# 安全軟體

```

1.安全軟體

1.1資訊安全工具

1.2Intrusion

1.3入侵預防系統

1.4 Statistical Anomaly Detection

1.5 Distributed Intrusion Detection

2.用戶端保護

2.1 Antivirus

2.2 UAC

2.3 LDAP

2.4CooKe

2.5追蹤保護名單

2.6伺服器

3伺服器保護

3.1伺服器

3.2伺服器安全性原則管理

3.3主機防禦

3.4Keeping Server Updated

3.5阻止 DNS 定位

4.電子郵件保護

4.1病毒、蠕蟲、特洛伊木馬程式、垃圾郵件以及網路詐騙

4.2避開駭客和攻擊者

4.3黑名單

4.4 Spam

4.5 Phishing

4.6 Pharming

4.7 SPF

4.8P GP

```

## 1.安全軟體

### 1.1資訊安全工具

```

1.Microsoft Assessment and Planning ( MAP ) Toolkit 評估電腦安全性

您可以使用這個免費工具組,就桌上型和膝上型電腦易遭病毒和惡意程式碼侵害的弱點來評估整個订環境,

判斷您的電腦是否可以安裝Forefront Client Security

惡意軟體移除工具檢查您的電腦是否有感染特定、常見的惡意軟體,並協助將找到的惡意軟體移除。

2.Microsoft Security Assessment Tool

取得協助以便評估您的組織目前安全性環境的弱點。此工具會列出一份問題優

先順序的清單,並會提供有助於將安全性風險降至最低的特定指引。

3.Microsoft Update

在單一位置尋找 Windows Update 與 Office Update 提供的更新,並且選擇自動傳

輸和安裝高優先順序的更新。

4.Windows Server Update Services

管理網路内各電腦部署最新 Microsoft 產品更新的流程。

5.Microsoft 資訊安全評估

Microsoft 資訊安全評估工具(Microsoft Security Assessment Tool) (MSAT) 是一個免費工具,

其設計可以協助您的組織評估目前資訊安全環境的弱點,列出一份問題優先順序的清單,並提供有助於將問題風險降至最低的特定指引。

MSAT 是您著手加強運算環境與商務資訊安全極具成本效益的簡易方式。

程序開始時先概覽您目前的資訊安全狀態,再使用MST持續監控基礎結構因應資訊安全威脅的能力。

6.反間諜軟體

反間諜軟體能防止間諜程式及其他垃圾軟體所導致的快顯視窗、效能低落和安全性威脅。

若要隨時得知最新的間諜軟體形態,則必須持續更新反間諜軟體。

>會在電腦上顯示快顯廣告、收集並轉送個人資訊,或未事先取得您的同意而變更電腦設定的軟體就稱為間諜軟體。

>許多垃圾軟體(例如間諜軟體)的設計本意就是要讓使用者難以移除。如果您嘗試使用和其他程式一樣的方式解除安裝此軟體,

則重新開機后這個程式可能又會出現。

>>Windows Defender 乃設計用於保護您的電腦免受間諜軟體的威脅。WindowsDefender還具備即時保護功能,

其監視系統可在偵測到間諜軟體時提供建議處理動作,並能將工作中斷的情況降至最低。

```

### 1.2Intrusion

```

對網路系統而言,不論是不懷好意或是無意的入侵,都是重要的資訊安全議題。

攻擊者可以透過非法登入來入侵系統,而已授權的使用者可能會非法取得超出原本的權限,而搖身變成攻擊者。

攻擊者也可能藉由病毒(virus)、蠕蟲(worm)或特洛伊木馬程式(Trojan horse),

來達到入侵的目的。

偽裝者(Masquerader):冒用合法使用者身份,或是破解系統存取控制機制,而取得

合法使用者帳戶的人。

