資訊專題研討課程心得報告

講題: 資安事件防護與處理簡介

演講人: 辜國隆 處長 資策會南資處

報告撰寫人: 廖峻鋒 政治大學 資科所 二年級 g9104@cs.nccu.edu.tw

2003/10/12

1 演講主題及摘要

近年來一連串層出不窮的資訊安全事件, 不僅引起社會各界的重視, 甚至成爲媒體爭相報導的焦點。許多機關企業也開始重新審視資訊安全問題, 無不希望提早做好資訊安全防護, 以免成爲下一波駭客攻擊的目標。辜國隆處長是前任國家資通安全會報技術服務中心主任。在這場演講裏, 他分享了過去處理國內外重大資安事件的經驗, 說明資安事件的防護與處理程序, 並針對幾個重要的資訊安全相關標準與規範加以介紹。

2 演講要點整理

2.1 回顧歷年資訊安全事件

近年來, 資訊及網路應用的普及, 除了帶給人們資訊應用的方便外, 也帶來了許多資訊安全問題, 據 CERT 統計,2001 年發生的資安事件約5 萬件, 足足是2000 年2 萬餘件的兩倍以上, 而2002 年第一季截止, 已發生近3 萬件的資安事件。

資安事件頻傳除了資訊網路技術普及, 造成有意及無意的駭客能輕易進行木馬程式、DoS、竊取資料等攻擊外, 另一個值得注意的是資訊系統及網路的弱點, 如 IIS 漏洞、SQL Injection 等, 據 CERT 統計資料顯示, 自1999 年來發佈的系統弱點成倍數成長,2001 年發現約2500 個系統弱點, 2002 年至第一季已發現1000 餘個弱點, 而這些弱點如同在一個以設下高牆 (防火牆、防毒牆)、加上有精明的守衛及監視設施 (入侵偵測、VPN、資料加密、病毒防護...等) 防守的嚴密城堡中, 仍有一些漏洞, 讓不速之客能輕易的盜取及破壞企業內的重要資訊設施及資料。

2.2 一般駭客入侵系統之手法與流程

綜觀駭客入侵的流程, 駭客挑定目標可不是亂槍打鳥, 一定會先做功課, 利用網路資源或搜尋引擎, 蒐集相關資料, 標定出目標網路與主機的位址與名稱, 而且會幾乎無所不用其極, 盡可能蒐集最多的目標資料。

接著會利用 Ping、埠號掃瞄、Netbios 等軟體工具, 進行弱點掃瞄, 以辨識目標主機與網路所開放與提供的網路服務, 和所使用作業系統的版本, 這些可作爲後續攻擊的途徑。然後進行弱點刺探, 也就是進一步找出目標主機的使用者帳號或未受保護的網路分享資料, 應用到的技巧包括列舉使用者帳號、所執行的應用程式、空白密碼等。

再利用上述方法所蒐集到的資料, 嘗試登入目標主機, 同時透過密碼猜測工具、網路監聽器或是緩衝區溢位攻擊等方式, 來取得系統的使用者帳號、密碼和存取權限。如果駭客到此地步, 還僅獲得一般使用者的帳號密碼, 必須提昇權限, 此時很可能會再請出密碼檔破解工具, 進而取得管理者的帳號和密碼, 完全控制被入侵的主機。

完全控制後, 就可進行破壞了, 比如說更換網頁或是竊取資料, 甚至「善用」作業系統或伺服器程式現存的弱點與漏洞, 搜尋網路上的其他目標, 以跳板方式, 繼續攻擊其他主機。如果這台主機尚有利用價值, 駭客就會於此植入「後門」, 方便日後利用, 方法有新增帳號、建立定時執行程式、安裝監聽側錄程式、將原系統程式替換爲後門程式等, 方便下次繼續登入或控制該主機, 並再利用受駭主機爲跳板, 繼續攻擊其他目標, 隱藏自己的位址。

駭客的攻擊如果到此爲止, 還差最後一步。這關鍵的步驟就是要消滅證據, 以免被發現或是追蹤, 盡可能掩蓋任何蛛絲馬跡, 這時候駭客會刪除記錄檔 (Log file)、隱藏所植入的攻擊程式或是更換檔案名稱。

2.3 如何制定完善的資訊安全政策

資訊安全政策不應該只是資訊人員的責任, 它應該取得決策階層的授權與支持, 以及同仁的認同, 同時資訊安全政策不應該好高騖遠, 因爲過於嚴苛的政策或要求, 只會窒礙難行, 最後大家只好敷衍了事, 結果適得其反, 非但無法確實執行安全政策, 反而造成更多的資訊安全問題。

