資訊處
Office of Information Technology

資安弱點通報機制(VANS)及教育部資安專案稽核研討會

簡報人員：薛雅芳

中華民國111年03月24日

報告內容

一、政府組態基準(GCB)及資安弱點通報機制(VANS)說明
二、導入VANS說明
三、導入GCB說明
四、各單位配合事項
五、教育部資安專案稽核說明

一、政府組態基準(GCB)及資安弱點通報機制(VANS)說明

附件1-廠商簡報

資訊處GCB諮詢窗口：許技正　分機14103　shuyu@ccu.edu.tw
資訊處VANS諮詢窗口：薛小姐　分機14109　yafang@ccu.edu.tw
廠商窗口：黃瑞芬 michelle@rapixus.com　辦公電話：(04)2202-5688

二、導入VANS說明

為何要導入VANS

- 因應行政院資通安全責任等級分級辦法資通安全責任等級C級之公務機關應辦事項要求

資通安全弱點通報機制	一、 初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。

- 主管機關指定之方式提交資訊資產盤點資料
  - ✓定期提報本校安裝之軟體資料

行政院技術服務中心對VANS簡介

前言

- 不定期爆發之重大弱點，若未能即時反應，將嚴重影響機關業務正常運作，亦可能造成機關形象受損
- 當弱點爆發時，如能確實掌握機關資通系統與使用者電腦情況，即可快速因應，將損害降至最低

快速反應	如何在弱點發布後，快速反應所面臨的威脅與掌握受影響版本
確認範圍	如何在確認受影響版本後，可確實掌握受影響範圍
應變處理	如何在確認受影響範圍後，快速因應處理
事後追蹤	如何在應變處理後，持續追蹤弱點修補情形

5

VANS目標

- 確認資訊資產弱點
  - 蒐集政府機關使用之軟體資訊，並與國際權威弱點資料庫進行比對，當使用軟體存在重大弱點時，即時得知與應變處理
- 降低重大弱點管控與追蹤之成本
  - 利用弱點資料庫搭配自動比對方式，提供政府機關相關弱點資訊與自我檢查機制
- 追蹤資訊資產弱點修補情形
  - 依照機關訂定之風險值門檻，及時提醒資訊資產風險情形，並進行弱點評估與修補作業
- 強化安全性更新落實情形
  - 搭配上傳已安裝安全性更新，以協助機關確認微軟資產之安全性更新缺漏項目，更精準呈現微軟弱點修補情形

12

➢2021年學校與研究單位成攻擊最頻繁目標，臺灣每週遭攻擊次數是全球平均3倍-ITHOME 2022/03/16

資訊資產呈現方式

- 蒐集範圍為Windows平台安裝軟體資產
- 回報資料須轉換CPE格式+定期回報

資訊資產盤點標的

- 蒐集範圍：Windows平台資通系統與使用者電腦之軟體資產

- 軟體名稱
- 開發廠商名稱
- 版本資訊
- 軟體安裝數量

15

資訊資產呈現方式(2/2)

- CPE條目範例
  - Microsoft Windows Server 2012 R2 Service Pack 1 on X64

  - Oracle JDK 1.8.0 Update 92

人工處理不現實不可行

17

導入VANS中控系統

優點	缺點
1. 一鍵安裝，軟體資產自動更新 2. 中控台即時監控各Windows設備硬體及軟體安裝資訊 3. 輔助每年資訊資產盤點 4. 應付教育部緊急調查重大漏洞軟體安裝資訊，或許可減少各單位回報工作 **5. 滿足上級機關(行政院+教育部)要求**	1. 每年固定支出 2. 上級機關可即時得知各單位弱點修補情形 1）請各單位定期關注弱點資訊，落實更新 3. 目前僅適用於Windows作業系統，其他平台仍需逐台管理

三、導入GCB說明

為何要導入GCB

- 因應行政院資通安全責任等級分級辦法資通安全責任等級A、B級之公務機關應辦事項要求

政府組態基準	初次受核定或等級變更後之一年內，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。

- 本校已非資安責任等級B級機關，依教育部109年資安稽核後續追蹤仍建議持續完善使用者電腦端資安防護

教育部「資通安全技術檢測」建議事項之矯正預防措施					審查結果		
項次	分類	項目	因應作為辦理情形	時程規劃日期	審查意見	建議修正事項	歷程概要及調閱資料清單
14	組態設定安全	基本資料調查表回覆「資訊處訂定管理清單13項如下，其餘為例外清單。」，並未說明例外清單之原因。建議單位未來可考慮導入更多之GCB相關規則，完善整體資安防護。	(一)將持續檢討增加GCB規則導入數量，並視預算經費狀況採購GCB管理軟體。 (二)110年6月9日行政院核定本校資通安全責任等級為C級，政府組態基準(GCB)導入作業為非必要辦理項目，本案申請解除列管。	110年12月31日 (申請解列)	■同意(依計畫辦理) □建議修正	111/1/21回覆： 惟仍建議學校持續完善使用者電腦端資安防護。	110/4/30審查人員同意受檢單位回覆資訊。 111/1/21審查人員同意受檢單位回覆資訊。

