清流月刊中華民國一百零三年二月號

資訊系統隨著電子商務的興起，不僅在技術架構上要有所修正，另亦可從入侵攻擊的成本效益考量，方能讓駭客無功而返。

資訊系統的安全設計

◎魯明德

高速公路電子收費系統（Electronic Toll Collection, ETC）喊了多年之後，在贊成與反對聲浪的糾葛中，終於在今（103）年上路了。原先報導ETC系統才上路，即在第一天的三個半小時內，遭到來路不明的阻斷式服務攻擊達82億次，造成系統緩慢而無法回應餘額查詢；後來雖證實純屬烏龍，但科技新貴小潘看到這則新聞後，想起以前在上課時，好像也沒有見過這麼密集的攻擊方式，設想如果自己公司的系統遭到類似的攻擊，該怎麼預防？於是，趁著農曆年前的師生下午茶約會，趕快提出來跟老師討論。

司馬特老師聽完小潘的問題，喝口咖啡表示，網路越來越普及，人們對網路的依賴也越來越大，尤其在雲端技術成熟後，當大量的資料都透過網路存取時，資訊安全的議題更顯重要。

早期的觀念中，建置資訊系統的目的是資料共享，所以在設計資訊系統時，會把各部門獨自存取、管理的資料，放到資料庫以求資料一致性，並減少各部門重覆建置的工作。但是，之後的資訊系統已經不再只是intranet，除了內部顧客外，還要把供應商、經銷商整合進來，成為一個供應鏈，事情也就開始複雜；直到B２C（Business to Consumer）的電子商務興起，使用者已無法有效控制，資訊系統的安全就變成重要的議題。

在資訊共享的時代，因為系統環境是intranet，外部威脅較輕，在規劃資訊系統時，可以允許應用程式直接存取資料庫。當系統放到internet上讓外部客戶使用時，直接存取資料庫的設計比較簡單，但相對地系統的風險就會變高，因為我們不知道會有哪些人在何時將非法入侵系統，也無法預期他們入侵後會對系統做些什麼事。

為了增加系統的安全性，在系統設計時，開始把以往二層式（２-Tier）的主從式（Client-Server）架構做些修正，把用戶端及伺服端涉及商業邏輯的部分單獨分離出來，變成使用者介面層（Presentation Tier）、商業邏輯層（Business Logic Tier），以及資料服務層（Data Services Tier）的三層式（３-Tier）架構。

其中使用者介面層負責接收使用者的資料輸入，並將結果顯示出來，如瀏覽器或其他用戶端的應用程式。商業邏輯層為使用者介面與資料庫的橋樑，負責商業法則、與業務有關的資料處理、網站伺服器等工作，如使用網際網路資訊服務（IIS）的網站伺服器，取得應用服務提供商（ASP）撰寫程式，並透過分散式元件物件模型（DCOM）與MTS（Microsoft Transaction Server）的元件相溝通，再透過開放資料庫互連（ODBC）與各種支援ODBC的資料庫相連接。資料服務層負責資料庫或訊息的處理，譬如使用結構化查詢語言（SQL） Server資料庫的預儲程序，或使用微軟訊息陣列（MSMQ）做資訊處理等。

這樣的架構在存取資料時，使用者的需求，需經過商業邏輯層的中介處理，可以適度防止使用者直接存取在第三層的資料庫，也減少危安事件發生的機率。

小潘聽到這裏，對於資訊系統的設計有更深一層的認識，也發現在學與用之間的知識落差。小潘接著想到非法入侵可能造成個人資料洩漏的問題。司馬特老師繼續說明，資訊系統不僅是資訊科技的問題，也要從經濟學的角度去思考。駭客的入侵其實也有其成本效益的考量，如果入侵的成本與預期的成果不成比例，他就不會來了，例如花費許多的時間與人力，拿到的卻是沒有價值的資料，或是不能造成對方系統的損失，他就不會再發動攻擊。

