淺談雲端儲存的資安維護

〈摘錄自清流月刊 103 年 6 月號〉

雲端運算是近年席捲各大媒體版面的新興概念，運用網路溝通多臺電腦或是透過網路連線取得遠端主機提供的服務，以此為基礎衍生的眾多網路服務紛紛被提出。而與我們最息息相關的，莫過於雲端儲存，簡單而言就是將儲存資源放到網路上供人存取的新興方案，使用者可以在任何時間、地點透過網路存取資料，省去購買硬碟、隨身碟等儲存設備的支出。這種跨越裝置、網路及時空的特性使得雲端儲存的應用範圍甚廣，大至企業集團及學術研究單位的資料交流，小至個人的資料處理，都能透過雲端儲存節省可觀的人力及成本。

看準雲端儲存服務的市場需求，許多雲端業者也紛紛推出「公有雲」的雲端儲存服務，常見的全球雲端儲存服務有 Google Drive、Amazon S3、Microsoft SkyDrive、Apple iCloud、Dropbox，而國內也有業者開發華碩 webstorage 及中華電信提供的 hicloud S3 雲端儲存服務。富士比雜誌 2012 年刊出文章〈Dropbox 全球會員目前已超過一億〉，大幅報導雲端儲存的崛起及快速普及，每天存取資料量高達十億個檔案，可見雲端儲存服務受歡迎的程度。

雲端儲存服務固然帶來許多好處，但也增添不少隱憂，過去使用者習慣在單一主機上編輯資料，當機時尚有其他替代性儲存設備可供備份查詢，而若使用雲端儲存，將資料全數集中在一個供應商，假設該供應商突然因設備故障或其他不可抗力因素停止服務，資料可能無法回復；另外，使用者的習慣、行為及愛好等都將隨著雲端服務一同被記錄下來，換句話說，使用者將資料上傳至雲端儲存系統的同時，資料也受到種種資安風險的考驗。先前臺北市萬芳醫院曾因病歷外洩事件引發社會關注，病患的病史、用藥狀況等隱私均有曝光之虞；衛生署則宣布在全國 126 家醫院實施「雲端病歷」，再逐步推廣到全國 500 家醫院及兩萬多家診所，全面透過雲端分享病歷，可避免重複開藥或誤診等情。

隨著人們對雲端儲存的依賴度提高，種種資安風險也浮上檯面，問題包括：

一、網路資料傳輸：資料上傳至雲端的過程中，將面臨網路資料傳輸的安全威脅，這些資料若缺少安全加密防護，將可能被非法的第三方監控並擷取，或是被更改破壞。

二、雲端資料保密：倘若資料已成功且安全地傳送至雲端儲存系統上，這些資料在遠端系統上是否能受到足夠的保密與保護，以致其於雲端儲存系統能不被竊取或外洩。

三、資料儲存穩定:使用者儲存於雲端儲存系統上的資料,是否能穩定地被保存,不會受到斷電、停電等外在因素而消失。

四、個人帳號管理:存取雲端儲存的資料必須透過個人的帳號才能登入並存取,若個人的帳號密碼管理不當或遭他人盜用,則個人帳號、隱私及其儲存之資料將受到非常嚴重的安全威脅。

除了上述幾項雲端儲存服務的安全議題,還須注意該服務經常要求使用者同意在維護雲端儲存服務順利營運的情況下,允許該系統複製、修改、建立延伸內容及傳遞相關內容;這些雖是該服務為了提供資料儲存穩定的保證,但卻也衍生出雲端儲存服務能輕易取用使用者資料的安全問題。因此,許多企業基於保護公司重要資料的立場,紛紛禁止員工使用公開的雲端儲存服務進行資料交流,並自行購買且維護公司私有之雲端儲存裝置,一方面保證資料僅於公司內部私有網路傳遞,另方面也避免使資料暴露於公司以外之第三方儲存處所。

一般民眾使用雲端儲存時,則可透過以下的資料保護方式,避免資料遭受外在的安全威脅:

一、資料加密:先對資料進行安全加密,再將資料上傳至雲端儲存系統,確保該資料日後僅可被資料擁有者解密並且取用。

二、安全加密傳輸:使用者在選擇服務商時,可參考有無透過SSL(Secure Sockets Layer)加密,確保資料在傳輸過程不被攔截或受到病毒感染,可使資料在傳輸時有多一層的保障。

三、重要資料備份:上傳至雲端之資料,最好能先備份於本機端,確保雲端資料若受損,使用者仍存有備份資料。

四、加強帳號管理:為避免帳號被攻擊者盜用,可透過雲端儲存服務提供的多重認證(手機或E-Mail)進行保護。另外,也盡量避免於非安全的電腦主機上進行帳號登入,減少帳號資料被側錄或竊取的風險。

最後要強調的是,雲端儲存服務只是一項資料傳遞與儲存的管道,其無絕對的安全保證,不可將其視為個人資料儲存的空間。由於網路原本就是開放的空間,若檔案具有高度隱私或機密性,最好審慎考慮是否上傳至雲端,若不得不使用,也一定要進行加密保護的動作,方能確保個人資料及隱私不致外洩。

臺灣屏東地方法院檢察署關心您