檔案知識+

文書檔案管理系統資訊安全自我檢查

文書及檔案管理系統（簡稱文檔系統），為政府機關日常業務運作不可或缺的工具，其資訊安全益顯重要。為加強對文檔系統資安防護措施，各機關每年宜透過資訊安全管理系統（ISMS）落實資安自我檢測及內、外部稽核，以減少遭受惡意攻擊之風險，順遂政府業務之運作。

國家發展委員會檔案管理局文書檔案資訊組科長　戴慧明

談到文檔系統安全自我檢查，以一般資安健檢檢測項目及範圍來看，不外乎包含「網路架構檢視」、「有線網路惡意活動檢測」、「使用者端電腦檢測」、「伺服器主機檢測」及「安全設定檢測」等5個類別之11個檢測項目（詳見表1）。以下將介紹其檢測重點及檢測結果之追蹤矯正。

表1 檢測項目與範圍

項次	檢測類別	檢測項目
1	網路架構檢視	網路架構設計邏輯檢視
		網路區域配置檢視
		主機位置配置檢視
2	有線網路惡意活動檢測	封包監聽與分析
		網路設備紀錄檔分析
3	使用者端電腦檢測	使用者電腦惡意程式檢測
		使用者電腦更新檢測
4	伺服器主機檢測	伺服器主機惡意程式檢測
		伺服器主機更新檢測
5	安全設定檢測	AD伺服器群組原則設定
		DB伺服器群安全設定項目

壹、檢測項目

首先，「網路架構檢視」告訴我們系統網路架構（Architecture）的五臟內腑是否一應俱全或網路備援可用性情形、「有線網路惡意活動檢測」即檢測網路封包（Packet），透過封包檢測即可獲知惡意行為、「使用者端電腦檢測」檢測個人電腦（PC）環境設定、「伺服器主機檢測」檢測伺服器（Servers）環境設定，及「安全設定檢測」確認目錄伺服器（AD）及資料庫伺服器之安全設定（Rules）問題，簡稱APPSR檢測，有了檢測結果，就可以瞭解系統資訊安全的全貌。

一、網路架構檢視（Architecture）

針對系統骨幹網路與防火牆設備之架構圖、設定檔、防火牆規則（policy rule）以及訪談資訊進行相關之檢視作業。

針對「網路架構設計邏輯」、「網路區域配置」及「主機位置配置」進行相關安全性檢視作業，並依檢視結果以了解網路架構防護之情形，及了解相關風險所在。

二、有線網路惡意活動檢測（Packet）

針對「封包監聽與分析」及「網路設備紀錄檔分析」進行相關安全性檢測作業，並依檢視結果了解有線網路惡意活動之防護情形。

透過封包監聽與分析檢測即可獲知惡意行為，由核心交換器或對外流量出口端，將流量複製一份到側錄系統進行封包側錄，流量內容包含使用者個人電腦區域（User Farm）、伺服器區域（Server Farm）及DMZ（非戰區）等區域，側錄至少6小時後，將封包取回分析產出報告，並由「網路設備紀錄檔」進行異常連線紀錄分析作業。

三、使用者端電腦檢測（PC）

就「使用者電腦惡意程式或檔案」及「使用者電腦更新」進行相關安全性檢測作業，並依檢視結果提出說明，以瞭解使用者端電腦防護之情形。

（一）使用者電腦惡意程式或檔案檢測

由使用者電腦清單協助經由目錄伺服器（AD）或資產管理系統，派送免安裝之檢測工具到使用者電腦進行檢測，並將檢測結果回傳至管理主機並產出報告。本項檢測將採用木馬後門檢測工具及惡意程式檢測工具，經由3項不同工具比對分析。

（二）使用者電腦更新檢測

如透過微軟視窗系統更新（WSUS）伺服器、防毒伺服器及Adobe更新檢測工具，檢視使用者電腦更新項目是否已更新至最新版本。項目包括：作業系統更新、Office應用程式更新、防毒軟體更新、Adobe Acrobat及Adobe flash player更新。

四、伺服器主機檢測（Servers）

就「伺服器主機惡意程式或檔案」及「伺服器主機更新」進行相關安全性檢測作業，並依檢視結果了解有關使用者端電腦防護之情形。

（一）伺服器主機惡意程式或檔案檢測

使用免安裝工具進行惡意程式檢測，逐一登入伺服器主機清單每部伺服器主機，並針對重點目錄查詢可疑檔案軌跡，彙總系統紀錄Log取回分析產出報告。本項檢測將採用木馬後門檢測工具及惡意程式檢測工具。

（二）伺服器主機更新檢測

可透過微軟視窗系統更新（WSUS）伺服器、防毒伺服器及Adobe更新檢測工具，檢視伺服器主機更新項目是否已更新至最新版本。項目包括：作業系統更新、資料庫版本更新、Office應用程式更新、防毒軟體更新、Adobe Acrobat及Adobe flash player更新。