```

### 1.3入侵預防系統

```

入侵預防系統(Intrusion Prevention System) 是對防病毒軟體(Antivirus Softwares)和

防火牆的補充。

入侵預防系統是一部能夠監視網路或網路設備的網路資料傳輸行為的計算機網路安全設備,能夠即時的中斷、

調整或隔雖一些不正常或是具有傷害性的網路資料傳輸行為。

如果可以快速的偵測到入侵,除了可以確認入侵者,更可以在入侵者危及系統之前將入侵者逐出系統。

越快偵測到非法入侵,就越能降低系統所招受的損失,並且也能快的復原系統。

有效的入侵偵測也是嚇組入侵的力量,經常也能收到阻止入侵的效果。

要做好入侵偵測,勢必得大量收集入侵相關的資訊,而這些資訊更可以用來加強防範入侵的能力。

入侵偵測的技術是以「入侵者的行為與合法使用者的行為有所不同」為前提·而且可以量化的方法來辨識入侵者的行為。

兩者之間依然會有重複之處。因此,擴大界定入侵行為,就越能找到較多的入侵者,但同時也會導致更多的誤判,

也就是將合法使用者誤以為是入侵者。反之,卻會讓某些入侵者成了漏網之魚。

```

### 1.4Statistical Anomaly Detection

```

異常統計偵測法(Statistical anomaly detection):這種方法是在一段時間之內收集

合法使用者的行為,並且統計這些行為資料進而產生檢驗規則,然後以這些規則檢視使用者是否出現不合法的行為。

偵測方法要定義檢測各種事件的發生頻率,也就是門檻值(Threshold)。另一種異常統計偵測的作法,

是記錄每位使用者的行為,然後以此來偵測使用者是否出現異常行為。

```

### 1.5Distributed Intrusion Detection

```

分散式入侵偵測(Distributed Intrusion Detection)是在網路各節點都裝置入侵偵測系

統,並讓各個系統互助合作,以達到最有效的偵測。

分散式入侵偵測系統需要處理不同的稽核記錄格式,而且網路上各個節點都將提供資訊收集和分析的服務,

所以必須利用網路傳送相關的稽核資料或即時資料,也因此要確保這些資料的完整性與機密性,

才能阻止入侵者更改傳送的稽核資訊來掩護入侵者的行為。

```

## 2.用戶端保護

### 2.1 Antivirus

```

用於偵測惡意電腦應用程式、防止其感染系統以及清除已感染電腦病毒的檔案或應用程式的軟體和技術。

```

### 2.2 UAC

```

User Account Control(UAC),使用者帳戶控制是安全性元件,

允許系統管理員在非系統管理員的使用者工作階段期間輸入認證,以執行臨時性的系統管理工作。

UAC 也可以在允許系統管理動作或應用程式執行之前,要求系統管理員明確地核准這些動作或應用程式。

使用者帳戶控制(UAC)不需要系統管理權限即可完成作業系統的部署。

推出使用者帳戶控制(UAC)之前,如果使用者是以系統管理員的身分登入,則該使

用者會自動獲得所有系統資源的完整存取權,

雖然使用者以系統管理員身分執行時可以安裝合法軟體,

但也可能會有意或無意地安裝惡意程式。由系統管理員安裝的惡意程式可能會徹底危及電腦,並影響所有使用者。

```

### 2.3 LDAP

```

目錄訪問協定(Directory Access Protocol即 DAP)對於網際網路客戶端使用太複雜,

ETF設計並指定LDAP做為使用X.500目錄的更好的途徑:LDAP在TCP/IP之上

定義了一個相對簡單的升級和搜索目錄的協定。

```

### 2.4CooKe

```

Cookie 是當您第一次造訪網站時,網站放到您電腦硬碟中的小檔案。把Cookie想成是您個人特有的識別卡。

Cookie不應和病毒混為一談。雖然有可能會因Cookie中存放個人資料而導致不當使用Cookie,但是 Cookie 本身是沒有惡意的。

許多網站包括 Microsoft 的網站都會使用 Cookie 。

Cookie會告訴我們您造訪網頁的頻率,協助我們瞭解您對哪些資訊感興趣。

您是否曾在線上商店將某些物品放到虚擬購物車上,過幾天之后回來發現那些物品還在車上?

這就是Cookie運作的例子。

如果您不曾在網站上註冊或是留下個人資訊,那麼伺服器只曉得某個使用您的 Cookie 的人曾回來造訪網站。

但是網站無法得知其他資訊。

Cookie 是包含在「超文字傳輸協定」(HTTP)要求與回應中的文字字串。

當您瀏質網站的不同網頁,或是稍后返回網站時,Cookie 可以用來維護狀態資訊。

停用Cookie可能會使某些Web服務無法正確運作,

停用Cookie並不會使您匿名,或是防止網站追蹤您的瀏覧習慣 HTTP 要求還是會包含有關您從何而來的資訊、

IP位址、瀏覧器版本、作業系統及其他資訊。

