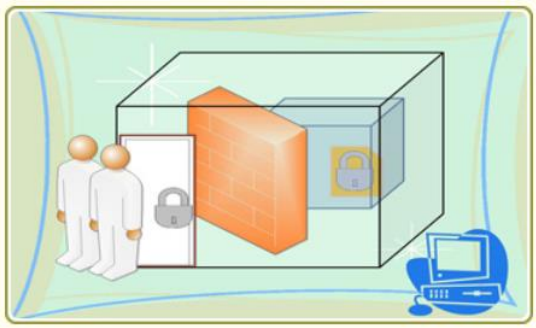
檔案知識+

多層防護資訊系統更安全



面對複雜且瞬息萬變的資訊科技時代，資訊系統由單一性的防毒軟體或防火牆等機制，已不足建立安全的資訊環境，惟有仰仗全方位且多層次架構的聯防機制，以降低風險。

國家發展委員會檔案管理局文書檔案資訊組 分析師 林其範

壹、前言

陸軍作戰時，布署了龍齒(圖1)雖可使裝甲車難以前進，但卻無法阻擋步兵，此時再增加鐵絲網阻礙，便可達到互補性之功效，這正是多層式防禦(Defense in Depth)的基本概念。

圖1 龍齒(註1)

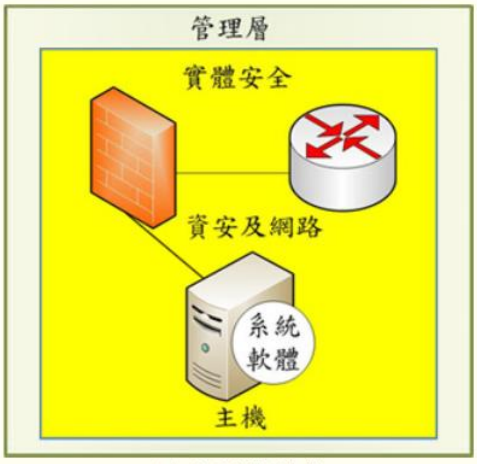


圖2 多層次管理架構

類似地，資訊系統採用管理及實體安全等多層式防禦(如圖2)，經由多面向的管控措施，可增加防護效果。例如主機雖有帳號權限管控，惟作業系統為增加管理彈性，都會保留一個最大權限之管理者帳號，當其密碼忘記或失落時，可至實體伺服器本機，透過開機片重開機後重設密碼。若實體環境管理發生缺失，造成未經授權人員進入電腦機房，取得前述帳號、密碼，將使主機系統權限控管失效。另在電子郵件安全議題方面，目前的技術已可過濾垃圾郵件及病毒郵件，但推動公務電子信箱僅限公務使用，在技術上仍有其判別的困難處，惟有透過宣導、教育訓練及相關管理規範等措施，以求成效。總言之，建立交叉防護網，達成相輔相成的作用，將可以降低威脅與風險。接下來就管理及實體安全層面，為您介紹相關的防護概念。

貳、管理層面

管理層面主要是制定資訊安全政策及規範資訊安全活動，以管理活動進行規劃(Plan)、執行(Do)、查核(Check)、行動(Action)，周而復始，持續精進(如圖3)，甚至進行相關資安管理系統驗證作業， 以確保管理系統有效性。

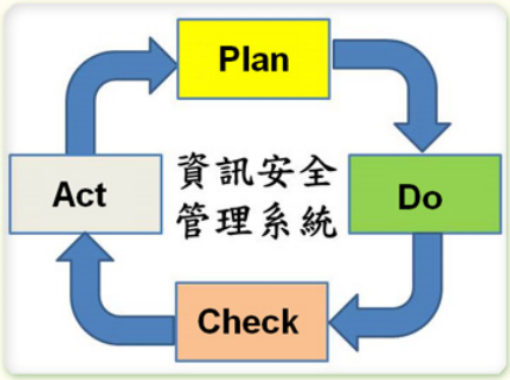


圖3 PDCA示意圖

以ISO 27001:2013國際資訊安全標準驗證為例，每年至少須進行一次內、外部稽核作業與資訊資產盤點，再就盤點結果進行相對風險評鑑，依據風險評鑑結果作為後續改善措施，並定期辦理資安健診、弱點掃描、滲透測試、弱點修補、帳號清查與防火牆規則審查等作業。

此外，平時管控作業也非常重要，例如須取得授權才可進行資安設定變更作業，啟用資安設備與系統主機日誌功能及專人檢視日誌報表；導入資安監控管理平台(Security Operation Center ， SOC)機制，發揮即時監控與預警效果。又鑒於網路釣魚及進階持續性滲透攻擊(Advanced Persistent Threat ，APT)之威脅日益嚴重，須定期辦理同仁資訊安全教育訓練，加強資安意識。

