行政院及所屬各機關出國報告
（出國類別：實習）

『可靠性影音串流服務系統』之系統安全性建置及規劃出國報告

服務機關：中華電信研究所
出國人　職　稱：助理研究員
　　姓　名：仝興倫

出國地點：美國
出國期間：91年11月17日至29日
報告期間：92年1月24日

系統識別號:C09200750

公 務 出 國 報 告 提 要

頁數: 18　含附件: 否

報告名稱:

實習『可靠性影音串流服務系統』之系統安全性建置及規劃

主辦機關:

中華電信研究所

聯絡人／電話:

楊學文／03-4244218

出國人員:

仝興倫　中華電信研究所　網路及多媒體應用技術研究室　助理研究員

出國類別: 實習

出國地區: 美國

出國期間: 民國 91 年 11 月 17 日 -民國 91 年 11 月 29 日

報告日期: 民國 91 年 01 月 24 日

分類號/目: H6／電信　／

關鍵詞: 可靠性,影音串流,安全性

內容摘要: 在這個網路普及的世代，電腦已經是不可或缺的電子設備之一，這也使得電腦遭遇到駭客入侵的機率急速地成長。同時，更精緻的攻擊手法，更快速的傳播方式及多變的型態幾乎已是現行駭客必備的能力了。本報告藉由規劃建立安全之網路環境及適當的系統安全調較，以期降低駭客對企業所造成的威脅及影響。此外期望透過防治及管理的機制，以期能有效達成阻絕電腦駭客的目的。 本報告將分別藉由主機系統安全、網路系統安全及整體網路架構來介紹如何建立一完整之安全系統。以期提供各相關系統建制及規劃之參考，爲建立中華電信相關資訊網路系統盡一份心力。

本文電子檔已上傳至出國報告資訊網

摘要

在這個網路普及的世代，電腦已經是不可或缺的電子設備之一，這也使得電腦遭遇到駭客入侵的機率急速地成長。同時，更精緻的攻擊手法，更快速的傳播方式及多變的型態幾乎已是現行駭客必備的能力了。本報告藉由規劃建立安全之網路環境及適當的系統安全調較，以期降低駭客對企業所造成的威脅及影響。此外期望透過防治及管理的機制，以期能有效達成阻絕電腦駭客的目的。

本報告將分別藉由主機系統安全、網路系統安全及整體網路架構來介紹如何建立一完整之安全系統。以期提供各相關系統建制及規劃之參考，為建立中華電信相關資訊網路系統盡一份心力。

目　　錄

1.　目的.....1

2.　過程.....2

2.1.　行程概要.....2

2.2.　受訓內容.....3

2.2.1.　主機系統安全.....4

2.2.2.　網路系統安全.....8

2.2.3.　安全檢測及稽核.....12

3.　心得.....16

4.　建議.....17

1. 目的

職此次奉派出國研習『可靠性影音串流服務系統』之系統安全性建置及規劃，出國時間自民國九十一年十一月十七日至民國九十一年十一月二十九日，含行程共十三日。其中十一月十八日至十一月二十七日於美國接受系統安全性建置及規劃之訓練。

國外對於網路及系統安全建設早已行之多年，因為不良的安全設定及系統建置，當真正遭遇到所謂駭客或是病毒入侵時，輕則網路擁塞不通造成使用者的不便，重則資料遺失或是被竊取，這對一個企業可說是損失相當的嚴重。國內今年也因為Code Red及Nimda病毒造成不少的損失，也喚起大家對於網路及系統安全的重視。但是隱藏在這背後還有更大的一群駭客是無聲無息的隨時可能正在竊取您公司的機密文件及資料，因為數位化帶來了便利同時也帶來了危機，如何同時兼顧兩者的優點就是資訊安全的重要課題。今年被定義為資訊安全年，也就是說，系統安全服務之提供勢在必行，因此中華電信公司需及早進行規劃及相關作業，以維護未來中華電信公司企業安全及相關服務建置。