```

### 2.5追蹤保護名單

```

微軟也在1E9加入「追蹤保護名單」功能,供使用者編輯網路追蹤業者名單,避免清單上的業者窺視自己的上網習慣。

隨著監管當局和消費者向業者施加的保護隱私壓力增加,微軟也藉此宣示更積極捍衛網路隱私。

```

## 3伺服器保護

### 3.1伺服器

```

其實伺服器只是一部連上網路的電腦,只是這部電腦是用來執行某些特殊功能的,

例如分享印表機、儲存檔案,或傳輸網頁等。

別忘了,當您將筆記型或案上型電腦連上Internet時,它們也就像伺服器一般,

如果没有防火牆,就可能從Internet 接收到惡意的傳輸。

```

### 3.2伺服器安全性原則管理

```

安全性原則是一組可設定的規則,當作業系統回應存取資源的要求時,會根據這些規則來決定所要授與的權限。

```

### 3.3主機防禦

```

使用深度防禦時,「網際網路資料中心」的每一個主機都得一一接受評估,並且建立個別原則,

只讓伺服器執行必要的作業,駭客們想要圖謀不軌,還得先攻破這層障礙才行。

個別原則則是根據每個伺服器的資料分類和類型而建立。

比方說,公司原則規定,所有的Web伺服器都是不分類的,因此只能接受公用資訊。

而資料庫伺服器是最高機密,也就是說,這些資訊必須竭盡全力加以保護。

伺服器分四類

1不分類

這類資訊的傳饰是没有限制的。

這些資訊包括行銷資訊業務資訊以及明確要對外公開的資訊在內。

公用網際網路伺服器上的資料,應該都是不分類的。

2.機密

這些資訊曝光的結果,可能會對公司產生有形的傷害。

機密資訊必須經過加密,才能發饰於該環境下。

3.秘密

這些資訊曝光的結果,可能會對公司產生非常嚴重的損害。

秘密資訊一定要置於防火牆後面,而且在發饰之前,一定要經過加密。

4.最高機密

這些資訊一經曝光,就會對公司造成極為嚴重且無法彌補的損害。

最高機密一定要極盡所能的加以保護和監控。

```

### 3.4Keeping Server Updated

```

将Service Pack 和問題修正保持在最新狀態

Windows 伺服器的service pack 和問題修正程式、新的安全修補程式、

IIS修補程式、以及應用程式,一定要隨時更新。

同時,一定要在完全模擬生產環境的測試環境下,慎審進行規劃和測試,

以確認任何一項要套用到生產系統的變更。

在套用維護之前,也應該將伺服器做一份完整的備份

```

### 3.5阻止 DNS 定位

```

其實在架構當中,DNS伺服器是更需要保護的部份,

因為所有的網路用戶端都要查詢DNS,尋找它們需要通信的伺服器。

駭客們可能會使用DNS定位方式來攻擊 DNS。

比方說用各種滲透技術,以惡意資訊覆蓋DNS伺服器的快取檔案。

這時候,如果使用者要查詢生產 DNS,便會被轉送到由駭客控制的冒牌DNS伺服器,而造成損害。

對於這種攻擊,您可以用好幾種方法加以防治,例如:

1,在内部網路使用不同的DNS伺服器,確保這些DNS伺服器不對外來電腦的查詢做出回應。

2.使用唯讀DNS,不准進行任何更新作業。

3.保護DNS資料庫。「網際網路資料中心」架構是採用Active Directory 安全保

護,只准進行安全的 DNS更新作業。

