區網網管會議

臺灣大學計資中心
李美雯
mli@ntu.edu.tw
3366-5010

大 綱

- 資通安全管理法
- 資安案例分享
  - 大規模電子郵件疑似帳密外洩
  - WinRAR 重大安全漏洞
  - 惡意程式 ShadowHammer
  - Windows 遠端桌面服務重大漏洞

資通安全管理法(教育版)

- 應辦事項_管理面

附表二 資通安全責任等級B級之各學校應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表七完成資通系統分級，並完成附表八之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或教育體系資通安全暨個人資料管理規範，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置二人；公立學校應以專職人員配置之。
	內部資通安全稽核		每年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
	資安治理成熟度評估		公立學校須每年辦理一次

資通安全管理法(教育版)

- 應辦事項_技術面

技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次。
		系統滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，臺灣學術網路連線單位得結合臺灣學術網路資安監控系統。
	政府組態基準		公立學校初次受核定或等級變更後之一年內，依本部公告之項目，完成政府組態基準導入作業，並持續維運。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必
		網路防火牆	
		具有郵件伺服器	

資通安全管理法(教育版)

- 應辦事項_技術面

		者，應備電子郵件過濾機制	要更新或升級。
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統者，應備應用程式防火牆	
認知與訓練	資通安全教育訓練	資通安全及資訊人員	每年至少二名人員各接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。
	資通安全專業證照及職能訓練證書	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有二張以上「資通安全專業證照」及二張以上「資通安全職能評量證書」；私立學校應持有二張以上「資通安全專業證照」或「資通安全職能評量證書」，並持續維持證照、證書之有效性。	

大規模電子郵件疑似帳密外洩

- 背景說明
  - GISAC透過情資交換給AISAC，請學術單位處理電子郵件帳號疑似密碼外洩
  - 108年1月18日新聞報導”史上最大規模電子郵件帳戶密碼外洩”

資訊安全

史上「最大規模」7.73億筆電子郵件帳密遭駭外洩！一招檢查有無中標

文／記者劉惠琴 ／ 2019-01-18 13:45

(圖片來源／GETTY)

大規模學術單位電子郵件疑似帳密外洩

- 外媒報導Mega上出現一份文件，超過1.2萬個資料夾，包含大宗外洩的電子郵件帳號密碼。建議措施
- 各校系所或單位之mail 服務集中於學校資訊中心，以減少維護人力、成本及符合**資安法**要求。

WinRAR 重大安全漏洞

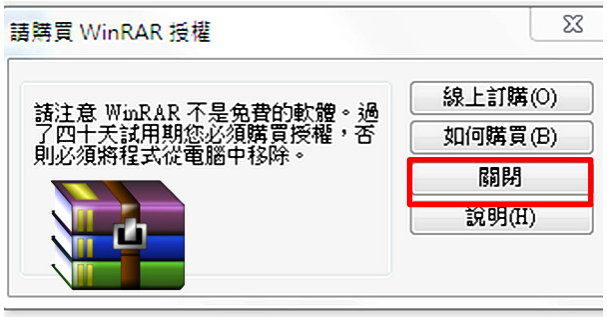
- 背景說明
  - WinRAR是一個Windows平台上，經典的壓縮檔案工具，使用此工具的人數多到不勝枚舉
  - 因資安業者Check Point在二月底公布此漏洞，一旦有人利用此漏洞可能造成大規模資安事件
  - 根據WinRAR官網顯示，使用人數已經超過5億

圖片來源：https://win-rar.com/

出處:北區ASOC整理

WinRAR 重大安全漏洞

- 背景說明
  - 大部分使用者是不會購買軟體授權(右圖，1套1050元)
  - WinRAR在授權過期後，會跳出購買授權資訊，忽略此資訊仍然可以繼續使用WinRAR(左圖，按下關閉即可繼續使用)
  - 因為這樣的原因，導致使用者不會主動去更新軟體版本



圖片來源：https://www.ettoday.net/dalemon/post/29867

圖片來源：https://rar.tw/order.html

WinRAR 重大安全漏洞

- **漏洞描述**
  - WinRAR可以解壓縮.ace檔案格式，而該檔案格式會使用到UNACEV2.dll檔案
  - .ace檔案是由壓縮軟體WinAce產生，該軟體在2007年後就沒有更新維護
  - 經資安業者測試後，發現是UNACEV2.dll內部函式因為過濾(壓縮)路徑不嚴謹導致路徑穿越漏洞
  - 當受害者解壓縮漏洞壓縮檔時，可不經受害者同意植入惡意程式

