網路安全淺出深入(1)

張貼：matt 發表於 Wednesday, April 04 @ 16:41:10 CST

1.前言

網際網路，這個大家耳熟能詳的名詞，在這幾年之間風起雲湧，橫掃全球，諸不論它是否是真的能為企業推向另一個新的經濟，不可至否的，它已經漸漸的融入我們的生活，為個人或企業提供了另一種相互溝通的媒介，供給人們一個跨越族群、跨越國家、一個突破空間與時間的開放通訊空間。

隨著網際網路的科技逐漸普及與複雜，網路上的資料是以電子的方式傳遞，因些資料安全性便變的格外的重要，但不幸地，關於網際網路基礎建設的安全性，所有的努力還是不夠的。先來看看下面的研究報告。

◆台灣網路危機處理中心（TW-CERT）提出的「國內網路安全現況」報告指出，國內網路伺服器的 Web 程式若被駭客攻擊，存活比例將不到五成五。

◆一項新的 Gartner 報告顯示：將有半數以上的公司在三年之內會遭受駭客入侵，同時，除非有嚴重的損失產生，否則有近 60%的公司行號未曾發現自己的防禦系統已被破壞。

◆美國國防資訊安全局的統計數字指出，在所有駭客侵入事件中，僅有 4%至 5%會被呈報給有關當局。

◆美國聯邦調查局與 CSI 安全局的電腦犯罪與安全調查報告指出，有 55%的企業曾遇到來自區域網路的內部入侵或嘗試未經授權存取資料。

近一年來網路安全相關新聞	
日期	事　件
2001/02/13	反全球化駭客已取得近年來到瑞士達弗斯參加世界經濟論壇（WEF）的各國政府及企業領袖的個人資料。
2000/11/13	刑事局接獲美國 FBI 告知，電腦駭客利用木馬程式進行攻擊台灣核能電廠的電腦主機。
2000/11/07	微軟網站再遭駭客攻擊
2000/11/07	電腦駭客詐領南非銀行 46 萬 2 千美元
2000/10/30	微軟遭入侵，駭客自 9 月底就潛伏在網路中，窺見微軟開發中的軟體原始程式碼
2000/10/26	根據國安局與刑事警察局調查，保守估計國內至少超過十分之一的電腦被植入所謂的「木馬程式」
2000/09/22	總行設在倫敦的匯豐銀行（HSBC）二十日宣布，該銀行位於網際網路的網站，日前遭電腦駭客入侵。
2000/09/11	三個政府單位網站遭國外駭客入侵
2000/07/13	國際駭客作案台灣被當跳板
2000/03/23	駭客攻擊美企業財損暴增一倍
2000/02/16	台灣六成主機難逃駭客入侵

網路安全淺出深入(2)

張貼：matt 發表於 Wednesday, April 04 @ 16:43:12 CST

2.網路安全為何

網路安全可以概分為三個部分：保護資訊（Information）、保護資源（Resource）和保護隱密性（Privacy）。保護資訊是確保資訊不被未獲授權的使用者取得或竄改；保護資源是確保資源不被未獲授權的使用者使用，這裡的資源可以是網際網路上網站提供的服務或是網路的頻寬；保護隱密性是確保個人在網路上的私密資料和在網路上的行為資訊不被其他人取得。
「網路安全」所訴求的重點是整個電腦和網路環境的安全問題，所以包含有認證、存取控制、入侵偵測，以及軟體弱點等問題，而大部份的駭客都是用網路所造成的安全漏洞，入侵大家的網路、系統造成傷害，尤其當個電腦連接到 internet 以後，所有的安全風險就和一個網站伺服器在網路上一樣多，而且頻寬愈高，上網速度愈快，泡在網上的時間愈長，就更容易地讓駭客侵入，因此在安全的風險更高。

網路安全淺出深入(3)

張貼：matt 發表於 Wednesday, April 04 @ 16:48:05 CST

3.「安全」表示什麼

首先需要了解到沒有任何系統可以號稱「完全的安全」，您所能做的增加某人危及您系統的困難度而已。因為安全是一種執行的過程，就如同買保險一般，沒有說您買了保險後就不會發生事情。

網路安全也是一樣，當您花了心思與力氣將網路安全做好，並不代表就不會發生駭客入侵事件，您做的安全只是將可能發生的安全事件降到最低，減低可能對企業的損害。舉個例子來說，你認為美國國防部的網路一定夠安全了吧，但它還是有發生過駭客入侵的案例。
所以網路安全是需要持續做的，不是一次就能做好，再多的防範措施，也需您持續的注意與維護。

網路安全淺出深入(4)

張貼：matt 發表於 Wednesday, April 04 @ 16:52:08 CST

4.您要保護什麼

在您開始著手網路安全之前，您先想想如下的問題：
◎您要避免那些人的威脅?
　是好奇的人、蓄意破壞者、只是想利用入侵出名的人、還是競爭者。
◎那些風險您需要關心、那些不用?
　入侵者可以讀寫檔案或執行程式而導致損壞嗎? 他們可以刪除重要的資料嗎? 阻礙公司重要工作的完成?

