校園活動

Subject 校外研習分享-111年教育體系資安健診基礎訓練課程

圖書資訊處 / 陳顗夫

此研習旨在培養教育體系人員資通安全專業技能，強化針對資安的瞭解，並透過講師經驗分享與實務相關操作訓練演示提升相關警覺性。

資通系統指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。因為越來越多操作都仰賴網路以及各種伺服器資料庫完成，因為在建置與操作上，需要多加留意各種漏洞扣或是惡意行為。而單位的自我檢視行為包括了系統檢測、弱點掃瞄以及滲透測試。然後這些檢測的行為可能觸發各區網中心或是學校單位的警報系統，造成資安事件。因為在進行這些行為之前，必須取得機關同意，並且留下相關的佐證資料，避免觸法。在進行這些檢測時，因為不是攻防演練，因此不建議使用具有攻擊性的檢測手法，例如釣魚、在檢測目標安裝惡意程式或是進行暴力破解。宜使用較為普通的掃瞄、檢視系統版本與相關流程文件記錄等方式。

檢測時也應將現地的實際狀況一併考量進取得的結果當中做評核，而非檢測到不符合現時最新版系統或是工具，而將之列為不合格、不安全或是具有高風險。例如：單純為設定電子看板而架設的WIN7主機，因為不需要連網而且用途單純，因此在評核這台安裝了微軟不支援的系統的主機時，不宜直接判斷為高風險。

而在使用者電腦的相關檢測，則應注意使用者是否有適時的更新作業系統，安裝防毒軟體以及更新到最新的病毒定義檔，安裝合法的應用程式且更新到最新版本…等基本檢視。如不需要遠端連線，則關閉遠端桌面的選項。若有遠端需求，則應使用符合單位規定的VPN軟體，確保連線安全。

網路活動日益增加，因此政府的相關單位也有針對網路上常見的惡意IP提供了黑名單，或是各網通設備的廠商也有提供屬於他們自身設備可以用的黑名單。應當適時的採用這些黑名單來確保單位內的主機避開來自這些黑名單的攻擊。

當然也可以利用一些工具程式間監控自身的流量使用，如有發現異常則需要將異常的連接中斷，並檢查自身的電腦是否已被植入病毒或是因自己操作不當造成中毒。

然而事前預防勝於事後治療，平常就應該養成良好的習慣，對於不明連結不應該隨意點擊，可以先利用一些線上掃描的網站，對於該網址進行確認。像是最常見的virustotal網站，可以掃描網址跟檔案。如對即將點擊的網址有疑慮，可以先利用複製連結的功能，將網址複製起來，貼到virustotal裡面進行確認。再根據結果來決定是否進行點擊連結。

網路連線越來越成為生活的重點，很多事情不透過網路連線就無法達成。也因此會有很多惡意的行為在網路上發生，提高自己的警覺，從而避開危險也成為了現代人生活的課題。再加上一些制式的輔助工具的協助，如防毒軟體是一般人最容易取得的輔助工具之一，就可以避開大部分已知的風險。