安全之議題包含許多範圍，其中資料加密、安全認證也都是重要之課題，本行主要是實習系統及網路面相關解決方案，期望建立更可靠之網路及主機系統提供企業內部使用，並防止駭客及病毒之入侵。當然隨者網路的日益發展，新的駭客技巧及病毒也會更加的日新月益。惟有不斷的學習及精進相關之技術，才能為網路及系統安全提供最終解決方案。

本份報告分為：1.目的、2.過程、3.心得、4.建議。

2. 過程

2.1. 行程概要

整個行程從11月17日出發，至11月29日返國，共計13天。其受訓過程如下表：

日期	主題
11/17	起程
11/18~11/22	Sun system fault analysis workshop for system, network and security
11/23~11/24	資料整理
11/25~11/27	Internet and Intranet network security concept, planning and technology
11/28~11/29	回程

2.2. 受訓內容

建立系統及網路安全是目前世界的趨勢，如何建立及調整現有資訊系統並仍能保有原系統之正常運作是當前重要議題。依據安全範圍之不同，此報告將從主機系統、網路設定及網路安全規劃等方面來分別說明。

首先先從主機系統安全做起，其中包含主機的安全設定、root 的安全設定、網路服務、帳號與檔案管理及安全檢測。其次為網路安全設定，包含網路設備實體配置及相關安全設定的問題。最後提供相關整體網路建置及規劃的建議，以期建立一個整體安全的網路環境。網路及系統安全在目前網路環境中已被大眾所接受，並更加的重視。因此建立安全之網路環境不僅為中華電信公司本身提供一穩定安全的網路環境，並可提供 IDC 機房如 Co-Location 或是 Hosting 更多樣化的加值服務以滿足客戶的需求。

本報告即是實習在現有網路架構下，建立一較安全之網路環境，所用的方式包含系統主機安全校正、網路設備安全設定及整體規劃。期望在如此的規劃及設計下提供企業及使用者更安心的操作環境。

2.2.1. 主機系統安全

主機系統安全一般需滿足下列四項要件：

- 機密性(Confidentiality)
  防止資訊洩漏給未經授權者。
- 存取控制(Access Control)
  授權策略，系統需先對使用者作授權驗證，以確認其是否為合法授權使用者，以防止未經授權者存取系統資源。
- 可用性(Availability)
  持續維護系統所提供服務之正常運作。
- 稽核(Audit)
  藉由稽核記錄可追蹤非法使用者，提供回復方案，並能偵測可疑活動防止其侵入系統。

以下將針對上述四點提供相關安全上之設定及方法。

2.2.1.1 定時更新修正檔

定期至 SunOS 的網站去檢查修正檔，網站上會提供建議修正的安全修正檔案，可由下列網址取得相關資訊http://sunsolve.sun.com/。同時檢查系統已經安裝的修正檔案列表 showrev –p。