行政院技術服務中心對GCB簡介

前言

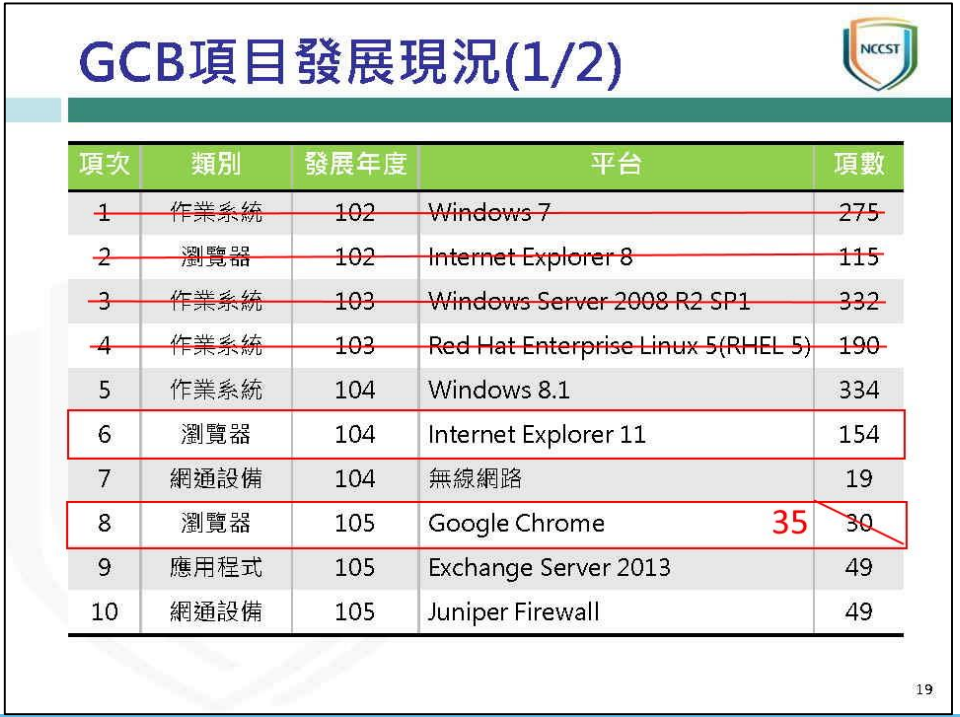
- 政府組態基準(Government Configuration Baseline，以下簡稱GCB)目的在於規範資通訊終端設備(如：個人電腦、伺服器主機及網通設備)的一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮

