本校資安措施

成大計網中心
楊峻榮
2004/5/20

資訊安全Life-cycle

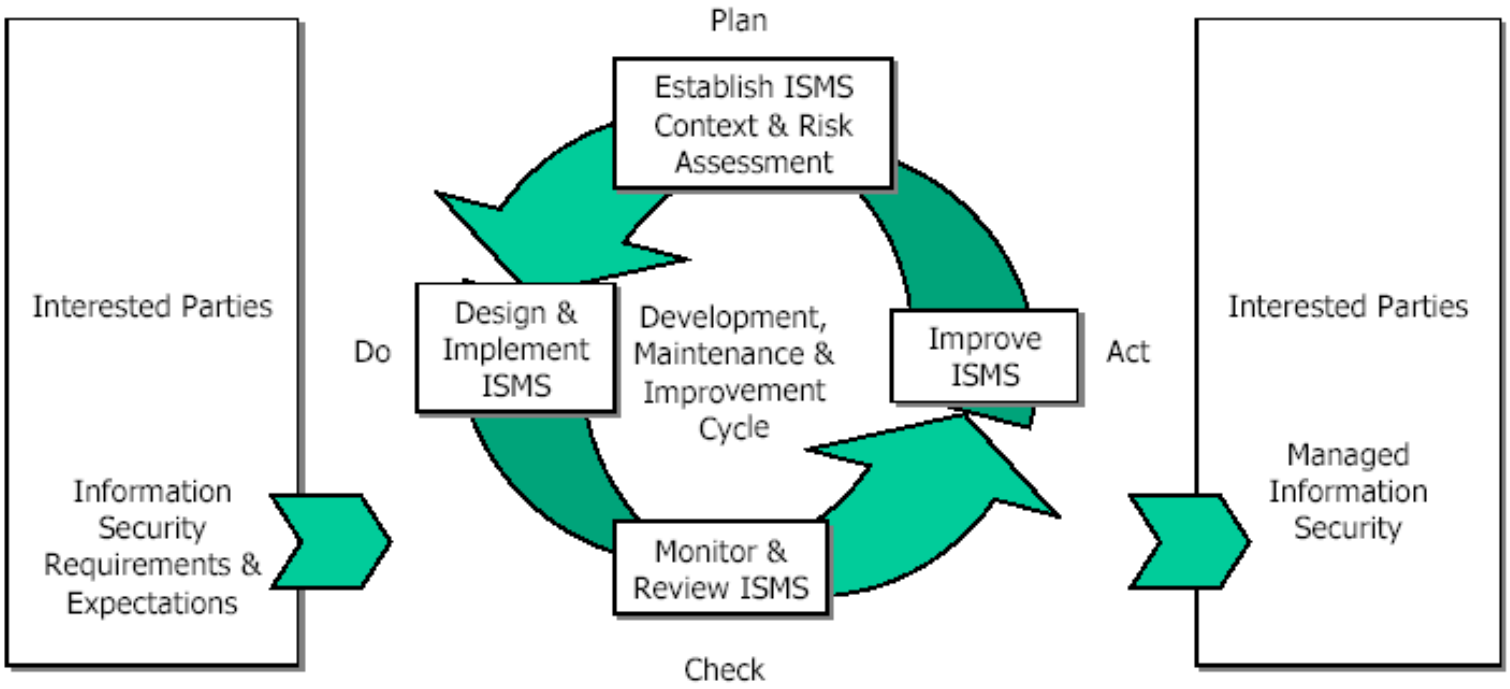


Figure 1 PDCA Process Model

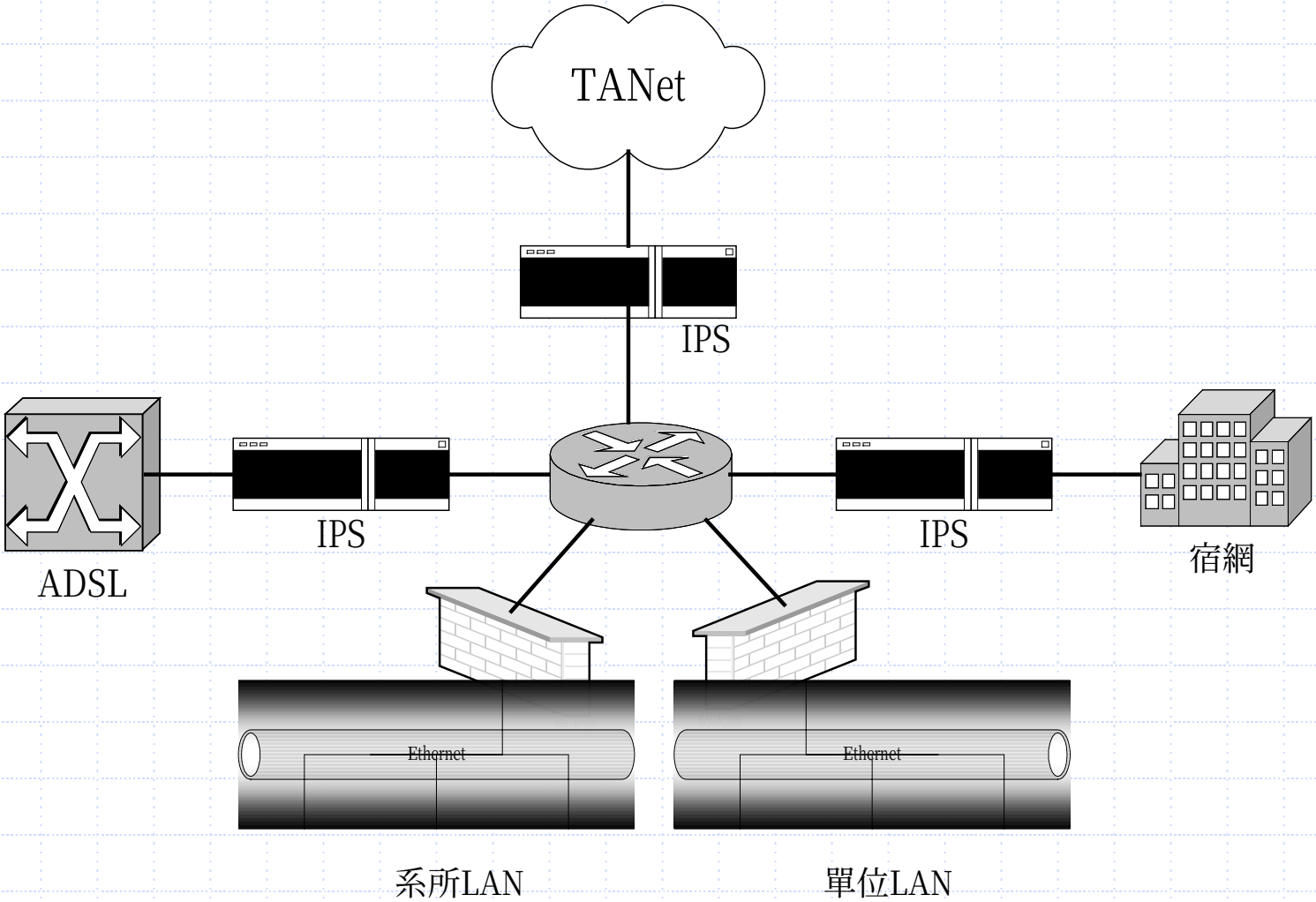
資訊安全機制之建立

- 以 Information Security Management System 為規範(BS7799導入)：Top-Down，先由政策定義、定義資產、風險評估、選用控制措施.....。著重於整個組織制度及管理。
- 先由控制措施著手：Bottom-Up，先由個別系統之控制措施著手。著重於技術層面。
- 雙管齊下:考慮到現階段之環境與急迫性之考量，在管理及技術層面能以本校之組織文化及環境為背景，建立起本校之資訊安全系統。
- 考量本環境之上層規範，不能相抵觸，例如台灣學術網路使用規範。

本校資安措施考量之範圍別

- 行政單位
- 系所
- 研發單位
- 宿網
- ADSL(Dial-up)
- 人員(教職生)

本校網路安全設備配置規劃圖



本校資安措施(決策層)

- 政策發佈
- 提供資源
- 權限支援

資安投資是較難表徵投資績效，所以有賴決策層(本校高層及各單位主管)充實資訊安全概念。

本校資安措施(計網中心)

- 防毒機制
- IP控管及列管
- 弱點掃描
- 資安檢視
- 事件通報及處理
- 教育訓練
- 訊息通告與資安網頁

防毒機制

- 提供PC及Server與閘道型(InterScan)之防毒軟體，在校內均可自由安裝使用。
- 與趨勢科技(Trend)簽訂全校授權之防毒軟體(不含PC-cillin)
- Windows 95/98/me/xp/NT workstation/2000 professional 等非server版本直接上網安裝officescan client : http://140.116.6.10/officescan/clientinstall
- 各單位系所也可自行安裝officescan server 以管控單位內之PC 。
- 其餘至http://www.cc.ncku.edu.tw/security下載安裝。
- 本中心之mail server也裝設防毒軟體。