2.2.1.2 本機的安全設定

設定EEPROM安全模式

- 完全模式：最高安全等級，重新開機時需要輸入密碼才會執行開機程序，若需要自動重新開機的伺服器不適合採用此模式。

  eeprom security-mode=full

- 命令模式：在OpenBoot PROM狀態下無法修改EEPROM設定

  eeprom security-mode=command

2.2.1.3 root的安全設定

設定 root 只能在本機上登錄

- 確定 /etc/default/system 檔案內容，CONSOLE=/dev/console 前面沒有

加上『＃』符號。

設定 root 密碼

- 最少六個字元，最多八個字元。
- 絕不能使用英文字典中可以查到的字。
- 最好加入非英文字母的標點符號。

root 設定檔權限

- 確定 root 個人設定檔不被其他使用者讀取、執行或是更動。chmod 600 .cshrc .profile .login .forward

2.2.1.4 網路服務

建立/etc/init.d/nddconfig檔案，並且鏈結到/etc/rc2.d/S70nddconfig，將下列的內容加到"/etc/init.d/nddconfig"檔中

```
#!/bin/sh
#
# /etc/init.d/nddconfig

# Fix for broadcast ping bug
/usr/sbin/ndd -set /dev/ip ip_respond_to_echo_broadcast 0

# Block directed broadcast packets
/usr/sbin/ndd -set /dev/ip ip_forward_directed_broadcasts 0

# Prevent spoofing
/usr/sbin/ndd -set /dev/ip ip_strict_dst_multihoming 1
/usr/sbin/ndd -set /dev/ip ip_ignore_redirect 1

# No IP forwarding
/usr/sbin/ndd -set /dev/ip ip_forwarding 0

# Drop source routed packets
/usr/sbin/ndd -set /dev/ip ip_forward_src_routed 0
```

 # Shorten ARP expiration to one minute to minimize ARP spoofing/hijacking

 # [Source: Titan adjust-arp-timers module]

/usr/sbin/ndd -set /dev/ip ip_ire_flush_interval 60000

/usr/sbin/ndd -set /dev/arp arp_cleanup_interval 60

把/etc/inet/inetd.conf 檔案裡面所有不必要的服務做上標記或者是直接移除，其中不必要的服務包含了以下各項。

shell	login	exec
comsat	talk	uucp
tftp	finger	sysstat
netstat	time	echo
discard	daytime	chargen
rquotad	sprayd	walld
rexd	rpc.ttdbserverd	dtspc
ufsd	printer	rpc.cmsd

2.2.1.5 帳號管理

將不必要的帳號移除或者是鎖住(sys,ucp,nuucp,listen)。

- 在/etc/shadow檔中將它們的密碼欄位中填入"NP"。
- 將帳號從/etc/passwd和/etc/shadow中刪除
- 將帳號從/etc/passwd和/etc/shadow中鎖住
- 在/etc/passwd和/etc/shadow檔案中，將使用的shell更改掉

2.2.1.6 遠端執行權限管理

強迫遠端執行命令時需通過認證的程序，其方法為將列出在/etc/pam.conf 檔中所有『r』開頭的列標註起來，並且變更 rsh 列為讀取的權限。

更安全的作法，完全禁止遠端執行的動作。

- 移除系統設定檔案/etc/host.equiv 以及每個帳號下的/.rhosts 檔案。
- 編輯/etc/inetd.conf 檔案，將所有『r』開頭的相關命令移除。
- 重新啟動 inetd 讀取新的設定內容。

2.2.1.7 檔案權限管理

檢查/etc/vfstab檔案內容，以下幾個項目需設定為 nosuid,ro。

- /，/var，/usr。

清查所有setuid/setgid的檔案，整理成清查列表之後，妥善儲存便於週期性檢查比對是否被更動。

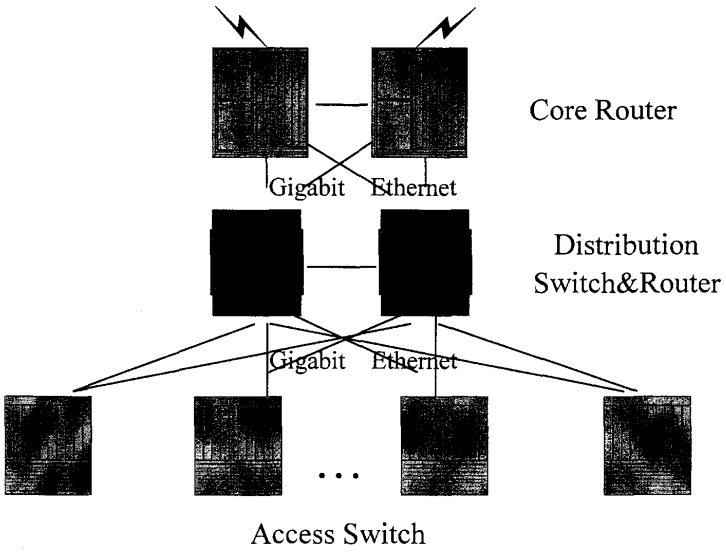
啟動預設的umask，以免其中包含未設限的存取權。將umask 027加入下列的檔案之中。

