落實個資保護的 6 大金鎖

撰文：叡揚資訊安全事業處 資深專業顧問 陳惠群 博士

搜尋關於個資洩漏事件的報導，不難發現惡意攻擊與疏失最為常見。近期幾件入侵事件，造成 Twitter 25 萬筆用戶資料洩露、台灣諾基亞至少 17 萬筆消費者紀錄外流；知名雲端筆記服務商 Evernote，不久前也呼籲全球 5,000 萬名用戶重新設定密碼。至於因為疏失而造成個資外洩，最近也有不少實例。例如員工寄發電子郵件時，誤將個資檔案當成附件；應用系統未做好防護而讓搜尋引擎取得帶有個資的網頁；或是開放下載的文書檔案帶有未經遮罩處理的個資。

沒有任何單一防禦機制，可以有效對抗不斷演化的攻擊手法；人為疏失更是不定時炸彈，即使有良好制度與程序，缺乏監控與稽核，照樣可能出現個資外洩。唯有充分了解面臨的資安問題，據此建立多重防護體系，才能降低個資洩露風險，保障當事人權益。

日本網路安全協會 (JNSA) 資安事故報告 (http://www.jnsa.org/result/incident/data/2009incident_survey_v1.1.pdf) 就指出，雖然超過 70% 是紙本個資洩露案件，但其平均個資洩露數量則遠低於可攜式媒體 (如 USB)、網路、與電腦本體；而且合計超過 80% 的事件，與惡意攻擊無關。換言之，強化網路與端點裝置防護並且避免操作或管理疏失，必收事半功倍之效。

1 攔截網路洩露

無論是惡意或疏失，網路很明顯都是主要洩露管道。網路型 DLP (Data Loss Prevention，資料外洩防護) 工具，可以過濾向外傳送的網路封包，分析包含電子郵件、即時通訊、檔案傳送等多種協定；一但發現疑似個資向外傳送的行為，就會發出警告。

2 管制端點裝置

有些機構完全禁止使用 USB 儲存裝置。但實務上，由於這類裝置具便利性，全面禁用易招致強烈反彈。因此目前端點防護型的 DLP，已經能做到只管制疑似個資儲存至 USB 裝置的行為，而不會禁止一般資料的存取。

3 加密敏感資料

加密是降低個資外洩損失的重要方法，許多機構都明確要求敏感資料欄位或是檔案，必須加密。不過當這些資料下載至合法用戶端時，都會解密，用戶才能閱讀與利用。NASA 前不久才發生員工筆電失竊，洩露個資的案件。所以無論是存放在伺服器端或是在用戶端的個資，都應當加密保護，降低風險。

4 加強系統安全

資訊管理部門通常都會執行作業系統與各種軟、硬體設備的安全更新，許多網站也會執行各種安全檢測。根據 WhiteHat 的統計，網站年度平均弱點數，由 2007 年的 1,111 項，已降至 2011 年的 79 項。這表示駭客想要硬碰硬地強攻，穿越層層防護，難度已提高許多。然而許多資安報告也指出，駭客攻擊策略已經轉變，先攻擊廣大而且防護脆弱的用戶端，取得帳號，以便進行下一階段的攻擊；許多網站被駭的可能原因，是高權限帳號被盜。因此網站防護的策略，也必須調整，例如主動偵查 偽冒網站，避免用戶進入釣魚網站等。

5 保護行動裝置

就本質而言，行動裝置防護與個人電腦防護並無不同；但實際上，行動裝置防護的成熟度遠不及個人電腦，安全漏洞型態也有差異。如同前述駭客已轉向攻擊用戶端，像是智慧型手機或是平板電腦這類不易區分公用或私用，可能隨時暴露在公開網路的行動裝置，更容易成為攻擊目標。

6 多重防護， 降低風險

三月初韓國才爆發韓國史上最大規模的駭客攻擊事件，韓國官方報告指出，攻擊事件為北韓主導，最後統計有 4 萬 8 千臺設備故障。台灣亦是駭客攻擊頻繁的國家，特別是針對政府機構的攻擊。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL ： (02) 2586-7890 FAX：(02) 2586-8787
高雄辦公室： 80453 高雄市明華路 317 號 6 樓 TEL ： (07) 586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 http://www.gss.com.tw