苗栗縣政府政風處111年2月份廉政宣導

公務機密維護宣導-雲端儲存安全問題

-Line來Line去出問題

目錄

公務機密維護宣導-雲端儲存安全問題

雲端運算（Cloud Computing）是目前相當熱門的資訊技術，現今我們的日常生活已幾乎離不開「雲端」二字，而其應用之一的雲端儲存（Cloud Storage），與我們的關係更是密切，只要能連上網，使用者可以隨時隨地存取網路上的檔案，省去攜帶隨身碟、筆電的困擾；也不像傳統硬碟，若是不小心毀損或遺失，所有資料將付之闕如。對企業來說，雲端儲存服務能讓公司不必在自己的資料中心或辦公室內安裝實體的儲存裝置，而日常的維護工作可交給服務供應商；對一般使用者來說，雲端儲存大幅減少了舟車勞頓及運輸的成本。

公務機密維護宣導-雲端儲存安全問題

搭著這股熱潮，業者紛紛推出雲端儲存服務來搶雲端市場這塊大餅，包括Dropbox、Google Drive、AppleiCloud、MEGA以及國內的中華電信Hami＋個人雲和Asus WebStorage等，這代表我們所能選擇的雲端儲存服務非常多樣化。惟一般人在選擇或使用雲端儲存服務時，優先考慮的往往是它的儲存空間有多大、使用介面是否便利，卻忽略了雲端儲存服務潛在的安全隱憂。使用者也許認為雲端技術相當成熟，所以放心地把一些重要或私密的檔案和資料放在雲端上，但這可能還是防不住有心入侵的駭客。

舉例來說：

2014年8月31日晚間在美國的Reddit、4chan網站流出大量好萊塢女星的私密照片，造成網路上一片恐慌，雲端技術安全備受質疑；其實這些照片是駭客經由Apple iCloud的漏洞入侵所盜取，即便是運行多年的Apple iCloud服務也存在漏洞。

公務機密維護宣導-雲端儲存安全問題

根據趨勢科技的分析，上述事件的發生有以下幾種可能原因：

一、使用不安全、易遭駭客破解的密碼：

使用與個人資訊高度相關的密碼，相當容易遭到破解，駭客只需找尋相關資訊即可盜取資訊。

二、受害者未啟用iCloud的雙向認證：

當攻擊者知道受害者的iCloud電子郵件地址，攻擊者就可能透過「忘記密碼」功能進行密碼重置。因明星多數的個人資料可從網路上取得，包括寵物名稱等等，大幅提升帳號被入侵的可能性。

三、攻擊者侵入另一個安全性較弱的帳號，以接收iCloud的密碼重置郵件。

四、重複使用相同密碼：

許多人常在多個服務使用相同的密碼，若其他網路服務的帳號已被入侵，則iCloud的帳號也可能遭受攻擊。

公務機密維護宣導-雲端儲存安全問題

五、網路釣魚：

攻擊者發送針對性的釣魚郵件給明星，引誘她們輸入自己的iCloud認證資訊到假的登入畫面，藉此蒐集帳號與密碼。

除此之外，當我們在選擇各種業者所提供的雲端服務時，必須在使用前看清楚其服務條款，否則這些服務也很有可能造成隱私上的隱憂；例如：Google Drive在推出時，其中一項服務條款便惹來爭議，內容為「當你將資料上傳或用其他方式提交到Google Drive後，你就給予Google（以及我們的合作夥伴）全球授權，可以使用、代管、儲存、再製、修改、建立衍生內容、溝通、出版、公開呈現，和遞送這些內容。」雖然Google表示使用條款中已載明內容的所有權歸用戶所有，但是並沒有保證只有在「為維持服務運作相關」的情況下，才可以使用部分的資料，這表示Google有更大的權利來操控我們所上傳的資料，這些內容甚至可能淪為廣告用途。

平時我們便需要做好個人資料的保護，以下列出幾種保護方式提供參考：

一、請使用強度高的密碼：

千萬不要圖方便記憶而設置過於簡單的密碼，切記勿將生日加入密碼組合、容易被破解，好的密碼應至少使用八個字元以上、英文大小寫與數字混合使用、盡可能包含一些特殊字元等；即使設置強度高的密碼，也不應重複使用此密碼，應定期更新密碼。