五、安全設定（Rules）檢測

就「AD伺服器群組原則設定」及「DB伺服器群安全設定項目」進行相關安全性檢測作業。

（一）AD伺服器群組原則設定

就AD伺服器群組原則設定，針對稽核原則、帳戶鎖定原則、密碼原則、螢幕保護原則、AD伺服器安全管理等，進行檢視。

（二）DB伺服器安全設定項目

資料庫伺服器系統除就系統存取，於實際登入資料庫主機，使用資料庫語法（SQL）方式及資料庫系統設定逐一進行安全設定檢視外，每年亦應透過滲透測試及每季例行弱點掃描作業以強化資料庫之資訊安全。前述有關安全設定檢視項目如下：

1. 資料庫存取應依角色具有分權機制。
2. 資料庫存取應具有log紀錄。
3. 資料庫最高權限帳號存取授權，應僅限資料庫管理人員擁有。
4. 資料庫帳戶之密碼需為英數字混合，並不得與帳戶名稱相同，且至少為8碼以上。
5. 資料庫預設帳號與密碼應予以變更或停用。
6. 正式用系統與測試用系統所需使用之資料庫系統，應分別在不同的伺服器主機下執行。

貳、檢測結果矯正追蹤

就像例行的健康檢查一樣（圖1），需針對上述每一類別的檢測結果產生報告，依據檢測報告，就可以瞭解系統資訊安全的現況及風險問題所在，緊接著即針對逐項問題設法處理解決。首先就原因逐一分析，提出矯正預防措施，再進行分工及確認完成日期，執行完成後並應進行複查，以確保問題的根本解決。

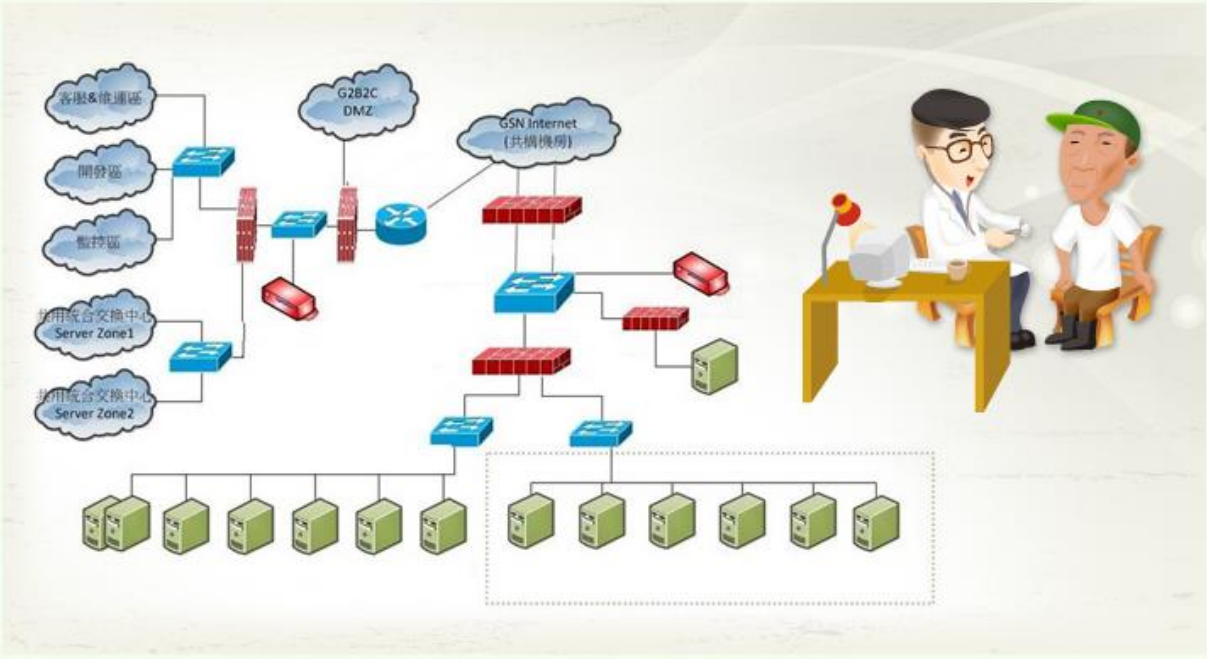

圖1：系統安全自我檢測圖

參、結語

為降低文檔系統資安發生的風險，透過年度資訊安全管理系統（ISMS）定期執行內、外部稽核之自我查檢，以上述程序進行抽測，就不足處提出立即改善之具體建議措施，透過系統設定、架構調整或程式移除等方式即時解決問題。如為短期無法解決者，則列入中、長期改善作為，視預算、設備到位情形進行改善。透過上述例行的資訊安全自我檢測，以提早發現問題，減少系統遭受惡意攻擊之風險，並強化系統體質，確保政府各項政策推動及日常業務正常運作。