

OUCH!

本期話題

- 主要概況
- 選擇雲端提供商
- 保護你的數據

雲端的安全使用

主要概況

“雲端”是一個功能強大的技術，人們和組織正在迅速採用。 “雲端”對於不同的人可能意味著不同的意思，但一般是指服務提供商在互聯網上存儲和管理你的資料。雲端計算的好處是不僅可以很容易地在世界任何地方從多個設備訪問和同步你的數據，你也可以和任何人共享你的信息。我們之所以稱這些服務“

雲端計算”，是你因為你經常不知道你的數據的物理存儲在哪裡。雲端計算的例子包括建立在Google文檔文件，通過Dropbox的文件共享，設置你自己的服務器在Amazon的雲端上，或存儲你的音樂或圖片在Apple的iCloud。這些在線服務都提供你更高效的潛力，但它們也帶來了獨特的風險。在本月刊中，我們會講解如何安全地利用雲端計算。

編輯嘉賓

James和 Kelli Tarala (@isaudit/@kellitarala) 是 Enclave Security的主要顧問，並撰寫了大量SANS的培訓課程，包括SANS「審計566：實施和審計二十個關鍵的安全控制」和「MGT415：風險評估實用入門」。

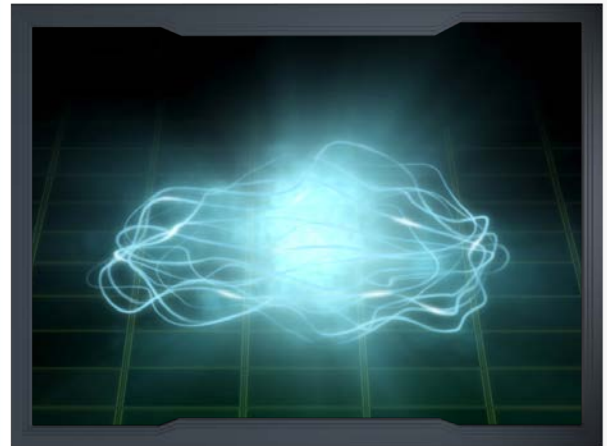
選擇雲端提供商

雲端無善無惡，只是一個做事情的工具，無論是在工作還是在家裡。然而，當你使用這些服務，你把你的私人數據交給陌生人，而且希望他們保持數據的安全和可用性。因此，你要確保你的選擇是明智的。關於你的工作電腦或工作相關的信息，請諮詢您的主管關於是否可以使用雲端服務。如果允許雲端，請務必確認哪些雲端服務可以使用，以及關於如何使用它們的政策條例。如果你正在考慮你個人使用雲端服務，請考慮以下。

1. **支持**: 有多容易得到幫助或問題解答? 有沒有可以聯繫的電話號碼或電子郵件地址? 是否有其他可供選擇的支持, 如公共論壇或常見問題在他們的網站?

雲端的安全使用

2. **簡單:** 該服務是否容易使用? 越複雜的服務, 你就越有可能會犯錯, 不小心暴露或丟失你的信息。選擇一個雲端服務提供商你認為很容易理解, 配置和使用。
3. **安全性:** 如何將你的數據從電腦轉到雲端? 是否經加密保護的連接? 如何存儲在雲端中的數據, 它是否加密? 如果是的話誰可以解密你的數據?
4. **服務條款:** 花一些時間來審查服務條款 (他們往往非常容易閱讀)。確定誰可以訪問你的數據, 什麼是你的合法權益。



雲端可以讓你的信息更方便使用, 幫助你更有效率, 但要小心你如何存儲和共享你的信息。

保護你的數據

一旦你選擇了一個雲端服務, 下一步就是要確保你正確使用你的雲端服務。如何訪問和共享你的數據往往能對你的文件的安全性產生巨大的影響。你可以採取一些關鍵的步驟包括:

1. **驗證:** 使用一個強的, 獨一無二的密碼來驗證你的雲賬號。如果你的雲供應商提供兩步驗證, 我們強烈建議您啟用它。
2. **共享文件/文件夾:** 雲可以很簡單的分享, 有時候太簡單了。在最壞的情況下, 你可能會不小心讓你的文件甚至整個文件夾公開提供給整個互聯網。保護自己的最好辦法是設定默認不與任何人分享任何文件。然後, 在有需要的基礎上, 只允許特定的人 (或一群人) 訪問特定的文件或文件夾。當一個人不再需要訪問你的文件, 就將其刪除。你的雲供應商應該提供一個簡單的方法來記錄誰有權訪問過您的文件和文件夾。
3. **共享文件/文件夾使用友情鏈接:** 有些雲服務的一個共同特點是, 創建一個指向文件或文件夾的網絡鏈接。此功能讓你只需提供一個網站鏈接到這些共享文件就可以和別人共享。但是這種方法有很低的安全性, 任何人知道這個鏈接就可以訪問你的個人文件或文件夾。如果你發送的鏈接只給一個人, 那個人可以與他人

雲端的安全使用

共享該鏈接，從而也就有可能出現在搜索引擎上。如果你使用鏈接共享數據，請確保鏈接一旦不再需要就要關閉它，或者如果可能的話，使用密碼保護的鏈接。

4. **設置**: 瞭解你的雲端供應商所提供的安全設置。例如，如果你與別人共享文件夾，他們能否在你不知情的情況下與其他人分享你的數據？
5. **防病毒**: 確保最新版本的防病毒軟件安裝在你的電腦，以及能共享你的數據的任何其他電腦上。如果共享文件被感染，其它電腦訪問相同的文件也會被感染。
6. **備份**: 即使你的雲端供應商備份你的數據，你也要考慮把自己數據的定期備份。這不僅在你的雲端供應商歇業，關閉或由於某種原因不可訪問的情況下保護你的數據，它也可以更容易地從本地備份恢復大量數據而不是從雲端拉下來。此外，確認你的雲端提供商備份文件的頻率，以及能否讓你恢復你的文件的先前版本，以及他們會保持你的備份可用多久？

進一步了解

歡迎訂閱OUCH!電腦用戶安全意識月刊，以及瀏覽前期OUCH!檔案。想要進一步了解SANS安全意識的方案，請瀏覽我們的網站<http://www.securingthehuman.org>。

參考資料

- 強密碼: <http://www.securingthehuman.org/ouch/2013#may2013>
- 密碼管理: <http://www.securingthehuman.org/ouch/2013#october2013>
- 備份: <http://www.securingthehuman.org/ouch/2013#september2013>
- 安全術語: <http://www.securingthehuman.org/resources/security-terms>

OUCH! 由SANS Securing The Human發行刊登，遵從[Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/)(創意公用授權條款4.0版)。在不更改本刊物內容的前提下，你可以自由分享此月刊或使用於你的安全意識計劃。有關翻譯或更多諮詢，請聯絡ouch@securingthehuman.org。

編輯委員會: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻譯: 巴珊珊



securingthehuman.org/blog



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.org/gplus](https://plus.google.com/securingthehuman.org)