交通部

政府機關資安弱點通報機制推廣說明會_機關分享

交通部

108年11月27日

大綱

- 前言
- 環境說明
- 實作過程
- 實際效益與心得分享

前言

- 為何使用「政府機關資安弱點通報機制（簡稱VANS系統）」
  - 108年參與資安服務團之輔導訓練，了解VANS運作機制與系統操作
  - 108年接受資安服務團之實地輔導，挑選標的系統與使用者電腦導入VANS系統

環境說明

資訊環境概況

- 資通系統為49個，主機數量共約278台(包括實體與虛擬主機)
  - 軟體盤點頻率：每年
  - 軟體盤點方式：以人工方式進行盤點

使用者電腦共約678台

- 軟體盤點頻率：每日
- 軟體盤點方式：透過資產管理工具於使用者電腦開機時自動進行盤點

弱點管理

- 接收「行政院國家資通安全會報技術服務中心」與「SOC廠商」發布的漏洞/資安警訊
  - 警訊處理方式
    - 於資安管理平台檢視警訊，且風險等級為3以上須修復並進行回報
    - 透過資產管理系統確認受影響的使用者電腦範圍
- 安全性檢測

項目	執行頻率	執行範圍	弱點處理方式
弱點掃描	每年	• 主機弱掃：挑選50個IP • 網站弱掃：核心資通系統與挑選部分非核心系統	• 針對風險等級為中級以上的弱點進行修復 • 透過複掃確認弱點是否修補完畢
滲透測試	每年	核心資通系統與挑選部分非核心系統	• 針對風險等級為低級以上的弱點進行修復 • 透過複掃確認弱點是否修補完畢
資安健診	每年	全機關	由硬體維護廠商進行確認與處理

Microsoft安全性更新管理

執行項目	安全性更新週期	安全性更新方式	安全性更新檢核方式	缺漏安全性更新處理方式
資通系統	每月	以人工方式進行手動更新	以人工檢視是否已完成更新	個別系統進行確認，經測試確定不會影響系統方進行更新
使用者電腦	每週	連線至內部WSUS更新伺服器	• 透過每年的資安健診，檢測作業系統與Office應用程式的更新情形 • 透過資產管理工具查看已安裝安全性更新的清單	透過排程每日進行安裝更新

實作過程

挑選導入標的

執行項目	挑選原則
資通系統	• 挑選資通系統資安等級高之系統先行導入 • 以「電子公文交換系統」進行導入
使用者電腦	從資產管理工具挑選10台使用者電腦先行導入

資訊資產盤點與正規化

挑選導入標的 | 資訊資產盤點與正規化 | 登錄VANS系統 | 弱點通知與修補規劃 | 更新資訊資產

執行項目	盤點方式	正規化方式
資通系統	• 人工盤點 • 針對7台實體主機進行盤點，盤點步驟如下： 1. 透過WMIC批次檔，逐台執行批次檔盤點並匯出資產資訊 2. 使用Excel彙整成資訊資產清單，共計297筆資訊資產	• 人工正規化 • 正規化步驟如下 1. 至VANS系統下載「完整軟體資產CPE清單」 2. 資訊資產清單與步驟一下載的CPE清單進行搜尋比對，建立CPE格式資訊資產清單 3. 於資通系統與使用者電腦，分別對應出4筆與41筆CPE格式資訊資產
使用者電腦	• 透過資產管理工具 • 從資產管理工具挑選10台使用者電腦，匯出資產資訊，共計808筆資訊資產	
資產管理工具POC環境	• 透過資產管理工具 • 從資產管理工具挑選3台電腦，匯出資產資訊，共計171筆資訊資產	• 透過資產管理工具 • 執行資產管理工具的CPE模組，自動產出CPE格式資訊資產清單，共計4筆CPE格式資訊資產

