行動裝置的安全管理

◎魯明德

在資通訊環境日益進步之際，除可看到很多人邊走邊滑手機外，我們在餐廳、捷運、車站各處，也都能看到人們滑著手機，專注於自己的社群網站、即時通訊軟體，或在處理公司的事情；不管是哪一種，這些行為都顯示我們在日常生活中對行動裝置的依賴越來越深。

根據研究機構Gartner調查指出，全球至2016年將有38%的企業停止配發資通訊裝備給員工，而讓員工直接使用自己的資通訊裝備來公司工作；趨勢科技也進行類似的調查，70%的受訪企業認為讓員工使用自己的裝備來公司工作，能強化工作效能、降低企業成本，不過也有85%的企業擔心因此會提高企業資料外洩的風險。

就在今(103)年7月底，蘋果首度鬆口承認iOS有後門程式，使用者在iPhone上的簡訊、通訊錄、照片等個資，都有可能經由這個後門被竊取；至於Android系統有沒有這個漏洞，尚不得而知。7月初，行政院消費者保護處也公布一項委由資策會資安科技研究所進行的抽樣檢測結果，發現三大智慧型手機品牌的資訊安全系統都存在著資訊安全疑慮，這些資安疑慮可歸納為兩大類：重要資訊未加密就儲存、連結不安全的網站時手機不會主動告知。因此，使用者的私密資料可能輕易被駭客竊取，成為網路犯罪的受害者。

看到這些企業發展趨勢與系統安全的報導，從事高科技工作的小潘開始擔心：目前員工上班所用的電腦是由公司統一配發，可以在電腦上做些資訊安全的防護措施，未來如果讓員工自備電腦變成一種主流，資訊安全要怎麼管制呢？現在連封閉系統的iOS都有資安的疑慮，那麼號稱是開放式系統的Android會不會也有不為人知的漏洞呢？在這種複雜的環境下，企業的資訊安全如何維護？

帶著這麼多的疑問，小潘在這個月的師生下午茶約會中，把這些問題逐一提出跟司馬特老師請益。司馬特老師喝口咖啡後，先對小潘分析當前的產業趨勢，由於3G與Internet技術的成熟，加上行動裝置普及，造就了企業將電子化延伸為行動化的趨勢。

以往房屋仲介業者都要準備很多的紙本、照片等資料，才能跟客戶推薦物件，而且只能在店裡才有資料可看；現在，各個房仲公司都開發出他們自己的系統，讓仲介業務員透過手機或平板電腦就能提供購屋者各種參考物件，甚至可讓賣屋者自己上網去張貼物件資料。考量人員的流動及裝備的購置成本，未來仲介人員的手機、行動裝置都可能會讓他們自己去購置。當裝備是自己的，很容易就會公私混淆，裝備裡面有公司的資料，也有個人的資料，這時，資訊安全就很重要了，如何能讓公司的資料不外洩，就成了資訊部門的一項重大挑戰。

這可從三個方向來思考，首先是員工認證，必須是合法的員工才能透過裝置登入公司的系統，為了簡化員工的作業，可以將認證及安控機制寫成一個APP，所有員工自己的裝備都要安裝這個APP，才能登入公司的系統，如此可以防止非法登入。經由認證賦予使用者包括存、取、讀、寫等必要的權限，以避免使用者看到不該看的機密資訊。其次是資料的處理，在系統設計時，應盡量把工作放在server端來執行，以減少client端的資料存量，讓資訊集中存放，即可減少機密資訊在client端被入侵竊取的風險。

為避免合法的使用者對機密資料的監守自盜，除了和管理面上從規章制度去要求外，也應透過系統設計加以防範。這點可以結合前述之認證與權限管理，當資料集中管理後，就要嚴格控管員工下載資料的權限，可利用系統讓員工不能輕易地下載資料；即使有權限下載資料的員工，系統也要對下載的內容做成紀錄，以便日後追蹤；對於異常的下載，則要隨時出現警訊，讓系統管理者可以立即採取危機處理措施。

小潘聽到這裏，對資訊系統的安全管理有了更深一層的了解；但是，他又想到另一個問題，上個月他遺失了一支手機，將心比心，員工的手機也可能會遺失，撿到手機的人，不就可以堂而皇之地進入系統，看盡公司所有資料嗎？

對於小潘的舉一反三，司馬特老師很高興地表示，這也是管理層面的問題，我們的信用卡遺失，可以打電話到銀行掛失止付；同樣地，公司內部也必須建立一套機制，當員工的裝置遺失，要提供一個窗口讓他能掛失，這時，該裝置上的認證碼就會被終止，撿到手機的人就無法登入系統，而此一掛失的窗口可以是人，也可以透過系統來掛失。

小潘聽完司馬特老師的一席說明，深感企業讓員工用自己的資通訊裝備上班，是未來的趨勢，不但企業可以減少成本，員工也會因為用自己的裝備比較順手而提高工作效率；與其以資安問題跟員工對抗，不如提早針對資安問題，提出解決方案，從管理面與技術面雙管齊下，才可能創造企業與員工的雙贏！

(作者為科技大學資訊管理系講師)

我們可以成為資安強國

◎吳明蔚

在資訊化時代的今天，電腦與網路已深入各國的關鍵基礎建設，國家整體競爭力和人民福祉均與之息息相關，此變革也決定了資訊系統成為現代戰爭與區域衝突的重點攻擊對象。這種以電腦和網路為主要攻防的作戰目標，簡稱資訊戰。如今由特殊軟硬體所精心設計的電腦病毒與木馬後門，可有效達成以寡擊眾、決勝千里的目標；重新定義資訊化時代的世界強權，絕對是弱小國家脫胎換骨的最佳利器。