基於這樣的考量，如果ETC真的被入侵，那麼駭客想拿到什麼？不外乎是想竊取車主的個人資料，或竄改儲值餘額造成混亂。如果把系統中的車號與儲值餘額等資料，單獨放在另一個資料庫中，使用者查詢時都到這個資料庫去查，當駭客大費周章入侵後，便無法達到他的目的。

小潘聽到這裏，對於資訊系統的規劃及資訊安全的作為有新的認識，原來資訊系統的安全，不只是資訊科技的議題，也跟經濟學有關；他對司馬特老師全方位的學術素養更加景仰。本次的師生下午茶約會，隨著華燈初上也劃下休止符。

（作者為科技大學資訊管理系講師）

▲Top

清流月刊中華民國一百零三年二月號

國際間的權力競逐，戰場已從實體硬權力的對抗延伸至虛擬空間，各國之間表面和解，但在網路世界的衝突現象將會越來越常見。

中美競逐的虛擬戰場－網際網路

◎李政鴻

美國國家安全局前僱員史諾登揭露美國政府過去幾年所進行的機密監控稜鏡計畫（Prism），至少在全球執行六萬次任務，包括香港及中國大陸的學校、研究機構及政府機關等均列為目標，史諾登的爆料引起外界強烈批評美國政府。無獨有偶，過去數個月來，美國主流媒體紐約時報，也用大篇幅報導有關中共位於上海的網軍「61398部隊」；五角大廈在中國軍力報告書內亦指控不斷遭受中共網軍的綿密攻擊。

這兩起事件凸顯國際關係已開始邁入虛擬時代。網際網路創造虛擬空間，改變人類生活習慣，同時也替傳統國際關係開闢另一競逐場域。戰爭衝突的形式不再限於熱戰（hot war），舉凡人民、團體及組織，只要擁有電腦和網路，即可發動網路鍵盤戰。然而與電腦駭客不同的是，當國家正式編組、運用資源和選擇攻擊目標，亦即國家成立網路部隊，代表著網路戰爭將可能是國家間衝突的選項，規模幅度和攻擊能力，也隨著彼此的數位落差而產生鴻溝。

基本上，網路戰爭作為新型態衝突模式，具有以下幾點特色：首先，攻擊不以生命傷害為必要目標，而是破壞敵方指揮系統，或是擾亂金融秩序；其次，網路的隱密特性，使人難以確切掌握敵方攻擊的證據，縱使被懷疑發動網路攻擊，仍可推諉不知情；第三，經由網路系統及伺服器連結，即可簡單發動攻擊，門檻並不高；第四，資訊科技克服傳統地緣政治限制，以及地理空間對國家形成的自然障礙，網路攻擊可從全球各地發動。

九一一恐怖攻擊後，美國政府積極強化網路安全作業，2008年小布希政府推動「國家網路安全綜合計畫」（CNCI），並將其列為機密；不過根據媒體報導，美國政府花費約四百億美元。歐巴馬上任後，從部分解密文件中，可看到美國網路安全計畫的主要目標為以下三點：

一、以聯邦政府為核心，強化中央地方、公私部門連結與合作網絡，提升對網路威脅事前監控、防範能力，以及增加快速反應能力。

二、增強美國政府反情報能力以及資訊安全維護，提升應對全面網路威脅的防禦能力。

三、透過教育、協調和研發，重新定位美國的網路戰略。

此外，美國國防部成立「網路戰聯合司令部」，空軍成立「網路指揮部」，陸軍成立「陸軍電腦緊急反應小組」，海軍也成立「海軍電腦事件反應小組」，說明了美國制定網路戰略、提升網路戰力同時，也試圖結合實體軍事實力。