/etc/.login	/etc/profile	/etc/skel/local.profile
/etc/skel/local.cshrc	/etc/skel/local.login	

在/etc目錄下的系統設定檔是不需要給一般使用者更動權限的。執行chmod –R g-w /etc指令移除群組對檔案編輯的權限。

2.2.2. 網路系統安全

一般網路架構如下圖所示，因此各層級之網路設備需有相對應之安全設定及策略，以應付不同之需求。



網路主層

- QoS 策略制定。
- 傳輸速度要快，應此不會訂定其他存取控制。

網路分散層

- 網路路由策略訂定
- 網路服務策略制定

網路存取層

- 介面埠安全管控
- 安全密碼之制定

以下將針對各項細節作詳細之說明。

2.2.2.1 網路設備管理

實體網路設備管理。

- 適當的實體網路環境。

- 實體網路的直接管控限制。
- 網路系統的安全存取。
- OSI不同層級的管控及策略制定。

密碼及遠端連接控管。

- Out-of-band及In-band密碼控制。
- 不同層級之密碼控制。
- 遠端連結如Vty及Http連線密碼控制。

網路存取層控制。

- 通訊埠之安全控制。

  限制可連接此交換器之機器之MAC address數量。

  限制連接此交換器port之機器MAC address。
- 設定VLAN區隔不同網段。

  避免Broadcast現象，影響網路流量。

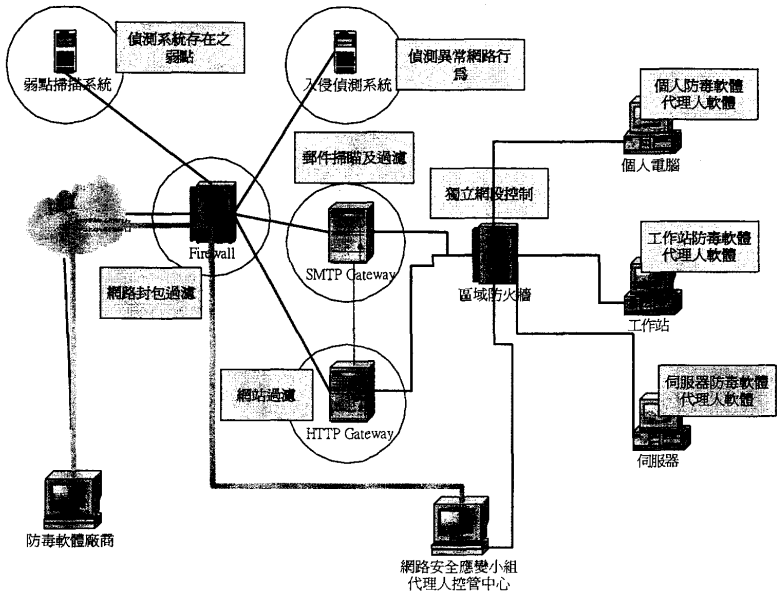
  避免病毒及相關駭客的攻擊及影響範圍。

網路分散層控制。

- 定義可存取之條件(Access Lists)。
- 針對網路設備介面(Interface)定義可進出之IP address及通訊埠(port)，以限制網路存取功能。
- 針對網路路由(Routing)定義可路由的條件，限制不同網段之間的路由情況，以限制不當之路由影響網路安全。

2.2.2.2 網路及系統安全防衛

當然除了網路相關設備本身設定上考慮到安全的條件，在整體網路架構下也可以利用其他輔助的相關安全防護措施。下圖顯示網路整體所外加的設備，以提高整體安全性，並於後針對各項作功能說明。



