常見社交工程的攻擊模式與防範之道

加強使用者辨識社交工程攻擊的能力，才能有效防制並降低損害。

資料來源：法務部調查局清流月刊(102 年 9 月號) ◎劉嘉明

近來偶聞政府機關遭受駭客入侵事件，在此簡單討論資訊安全的概念及如何避開駭客攻擊。

駭客攻擊最常見的方法是社交工程攻擊，亦即將背景危害行為隱藏在使用者允許之表面行為中。簡言之，任何經過使用者允許的網路行為是無法獲得資安設備保護，而僅能由後續行為分析發覺資安事件；而二者的時間若太長則很可能導致蔓延擴散、災情擴大。

最常見之社交工程攻擊包含「惡意掛馬網頁」、「USB 惡意程式」、「惡意郵件」以及「差異性攻擊」，簡述如下。

一、惡意掛馬網頁：係指網頁內嵌惡意程式，當使用者瀏覽網頁時會自動執行此惡意程式，造成資料外洩等危害。相關入侵方式另有藉由電玩隱藏後門，或網頁提供「清涼」照片、影片等引誘使用者點選中駭。

二、USB 惡意程式：常見的方式是透過自動執行程式（autorun.inf）進行病毒傳播與執行；最新方式是透過隱藏檔及變更副檔名的方式，引誘使用者點選執行偽造的檔案或資料夾導致中毒。

上圖係曾經插入中駭電腦的行動碟，行動碟被放入惡意程式「temp.exe」且不顯示副檔名，而正常目錄「temp」被修改成隱藏屬性，因此使用者很容易將惡意程式「temp.exe」誤認為是正常目錄「temp」，執行後將造成危害。防制方式是將隱藏檔及副檔名開啟顯示，如遇到無法將隱藏檔及副檔名開啟顯示，即可能是中毒之徵兆。

三、惡意郵件：因使用者皆受防火牆保護，無法採用正面的網路攻擊。主要方式是寄發引誘使用者開啟附件的惡意郵件，可能為惡意程式之副檔名格式包含 PDF、DOC、PPT、XLS、RAR 等。過濾惡意郵件可採用下列方式:(一)刪除不明的信件。(二)由虛擬電腦開啟(三)向寄件人確認郵件真偽；但須慎防寄件人是不知情的轉寄者，而將含有病毒之信件轉寄，若此則電話求證亦無法得到正確答案。

四、差異性攻擊：目前病毒或後門程式已逐漸不採用大量感染方

式散播，而是針對不同的特定對象分別使其感染不同的惡意程式；此種攻擊方式使防毒軟體無法透過病毒碼的更新來修復眾多個別對象的受感染電腦，進而降低防毒軟體之功用。

降低社交工程攻擊的主要方式是提升個人資安意識與觀念，加強使用者辨識社交工程攻擊的能力，才能有效防制並降低損害。受駭過程很有可能是先從住家的電腦串聯至公務電腦，因此建議自家電腦的資訊安全亦請一併改善。個人電腦資安依優先順序建議改善方式如下：

一、使用系統最小權限：盡量少用管理者權限開機。電腦使用者多數時間是使用文件編輯與網頁瀏覽，標準使用者的權限即可符合需求，如有必要進行系統設定或程式安裝，再使用系統管理者權限登入執行。因標準使用者的系統存取權限較系統管理員低，可避免中毒時病毒程式直接存取或修改系統檔案。

二、啟動個人防火牆：當內網有電腦中駭後，駭客即可藉由該受駭電腦作為中繼站輕易穿越防火牆，因此單位之公用防火牆立即失去功用。而作業系統提供之個人防火牆在此情況下仍可繼續提供保護，避免遭內部之受駭電腦波及。

三、運用虛擬電腦：使用虛擬電腦軟體（如：Virtual Box、VMWare、Virtual PC 等），在個人電腦建立虛擬的電腦環境可以安裝作業系統、

執行軟體測試或開啟不安全的檔案，兩個系統的資料與程式不會互相干擾或影響，可同時運作。因虛擬的電腦環境與實體的電腦環境有所區隔，可避免直接感染實體電腦或存取實體電腦的個人資料。

四、開啟事件檢視器：開啟較詳盡之 Windows 事件檢視器，如應用程式記錄檔、安全性記錄檔及系統記錄檔等，可記錄程式執行事件、有效與無效的登入事件，以及系統元件執行所記錄的事件，有助於事後判讀與調查非法入侵或存取的來源及原因。加大儲存事件紀錄之空間，可保留較長時間之事件紀錄。