CSCS 2018 工作報告

宗旨

公民團體本身的敏感性，同時又欠缺相關資源，讓他們在利用資訊科技進行他們的工作的時候，安全容易受到威脅，例如網路監控、針對性的網路攻擊、網路封鎖、干擾和審查。台灣活躍的資安社群和公民社會一直在世界上廣為人知。Civil Society Cyber Shield 期待掌握台灣此二強項，扮演科技人士和公民社會的橋樑，藉由連結雙方，提升公民團體使用資訊科技的安全。

摘要

- 資安提升服務涵蓋超過十個台灣的 NGO
- 志工講師共進行超過十場資安檢測或是培訓

檢測結果 - 常見的危險狀況

1. 多人共用線上服務的帳號密碼
2. 辦公室未區分訪客及員工用 Wifi, 導致訪客連上後即可存取內部系統（如網路硬碟）
3. 離職員工或實習生仍然可使用原有帳號密碼登入系統
4. 久未更新的軟體

檢測結果 - 嚴重的安全弱點

中華電信數據機外網存取未關閉，且使用預設密碼

檢測中，我們發現某組織所使用的中華電信數據機使用預設密碼，並允許辦公室內網以外的任何人連線到系統管理網頁界面。
透過該系統管理界面輸入管理員帳號密碼登入後，可以調整數據機的各項設定。
在此狀況下，攻擊者可以直接透過網際網路連線到數據機，並使用預設帳號密碼登入，再調整設定，就可以竊聽或是篡改辦公室內的所有網路流量。

建議

以下建議是針對台灣 NGO 普遍的狀況提供，具體實施的方式建議先與資安專業者討論，以避免不熟悉使用方式與設定，影響本來的工作。

不共用線上帳號密碼

每個組織會共用帳號密碼都有不同的原因和考量，需依照組織的使用習慣和需求，重新設計新的不共用帳號密碼的使用方式和流程。

參考 Google 非營利組織方案 https://support.google.com/nonprofits/answer/3367631

工作用帳號啟用二階驗證（二步驗證）

啟用二階驗證可以避免密碼外洩後帳號被盜用，登入時常見的簡訊驗證碼即是二階驗證的其中一種。
可以到 https://twofactorauth.org/ 查詢各線上服務支援的二階驗證種類還有啟用的說明文件。

辦公室 Wifi 區分員工用及訪客用

考慮購買支援「多重 SSID」功能的無線路由器。也可以在現有路由器外額外增購一台使用。設備如果需要設定協助。

定期更新軟體

Windows：打開自動系統更新，安裝完儘快依照指示重新啟動。使用 Windows 7,8,10， 更舊的版本微軟公司已經不提供軟體更新，強烈不建議使用。

MacOS：打開自動系統更新，安裝完儘快依照指示重新啟動。使用 MacOS 10.14 , 10.13 , 10.12， 更舊的版本蘋果公司已經不提供軟體更新，強烈不建議使用。

應用程式：定期更新（不是指要升級大版本，例如從 Office 2013 升級到 2017， 而是 2013 內的小更新建議要安裝）

聯絡

- OCF： hi@ocf.tw

最後更新

2019/2/27