TLP:AMBER

資通安全業務推動及重點工作

數位發展部 資通安全署
114年12月18日

大綱

一、國內外資安事件與趨勢

二、資安業務執行成果與未來展望

(一)全社會資安防禦

(二)提升關鍵基礎設施資安韌性

(三)壯大我國資安產業

(四)AI新興資安科技應用與合作

一、國內外資安事件與趨勢

威脅趨勢與資安事件掃描(1/2)

高風險漏洞未修

- 產品漏洞遭利用造成整體供應鏈風險
- 加拿大電信業者漏洞遭利用被成功入侵
- 未即時處理資安預警警訊導致個資外洩

AI驅動惡意程式

- AI 惡意程式具備高適應性、規避性

雲端風險加劇

- 雲端環境放置惡意檔案難以偵測
- 雲端設定錯誤致資料外洩

資料外洩
名聲受損

服務中斷

勒索攻擊
造成財損

威脅趨勢與資安事件掃描(2/2)

工業與關鍵基礎設施受威脅

- 多家人機介面製造商產品出現多項漏洞
- 利用太陽能變流器漏洞攻擊電網
- 法國商製造營運管理平台曝露高風險遠端程式碼遭執行漏洞，影響航空、汽車、電子等產業
- 海底電纜遭破壞、醫院受勒索軟體攻擊

偽冒軟體與即時通訊釣魚

- 透過社交工程誘騙下載含後門程式的偽冒惡意軟體
- 利用即時通訊軟體進行網路釣魚、散布惡意連結，或潛藏群組竊聽機敏資訊
- 濫用即時通訊「設備連結」功能至訊息外洩

API破口

- 調查顯示57% 組織在過去2年曾遭遇 API 資安事件
- API組態設定錯誤

資料外洩

服務中斷

勒索攻擊

應對策略(1/2)

強化合作與資安意識

強化供應鏈安全

- 簽訂資料處理協議 (DPA)，遵循資料最小化
- 將供應商服務納入資安協議
- 限制管理介面存取來源，落實最小權限

提升資安意識

- 落實資安意識訓練
- 僅從官方來源下載應用程式
- 即時通訊應用程式資安管理

推動跨界協作

- 推動公私協作:如我國「產品資安漏洞獵捕計畫」
- 運用開源平台:如美國開源惡意程式分析平台(Thorium)

應對策略(2/2)

持續強化防禦及流程管理

完善資安治理

- 持續完善資安治理體系，公私協力共同應對日益升級的資安威脅
- 關注國際情資、謹慎評估應對風險
- 完善資安應變機制

落實控制措施

- 儘速修補高風險漏洞
- 加強導入零信任架構
- 嚴謹網路區隔(IT/OT)
- 應用程式白名單與安全組態設定
- 雲端環境與 API 存取控制

強化端點偵測

- 部署端點防護機制、網頁應用程式防火牆，強化日誌監控與異常偵測
- 運用AI技術提升應對效能

二、資安業務執行成果與未來展望

全社會資安防禦

扣合第七期國家資安發展方案策略一

- 資安人員增能調訓機制
- 資安稽核

資安人員增能調訓機制

建立政府機關資安人員增能調訓機制

- 依所需**知能內涵**，採**分層設計規劃**
- 因應資安威脅變化，透過**年度調訓持續強化**各級資安人員防護知能

資安長

- **資安長共識營(每年1次調訓)**
  - 114年培訓逾159名資安長
  - 115年規劃**1場次**(暫訂5/6)
  - **與CYBERSEC臺灣資安大會等活動合辦**，透過公私協力強化資安韌性

資訊(安)主管

- **資訊(安)主管資安研習(每年1次調訓)**
  - 114年培訓逾360名資訊(安)主管
  - 115年規劃**1場次**(暫訂5/19)
  - 優先針對**督導辦理資安業務或資通系統開發、維運之直屬主管**，精進其資安管理職能