架設防火牆。

- 管制封包流量。
- 過濾封包。
- 網路位址轉換。
- 身分確認。
- 加密。

設置入侵偵測系統。

- 監督電腦系統，搜尋入侵者痕跡或使用者濫用系統的工具。
- 監測網路活動即時分析資料並在發現可疑入侵行為時馬上發出警告。
- 儲存不正常之行為模式資料並透過許多不同格式的表單、圖形進行檢查分析。

設置弱點評估系統。

- 模擬駭客入侵方式。

- 協助調查人員判斷入侵者所採取的攻擊方式。
- 針對系統進行徹底的檢查找出暴露在外的安全弱點。

安裝防毒軟體系統。

- 資訊系統作業環境。
- 網路環境之防毒機制含訊息(郵件)伺服器(Messaging Server)、檔案伺服器(File Server)、終端電腦(Client Computer)、防毒閘道(Antivirus Gateway) 。
- 網頁病毒的掃描。

資料加密。

確切系統維護及管理。

- 系統管理人員
  - 定期更換密碼檔。
  - 按照安全政策之規定設定系統。
  - 日常管理維護系統之運作。
  - 觀察檢視系統操作狀況。
  - 發覺和監督違反安全規範之使用者行為，並按規定步驟處置。
- 安全稽核人員。
  - 確認系統之安全設定符合安全政策之規定。
  - 督導系統管理人員按照規定執行工作。

2.2.3. 安全檢測及稽核

由於一般資訊人員對於系統及網路安全的知識並不是很完善，因此惟有透過整體系統網路安全檢查及稽核，才能進而強化系統整體安全機制，並降低安全威脅的風險。以下提供幾點相關查核之要點。

2.2.3.1 作業系統安全檢查要點

帳戶管理

- 遠端安全通道登入主機。
- 主機登入後 idle 達一小時候自動登出。
- 設定螢幕保護程式 5 分鐘。
- 帳號單一功能化。
- 更改管理者的預設帳號。
- 移除不必要的系統預設帳戶。
- 只允許管理者閱讀及更改密碼檔。
- 密碼必須達八位數以上，至少要包含二個以上的特殊字元。
- 使用者的資源(Process 數量、硬碟使用量)必須限制。
- 密碼必須經常更換。
- 密碼檔必須加密。
- 限制登入時間。

稽核

- 啟動稽核程式。
- 對密碼檔及系統設定檔案的更動做稽核。
- 啟動遠端稽核紀錄服務。
- 稽核紀錄檔必須做權限控制。

網路服務

- 移除不必要的網路服務。
- 設定網路服務的帳號並限制其權限，避免用管理帳戶啟動網路服務。
- 限制網路服務的使用資源。
- 關閉系統預設的網路服務

軟體安裝

- 所安裝之軟體必須經過安全檢查無問題後使可安裝。
- 軟體安裝非必要時，不得以管理帳戶安裝。
- 與系統所提供的服務無關之軟體不可安裝。
- 安裝軟體時必須更新至最新的修補版本。

2.2.3.2 服務安全檢查要點

相關服務軟體必須更新使用最新穩定版本之軟體及安裝相關修正檔，同時關閉遠端管理功能或採用SSH、SSL及廠商proprietary等通訊協定，SSL長度需大於128-bit。

WWW 服務

- 管理連線需設定 Timeout 時間。
- 設定 IP ACL 限制管理人員來源。
- 設定 daemon 使用系統中最低權限的帳號身份提供服務。
- 除需要執行 Script 之目錄外，其餘所有目錄禁止進行寫入及執行動作。
- 關閉目錄瀏覽功能。
- 禁止使用.htaccess 方式進行認證。
- 刪除所有不必要之範例目錄及相關檔案。
- 相關目錄及檔案設定為唯讀權限。
- 啟動 SSL（128 bits 以上）進行資料加密。
- 啟動 LOG 機制記錄管理訊息。
- 避免使用 Alias、Script Alias 相關設定。

