政府機關資安弱點通報機制推廣說明會_機關分享

勞動部

108年11月27/28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)」
  - 106年參與機關試行專案，導入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

- 資通系統約為60個
  - 軟體盤點頻率：每年盤點1次，並更新資訊資產清冊
  - 軟體盤點方式：透過資產管理工具產出清冊，再行人工比對
- 使用者電腦共約400台
  - 軟體盤點頻率：每年系統盤點1次，並於每半年一次之個人電腦保養時同步確認正確性（分批執行保養）
  - 軟體盤點方式：透過資產管理工具產出清冊，再行人工比對

弱點管理(1/2)

- 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
  - 透過資產管理系統確認受影響的伺服器及使用者電腦範圍。
  - SOC中級以上之警訊會交由負責人處理，於「警訊通報單」記錄執行方式與執行情形。
  - 若為技服中心發布之資安警訊，則填寫「資安警訊事件處理單」並交由負責人員處理，回報預計執行方式與執行情形後，再由資訊處主管核章確認。

弱點管理(2/2)

- 定期進行安全性檢測

項目	執行頻率	執行範圍	弱點處理方式
弱點掃描	每半年	• 主機弱掃：挑選指定網段 • 網站弱掃：核心資通系統與挑選部分非核心系統	• 強制風險等級為中級以上的弱點均須修復，由系統承辦人填具處理報告單。 • 2週內進行複掃，確認弱點是否修補完畢，再將結果陳核至資訊處長後歸檔。
滲透測試	每年	核心資通系統與挑選部分非核心系統	• 強制風險等級為中級以上的弱點均須修復。 • 2週內透過弱點處理結果並回覆資訊單位，資通安全科彙整弱點處理報告單後，陳核至資訊處長後歸檔。
資安健診	每年	全機關	由各機房管理人員及工程師進行確認與處理

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	每季	連線至內部WSUS更新伺服器	透過資產管理工具撈取WSUS報告進行檢視	個別系統進行確認，經測試確定不會影響系統，方進行更新
使用者個人電腦	即時	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 • 透過資產管理工具撈取WSUS報告進行檢視 • 於個人電腦保養時逐台檢視安全性更新並記錄於「個人電腦保養電腦確認單」	• 每日使用者電腦關機時，會自動下載與更新 • 若有更新條目出現異常而影響使用者電腦時，會至使用者端進行手動處理

實作過程

挑選導入標的

106年試行專案	執行項目	挑選原則
	資通系統	挑選2個資通系統，分別為「全球資訊網」與「勞雇雙方協商調整例假登錄系統」導入試行
	使用者電腦	挑選具代表性類型之30台個人電腦進行安全性更新檢測。(主要條件為MS Office版本不同2003, 2007, 2010, 2013等, 有無firefox, pdf maker等應用環境條件差異為考量)

108年實地輔導	執行項目	挑選原則
	資通系統	• 從資通系統安全等級為高之系統進行挑選先行導入 • 以「勞動債權精算平台及資料自動交換系統測試站」進行導入
	使用者電腦	從資產管理工具挑選資訊單位14台個人電腦先行導入（原則為Win7及Win10按當時分布比例分配，約為3:1)

資訊資產盤點與正規化

勞動部 Ministry of Labor

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
106年試行專案	資通系統	• 人工盤點 • 針對1台實體與3台虛擬主機進行盤點，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2,816筆資訊資產	• 人工正規化 • 正規化步驟如下： 1. 至VANS系統下載「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，共比對出29筆CPE格式資訊資產

	執行項目	盤點方式	正規化方式
108年實地輔導	資通系統	• 透過資產管理工具 • 針對1台虛擬主機進行盤點，並匯出資產資訊，共計16筆資訊資產	• 透過資產管理工具POC環境 • 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
	使用者電腦	• 透過資產管理工具 • 從資產管理工具挑選14台使用者電腦，匯出資產資訊，共計197筆資訊資產	• 透過資產管理工具POC環境 • 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13筆CPE格式資訊資產

資訊資產登錄與管理

勞動部 Ministry of Labor

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
- 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。於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，108年實地輔導共比對出2,631筆常見的弱點與漏洞項目(CVE)

弱點通知與修補規劃(1/3)

勞動部 Ministry of Labor

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
  - 於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)

- 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個人電腦的安全性更新清單，確認是否已安裝更新
    - 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
    - 評估是否可透過升版進行修補

弱點通知與修補規劃(3/3)

- 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
  - 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

- 透過VANS系統可快速掌握資訊資產弱點，達到即早得知與應變處理
- 透過VANS系統的弱點清單，掌握軟體資產弱點的處理進度
- 透過MBSA安全性更新檢測工具，快速確認未安裝安全性更新之電腦數量與範圍，並進行應變處理

心得分享

- 106年進行機關試行專案時，於正規化階段資訊資產要透過手動比對與勾選CPE清單並彙整資訊資產清單，消耗較多的人力成本。108年實地輔導時，透過試用資產管理工具的CPE模組，挑選標的後自動產出CPE清單，有效率地進行資產盤點、正規化及資訊資產登錄
- VANS系統會自動的與弱點資料庫進行比對，透過漏洞評鑑系統(CVSS)分數的設定，便可即時性的掌握機關中風險以上弱點。透過下載弱點清單，快速針對受影響的資訊資產進行弱點修補與紀錄，有效降低重大弱點管控與修補情形追蹤的人力與資源成本
- 透過VANS系統，針對使用者電腦與伺服器主機進行軟體資訊資產的弱點管控。再搭配MBSA安全性更新檢測工具，以提高安全性更新的落實程度，及提升安全性更新掌握能力

勞動部
Ministry of Labor

報告完畢
敬請指教