資通安全專職人員

- **資安專職人員資安研習(每年1次調訓)**
  - 115年首次辦理，規劃**8場次**
  - 結合資安防護巡迴研討會與資安人員專業訓練
  - 上午為**共通性課程**，下午**依職務分眾規劃交流性活動**

註： 114年針對資安專職(責)人員，透過職能訓練、增能培訓等活動培訓逾5,000人次

資安稽核成果-共通性發現

114年實地稽核 **40個** 機關

公務機關	關鍵基礎設施提供者	特定非公務機關
20個	14個	6個

強化各機關資安量能

策略面	•演練缺乏**複合式情境**與**業務單位參與**、未涵蓋**備份還原測試** •系統**分級**評估、**備份**及**備援**機制未臻妥適 •未落實持續**精進**及**績效**管理機制	共通性發現**函請各機關參考**，以**提升整體資安防護**
管理面	•未落實**委外管理**措施 •未確實**盤點**資產、盤點範圍未涵蓋全機關 •資安**風險評估**機制未臻妥適	待改善事項將**管考至全部改善完成**
技術面	•未落實執行**資安防護**控制措施 •未確實**修復弱點**、**帳號管理**、執行**安全性檢測** •資安事件**通報**未符規定	於資安專職人員訓練課程中**加強宣導**
OT面	•未落實OT**帳號管理**機制、未完整**盤點**OT資產 •未落實執行OT**資安防護**控制措施 •未落實OT資安**風險評估**	納入資安業務稽核評核，獎勵**績優機關**及**人員**獎勵金及獎座，提升士氣

115年資安稽核規劃

遴選曾受國家資通安全會報稽核之機關

線上作業

AI場外稽核

受稽機關提供自評資料及佐證文件，透過本署稽核資料分析平臺**AI分析**後，由資安署及稽核委員複審，確認機關資安法落實情形

1天 3人 /每場

內部資安風險檢測

使用**自動化工具**發掘潛在系統弱點與網域帳號權限異常狀況，據以研析可能攻擊鏈，並提供風險評估結果與改善對策

遴選未曾受國家資通安全會報稽核之機關

1天 5-10人 /每場

實地稽核

組成稽核小組，由稽核委員分策略、管理、技術及工控面至現地進行檢視及訪談，以發覺潛在之資安風險

3天 12人 /每場

技術檢測

以**人工檢測**為主，包含使用者電腦、物聯網設備、核心系統等多面向檢測角度切入，以協助機關改善為主要辦理重點

#擴大稽核範圍及場次 **#技術面及程序面並重** **#結合新興科技運用**

提升關鍵基礎設施資安韌性

扣合第七期國家資安發展方案策略二

- 關鍵資訊基礎設施資安防護
- 網路攻防演練(CODE)