參、實體設備層面

實體設備層面之防護主要分為實體安全、資安與網路設備、主機及系統軟體防護，略述如下：

一、 實體安全：主要為組織環境與機房實體環境之安全，包含門禁管制、設備出入管理、人員安全、消防設備等實體面的措施。

二、 資安與網路設備：隨著網路威脅事件層出不窮，攻擊方法也日益嚴峻，傳統網路架構僅架設防火牆防護，已明顯不足，取而代之的是各式各樣資訊安全設備的交互防護，惟有以各種不同功能資安設備多層次布署，才能達到最佳保護狀態。

依圖4網路架構之防護精神，萬一外層防火牆被入侵成功，內層防火牆還可提供另一道防護，而藉由多種防毒軟體交叉掃描，可提高發現病毒機率，當然也增加誤判機率。以下就多層資訊安全防護設備中，為您介紹較為普及的設備：

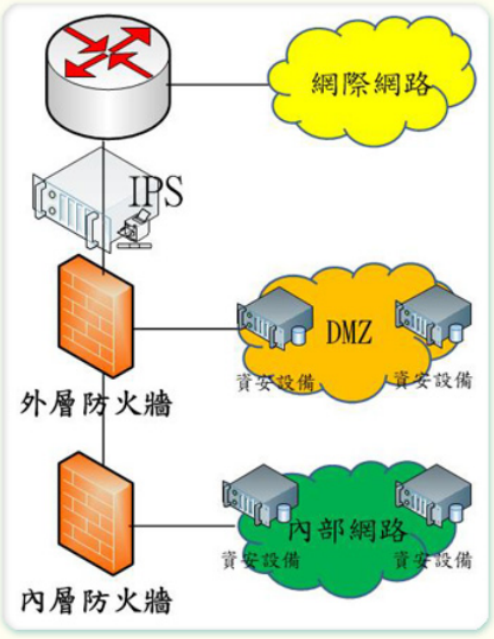


圖4 網路架構多層次防護

（一） **防火牆(Firewall)**：
依照特定規則，通常以來源與目的端的網路位址(IP)及埠號(Port)決定允許或拒絕資料傳輸，可降低異常連線情形，並可將網段分割成數個，加強網段間安全性。

（二） **入侵防禦系統(Intrusion Prevention System,IPS)**：
可與防火牆一起搭配，輔助防火牆功能，主要分析網路行為，能夠及時中斷與隔離異常連線。

（三） **網站應用程式防火牆(Web Application Firewall,WAF)**：
網站為現今使用最頻繁網路服務之一，係針對系統對於網站防護不足所延伸開發之產品，就網站常面臨到編碼攻擊、SQL隱碼注入(SQL Injection)、跨網站指令碼攻擊(Cross site Script，XSS)等等，給予更深入的防護措施。

（四） **日誌收集伺服器(Log Server)**：
收集設備產生的日誌，統一存放，可保護各系統日誌資料，又可交叉比對及產出日誌報表，以利資安審核，此外可與SOC監控機制結合，進行事件監控與通報。

（五） **垃圾郵件過濾器(AntiSpam)**：
使用在電子郵件服務，可過濾垃圾郵件、病毒信、廣告信，降低組織風險與增加工作效率。

三、 主機及系統軟體防護：安裝防毒軟體、定期修補漏洞或安全性更新、開啟主機防火牆(如Linux iptables)、使用虛擬化技術、沙盒(Sandbox)、帳號權限設定等等。

肆、結論

資訊安全已不僅是資訊單位責任，因其活動範圍為全組織，落實同「資訊安全、人人有責」，需大家一同參與精進，儘可能將所面臨風險降至最低，才能提供安全又優質的服務。

註釋：

註1. 維基百科，龍齒。<https://zh.wikipedia.org/wiki/%E9%BE%8D%E9%BD%92>(民國105年3月14日檢索)。

本文檔案下載：知識No110.pdf
本頁最後更新日期：105.8.16

110期專區	資訊專區	會員專區	下載專區
檔案瑰寶	徵稿訊息	訂閱電子報	簡報及桌布下載
檔案知識+	各期電子報查詢	取消電子報	精華版下載
檔案搶先報	回最新一期首頁		
回本期首頁			

歡迎您對檔案樂活情報提出寶貴建議，請聯絡：alohas@archives.gov.tw

列印 上一頁 回頂端

24220新北市新莊區中平路439號(北棟)9樓 總機：(02)8995-3700 傳真：(02)8995-6469