行動裝置的安全議題

◎魯明德

當行動裝置的功能如同電腦，且員工習慣用自己的行動裝置上班時，資訊安全就變成一個不易控制的怪獸。

由於行動裝置的普及，不但企業把它拿來做管理的工具，政府機關也不落人後，紛紛以通訊軟體進行單位間溝通作為先進的指標。不過也因為不熟練，意外頻生，顯現資訊安全產生問題的先兆。據報載，某單位高層於上班時間跟太太談論股票買賣，結果誤傳到群組上，讓全部的人都看到；同時間，有人用手機的通訊軟體關心朋友分發工作的事情，皆激起了不小的漣漪。

科技新貴小潘看到這些報導，想到自己的公司也是行動裝置的重度使用者，會不會發生類似的事情？如果行動裝置一旦被駭客入侵，連到了公司內部的系統，豈不是機密全都露了？但是一味防堵、不准使用，似乎也不是辦法，有什麼方法可以確保資訊安全呢？

趁著師生下午茶約會，小潘迫不及待把這個問題提出來，司馬特老師喝口咖啡娓娓道來，行動裝置看似輕薄短小，但其實就是一個微型的電腦，從事資訊的人不能再把它視為手機、PDA 之類的裝置。從使用者的角度來看，行動裝置資訊安全風險的高低，其實跟使用者的使用習慣與方式息息相關，一個行動裝置的重度使用者經常會下載各種應用程式、上網、使用社群通訊軟體等，這些都會使資訊安全的風險增加。

當使用的APP 變多，加上行動裝置都具備上網功能，難免會有一些惡意程式跟著來，如：蠕蟲、木馬、間諜程式等，除了這些惡意程式之外，當行動裝置的功能跟微型電腦一樣時，自然也會面臨遭受網路攻擊的機會。所以在電腦上的各種防護措施，在行動裝置上亦不可少。小潘聽到這裡，立刻聯想到上一次公司業務出差時弄丟電腦，就讓資訊部門兵荒馬亂了好幾天，行動裝置比電腦更輕薄短小、更容易弄丟，尤其是智慧型手機，一旦這些行動裝置遺失，裡面的機密資料不就隨之曝光了嗎？但是又不能不給業務人員配備行動裝置。

司馬特老師喝完咖啡繼續說下去，的確，資訊安全不可因噎廢食，不能因為有危安疑慮就捨去不用，而是要設法排除障礙。以行動裝置遺失而言，資訊部門在配發行動裝置時，就要跟電腦一樣設定開機密碼及螢幕鎖定功能，在閒置一段時間後，系統即自動鎖定，一旦裝備遺失，撿到的人沒有密碼，也不能輕易打開。

由於資訊技術越來越進步，讓資訊產品的淘汰也越來越快，加上最近企業考量汰舊成本，流行讓員工使用自己的設備上班，往好的方面看，企業可以節省資訊設備的購置、維護成本，但是這個措施同時也讓企業曝露在資訊安全的風險中，當行動裝置成為風潮之後，要面臨的問題就更複雜了。

同時，由於行動裝置的容量有限，大多會另行增購SD 卡，這也是一個可能洩密的管道，在配發行動裝置給員工時，應安裝加密程式，萬一遺失時，撿到的人也無法拿到其他裝置上去讀取。

其次，要持續對使用者做教育訓練，不要隨便下載APP，以免惡意程式進駐。根據知名防毒軟體公司McAfee 的調查發現：2013 年Android 的惡意APP 數量是2012 年的3 倍， 而且有82%的APP 會追蹤個資。較常見的惡意APP 型態有：山寨版的遊戲或付費APP、色情APP、假的防毒APP、號稱可以賺錢的APP 等。

小潘聽完司馬特老師的一席話，體會到行動裝置的資安課題，顯然只有從管理層面去改善，才是所有問題的解決起點。

摘自清流月刊104年12月號 第39-41頁

（作者為科技大學資訊管理系講師）