關鍵資訊基礎設施資安防護

強化關鍵基礎設施資安縱深防禦，全面提升國家數位韌性

- 持續辦理安全檢測
- 異常監控、經驗共享、建立本土威脅資料庫、提升整體防護效率

規劃執行

- 關鍵基礎設施OT資安訪談
- 關鍵基礎設施實地正式檢測
- 關鍵基礎設施資安桌上推演

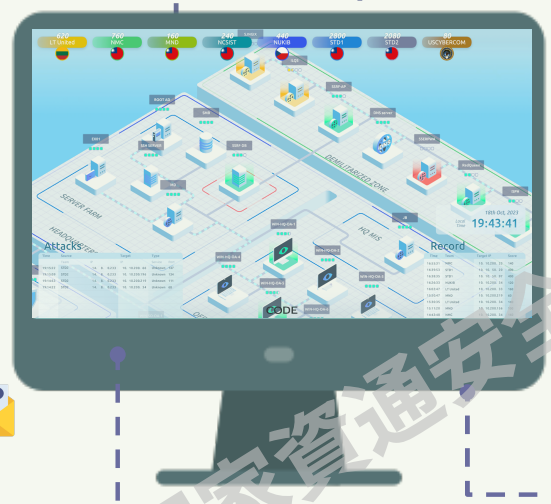
機關配合事項

- OT或資安人員配合訪談作業
- 配合檢測，及從檢測過程中交流學習
- 機關資安長或決策主管配合參加推演

網路攻防演練(CODE)執行成果與效益

※ CODE : Cyber Offensive and Defensive Exercise, 網路攻防演練。

2025 醫療領域



高度擬真關鍵基礎設施場域

關鍵基礎設施防護及聯防

情境納入真實攻擊手法

友好國家之資安國際合作

執行成果

演練隊伍成長至16隊

國外自3國增加為6國

11家大型醫學中心

提高醫療領域應變能力

推動國際資安聯防

活動逾20餘國參與

效益 #真實事件應處實務 #資安事件應處能力 #納入情資分享與資安聯防

壯大我國資安產業

扣合第七期國家資安發展方案策略三

- 危害國家資通安全產品政策及宣導
- 強化政府採購供應風險管理

危害國家資通安全產品政策及宣導

1 公務機關禁用陸牌資通訊產品

- ✓ 辦理「資安高風險APP」記者會，宣導中製App潛在風險，如蒐集敏感性資訊、讀取儲存空間、踰越使用權限、掌握生物特徵、擷取系統資訊、數據回傳及分享等。
- ✓ 目前政府提供之網際網路接取服務，如政府網際服務網GSN、臺灣學術網路TANet（高中以下），已不提供抖音、小紅書、微信、微博、百度雲盤這5款中製App之公共傳輸服務。

2 契約納入「採購契約範本附記條款特別聲明」

- ✓ DeepSeek AI經測試證實抵禦越獄攻擊的能力不足，模型缺乏外加安全防護機制等，且為大陸廠牌服務，多次宣導公務機關禁止使用。
- ✓ 工程會114.5.20修正政府採購契約範本，訂定「採購契約範本附記條款特別聲明」，履約禁用DeepSeek(含禁止廠商使用DeepSeek製作書面履約成果)。

3 協助機關諮詢危害國家資通安全產品議題

- ✓ 114年度協助各公務機關諮詢，超過50件。
- ✓ 協助機關使用合規資通訊產品、減少民眾疑慮與提升對政府信賴度。

強化政府採購供應風險管理

推動策略

1.套裝軟體 強化產品安全

- 使用機關數、金額、訂購數量
- 高風險產品(例如資產管理、GCB、防毒等)

1. 推動產品漏洞獵捕計畫
2. 增訂上架共契資安規範
   (須通過資安檢測、漏洞更新機制等)

2.雲端/資訊服務 落實資安管理

- 國內雲端服務產商
- 國內資通系統開發及維運廠商

1. 推動導入PSIRT機制
2. 透過資安訪視輔導廠商落實管理

3.資安服務 精進資安技術

- SOC服務
- 資安健診
- 弱點掃描
- 滲透測試
- 社交工程
- 紅隊演練

1. 精進廠商評鑑機制
2. 強化產官合作
   (資安攻防演練、資安自主產品)

AI新興資安科技應用與合作

扣合第七期國家資安發展方案策略四

- 後量子密碼遷移程序規劃
- AI新興科技應用與合作規劃

後量子密碼遷移程序規劃

迎接量子時代挑戰
打造數位安全韌性

規劃後量子密碼遷移程序

- 擬定我國政策並對齊國際趨勢
- 盤點現行密碼現況與風險
- 推動政府與CI建立遷移計畫

評估後量子產品評測制度

- 建立一致性的測試流程
- 提供機關透明決策依據
- 發展標準化測試項目及自動化測試流程

預期達成效果

- 提升密碼安全意識
- 政策與制度接軌
- 政府整體遷移規劃

AI新興科技應用與合作規劃

以AI驅動國家資安韌性
打造可信任AI發展環境

推動AI安全治理

- 調適因應AI之資安法制
- 觀測國際AI安全法規政策
- 研擬AI安全風險指引

強化AI安全驗測

- 擴大AI安全驗測量能
- 研擬我國AI安全驗測規範

人才培育與交流合作

- 提升AI安全專業技能
- 公私協力及跨國交流

報告完畢 敬請指導

資安是持續精進的風險管理