SMTP 服務

- 管理連線需設定 Timeout 時間。
- 設定 IP ACL 限制管理人員來源。
- 設定所有 return 給郵件伺服器管理員之信件均直接丟棄。
- 嚴禁任意使用 alias 功能。
- 設定 relay-domain 檢查機制。
- 啟動外寄郵件伺服器使用者驗證機制。
- 啟動安全認證機制。
- 啟動 LOG 機制紀錄客戶寄送郵件相關訊息。
- 設定每封信件最大 size。
- Mail Quota 保護機制。
- 設定適當的 mail returning time。

DNS 服務

- 啟動 check-name 機制。
- 更新並檢查 root file。
- 設定 IP ACL 限制 Zone Transfer。
- 啟動 DNS Security 機制。
- 啟動 IPv6 功能。
- 啟動 LOG 機制紀錄重要錯誤相關訊息。

FTP 服務

- 不允許 root 登入。
- 設定 chroot。
- 限制 guest 及 anonymous 會對系統安全威脅的操作指令。
- 上傳檔案之目錄不可與系統重要檔案同一磁區。
- 啟動稽核程式。
- 限制登入來源位址。
- 限制登入帳號及群組。
- 限制登入時間。
- 關閉匿名登入功能。

Proxy 服務

- 關閉 IP Forward。
- 使用較安全的檔案系統。
- 限制管理的 IP 位址。
- 不允許管理帳戶之外的使用者登入管理介面。
- 使用 HTTP + SSL 做為管理的通道。

2.2.3.3 網路設備安全檢查要點

交換器、頻寬管理器

- 更新使用最新穩定版本之韌體（軟體）。
- 啟動驗證機制。
- 變更網路設備預設之管理員名稱及密碼設定。
- 所有密碼使用加密方式儲存。
- 關閉網路設備之遠端管理功能（含 Telnet、WWW、SNMP、FTP、TFTP）或採用 SSH、SSL（大於 128 bits）及廠商 proprietary 等通訊協定。
- 管理連線需設定 Timeout 時間。
- 變更 SNMP 預設使用之 community string 值。
- 關閉 ICMP echo reply 功能。
- 設定 IP ACL 限制管理人員來源。
- 設定 SNMP ACL 限制 SNMP 存取。
- 設定 MAC ACL 進行 port-based 設備管制。
- 啟動 LOG 機制紀錄管理訊息。

路由器、L4 交換器

- 更新使用最新穩定版本之韌體（軟體）。
- 啟動驗證機制。
- 變更網路設備預設之管理員名稱及密碼設定。
- 所有密碼使用加密方式儲存。
- 關閉網路設備之遠端管理功能（含 Telnet、WWW、SNMP、FTP、TFTP）或採用 SSH、SSL（大於 128 bits）及廠商 proprietary 等通訊協定。

- 管理連線需設定 Timeout 時間。
- 變更 SNMP 預設使用之 community string 值。
- 關閉 ICMP echo reply 功能。
- 關閉各介面上 IP directed broadcasting 功能。
- 設定 IP ACL 限制管理人員來源。
- 設定 SNMP ACL 限制 SNMP 存取。
- 啟動 IP-Spoofing 檢查機制。
- 啟動 SYN-Flood 保護機制。
- 啟動 LOG 機制紀錄管理訊息。