二、重要資料加密備份：

資料需多次備份並加密，除儲存於雲端之外，應再儲存於本機端或私人的硬碟和隨身碟中，重要資料切勿只存在雲端中。

三、避免使用公用電腦存取個人資訊：

使用完公用電腦時，記得切勿儲存密碼，在關閉網頁前先登出並刪除瀏覽紀錄。

平時我們便需要做好個人資料的保護，以下列出幾種保護方式提供參考：

四、慎防網路釣魚：

網路釣魚是一種誘騙電腦使用者透過手機、電子郵件、網站或通訊軟體，竊取個人資料或財務資訊的手段。所以在收到任何簡訊、電子郵件時，需再三確認其內容，切勿輕易回覆。

雲端儲存服務固然方便，但卻無法保證其安全性。個人私密或重要的資料應盡可能避免儲存在雲端上，若要儲存，也必須做好加密保護的動作。科技發展是一體兩面的，以雲端儲存服務而言，在運用其方便性之餘，我們也應正視它所帶來的安全議題，才能享用科技而不淪為駭客的目標。

Line來Line去出問題

據根據iThome於107年3月間的報導，LINE用戶已突破1,900萬，每天使用LINE進行語音通話人數也突破700萬，毫無懸念地，LINE已成為臺灣最主要的社群通訊軟體。舉凡學生喜歡用LINE溝通，老師用LINE教學分享、指導課業，公務機關亦起而效尤，隨手建立公務群組，藉此橫向連繫、有效溝通。但是每天使用的你，知道它也存在一些「黑歷史」嗎？每天LINE來LINE去到底會不會出事？其他通訊軟體像是WhatsApp、Instagram會不會比較安全？這些疑問從來就沒有消停過！

東森新聞於2018年11月29日報導「手誤傳錯群組，潘姓員警被依過失洩密罪送辦，檢方給予緩起訴處分」，內容陳述2017年間偵辦擄人勒贖案的潘姓員警，原本要傳「偵辦進度報告」給負責調閱監視器的同事，卻誤傳到反年金改革的群組「台灣憤怒鳥」，該案檢方於2018年給予緩起訴處分，需繳交公庫3萬元。另外LINE最常遇到的態樣，當屬詐騙集團竊取個資及財務等問題；此外LINE也成為假訊息散布平台。

LINE潛藏風險可約略將之分為「操作風險」及「軟體風險」，分述如下：

一、操作風險

（一）如前述案例所載，使用者於公務上可能同時與多群組人員聯繫，稍有不慎，易誤傳公務相關文件予不相干第三人，即使LINE具備「訊息回收」功能，也難得知第三人是否已知悉內容。

（二）許多人使用LINE未了解軟體具備之功能，像是LINE聊天室的「相簿」、「儲存至 Keep」功能等，可將檔案上傳雲端，若不善用而隨意儲存在手機目錄、相簿內，一旦手機誤植木馬軟體等，手上資料恐遭外洩。

（三）LINE若設定不當，允許陌生人加為好友，讓有心人士有可趁之機，偽冒熟識、家人，誘騙點選連結進行APT（Advanced Persistent Threat）攻擊或交付資料等，均可能引發資安風險。

（四）公務機關人員為求跨部會聯繫提升效率，往往建立許多群組，群組成員間彼此也未必熟識；又尚未在LINE群組裡指定管理者時，任何成員均可邀請他人進入該族群內；倘若誤加入非此公務相關人員，將滋生公務資料外洩疑慮。

LINE潛藏風險可約略將之分為「操作風險」及「軟體風險」，分述如下：

二、軟體風險

（一）LINE可隨意轉貼及點選任何網址，若是該網址潛藏惡意代碼，手機極可能被植入惡意程式，導致機敏資訊遭竊。

（二）LINE建置雲端資料庫能儲存用戶或群組對話內容及檔案，但若LINE公司遭駭客入侵，即可能洩漏用戶或群組之檔案及對話內容，即使循司法調查管道，亦因LINE屬國外公司而增加偵辦難度；此外，使用者在通訊過程中亦存在遭LINE公司側錄對話內容之風險，故以國安角度考量，確實不宜在機敏公務上使用。

因應風險防制有5點：

1. 安裝訊息加解密軟體。
2. 「LINE」群組中建立管理人員。
3. 持續更新LINE版本。
4. 安裝防毒軟體。
5. 不隨便加好友、加官方帳號。

LINE在臺灣儼然成為生活不可或缺的一部分，公務機關也常藉此開設公務群組，期以「行動辦公室」增進行政效率，然而在享受便利的同時，我們也要明白使LINE所必須承擔的資安風險，盡可能不要在LINE上處理公務，倘仍須處理公務，務必考量LINE使用上的安全性。您可透過安裝加解密軟體、調整LINE操作等預防方式，在最低的風險下，方能享受LINE帶給我們的便利。

Thank You

廉政專線:

037-356639

苗栗縣政府

政風處關心您❤