工作效率與資訊安全間的兩難

◎魯明德

由於平板電腦及智慧型手機越來越普及，且功能越來越強大，很多企業剛開始為方便高階主管出差在外，處理公事不便，而開放高階主管可以使用手持式裝置登入公司電腦，以免耽誤公事；漸漸地，這股需求已經蔓延到員工了。公司的業務人員因為需要長期在外，常常乘著空檔利用自己的電腦就把工作完成，等回公司再複製到公司的電腦，導致公司的電腦常因此而中毒。在資訊部門工作的小潘，接到長官指示，要他研議如何提升公司的資訊安全。

小潘心想：如果把電腦的USB介面都封起來，不就可以解決了嗎？但是，資訊部門的工作應該不是防弊，而是積極興利才是；業務人員利用工作空檔整理資料，等回公司再複製到公司的電腦，可以提升工作效率，資訊人員要防止的應該是危安事件才是。

利用師生下午茶約會的時間，小潘把這個問題提出來跟司馬特老師討論，司馬特老師喝口咖啡後娓娓道來，讓員工使用自己熟悉的設備，是可以提高工作效率，且對企業主而言，還可以節省軟硬體設備的支出，以及另外花費時間和金錢安排教育訓練；但是，相對地也隱藏了一系列企業資料外洩與安全性的問題。

根據國際電腦安全協會報告：60%的洩密事件，是來自企業內部，只有15%是來自外部入侵；表示企業對於自己內部資訊機密的保護作為，還不是很周全。商業管理協會的研究報告也指出：白領工作者平均每週處理11份機密營業文件，而且這些機密文件常常會在不必要的情況下曝光。另外，39%的工作者曾經將客戶資料寄出公司；52%的員工曾在離職時，將工作資料帶走；86%的員工坦承習慣性將郵件轉寄其他人；26%的員工甚至會使用免費信箱寄送工作資料。由以上的研究發現：企業的危安事件大部分來自內部。

以往企業對於資料外洩防護所做的資訊安全措施，不外乎是：檔案加密、可移除式媒體控管及網路監控。採用檔案加密的方式，需要額外的軟、硬體配合，初期有建置成本，執行中有維護成本。也有企業採用可移除式媒體控管的方式，它的主要做法是：要求人員出入辦公場所時，交出手機，或是在電腦的USB介面上貼封條，並由中央控管所有終端電腦的儲存裝置，需特定人士核准才能使用。此舉不但不夠人性化，還會造成工作上諸多不便。至於透過側錄、監控、記錄，或限制藉由網路流通的未加密文件檔案的方式，如E-mail、Skype、http、ftp等作業，防範機密文件透過網路而外洩的方式，除不夠人性外，這些管制行為，通常無實質控管功效，僅能在事後稽核時產生作用。

聽完司馬特老師的說明，小潘又問道：現在手持式裝置的功能強大，又可提升工作效率，應該如何管理才好呢？司馬特老師喝口咖啡繼續說：由於智慧手持裝置的規格接近PC，包括大容量的儲存能力、各式各樣的應用軟體等，許多PC可能遭受的攻擊，包括詐騙網站、惡意軟體，一樣可能透過這些智慧手持裝置而入侵企業內部。此外，由於智慧手持裝置的體積小，又容易攜帶，遺失或失竊的風險大增，存放其中的客戶資料、公司機密或財務資訊，可能就會因此外流。

但由於它可以讓員工利用瑣碎的時間處理公事，提升工作效率，禁止或開放對企業而言是個兩難的問題。日本的NTT調查發現，超過50%以上的員工會自行攜帶智慧型手機上班，但只有20%左右是真正得到企業正式同意，顯示員工真的有此需求。

對於資訊安全的管理，應該是從需求面去疏導而不是一味地防堵。在硬體上，可以透過雲端服務、加密通信網路及多重身分驗證等機制，讓員工即使是使用自己的私人設備，也不會讓企業的重要資訊留存在裝置上，如此一來，如果員工的手持式裝置遺失或失竊，也不會造成企業的機密或客戶的資料外流，從而維護資料的安全。在管理上，也要訂定使用規範，讓員工知道自己的權利與義務，並時時稽核。唯有落實管理制度，才能維持資訊的安全。

（作者為科技大學資訊管理系講師）

▲Top

清流月刊中華民國一百零二年九月號

DNS反射式攻擊所進行的分散式阻斷服務攻擊雖然難以防禦，只要DNS伺服器正確地設定，還是可以降低其成功的機率。

認識DNS反射式攻擊

◎李柏毅

不久前，全球最大的非營利反垃圾郵件組織Spamhus遭到代號「Operation Stophaus」的大規模網路攻擊，該波網路攻擊的最大流量高達300Gbps，除了導致Spamhus的網路服務中斷超過一個星期外，也嚴重影響全球用戶的網路使用。在Prolexic的數位鑑識報告中指出，上述「Operation Stophaus」的攻擊有92%是透過DNS（Domain Name Server）伺服器所進行的反射攻擊。攻擊者使用Spamhus伺服器的網路位址來偽造網域名稱查詢需求，同時傳送給上千臺DNS伺服器進行遞迴查詢（Recursive query）；透過遞迴查詢，原本的攻擊流量迅速增強數倍，並透過合法的DNS伺服器傳送給Spamhus的伺服器，在短時間內造成系統過載，導致中斷Spamhus的外部服務。

在這個案例中，攻擊者就是使用DNS反射式攻擊來進行分散式阻斷服務攻擊（DDoS）。攻擊者對目標主機發動密集且來源分散的網路存取行為，來達到消耗目標主機網路頻寬以及運算資源的目的，藉此降低目標主機的對外服務品質，甚至導致服務中斷。

這樣的攻擊手法大幅降低了DDoS攻擊的啟動門檻。以往攻擊者想要發動大規模DDoS攻擊，都必須指揮全球各地超過百萬臺的電腦主機組成的殭屍網路（Botnet），同時對目標進行密集的網路存取動作；但是透過DNS反射式攻擊，攻擊者只需要使用一臺電腦主機，就可以利用全球超過百萬臺開啟遞迴查詢的DNS伺服器，作為攻擊流量的增幅器（Amplifier），可在短時間內創造超過100Gbps的攻擊流量。

這種新型態的攻擊手法雖然難以防禦，但還是有方法可以降低其成功的機率。只要單位內的DNS伺服器能夠被正確地設定，關閉預設的遞迴查詢功能，並僅開放DNS查詢服務給予經過授權的客戶端使用。如此一來，DNS伺服器就不會遭到有心人士的利用，成為另一波DDoS網路攻擊的幕後幫凶，同時也可以為網路安全盡一己之力。

（作者為國家實驗研究院國家高速網路與計算機中心網路與資安組助理工程師）

▲Top

清流月刊中華民國一百零二年九月號

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。

常見社交工程的攻擊模式與防範之道

◎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。

▲Top