近年各國都在大力厚植自身的資訊戰實力，作為資訊戰根基的資安人才更顯得重要與難求。全世界最頂尖的資訊安全會議當屬美國源自1997年的黑帽大會（Blackhat）和源自1993年的戰備大會（Defcon），前者的與會聽眾定位在高階主管；後者則是學有專精的電腦駭客，這兩場大會每年都遴選上百篇驚人之作，吸引上萬名各路好手齊聚拉斯維加斯切磋最新的資安攻防技術。這樣的平臺正好提供美國政府廣募資訊戰新血，甚至各國的產官學高階主管也會來此選才挖角。

美國過去曾飽受維基解密（WikiLeaks）不時爆料外交祕辛，現在又有史諾登（Snowden）揭露稜鏡計畫（PRISM）等機密資料，其文件顯示電信與網路已成為國家機器在蒐集反恐情資甚至輿情分析的重要管道，且手段已化被動為主動；當情治單位掌握關鍵技術後，即可在各家網通設備與伺服器植入後門，並遠端啟動木馬蒐集資料。當國家利益至上時，一國在資安技術的領先就會變相地危及其他國家的整體競爭力。近年已發生多起國際性的先進資安入侵事件，包括針對跨國集團（如Google）、國防工業（如美國洛克希德馬丁、日本三菱重工）、能源事業（如美國各大能源公司、伊朗核電廠）、金融單位（如韓國DarkSeoul事件癱瘓多家韓國銀行達數萬臺電腦與ATM提款機）等。

臺灣也面臨嚴峻的資安問題，自民國92年以來，各政府機關就長期飽受有組織、有計畫的資安攻擊，這類攻擊簡稱APT（Advanced Persistent Threat），亦可俗稱為「網軍攻擊」。筆者與惡意程式分析專家Birdman，以及數位鑑識專家PK長期在追蹤APT活動，歸納高風險的目標族群遍及政府機關（機敏資料）、學校機構（研究成果）、新聞媒體業（政經內幕）、金融單位（交易紀錄）、跨國集團（營業秘密）、高科技廠商（智財和程式碼）等。在部分資安調查中發現這類攻擊有能力潛伏在受害單位達數月至數年之久，甚至有人侵時間可追溯至97年，而迄今惡意程式仍在竊取資料。這表示受害單位全然不知已遭入侵，這段期間不論是設備汰換、人員異動、系統重建、防毒更新均未能擺脫網軍監控。這類攻擊行動是經過精密策劃，可略分五個階段：1.情蒐、2.攻擊、3.擴展、4.打包、5.外洩。攻擊方透過事先的情報蒐集，以協助精準地發動目標式攻擊到特定對象的電腦或個人信箱，當輔以新發現的漏洞或巧妙的社交工程就有很高的機會入侵成功；接著進行橫向擴展以竊取管理人員的密碼並入侵其他內網系統，逐步蒐集過濾更多機敏資料並加密打包；最終隱匿地後送這些資料，並將其外洩給攻擊方。

有鑑於資訊戰的強大威力，韓國已傾全國之力發展資訊戰能量。據我國年輕駭客GD統計，韓國有四百餘所學校成立資安社團，每年均有諸多國際規模及高額獎金的資安競賽，如Codegate、SECUINSIDE和PoC（Power of Community）等。韓國政府更推展BoB（Best of the Best）菁英計畫，延攬世界頂尖的駭客前來指導韓國的資安菁英。這些優異的年輕學子未來不僅可在各行各業大放異采，在國防方面，韓國國防部與高麗大學均有軍官養成計畫，全額補助資訊防衛系的學生畢業後可進入國家的資電作戰部隊，為韓國的資訊作戰效命。

我國不是世界強權，論資源、腹地、人口、武器等硬實力，我們均面臨諸多困境。但臺灣擁有創新、創意、創業的環境，總能以小博大並發揮綜效，非常適合發展軟實力。臺灣最有口碑的資安社群之一是Chroot，此社群已在我國舉辦10年的年度資安盛會HITCON（臺灣駭客年會），吸引近百篇的國際投稿，遴選十幾位國際級駭客來臺與國人分享其最新資安研究，歷年門票都是秒殺完售，足見國人對資安具有高度興趣。今（103）年5月代表臺灣的HITCON團隊在隊長Alan帶領下於中國大陸百度盃駭客競賽中奪冠，接著將挑戰全球駭客競賽（Defcon CTF），目前已入圍全球前十大。

其實我國資安人才濟濟，藏富於民。若要厚植臺灣的資安能量，化危機為轉機，當務之急是加速整合國內的資安能量，發揮政府、學校、產業與社群的綜效，政策上要從嚴落實資安防護（例如要求機關的分類分級與應辦資安工作事項、增設專任資安人員等），並提高資安層級的高度，將資安問題視為國安問題、國防問題。

資安人才是以鍵盤保家衛國的人才，因此學校應成立資安專門系所，延攬頂尖駭客參與課程設計與授課；產業亦應重視資安人才與資安防護，將其視為風險管控的一環，並提撥一定的營收做為資安投資；而社群傳承經驗與技術，則可讓更多青年學子了解資安，共同維護資安。

當一個國家不具有強健的資安能量，就只能一次又一次地成為受害者。我國距離資安強國還有很長的一段路亟待急起直追，然而只要全國一起努力，相信臺灣也可以做得到！

（作者為Xecure Lab 共同創辦人、臺灣大學電機博士、Chroot成員）

▲Top