報載的稜鏡監控計畫，充其量僅算是美國網路大戰略的一環。然而實際上，美國的網路戰力並未如實體軍事能力在全球享有絕對的超強地位。在網路虛擬的世界裡，中國大陸是美國最大的挑戰者，去（102）年４月中國大陸發布的《中國武裝力量的多樣化運用》白皮書，雖然公布各兵種及總軍力280萬，但未詳列戰略導彈部隊二炮及網軍人數，顯示中共推動國防透明化的過程，仍不願公開敏感軍種。不過根據國安局估計，中共網軍人數超過10萬，而上海浦東「61398部隊」則是中共網軍的大本營。在中共極度機密維護下，外界很難真正評估其實力。

中共網軍實際上面臨著雙面作戰局面：一方面對內建立「超級防火牆」，以網路過濾裝置對人民進行網路言論限制，封鎖外界不利於北京當局的網頁內容。最著名的例子為北京試圖實行綠壩措施，以進入廣大的中國大陸市場作為條件，強制所有廠商出售電腦設備時，必須事先安裝「綠壩－花季護航」軟體，此一措施美其名為防止青少年遭受網路的不良資訊影響，實際上在監控人民的網路言論，最後則在民間壓力下終止；另一方面，中共網軍不斷對外測試虛擬戰力，駭入各國目標的結果，反而引發新一波網路軍備競賽，有組織的駭客任務層出不窮，網路空間儼然呈現熱戰局勢。

根據聯合國報告，目前全球共有46個國家成立網路作戰部隊，換言之，除陸地、海洋、天空及太空之外，網路空間這一「第五空間」已被正式納入作戰範圍。國際之間的權力競逐，特別是「中」美之間，戰場將從實體硬權力的對抗延伸至虛擬空間，網路戰爭不再是遙不可及，已成為新式戰爭型態，各國也紛紛投入資源建立此一新興戰力。整體而論，網路科技使得既有的國際政治結構更趨複雜，難以捉摸，於是各國之間表面和解，但在網路世界的衝突將會越來越常見。

▲Top

清流月刊中華民國一百零三年二月號

電子郵件社交工程演練應該是一種長期性、持續的演練工作，才能時時讓電腦使用者有所警覺，不輕易開啟可疑的信件。

淺談電子郵件社交工程演練

◎吳信東

資訊安全工作一直都是各公、私立機關、公司、學校的電腦部門最重要的工作之一，資訊安全除了仰賴價格不便宜的軟、硬體設備，如入侵防禦系統（IPS, Intrusion Prevention System）、防火牆系統、防毒軟體、郵件過濾系統及漏洞修補系統…等之外，更重要的是，所有的電腦使用者也必須要有高度的警覺心，對於任何可疑的檔案複製、超連結、電子郵件，以及上、下載傳輸資料，都要小心謹慎地使用，避免因為一時的疏忽，輕則個人的電腦資料遭毀損或竊取，重則整個機關、公司、學校的資料被竊取或毀損。要提高電腦使用者的警覺心，資訊人員便需要定期或不定期辦理各種資安工作演練。

電腦使用者之間互相傳遞或分享照片、檔案、訊息等，可以使用的工具相當多，常見的包括社群軟體（如臉書Facebook）、Skype、Line及雲端硬碟，而電子郵件可以算是歷史最久，也依然最普遍被使用的工具。各式各樣利用電子郵件的攻擊和威脅，如病毒郵件、釣魚郵件、炸彈郵件、內部異常濫發郵件等攻擊，也如影隨形存在至今。如何提醒電腦使用者不要開啟來路不明的電子郵件，或可疑的電子郵件，不僅成了資訊管理人員的重要工作之一，也是資安工作重要的一環。

為了訓練及養成電腦使用者不開啟可疑或來路不明電子郵件的習慣，資訊管理人員大都使用「電子郵件社交工程演練」方式，即利用假名字的寄件者，以吸引人閱讀的郵件主旨，誘惑收件人打開電子郵件，甚至點閱該郵件的附件，進而回傳至系統後台，統計有哪些電腦使用者點閱了多少封可疑的電子郵件；資訊人員便可針對警戒心較弱的同仁，加強教育訓練宣導，以提高資訊系統的安全度。