IP控管及列管

- 計網中心與單位系所屬階層式控管。
- 各單位針對本中心所分配之實體IP及各單位建立之虛擬IP須詳實列管。
- IP控管乃是非列管之IP限制其使用，其技術有IP與MAC之binding或是以帳號管制。
- IP控管可應用防火牆之附屬功能。
- 超流量或不當使用之IP管制。

弱點掃描

- 定時或不定時掃瞄各IP，並給予報告及建議。
- 各單位針對有疑慮之主機及伺服器也可隨時委請本中心掃瞄。
- 與檢視(稽核)機制配合,做為重點檢視項目之參考依據
- 一個弱點(足以造成威脅)可能是由幾個hole組合產生。
- 可能會因應用軟體服務之需要，或版本之關係，而會有誤判之情況(是否形成弱點)，故其報告應視為改善之參考依據，但也不能視而不見。

資安檢視

- 以改善資訊安全之強度為出發點。
- 以定時並事先通知受檢單位實施。
- 範圍選定以上次有重大缺失項目及事先弱點掃瞄結果為依據。
- 檢視結果供單位主管做為改善之依據。
- 預計六月中旬開始實施。

資安檢視(項目)

- IP列管：針對IP登記列表，包含負責人姓名、主機所在位置、作業系統、用途。
- IP管制：針對非IP列管表中之主機，限制其使用。
- 網路存取控管（防火牆）：針對外部網路對單位內之存取控制
- 主機設備是否有專責負責人。
- 主機是否不需密碼之登入。
- 主機系統是否有不明之帳號。
- 檔案分享之控制機制：是否有檔案分享之存取控制。
- 螢幕淨空（screen lock有密碼保護）。
- 是否提供非必要之Service 。
- 各重要主機或Server之備份機制。
- 各主機或Server之弱點及漏洞修補（patch） 。
- 防毒軟體之有效性：是否裝設防毒軟體及是否及時更新病毒碼。

事件通報及處理

- 依據行政院資通安全會報之規定,資安事件需向該處通報處理。
- 本校之資安事件由本中心通報，故各單位之資安事件需向本中心通報，以mail或電話方式皆可。
- 資安事件之處理可委由本中心之負責人協助，但其原則如下:
  a.經由本中心網管查覺影響正常流量。
  b.經由單位網管或資安負責人認定重大事件或無法處理。
  C.系統負責人已處理，尚無法解決問題。
  d.研判為人為模式之入侵行為。
- 負責人:楊峻榮61016，0919-110455（緊急狀況）
  yang@mail.ncku.edu.tw

教育訓練

- 範圍針對各種資訊安全之技術及概念。
- 對象針對一般使用者，系統管理者及資安網管負責人，單位主管。
- 每半年最少一次。
- 可提出課程需求。

訊息通告與資安網頁

http://www.cc.ncku.edu.tw/security

各單位之資安措施與責任

- IP控管與列管措施。
- 建置及管理網路存取控管機制。
- Server詳細列管(所開啟之Service) 。
- 連絡體系(資安負責人及單位內Server負責人) 。
- 定時檢視單位內設備狀況(設備流量或各主機之狀況)。
- 資安事件之初期判斷及處理。

IP控管與列管

IP控管之目地：禁止單位內非法IP之使用

- 直接由入口設備設定IP及MAC Table
- 另加裝控制閘道器
- 加以其它管理界面
- 可由閘道式防火牆之附屬功能實施

IP列管之目地：掌握IP之位置與資訊

- 通常與IP控管配合
- 紙本或電子檔
- 資訊儘量齊全

防火牆機制

- 單位內資源存取控制，包含範圍與服務種類及程度控制。
- 由單位內之網路服務政策來規劃存取控制措施。
- 建立一個外部與內部網路間的管制界面，或是單位內各主機（伺服器or PC）各自建立存取管制界面。
- 所採用之措施不一定得架設實體防火牆閘道。
- 雖非一定得架設實體防火牆設備，但得考量單位存取控制管理的效率性。

建置防火牆考量點

- 經濟效益(風險及成本)
- 位置及管制政策
- 網路型或主機型，硬體型或軟體型
- 效能（Throughput，session數量）
- 功能（阻絕程度，管理界面，附加功能：anti-virus,IPS）
- 技術支援
- 可靠性
- 若含anti-virus，IPS需考量其病毒碼及特徵資料庫之更新成本

防火牆功能

- 隔絕或位址轉換 (Network Address Translation NAT)
- 封包過濾(IP, PORT)
- 應用層代理(Application Porxy)
- 狀態檢驗
- 虛擬私人網路(Virtual Private Network VPN)
- 即時監控及警報
- 附加Intrusion prevention 功能