資訊系統密碼的管理

◎魯明德

我國漁船廣大興 28 號遭菲律賓公務船掃射致一名船員被槍擊死亡事件，引發國人不滿情緒高漲，造成兩國關係緊張，意外地演出一場網路大戰。首先是匿名的菲國駭客對我國政府及民營企業發動網路攻擊，緊接著國內網友也在網路上發起反擊行動，甚至直接拿下菲律賓的 DNS，同時也取得大量菲律賓網站的帳號、密碼，並在網路上公布。

這個新聞事件引起小潘的注意，心想：在高度資訊化的時代，我們每天都要接觸網路，而大多數具有權限管理功能的網站，在登入時均會要求使用者輸入帳號、密碼，以做為身分認證之用；如果這些網站的帳號、密碼這麼容易被取得，對使用者而言，豈不是危機四伏嗎？

在師生的下午茶約會中，小潘把握時間提出他的疑問：如果網站的帳號、密碼這麼容易被竊取，為了避免損失，我們是不是要在不同的網站使用不同的帳號、密碼？難道網站管理者不需要有什麼作為嗎？

司馬特老師喝口焦糖瑪琪朵後娓娓道來：網路安全不是只靠使用者或網路管理者單方面可以完成；除了防火牆、防毒軟體等設備外，管理上也是不可或缺的；在系統端的密碼管理，要從系統設計上去考量，存放使用者帳號、密碼的資料庫，如果只用明碼來儲存，就會產生這次菲律賓的案例，一旦遭到入侵，使用者的帳號、密碼就會全部被竊取。所以存放使用者帳號、密碼的資料庫，應該用加密的方式儲存資料。

司馬特老師看出小潘略顯疑惑，就提了一個問題：你郵局提款卡的密碼忘記了怎麼辦？小潘剛好前陣子發生過，於是很有經驗地回答：郵局會給一組新的密碼，讓您登入後再去改。司馬特老師接著問：郵局為什麼不能告訴你原來的密碼，而要另外給你一組新的？如果系統管理者能看到你的密碼，你會擔心什麼事？小潘直覺地回答：當然是擔心錢可能會被盜領，可是這跟給新密碼有什麼關係？

司馬特老師繼續說：郵局之所以給你新的密碼？就是因為連系統管理者也看不到使用者所設定的密碼；所以當使用者忘記密碼時，他只能給一組新的密碼，這樣做的好處除了可以防止系統的管理者監守自盜外，即使系統遭到入侵，也能確保使用者密碼的安全。

小潘又開始好奇了，接著問道：什麼是加密？要怎麼做？司馬特老師喝口咖啡後繼續說：加密就是透過一個演算法，把原來用明文顯示的資料，轉換成用亂碼顯示的密文。以郵局的密碼為例，當存戶在提款機上更改密碼時，所輸入的密碼資料是明文，系統會以其內定的加密演算法，把存戶所輸入的密碼轉換成密文，再儲存於資料庫中；既然在資料庫中存的是密文，自然連資料庫管理員都無法看到，這就是為什麼存戶忘記密碼時，系統需產生一組新密碼的原因。透過這樣的機制，即使系統遭到駭客入侵，也可確保密碼的安全。

對於網站帳號、密碼的管理，除了系統端要有管理制度外，使用者對密碼的管理也要注意。國外 SplashData 網站每年都會公布最糟糕的密碼排名，根據該網站的調查，最近 3 年最糟糕密碼排名前 3 名是：password、123456、12345678，這也間接提高密碼被破解的可能性。

Intel 最近推出一個可以評估密碼強度的網頁，當使用者輸入任何字元，網頁便會計算以暴力破解密碼所需的時間。結果發現：由數字及字母組成 6 個字元的密碼，在 1.18 分鐘就被破解；如果密碼結合了數字與英文大小寫字母，則強度馬上暴增，需要很長的時間才能破解。

從這些容易被破解的密碼資訊可知，在使用者的密碼管理上，應該要避免使用順序或重複的字元、避免使用與登入名稱相同的密碼、避免使用任何語言字典中的單字作為密碼，才能提高密碼的安全性。

小潘在聽完司馬特老師的一番說明後，對於資訊系統的密碼管理，有了更深一層的了解。原來系統的安全，除了靠防火牆、防毒軟體的工具外，管理制度也是很重要的；由菲律賓網站被入侵造成的密碼外洩事件，正好可以檢視自己單位的資訊系統安全性，適時地修補漏洞，以防止危安事件的發生。