另外，社交工程演練的電子郵件，必須具備多樣性才足以吸引使用者開啟。以筆者服務的機關而言，最近一次的演練郵件，類型包括休閒、娛樂、情色、保健、財經、政治等各方面，郵件主旨如「Candy Crush Saga全關卡破關攻略」、「主播吳O潔睡衣半開」、「善存的新聞—有在吃的朋友看清楚了」、「Costco十大必買」、「三流說風暴—七成網友認為陳〇文發言失當」、「睡不好又打呼 罹患惡性腦癌風險提高47%」等；其中被開啟點閱的信件，經過統計後，最高的是「善存的新聞—有在吃的朋友看清楚了」及「Candy Crush Saga全關卡破關攻略」，顯見保健相關資訊和熱門的Candy遊戲，比較容易吸引電腦使用者開啟閱讀；而原先以為可以獲得較高開啟率的情色郵件，可能因為電腦使用者易產生警覺心，實際被開啟率反而不高。

電子郵件社交工程演練本來應該是一種長期性、持續的演練工作，這樣才能時時讓電腦使用者有所警覺，不會輕易開啟可疑的信件。但是在實務上，礙於機關資訊人力有限，所以通常只能擇定一段時間範圍內（例如１年２次或每季１次），進行彈性不定時演練；以筆者服務的機關而言，101年進行了２次演練，第１次演練人數為803位同仁，其中188位同仁開啟郵件，112位同仁點閱郵件附件或點閱超連結，開啟率及點閱率分別為23.41%及13.81%；第２次演練人數為823位同仁，其中158位同仁開啟郵件及80位同仁點閱郵件附件或點閱超連結，開啟率及點閱率分別為19.19%及9.27%；102年第１次演練結果，演練人數為827位同仁，其中152位同仁開啟郵件及36位同仁點閱郵件附件或點閱超連結，開啟率及點閱率分別為18.37%及4.35%。

由這３次演練成果比較，開啟率由23.41%下降到18.37%，點閱率由13.81%下降到4.35%，顯見透過機關內部經常性的宣導，再加上實際演練後，電腦使用者確實會產生警覺心，因此開啟率及點閱率均有進步；但開啟率在101年第2次演練由19.19%到102年第1次演練僅下降到18.37%，進步較小，分析其原因，可能是有部分新進同仁初到機關工作，對於可疑電子郵件的警覺心尚未建立，致機關整體進步有限，也顯示機關對新進同仁的電腦教育訓練還可以再加強。

為了讓開啟及點閱演練郵件的同仁有所警惕，機關可以適當地以各部門為單位，公布演練不合格的同仁名單，通常這樣所得到的警惕效果相當大；但也會有部分同仁較難接受演練未通過的結果，進而打電話或親自到資訊中心詢問，此時資訊人員可提供更完整的演練資訊，如開啟演練信件的電腦IP、開啟日期、開啟時間等，並再耐心說明演練的目的及資訊安全的重要性，藉此加強宣導。

防範惡意電子郵件社交工程演練，只是資訊安全工作其中的一環；整體資訊安全的工作相當繁雜，其他重點工作尚有：從作業要點的訂定開始，就必須考量資安預防及危機處理；資訊人員本身也要不斷充實各種資安新知，甚至是通過專業證照考試；如果機關經費足夠的話，可以申請資訊安全管理系統ISMS（Information Security Management System）的第三者驗證；另外如系統防護設備的購置、安裝及設定等。包括這些防護設備的持續維護及更新，都需要資訊人員長期不斷地投入。希望藉由本篇淺顯的短文，讓電腦使用者了解電子郵件社交工程演練的意義、重要性，及整體資訊安全工作的概略。

（作者為基隆市政府研考處資訊管理科科長）

▲Top