# 作業報導

# ●文化部資安防護經驗

**文化部資訊處 黃泰豐**

1. **前言**

從7月份第一銀行ATM盜領案襲捲新聞版面，並佔上新聞頭版頭條，資安事件屢屢見報、層出不窮，讓人瞭解資安議題是一道難解，卻又不得不面對的關卡。隨著業務及服務不斷資訊化後，資安即是各機關或公司行號急需處理議題，加上先前個人資料保護法已通過施行，個人資料蒐集、處理、利用，更是法律規定應防護事項，也是必須正視審慎處理資安防護的理由。

由於我國與對岸政治身處敏感，公務機關一直都是進階持續性威脅（Advanced Persistent Threats, APT）頭號目標，對岸網軍透過量身訂作的社交工程信件，誘使攻擊對象開啟信件，進而埋入後門程式完成滲透，達到蒐集機關各式情資，本部亦是無法置身事外，如去年總統選舉期間曾收取標題「TISR：臺灣民心動態、大選與兩岸關係最新民調」之惡意信件，以其他機關公務信箱所發送「104年9月本局電話號碼異動彙整表」、「敬請於周五（4/15）下班前協填中興新村未來村案進度，謝謝」等，證實APT惡意信件的確不斷存在。

另104年9月19日iThome電腦報曾刊載「鎖定政府高官APT攻擊程式，將Google硬碟變駭客竊資後門」，內容略以「在2014年有一支鎖定臺灣政府跨部門、中高階主管的APT惡意程式PLEAD，日前在臺灣資安研究團隊Team T5惡意程式網路威脅分析研究員Charles Li和Zha0的揭露下發現，這隻惡意程式其利用同時間安裝的後門程式GD Rat將電腦內新增的文件資料，上傳到Google硬碟」及「因為連上Google網路硬碟所有傳輸內容都是加密，網管人員不可能阻擋這類的合法網路連線，除非該公司全面禁用相關的雲端服務。」，本部於104年中曾遭受駭客透過AD Computer Policy，將GDrive惡意程式派送至高階長官辦公室電腦，讓駭客利用Google API的方式，將竊取的資料傳送至其所申請的Google Drive，情節與上開報導相符。

1. **資訊環境及資安防護措施**

面對以上外部種種資安威脅挑戰，及真實攻擊事件存在，本部採取以下防護措施，改善整體資訊環境，分述如下：

1. 資通訊基礎設施整備

整併本部所屬各機關資通訊基礎設施，將其電腦機房逐步移轉為落地機房，採機房配置與設備標準化，另由本部統一建置4個共構電腦機房，北區國光及新莊機房、中區機房及南區機房，並租賃1個雲端機房，以利管理維護。

本部及所屬機關網路採GSN VPN連通，並關閉所屬機關自行對外連通之線路，統一由國光機房成為網路流入及流出單一閘口，達成出口流量統一控管，以減少所屬機關成為防護破口弱點。

1. 行政共通系統穩定維運及優化

行政處理資訊系統，採系統整合共構方式辦理，軟體模組可依機關業務作業流程不同設定參數辦理，系統功能共享，系統具彈性易於擴充導入，以利易於配合資訊組改與組織變動性，也可穩定維運、提高可用性。

共構建置本部及所屬共20個機關之員工入口網、公文管理系統、人事差勤管理系統、薪資系統等，19個機關電子郵件系統整併，達成系統整併減少散落開發風險。

1. 業務共通資訊系統整併及建置

推動文化業務資訊化與自動化服務，完成文化部資訊系統集中、開發與管理，如官網（專題）系統（13個機關構及5個專題網站）、文物典藏管理系統（iCollections）（17個機關）、獎補助管理系統（18個機關）、活動管理及報名系統（16個機關）、影音平臺系統（iMedia）（2個機關）、圖書自動化管理系統（12個機關），即各機關業務資訊系統或專題網站，原則由各業務司或機關各自開發應用軟體，系統置放於本部共構電腦機房。

