全民資訊安全意識月刊

OUCH!

本期話題

- 什麼是備份、何時備份以及如何備份
- 還原
- 重點

備份與復原

概述

電腦或行動裝置使用一段時間後, 總會因為某些錯誤或疏忽而遺失了儲存在裡面的個人檔案、文件或照片。比如說: 誤刪錯誤的檔案、硬體設備本身的故障、設備遺失或遭到如勒索軟體 (Ransomware) 之類的惡意軟體感染。這時, 資料備份通常是重建原本數位生活的唯一方式。在本期文章, 我們將解釋什麼是備份、如何備份資料及制定適合您的輕鬆備份策略。

客座編輯
Keith Palmgren是一位在IT安全領域擁有超過30年經驗的網路安全專家。他是SANS資深講師, 同時也是SANS SEC301「資訊安全簡介」的作者。Keith提供相當出色的資安顧問諮詢服務, 可以在Twitter上搜尋@kpalmgren與他聯繫。

什麼是備份

備份是將電腦或行動裝置內的檔案資料另外儲存在其他地方的資料副本。一旦不小心遺失重要資料時, 可以透過備份復原該資料。資料備份操作容易且成本不高, 可惜大多數人並不會定期執行。首先, 要決定哪些資料需要做備份, 這有兩種方法: (1) 僅備份重要的特定資料; (2) 備份全部資料, 包括整個作業系統。大多數的備份解決方案預設使用第一種方法, 它們從最常使用的資料夾備份資料, 通常這就夠了。然而, 如果不確定哪些資料需要做備份, 或是想要更為謹慎, 請備份所有資料。

何時備份

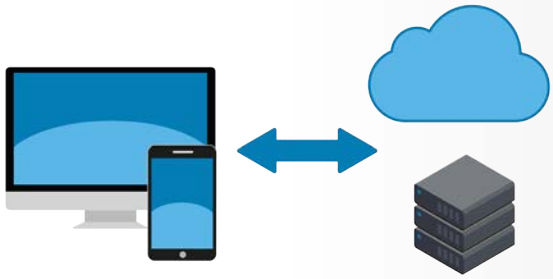
其次, 請決定多久該備份一次。以個人電腦而言, 內建的備份程式, 像是Apple時間機器 (Apple's Time Machine) 或微軟視窗備份和復原 (Window's Backup and Restore) 功能, 可以讓您建立自動執行備份的周期, 通常設定參數為每小時、每日、每週……等。有些解決方案則提供「持續保護」功能: 每次當您按下儲存鍵時, 新建立的或修改過的文件便會立即備份。我們建議至少設定每日自動備份。

如何備份

最後, 您需要決定如何處理備份。備份資料有兩種存放方式: 儲存在實體裝置或是網路雲端上。兩種方式各

備份與復原

有其優缺點。如果不確定何者更合適，兩種方式可以同時使用。實體裝置指的是您能夠控制的設備，比如說外接式USB或可透過Wi-Fi存取的網路設備。使用您自有實體裝置的優點是能夠快速地備份和復原大量資料；但缺點是如果設備不小心感染惡意軟體，例如：勒索軟體（Ransomware），則可能會擴散而影響整個備份資料。另外，如果不幸遭遇火災或竊盜等災害，您可能不僅損失電腦，甚至連備份資料也一併損失。因此，當使用外接裝置備份時，應該將該備份的副本存放在其他安全的地方。同時請確保正確地標記您所儲存的任何備份。



自動及可靠的備份往往是保護您資料的最後一道防線。

雲端解決方案則是將檔案儲存於網路上。通常須先在電腦上安裝特定的應用程式，然後，應用程式會依排程或當您修改檔案時自動備份。將資料備份在雲端的優點是操作簡單，幾乎是持續自動地在執行備份，而且通常可以隨時隨地存取文件。此外，由於資料存放於雲端，因此像火災或盜竊等居家災害發生時不會影響到您的備份。加上雲端備份能回復不慎被惡意程式（如勒索病毒）所感染的檔案，甚至許多雲端解決方案可從檔案被感染前的時間點還原。但是雲端備份的缺點是備份或復原大量資料時往往需要花較長的時間。另外，隱私和安全的考量也很重要。雲端備份服務是否提供足夠的安全控制措施，例如是否加密您的資料和使用嚴謹的身份驗證機制？

最後，別忘了您的行動裝置。大部分存放在行動裝置裡面的資料，例如：電子郵件，行事曆和聯絡人，都已自動被儲存在雲端。然而，您的app設定、近期照片和系統偏好設定卻可能不會被儲存在雲端。透過備份機制，不僅可以保留上述資料，在更換行動裝置時也較容易移轉資料。iPhone和 iPad可以自動備份到Apple的iCloud。Android或其他行動裝置則取決於設備製造商或服務提供業者。在某些情況下，您甚至可能需要購買專為備份設計的app。

還原

備份好資料只能算是成功的一半，您還必須確保資料可以被成功還原。透過定期檢查備份檔案是否和原始檔

備份與復原

案相同，以檢查備份資料是否能正常運行。此外，請確保在重大升級（如更換新電腦或行動裝置）或重大維修（如更換硬碟）之前已執行完整的系統備份，並檢查其可否用於還原。

重點:

- 不論以什麼方法備份資料，請確保裝置已設定自動執行備份功能，並定期檢查備份資料是否可正常使用。
- 當使用備份重建系統後，在使用系統之前請確保已取得最新的安全修補檔和更新。
- 不再需要的過期備份存在風險，請將其銷毀以防止未經授權的人員存取。
- 如果將備份資料儲存在雲端，請仔細研究服務提供商的政策和聲譽，並且確保它們符合您的要求。例如，您的資料是否會被加密？誰有權限存取您的備份？他們是否提供嚴謹的身份驗證機制，例如二階段驗證？

進一步了解

歡迎訂閱OUCH!　全民資訊安全意識月刊，以及瀏覽前期OUCH!檔案。想要進一步了解SANS資訊安全意識方案，請瀏覽我們的網站 securingthehuman.sans.org/ouch/archives.

德欣寰宇為台灣專業資訊安全顧問公司。我們為客戶提供全方位安全整合解決方案。請至官方網站 http://www.tsc-tech.com/或臉書@tsctech了解更多訊息。

參考資料

密碼短語:	https://securingthehuman.sans.org/ouch/2017#april2017
二階段驗證:	https://securingthehuman.sans.org/ouch/2015#september2015
雲端安全:	https://securingthehuman.sans.org/ouch/2016#november2016
加密:	https://securingthehuman.sans.org/ouch/2016#june2016
勒索軟體:	https://securingthehuman.sans.org/ouch/2016#august2016

編輯委員會：Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
翻譯群：邱俊傑、黃意雯、宋亞倫、孫權劭、王澤薇、葉力維、陳月娥