因此, 制定安全政策時, 應同時設置一常設性的跨部門組織, 有該組織成員共同來參與制定資訊安全政策的工作, 以取得最大的共識。所謂「知己知彼、百戰百勝」, 在制定政策時, 除了要考量企業營運的特性、風險之外, 應同時評估企業現有文件化或數位化資訊或資料, 以及處理資訊的設備、系統或人員所承受的威脅, 可能發生的影響與本身的漏洞與弱點, 並評估風險發生的可能性, 以了解現

有的資訊安全風險與未來可能發生的問題, 在做過通盤的考量之後, 才有可能以合理的費用, 針對可能遭受風險的資訊與系統找出其漏洞與弱點, 並加以控管, 以減少或避免風險的發生。

資訊安全政策制定的目的在提供一個管理與執行的方向, 不需是 step-by-step 的說明。安全政策不應改只是口號, 它必須適度的文件化, 以供相關人員參考。制定好的企業資訊安全政策, 應該以文件的方式在適當的場所公佈, 或是以數位化的方式, 透過電子郵件的傳遞, 讓所有人員能認識、了解資訊安全的規範與要求, 以期大家都能共同遵守。

2.4 資安標準及規範

2000年11月, 英國標準 BS7799正式被採納爲國際資訊安全標準 ISO17799, 國際上終於誕生了第一個屬於資訊安全的共通標準。腦筋動得快的資訊廠商與顧問公司, 看好這塊市場, 從年初開始不斷大力宣傳資訊安全標準的重要性, 而且推出相關的顧問輔導服務來協助企業取得 ISO17799認證。政府相關部會也正研擬將 ISO 17799引進成爲我國的資訊安全標準「CNS 17799」, 並研擬政府機關資訊安全管理辦法。預計此一標準公佈之後, 將嚴格要求國內政府機關與產業界配合執行。

除了 ISO17799之外, 目前全球已有許多不同的資訊安全政策, 列表如表一。

3 評論與心得

回顧過去幾年, 國內外陸續出現多次的資訊安全事件, 從年初國內某知名網站會員資料外洩、中美駭客大戰、網路銀行盜領事件、網路券商客戶帳號密碼被竊, 乃至於最近惡名昭彰的 Code Red 紅色警戒、Nimda Worm 娜坦病蟲及疾風病毒.....等等一連串層出不窮的資訊安全事件, 不僅引起社會各界的重視, 許多機關企業也開始重新審視資訊安全問題, 無不希望提早做好資訊安全防護, 以免成爲下一波駭客攻擊的目標。

根據2002年 FBI/CSI 調查報告也指出,90%的企業在一年當中曾偵測電腦遭受惡意攻擊, 其中包括了病毒攻擊、拒絕服務攻擊 (DoS)、系統入侵、機密資料竊取...等等數十種之多。其中, 又以『企業機密資料被竊取』所造成的經濟上的損失最大。(圖表 1) 也就是說, 雖然『企業機密資料被竊取』所發生的頻率並不是最高, 然而一旦發生, 損失往往是最爲嚴重的。

這麼樣多屢見不鮮的網路安全問題並不全然因爲駭客具有高深的技術, 若沒有使用者的大意與漠視網路安全漏洞的存在, 駭客的攻擊是無法得逞的。例如惡名昭彰的 Code Red 紅色警戒與 Nimda 娜坦病蟲能夠如此肆虐, 皆是因爲使用者疏忽了漏洞修補的重要性。網路安全一直無法落實的主因就在於,「漏洞本身並不可怕, 可怕的是您不知道漏洞的存在, 甚至不去即時修補漏洞, 那駭客鐵定比您

表 1:

名稱	說明	
COBIT	制訂標準:	資訊技術控制目標架構 (Control Objectives for Information and related Technology)
	提出單位:	國際電腦稽核協會 (ISACA)
	網頁位置:	http://www.isaca.org
BS7799	制訂標準:	BS7799 /c:cure code of Practice 1 and 2
	提出單位:	英國標準組織 (BSI)
	網頁位置:	http://www.bsi-global.com
ISO17799	制訂標準:	ISO 17799
	提出單位:	國際標準組織 (ISO)
	網頁位置:	http://www.Iso.ch
GAPSIT	制訂標準:	一般公認資訊系統技術之安全原則與實務 (General Accepted Principal and Practice for Securing Information Systems and Technology)
	提出單位:	美國國家標準與技術組織 (NIST)
	網頁位置:	http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
GASSP	制訂標準:	一般公認系統安全原則 (General Accepted Systems Security Principal)
	提出單位:	國際資訊安全協會 (ISC2)
	網頁位置:	http://web.mit.edu/security/www/gassp1.htm

