緊急應變及持續維運的成效。