1. 發展一致的安全組態設定
2. 提升政府機關資通訊終端設備使用安全性

5

GCB項目發展現況

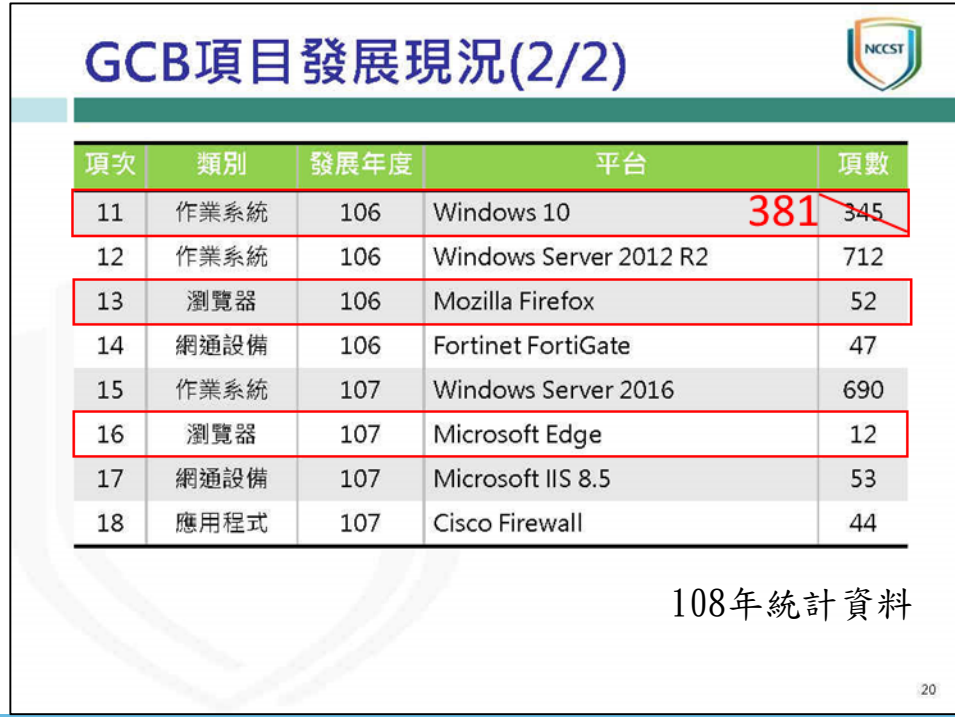
- Windows10為例，需**設定**項目至少154+381+12=**547**項
- 如果安裝Google Chrome(35項)、Firefox(52項)



GCB項目發展現況(1/2)

項次	類別	發展年度	平台	項數
1	作業系統	102	Windows 7	275
2	瀏覽器	102	Internet Explorer 8	115
3	作業系統	103	Windows Server 2008 R2 SP1	332
4	作業系統	103	Red Hat Enterprise Linux 5(RHEL 5)	190
5	作業系統	104	Windows 8.1	334
6	瀏覽器	104	Internet Explorer 11	154
7	網通設備	104	無線網路	19
8	瀏覽器	105	Google Chrome 35	30
9	應用程式	105	Exchange Server 2013	49
10	網通設備	105	Juniper Firewall	49

19



GCB項目發展現況(2/2)

項次	類別	發展年度	平台	項數
11	作業系統	106	Windows 10 381	345
12	作業系統	106	Windows Server 2012 R2	712
13	瀏覽器	106	Mozilla Firefox	52
14	網通設備	106	Fortinet FortiGate	47
15	作業系統	107	Windows Server 2016	690
16	瀏覽器	107	Microsoft Edge	12
17	網通設備	107	Microsoft IIS 8.5	53
18	應用程式	107	Cisco Firewall	44

108年統計資料

20

本校執行現況

- 回憶109年教育部資安稽核，採人工逐台電腦設定
  - ✓附件2-109年教育部資安稽核簡報
  - ✓只做13+1項
  - ✓新安裝電腦都有設定嗎？

- **以人工逐台設定不現實不可行**

導入GCB中控系統

優點	缺點
1. 一鍵安裝，免逐台逐項設定 2. GCB政策調整，中控台統一管理 3. 委託經驗豐富廠商協助導入，借重他機關導入經驗，排除不適合項目，避免踩地雷 **4. 滿足上級機關(行政院+教育部)要求**	1. 每年固定支出 2. 影響使用者操作習慣 3. GCB設定可能影響部分程式運作 1）初期僅導入部分項目 2）請反應資訊處調整設定 3）大絕-解除安裝恢復原設定 4. 目前僅適用於Windows作業系統，其他平台仍需逐台管理

四、各單位配合事項

導入範圍及時程

- 導入範圍
  - ✓限Windows作業系統(含Windows Server)
  - ✓行政用個人電腦及資通系統主機
- 導入時程
  - ✓3月28日至4月10日：派送GCB設定(密碼原則)
  - ✓4月18日至4月30日：舉辦各單位管理人教育訓練2梯次
  - ✓5月01日至6月30日：派送GCB設定(逐步調整)

各單位配合事項

- 指派各單位管理人至少1名
  - ✓協助於單位內行政用Windows個人電腦及主機安裝VANS代理軟體
    - 時間：3月28日至4月10日
    - 後續將以電子郵件寄送軟體下載網址
  - ✓提供各單位設備IP清單，供資訊處於中控台設定設備歸屬
  - ✓填寫權限申請表，申請單位管理者權限
    - 附件3-ISMS-208-01_資通系統設備帳號權限申請表
  - ✓定期登入中控台，檢視單位內軟體弱點訊息，通知當事人更新
  - ✓中控台網址：https://vans.ccu.edu.tw/

資訊處
Office of Information Technology

報告完畢、敬請指教