您應該去分析您整個網路系統上的企業資產，以了解什麼是需要保護的、為什麼要保護、被保護

內容對公司的價值，這樣您才知道做網路安全是為了什麼。

網路安全淺出深入(5)

張貼：matt 發表於 Saturday, April 07 @ 12:11:06 CST

5.訂定網路安全政策

一般的高階管理者對於網路安全工作普遍存在著錯誤的認知，以下就是常見的一些迷思：

◎我們已經有了防火牆！
◎我們用 SET 及 SSL 加密保護網路傳輸。
◎我知道不夠完善，但相信我們的 EDP 內控及稽核可達 90%。
◎對網路安全的投資划算嗎？

使用經過認證的網路安全產品並不代表網路就是安全的，ICSA 發現經過其認證的防火牆有 70%在實際使用時有安全的漏洞，而這些漏洞都是管理不善所造成的，這一點充分顯示網路安全是一項管理工作—安全是管理出來的。

再重另一角度來看，正確的網路安全投資是什麼呢？ 其實他就是以網路安全政策制定時所認定的網路安全風險成本為上限，因此網路安全政策的制定是管理活動，沒有資訊安全政策的制定就沒有網路安全成本效益的依據。所以在進行網路安全前，網路安全政策的制定也是必需的。

制訂網路安全政策時，企業應根據自己的需求及考量下列因素：
◎在安全與使用的方便性上取得平衡
◎成員之種類，高階主管、稽核、安控人員、系統管理、使用者…等
◎資訊分級及其保護措施，例如：一般、內部參考、機密
◎風險分析(Asset、Threat、Vulnerability、Loss、Safeguard)
◎企業可承受的風險
◎落實機制，例如：政策規定網際網路之使用僅限於公務，而落實機制可以是每日針對防火牆 Log 產生分析報表..等等
◎明訂責任
◎政策修訂辦法及其更新頻率

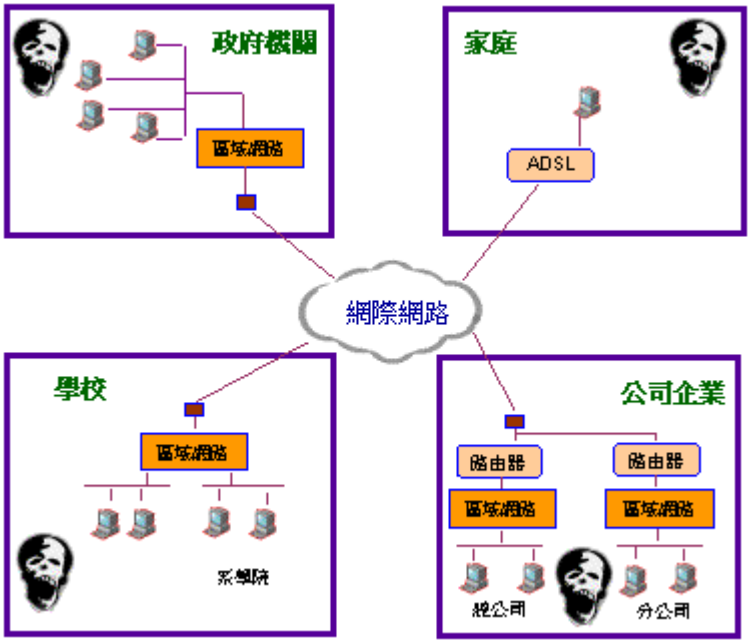
網路安全淺出深入(6)

張貼：matt 發表於 Saturday, April 07 @ 12:19:31 CST

6.駭客在那裡

任何連線到網際網路的電腦， 都是與世界各地同在網際網路上的電腦串接起來的，所駭客就有可能透過這四通八達的道路，連到你們家來，進行非法的行為；就如同現實社會中的情況，只要

有路可以通到您的家，小偷就有辦法到您的家光顧了。或許您會覺得下面的圖太聳動了，但真實情況下駭客可能存在於任何地方，不要以為駭客只會出現在你們家的外面，他也有可能是自己人喔。如下圖：



從前，在企業內部網路中，不必擔心外部的人入侵偷取資料，只要擔心企業內部人員透過企業內的網路做手腳，但現在一切都不一樣了，網際網路開放許多企業資訊大門，許多不當的防禦方法，依然讓駭客暢行無阻，其實不肖份子已在門外徘徊了許久。