1. 使用者電腦管理

個人電腦防護是資安端點防護最重要的一環，透過以下措施可防止病毒橫向擴散，避免災情擴大：

1. 每個樓層獨立一個VLAN網段，不互通。
2. 每臺電腦啟用本機防火牆，禁用網路磁碟機。
3. 每臺電腦須加入AD網域、套用GCB policy。
4. 每臺電腦之作業系統重大更新及通用性軟體版更作業，採自動化方式（WSUS、GPO軟體派送）辦理。
5. 每臺電腦安裝防毒軟體、資產管理軟體、端點管控軟體。
6. 每位同仁不具該臺電腦admin權限，無法自行安裝任何軟體。
7. 每週例行性防毒及惡意程式掃描作業。
8. 同仁電腦如有下列情況，暫時關閉上網。
   1. 未安裝防毒軟體。
   2. 防毒軟體病毒碼超過7日未更新。
   3. 未加入AD網域。
   4. 未安裝端點防護軟體。
   5. 作業系統重大更新未修補。
9. 資安防護縱深

除以上個人電腦防護，尚需通盤檢討資訊環境，從深度及廣度等採行不同措施，以達資安防護縱深：

1. 網路閘道端：佈署防火牆、APT攻擊防護設備、垃圾郵件及惡意附件過濾、IPS、頻寬管理、網頁內容過濾、網站應用程式防火牆（WAF）等防護設備，並採用多品牌產品，聯集產生最大防護面積。
2. 主機端：佈署主機入侵防禦系統（HIPS）、防毒軟體、系統效能監控，另高風險主機採本機登入，不得遠端連線操作；高可用性系統服務採HA機制。
3. 機敏文書：針對機敏電子檔案，於實體隔離電腦處理，並將檔案經加密後存放，另機敏電子檔案資料之列印，使用實體隔離之印表機，並顯示代碼浮水印，以利單位主管於審稿時判別，即採行實行隔離處理機敏電子檔案，降低資料被竊外洩之可能性；另與駐外館傳輸機敏資料，採用國安局保密裝備或紙本文書密件交換。
4. SOC監控管理及安全性檢測

本部及所屬機關統一委外廠商提供網路監控中心，接收本部及所屬之資安設備紀錄，以提供全年無休之資安事件（故）即時監控管理服務，包括日誌（Log）分析、警訊判讀、事件通報、處理建議等。

另透過定期辦理各式安全性檢測，查檢可能存在弱點風險，及早發現及修補，減少外對內入侵管道：

1. 主機弱點掃描：一年2次針對主機網段，掃描主機是否具有國際安全組織CVE （Common Vulnerability and Exposure）所披露的最新安全弱點，並進行複測掃描，確認弱點已排除。
2. 網站應用程式弱點掃描：一年2次針對重要網站，掃描網站是否存有Web軟體安全計畫OWASP（Open Web Application Security Project）所披露的最新安全弱點，並進行複測掃描，確認弱點已排除。
3. 滲透測試：針對本部與國光機房之服務主機、作業系統及各個網路應用服務程式可能存在的弱點，模擬內、外部駭客攻擊行為，嘗試取得合法使用者身分及內部電腦相關資料，如帳號及密碼等。
4. 電子郵件警覺性測試：一年2次針對本部及所屬機關所有同仁進行電子郵件警覺性測試演練，透過寄送各種誘騙而無傷害之電子郵件，誘使本部同仁開啟信件、點選附檔或連結，並分析本部同仁點選各類誘騙信件的比率，以瞭解同仁對電子郵件社交工程、網路釣魚等攻擊行為之安全意識的落實狀況與防護能力。
5. **導入資訊安全管理制度（ISMS）**

除採行各式資安防護措施，本部亦透過導入資訊安全管理制度（ISMS），從管理及制度面著手，建立資訊作業標準流程，及PDCA（Plan-Do-Check-Action）不斷滾動修正，讓資安防護更上層樓。