圖片來源：https://news.softpedia.com/news/WinAce-VS-WinRAR-VS-WinZip-17365.shtml#sgal_1

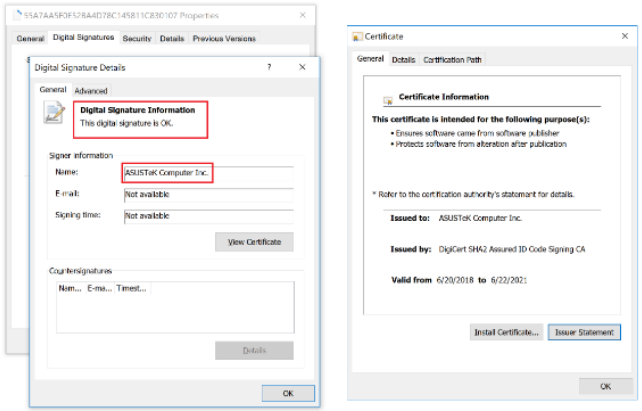
出處:北區ASOC整理

WinRAR 重大安全漏洞

- **建議措施**
  - 盡速更新至WinRAR 5.7.0
  - 更換解壓縮工具軟體

惡意程式 ShadowHammer

- 背景說明
  - 卡巴斯基實驗室（Kaspersky Lab）表示，去年華碩電腦遭到駭客集團入侵該公司的軟體更新Live Upadte伺服器，並藉此在使用者的電腦植入惡意後門程式
  - 此惡意程式利用華碩官方數位簽章，偽裝成正常軟體更新，凸顯了供應鏈資安的隱憂



▲ 被木馬化的華碩數位簽證序號 05e6a0be5ac359c7ff11f4b467ab20fc。（Source：卡巴斯基）

惡意程式 ShadowHammer

- 行為描述
  - 該後門程式推定為駭客對特定人士的針對性攻擊
  - 在發現的後門程式樣本中包含一份600多個MAC Address表單，受感染設備之MAC與該表匹配，才會進行下一步，下載惡意程式。反之，則尚未偵測到網路活動

惡意程式 ShadowHammer

- 解決方案
  - 卡巴斯基推出了線上版的mac檢測工具
    - https://shadowhammer.kaspersky.com/
    - 可偵測裝置是否為shadow hammer攻擊目標
  - 華碩官方釋出的檢測工具ASDT
    - https://dlcdnets.asus.com/pub/ASUS/nb/Apps_for_Win10/ASUSDiagnosticTool/ASDT_v1.0.1.0.zip

Windows 遠端桌面服務重大漏洞

- 背景說明
  - 根據微軟發布之安全公告，舊版本Windows 作業系統存在重大遠端執行程式碼漏洞，有引發類似類似WannaCry災難之虞
  - 罕見針對Windows XP、Server 2003釋出修補程式，並呼籲用戶儘速升級

Windows 遠端桌面服務重大漏洞

- 行為描述
  - 本漏洞可使未授權攻擊者得以利用RDP連上目標系統，成功開採者可於遠端執行任意程式碼、安裝惡意程式、讀取或刪改資料、或新開具完整權限的用戶帳號
  - “MS_T120”這個靜態虛擬Channel，它的RDP Channel編號為31，為微軟針對RDP通訊服務使用的Channel名稱。當攻擊者偽造另一個名稱為“MS_T120”，且Channel編號不等於31的連線請求時，就會造成目標系統記憶體崩潰或是能夠遠端執行任意程式碼
  - 此漏洞可透過蠕蟲程式擴散，可從一臺有漏洞的電腦複製擴散到其他電腦上

Windows 遠端桌面服務重大漏洞

- 影響系統

1. Windows XP
2. Windows 7
3. Windows Server 2003
4. Windows Server 2008
5. Windows Server 2008 R2

Windows 遠端桌面服務重大漏洞

- 解決方案
  - IPS Snort rule已可偵測阻擋
  - 微軟針對本次漏洞釋出KB4500705版本修補程式
  - 於系統註冊表中，修改RDP協議預設PORT