```

## 4.電子郵件保護

### 4.1病毒、蠕蟲、特洛伊木馬程式、垃圾郵件以及網路詐騙

```

電子郵件所構成的安全性威脅主要有五種:

1.病毒

病毒就是會自我複製,並可能進行破壞的程式,它們經常隱藏在看似無

害的其他程式裡。

電子郵件裡的病毒常會偽裝成小遊戲或是圖片,並利用誘人的標題(如「我的女友裸照」引誘使用者開啟並執行程式。

病毒會營試感染電腦上的其他程式,達到自我複製的目的。

2.蠕蟲

蠕蟲與病毒類似,都會自我複製,但是蠕蟲通常會透過散發電子郵件達到這個目的,而不僅是感染單一電腦上的程式。

3.特洛伊木馬

特洛伊木馬則是偽裝為普通應用程式的有害程式。

雖然這些程式不像病毒和蠕蟲會自我複製,但還是有能力造成不小的傷害。

很多時候病毒和 蠕蟲甚至是經由特洛伊木馬偷渡進來的。

4. 垃圾郵件

垃圾郵件或來路不明的廣告郵件往往造成頻寬和時間的浪費,光是其龐

大的數暈就不容忽視,有時還會夾帶病毒。許多垃圾郵件都是色情郵

件,如果公司不採取相應手段阻止,不但會造成工作環境壓力,還可能

造成法律上的責任。

5. 網路詐騙

網路詐騙電子郵件,例如謊報病毒醫告、連鎖信件或假的贈獎活動等

等·都只會浪費讀者的時間。網路詐騙郵件也常帶有病毒或是特洛伊木

馬程式。

```

### 4.2避開駭客和攻擊者

```

可以做四件事來提高安全性。

1.將Internet Explorer設定成「高安全性」層級

2,將您認為安全的網站加入「信任的網站」

3.使用純文字讀取您收到的電子郵件

4.封鎖瀏覧器的快顯視窗

```

### 4.3黑名單

```

1.黑名單是常用的存取控制方式,列入黑名單的用戶無法進入系統。

2,透過黑名單,阻擋某些E-Mal地址或伺服器發出的電子郵件,達到過海垃圾郵件的目的。

3.黑名單亦被用作防止盜版,例如受保護的光碟可能無法在某些軟體播放。

4.與黑名單相對的是白名單,即「除名列於上者外一律不准進入」的名單。

```

### 4.4Spam

```

Spam(垃圾郵件),未經收信人許可的電子郵件、郵寄清單發布或新聞群組發布通

常是為廣告目的而傳送。

傳送垃圾郵件會佔據郵件伺服器與網路,並阻塞收件者的信箱,是不良網路禮儀,可說是踐踏了網際網路基本精神。

1,不請自來的大量商業性電子郵件。

2.經過滤器識別為垃圾郵件的電子郵件。

```

### 4.5Phishing

```

phishing(網路釣魚)

用來讓收件者認為郵件來源正常,而開啟一些垃圾郵件。攻擊者會寄出類似官方來源寄發的電子郵件。

網路釣魚者會傳送電子郵件,偽稱自己是某個成立的組織或現有的合法組織,

網路釣魚會詐騙使用者提供私人資訊(用於身分竊取)。

該電子郵件會引導使用者造訪要求更新個人資訊(如密碼)的網站。

然而,該網站是假冒的,建立目的僅是為了竊取使用者的資訊。

```

### 4.6Pharming

```

pharming(網址嫁接),某種形式的線上詐縣,網址嫁接者依賴相同的偽造網站以及竊取機密資訊來進行線上詐騙,

但是使用許多方式更難偵測到這種詐騙形式,因為其並非依賴於受害者接受「誘餌」訊息。

```

### 4.7SPF

```

Sender Policy Framework,寄件者政策架構用於驗證電子郵件的一組標準實作。

如果寄件者的網域擁有者出現在SPF中,收件者的MTA就可以檢查是否有偽造的退回位址

Symantec Brightmail Gateway可讓您針對無法通過SPF 驗證的郵件指定要採取的動作。

```

### 4.8PGP

```

PGP (Pretty Good Privacy,PGP)是一種用在電子郵件的加密技術,

Paul Zimmerman除了發展了PGP的技術,同時也公開了PGP的原始程式碼和文件,任何人皆能取得PGP的原始資料。

PGP非常成功,因為這項技術提供了標準化的電子郵件加密方法。

```