教育體系資安檢核

臺灣大學計資中心網路組

游子興、童鵬哲

資通安全管理法

* 2019年資通安全管理法及子法與應辦事項簡介

資通安全責任等級應辦事項(續)

辦理項目	辦理內容	A	B	C
資通安全健診	• 網路架構檢視 • 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	每年1次	每2年1次	每2年1次
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，並持續維運及依主管機關指定之方式提交監控管理資料。	1年內	1年內	
政府組態基準	初次受核定或等級變更後，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。	1年內	1年內	

教育體系資安檢核
(上午)

* 個人電腦/伺服器主機 安全檢核
  * 深度檢核：防毒軟體、修補程式安全性更新、應用程式更新、惡意程式檢核
* 組態設定安全檢核
  * 組態基準設定(GCB)：作業系統、瀏覽器和應用程式、網通設備
* 網路架構檢核
  * 網路架構檢核: 網路及系統之管理安全控制
  * 防火牆規則及存取控制
  * 備援機制
* 網路惡意活動檢視
  * 封包監聽與分析
  * 網路設備日誌檔分析
  * 連線惡意中繼名單
  * SNORT RULE 特徵規則偵測

教育體系資安檢核
(下午)

* 個人電腦安全檢核
  * 弱點掃描
* 物聯網設備檢核
  * 物聯網設備包含：網路攝影機、門禁設備、網路印表機、無線網路基地台
  * 弱點掃描
* 伺服器主機惡意活動檢視
  * 弱點掃描
  * 滲透測試(選)

使用工具

- 個人電腦安全檢核
  - Microsoft Baseline Security Analyzer
  - Windows Update offline scan file
  - TCP View
  - Process Explorer
  - psinfo
  - Autorun
- 網路惡意活動檢視
  - Wireshark
  - Pfsense
  - SNORT/Suricata
- 弱點掃描
  - OpenVAS
  - OWASP ZAP
  - Nmap
- 滲透測試
  - Metasploit