1. 資訊安全（ISMS）目標
2. 強化網路安全，防止日益變化的內外部的攻擊、竄改及竊取，避免造成機密性、完整性及可用性的資安危害。
3. 建立ISMS制度，並通過第三方驗證。
4. 建立同仁資訊安全觀念與能力，落實資安保護。
5. 資訊安全（ISMS）策略
6. 建置確實的資訊資產實體隔離及權限控管機制，落實Bell–LaPadula Model。
7. 強化資安事件/事故管理，提高資安防禦與管理能力。
8. 提升系統及服務可用性，避免系統非預期中斷。
9. 強化軟體開發流程。
10. 加強查核委外廠商資料管理及遠端維護方式。
11. 導入ISMS、SMS及PIMS制度。
12. 提升人員資訊安全觀念及能力（含證照）。
13. 導入期程與驗證範圍

104年底完成資訊系統分級、資訊資產盤點及風險評鑑作業，105年6月8日訂頒資訊安全管理系統四階文件，正式導入ISMS作業。驗證範圍則先以本部5大核心資訊系統（公文系統、文物典藏系統、獎補助系統、EIP整合入口網、行動辦公整合服務網）為主，並包含主機所在之共構機房（新莊機房、國光機房），即以本部資訊處管轄為主，再逐漸推廣導入至業務單位。

1. 內外部稽核作業

內部稽核由資誠聯合會計師事務所於6月24日至7月13日辦理，發現21個次要缺失、15個觀察事項、2個改善機會，缺失均於第三方驗證外部稽核前改善完成；外部稽核由SGS於8月15至16日辦理，發現2個次要缺失、7個觀察事項，通過第三方驗證可取得證書。

1. 導入成效
2. 藉由利害關係人內外部議題分析，瞭解使用者需求與期待。
3. 落實資訊資產盤點及風險評鑑，確認高風險資訊資產標的及六大風險。
4. 強化高風險資訊資產之各項資安防禦措施，俾達服務安全性、完整性、可用性及法規遵循性。
5. 落實機敏文書實體隔離機制。
6. 高風險主機採本機登入，不得遠端連線操作。
7. 核心資訊系統BCP演練。
8. 訂定ISMS四階文件，管理制度化。
9. 權限盤點確認存取控制權限。
10. 透過變更申請確認變更可行性及可能發生之風險。
11. **未來展望**

即使本部採行眾多改善資訊環境及資安防護措施，另已導入ISMS增進管理制度，仍難以確保資安完全防護，就如同坊間所說，資安沒有做完的一天，惟有戰戰兢兢，精益求精，才能與時俱進，擁有充足資安防護能量。

1. 落實與推廣ISMS制度，及再精進資訊專業能力

週期辦理教育訓練，推廣ISMS制度，讓資訊相關人員瞭解資安政策及目標，並遵守資訊作業管理程序。另由於資訊科技日新月異，唯有不斷充實追求資訊新知，方能擁有跟得上時代之資安防護技術，因應不斷被發現資安漏洞。

1. 定期辦理內稽作業，確認資安管理作業落實度

透過辦理稽核，檢核同仁對資通訊安全認知及尊重法治觀念，健全本部資通訊安全環境，避免人為疏失、蓄意破壞或機敏資料外洩等情事發生，並提供同仁改善之建議參考，作為持續滾動修正之依據。

1. 擴大ISMS導入範圍

由於目前導入範圍以本部資訊處管轄為主，本部已成立資訊服務及安全暨個人資料管理推動會，將再逐漸推廣導入至業務單位，以本部全單位為目標。

1. 導入PIMS

未來推動個人資料保護管理系統（PIMS）驗證，並納入年度策略、目標及績效管理計畫中之資訊安全策略，另逐年規劃導入各單位。

1. 擴大版本控管機制

目前僅公文系統採自動版本控管機制，其餘資訊系統大多由承辦同仁自行存放於部內雲端，後續將可建立統一管理機制，以針對部內所有系統進行較有效之版本控管。