防火牆

- 更新使用最新穩定版本之韌體（軟體）。
- 啟動驗證機制。
- 變更網路設備預設之管理員名稱及密碼設定。
- 所有密碼使用加密方式儲存。
- 關閉網路設備之遠端管理功能（含 Telnet、WWW、SNMP、FTP、TFTP）或採用 SSH、SSL（大於 128 bits）及廠商 proprietary 等通訊協定。
- 管理連線需設定 Timeout 時間。
- 變更 SNMP 預設使用之 community string 值。
- 關閉 ICMP echo reply 功能。
- 關閉各介面上 IP directed broadcasting 功能。
- 設定 IP ACL 限制管理人員來源。
- 設定 SNMP ACL 限制 SNMP 存取。
- 啟動 IP-Spoofing 檢查機制。
- 啟動 SYN-Flood 保護機制。
- 啟動 LOG 機制紀錄管理及 policy 存取拒絕相關訊息。
- 禁止外界對 DMZ 區進行任何 ICMP 測試。
- 禁止外界對 DMZ 區進行 DNS Zone Transfer。
- 禁止 TFTP。
- 禁止 FTP 標準模式，只允許 PASV 模式。
- 使用 non-transparent 模式提供 Telnet、FTP、WWW 等服務。
- 每一條 policy 需實際驗證。
- 確認存在 deny all 之最終 policy。

3. 心得

綜合此次研習心得，系統及網路安全為現代網際網路之一項重要議題，其主要用途為防止網路攻擊事件及竊取公司重要資訊，再不影響正常網路運作下提供更安全及可靠的新服務。而達成此做法之關鍵除了系統及網路本身相關的安全設定及管理之外，更重要的是要訓練相關管理及維運人員安全知識以確保整體系統之安全。當然有關安全的領域是非常廣泛的，有些相關的資訊及技術還是需要仰賴供應廠商，但是企業本身還是需要了解相關的技術及運作模式。而且以中華電信公司提供外界網路服務更需要此項技術及安全維護，以提供客戶更好、更安全的網路服務需求。

4. 建議

綜觀此次研習，對於從既有網路架構下如何更進一步加強整體系統及網路安全提供出解決方式，使得企業內及企業外網路更加安全有保障。當然資訊日新月異我們無法保證建立絕對安全的資訊環境，但不能因為如此就放棄資訊安全的重要工作。因為如果你不付出心力準備相關安全的措施，一但發生了重要的資安危機，您將付出的代價勢必倍於預防準備的工作，這也應該是每一個管理者容易理解的概念。

如何做好網路及系統安全防治實在是一項相當困難且複雜的工作，因此針對企業提出下列建議的步驟。此步驟是一個循環的流程，每經歷一次事件的發生將可修正企業內部的安全策略，達成更安心可靠的網路環境。

A. 制定企業安全政策
   - 定期備份資料
   - 定期更改密碼
   - 適時更新版本或完成修補的動作
   - 安全的設定及測試
   - 安裝防毒軟體及定期更新病毒碼

B. 規劃企業安全網路環境
   - 企業防火牆的建置及規劃
   - 伺服器端關閉無使用的通訊埠
   - 內部網路的區隔
   - 使用者權限及密碼
   - 建立弱點掃描系統
   - 建立入侵偵測系統

C. 檢測及稽核網路及主機系統
   - 定期稽核企業內網路及主機系統
   - 完成相關安全設定

D. 監控企業安全事件
   - 觀察企業電腦的網路行為
   - 檢查系統相關異常的程序
   - 監控網路不正常流量行為

E. 隔絕入侵或感染區
   - 實體隔離
   - 網路設備控制隔離
   - 區域防火牆控制隔離

F. 救助及復原相關損失

需要復原的範圍
復原人員及時程的規劃
復原的方法及步驟

G. 分析安全事件原因
安全事件的發現點及時間
受威脅的是硬體平台或是軟體
入侵或感染的途徑及特徵
入侵或感染破壞的方式
安全事件修復的方法

H. 重新檢視企業安全政策
政策制定時不夠謹慎
安全政策落實的問題
便利與安全性之間的平衡問題
新型的入侵或感染型態出現，以致舊的安全政策不足以預防

在此特感謝孫主任三為、施計劃主持人君熹，給予此次學習之機會之，及多位工作同仁之協助與指導。