4 工作心得及研究報告

淺談個資與資安

技術課－張鈺苹

個人資料保護法即將正式上路，從個資法通過、母法公佈、施行細則草案預告，已將近一年多的時間，政府部門針對內部員工宣導，使員工對法條內容略知一二，但是，對於要如何遵循法令規範，從何踏出第一步，仍然無所適從，對擁有大量個資的政府部門而言，新版個資法更是營運上的一大挑戰。

無論政府部門有哪些因應措施，首先要做的就是先徹底瞭解個資法規範，一旦機關對法定要求程序不夠瞭解，在個資的搜集、處理、利用等作業上，就會有很多看似合法實則違法的情形，遇到這樣的狀況，即便功能多強大的資安工具，只怕也改變不了抵觸個資法的事實。

當公部門將個人資料鍵入、編輯、製成資料庫、建立查詢系統時，員工更應該注意公務電腦資訊安全。

目前手持行動裝置盛行，可說是人手一機，其功能可說是越來越強大，不只具備GPS更可行動上網，以常見的行動安全的事件所發生的型態，包括下載不明來歷的應用程式（Apps），使得個人的手持式裝置成僵屍電腦，或者不明的應用程式本身就是木馬程式，當員工不慎將行動裝置連結至公務電腦，並透過行動裝置對外連線，行動裝置上惡意程式將會不知不覺竊取個人資料，公務電腦所儲存的個資可能經由此管道外流。

4 工作心得及研究報告

淺談個資與資安

機關要找出那些連上企業網路的行動裝置或公務電腦透過行動裝置，並不是想像中那麼容易。目前針對有線網路架構的網路檢測工具，像是通訊埠掃描工具nmap、弱點掃描工具ISS的Internet Scanner、HP的網管軟體OpenView，這些工具軟體也許可以擔任搜尋行動裝置的角色，但是卻不能有系統地監控整個行動網路的狀況。

行動裝置可能利用不同的技術、方式，由本地端或遠端接上網路，以Pocket PC來說，它可能利用HSDPS、WIMAX連上機關郵件主機、或由WiFi 連上機關VPN、或利用機關內的無線網路與機關內網路連接、或是利用PDA底座連到機關裡的桌上型電腦。而這不過是一個員工的一種行動裝置而已，如果在考量到不同類型的行動裝置或作業系統，要偵測出這些行動裝置更是難上加難。

機關除了利用工具管理外，應訂定使用規範以降低行動裝置對機關造成的可能危害，必須定義哪些裝置，在哪些使用範圍內是可以被允許的。例如，行動裝置的使用規範需定義下列項目:

◎所允許使用設備及作業系統版本。

◎所允許使用的無線技術。

◎行動裝置上可以存放哪些公司資料。

◎行動裝置上必要的保護措施。

◎執行安全規範的方式與懲罰條文。

4 工作心得及研究報告

淺談個資與資安

可藉由偵測機關內目前現有的行動裝置，來訂立出這些使用規範，目前的使用狀況也可以作為風險分析的依據，來決定該如何採取預防措施。為了節省成本與相容性，可盡量利用現有架構與資訊。例如：找一個行動安全方案套用在現有架構與員工資料庫上，並利用現有的資產管理系統或軟體派送系統來達成。

大致來說，PDA和智慧型手機的保護措施跟筆記型電腦差不多，但因作業系統、內建的安全機制、I/O方式和使用方式不同，保護措施在設計上有些許差異。開機密碼可以防止失竊後被讀取資料，但是卻仍有多數人沒有啟用開機密碼。一個良好的行動裝置安全設計應提供密碼保護、能夠執行安全規範的程式、自動上鎖設定、以及認證失敗自動消除資料的功能。