資訊資產登錄與管理

挑選
導入標的 | 資訊資產盤點與正規化 | 登錄
VANS系統 | 弱點通知與修補規劃 | 更新
資訊資產

- 上傳CPE格式資訊資產清單至VANS系統，並於VANS系統進行資訊資產管理與風險管理
  - 透過資產列表，檢視已安裝資訊資產之項目與數量。接收弱點時透過查詢，了解機關內部是否有使用該資訊資產及所使用的數量
  - 透過資產列表，檢視已安裝資訊資產哪些有潛在的風險，並至弱點列表確認是否已進行修補
  - 透過風險列表，檢視資訊資產經與弱點資料庫比對出的弱點資訊，共計3,918筆CVE弱點項目

弱點通知與修補規劃(1/3)

挑選導入標的 | 資訊資產盤點與正規化 | 登錄VANS系統 | **弱點通知與修補規劃** | 更新資訊資產

- 透過電子郵件，接收VANS系統發送之弱點通知
  - VANS系統設定通知門檻值為4分，即可收到風險等級中級以上之弱點通知
  - 當VANS系統上之資訊資產比對到新的弱點，可即時接收弱點通知並進行處理

CVSS與安全等級對應表

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

- 至VANS系統進行弱點確認
  - 透過VANS系統「資訊資產風險列表」，檢視機關的資訊資產目前存在哪些潛在風險
  - 透過檢視弱點資訊並評估後續的修補方式

弱點通知與修補規劃(2/3)

挑選導入標的 | 資訊資產盤點與正規化 | 登錄VANS系統 | **弱點通知與修補規劃** | 更新資訊資產

- 至VANS系統進行修補規劃
  - 透過檢視資訊資產的弱點修補進度，得知哪些弱點尚未進行處理，並針對尚未處理之弱點進行修補
  - 微軟系列資訊資產之弱點修補方式
    - 透過微軟提供之安全性更新，於每日排程進行安裝更新
    - 針對重要的安全性更新，會透過資產管理工具查看使用者電腦的安全性更新清單，確認是否以安裝更新
    - 透過MBSA安全性更新檢測工具，確認安全性更新狀態，並直接上傳於VANS系統檢視安全性更新報告
  - 非微軟系列資訊資產之弱點修補方式
    - 透過風險資訊中的建議修補方式進行修補
    - 評估是否透過升版進行修補

弱點通知與修補規劃(3/3)

挑選導入標的 | 資訊資產盤點與正規化 | 登錄VANS系統 | 弱點通知與修補規劃 | 更新資訊資產

- 可於VANS系統下載弱點清單
  - 透過弱點清單匯出功能，檢視機關的資訊資產目前所存在的弱點，以及每個弱點之修補規劃或改善措施紀錄
  - 透過弱點清單匯出並提供給負責人，讓無權限進系統之負責人亦能接收弱點，並進行後續修補
  - 於管審會議或於每季季檢討會議，搭配弱點清單的匯出進行弱點修補情況報告

更新資訊資產

- 更新CPE格式資產清單，並上傳至VANS系統
  - 當透過升版或移除資訊資產進行弱點修補時，同步更新CPE格式資產清單並上傳至VANS系統，以維持資訊資產的正確性

實際效益與心得分享

實際效益

- VANS系統約10分鐘會與弱點資料庫進行1次比對，較弱點掃描有更高之即時性
- 定期安全性檢測，僅會針對伺服器主機弱點掃描、網頁滲透測試，藉由VANS系統可了解使用者電腦的弱點
- 可搭配MBSACLI安全性更新檢測，於VANS系統檢視安全性更新結果

心得分享

- 在實地輔導期間，得知使用的資產管理工具於更新版本後有提供CPE模組，並透過POC環境進行CPE模組試用。可於挑選標的電腦後即可直接產出CPE清單，透過資產管理工具可有效減少人力輸出
- 接收弱點時，現行需先透過資產管理工具查詢確認是否對機關有影響。可透過VANS系統自訂弱點通知門檻值，以即時掌握對機關有受影響的資訊資產及其數量
- 微軟產品會透過安全性更新來提供弱點修補，因此在實地輔導期間使用MBSA檢測工具檢測使用者電腦安全性更新情形，以有效掌握使用者電腦更新落實程度，提升使用者電腦資安防護能力
- VANS系統提供檢視更新報告之功能，可將回收的多份安全性更新報告上傳至VANS系統，有效降低報告彙整時間

報告完畢

敬請指教