公務機密維護 -「帳號密碼的安全」

前言

當資訊變成數位型式後，雖然傳遞的速度變快，有助於社會的進步，但是機密資料外洩的機率也相對增加；為了保護數位資料的安全，大多數的系統都是採用帳號、密碼的方式，做為把關篩選的工具。

據報載，美國佛羅里達州的坦帕大學（University of Tampa）的學生，在某堂電腦課程練習搜尋技術時，赫然發現可從 Google 上找到 6,818 筆該校的學生資料，包括學生證號碼、社會安全碼、姓名與生日等，這些資料外洩的時間從 2011 年的 7 月 12 日至 2012 年的 3 月 12 日，期間長達 8 個月之久，受影響的學生總計達三萬餘人。

幾乎在同一時間點的 3 月 15 日，世界著名的資訊安全大廠推出一種新的網路安全產品，號稱可以將會員的個人帳號、密碼，由客戶端（Client）的電腦主機移到該公司的伺服端（Server）保管儲存，要登入時可自動回填資料，如此一來，就可以減少客戶端的電腦被駭客入侵時，導致個人帳號密碼被竊的可能性。

小潘在看到這兩則新聞後，基於工作上的敏感性，很快就聯想到：我們在生活中經常要靠帳號密碼登入系統，如上班時開電腦要用帳號密碼，領錢的時候使用自動提款機也要密碼，上網寫 blog、登入 Facebook，都要帳號密碼，那麼多的帳號密碼存在不同的系統中，如果系統被駭客入侵，豈不是「全都露」了嗎？

趁著與司馬特老師下午茶的聚會，小潘提出他的疑問：資訊系統的安全大多靠帳號密碼來驗證使用者的身分，很多系統

在使用者輸入帳號密碼後，下一次再登入時，會自行帶出來，方便使用者不用重新輸入，系統為什麼會這麼聰明？

對於小潘的問題，司馬特老師喝著焦糖瑪琪朵說：當我們使用網頁瀏覽器登入系統需要輸入帳號密碼時，常因偷懶而勾選「記住密碼」，這些資料就會被系統記錄在 cookie 檔中；當使用者再次登入時，系統會自動到 cookie 檔中找到帳號密碼，以減少使用者重新輸入的麻煩。聽到這裏，機警的小潘又提出疑問：一旦系統遭到入侵，駭客把 cookie 偷走，找到使用者的帳號、密碼，駭客豈不是可以光明正大地登堂入室、為所欲為？司馬特老師在喝口咖啡後，一邊稱讚小潘能舉一反三，一邊繼續說明：為了要避免駭客入侵把個人的帳號密碼竊走，在設定密碼時，一定要選用複雜度較高的密碼，而且還要經常性更換，如此電腦較不易被駭客入侵；另外，在輸入帳號密碼時也要注意，盡量不要勾選「記住密碼」，以免增加遭駭客入侵的風險。小潘聽後又提出新的問題：微軟的作業系統常常不受控制，自動會記錄一些 cookie，一般人又不知道它記了些什麼，要怎麼防範？司馬特老師回答說：沒錯，微軟的作業系統會自動記錄使用者無法預期的資料，為了避免被記錄機敏資料，危害個人資訊安全，使用者應養成定期清理 cookie 的習慣，不要讓電腦中存在著可能的危安因子。小潘接著又想到在報上看到的網路安全產品，繼續問道：帳號密碼存在自己電腦的 cookie 中會被偷，如果放到雲端呢？因為像有專人看守著，是不是比較安全呢？司馬特老師喝了口咖啡笑著說，cookie 中的資料是以明碼的型式存放，安全性很低；而伺服端的資料若經加密，即使是管理者，如果沒有金鑰，也無法解密，安全性相對較高。但是，資訊並不是放在伺服端就百分之百的安全，因為解密技術的進步，駭客只需花較長的時間，雲端資料庫也有被入侵的可能性。

結語

資訊戰其實是一場矛與盾的戰爭，不管防禦方築的牆有多高，攻擊方總會不斷地精進武器攻破城牆；既然無法阻擋敵人竊取、破解我們的密碼，最好的方式就是要經常地更換新密碼，也就是說一個密碼不能使用太久，因為破解密碼需要花相當長的時間，即使舊密碼被破解，只要密碼一經更換，駭客就無法再登入系統竊取資料。因此經常性地更換密碼，是保護電腦不被入侵非常重要的一個觀念。。

政風室關心您