清楚如何利用它。」

辜國隆處長指出, 由於我們的政府.gov 網域對大陸的直接連線皆已受到管制, 所以欲侵入政府單位的網站勢必以國內其它 ISP 或 TANET 學術網路做爲跳板。因此教育單位, 尤其是大學院校, 因爲法規政策不易強制執行, 使用者又缺乏基本的網路安全知識, 因此最容易成爲資訊安全防範的死角。我們身爲大學的電腦使用者, 若大家都能盡個人力量爲電腦做好基本的防護措施, 相信資訊安全事件一定可以大幅減少。

在大學院校所使用的電腦中,Linux 及 Windows 爲最多人使用的作業系統, 這二種作業系統皆有不少安全漏洞。但做好基本的防護措施其實不難。

根據美國著名資訊安全機構 SANS 與 FBI 所發表的二十大常見網路安全漏洞[1], 一般資安事件的發生, 可歸類爲以下七大原因:

· 安裝時採用作業系統或應用程式的預設值
· 不良的使用者帳號/密碼設定與組合
· 缺乏資料備份或是備份不完整
· 開放過多的網路通訊埠
· 未針對進出入的 IP 封包做過濾
· 缺乏 Logging 記錄的機制或是記錄不完整
· CGI 共通閘道介面程式漏洞

以 Windows 來說, 我們只要依照規範, 設定合適的密碼, 定期下傳適當的更新程式並定期備份, 便可消除以上所列大部份的威脅。至於 Linux 作業系統由於可以免費取得, 再加上其穩定性及易用性, 所以國內許多大學的實驗室網站都是使用 Linux 來架設。但也因爲 Linux 是一個 OpenSource 的作業系統, 代表著一旦安裝好 Linux, 全世界的 Hacker 都會知道你 Server 的一切細節, 包含所有系統的 bug 及漏洞。稱職的 Linux 管理員應該在 Linux 安裝完成後, 馬上做一些基本的安全設定。

以下就個人在 ICRA 2003研討會及在電算中心管理 Ap Server 的經驗, 整理出一些非常基本的安全設定程序。這些設定雖然簡單, 卻可以避免掉大部份的一般入侵行爲。

· 使用 ntsysv 去除不必要的服務: 常駐服務愈少, 代表外界連進來的管道愈少, 被入侵的機會當然也相對降低。一般來說主機都只會有一、二種特殊用途, 除了此用途之外的不必要服務應儘可能關

[1]http://www.sans.org/top20

閉。假設此 server 只提供 dns 服務, 那麼其它服務如 pop3、smtp 或 apache 等都必須儘可能去除。

· 更新 kernel 及應用程式最新版本 (openssl、openssh): Linux核心或應用程式的漏洞被發現後, 一般皆很快就有修補版本, 應隨時注意 CERN 等網安網站發佈的訊息, 即時加以修補。

· 修改/etc/hosts.allow 及 hosts.deny: 修改這二個檔案可限制連接到 xinetd.d 上的服務的 IP。(如 telnet)

· 改用 ssh 做系統管理: 如果從「成員衆多的 LAN 環境」上要 telnet 到你的機器上 (如宿舍), 有很大的機會密碼會被 sniff, 這時最好是透過 ssh 來連上遠端機器。

· 修改 issue.net: 在/etc/issue.net 是指當你從別台主機登入時, 所看到的畫面, 預設值會把 linux 的版本、kernel都印出來。爲安全起見, 我們應該要將它拿掉。

· 使用 iptables 過濾來往的封包: iptables/ipchains中, 共分三種 Chains(INPUT、FORWARD 及 OUTPUT), 及二種 Policy(ACCEPT 及 DROP)。若是一般情況下只做簡單的 INPUT Chain 的設定即可。

4 結論

資訊安全大師 Bruce Schneier 曾說:「Security is a Process, not a Product !」的確, 它一句話道破了資訊安全的迷思 – 沒有任何一個資訊安全技術或產品可以做到100%的安全防護。技術的背後, 還有賴人的參與及管理。

此外, 資訊安全威脅除了來自於 Internet 之外, 從許多調查報告中可以發現, 源起於內部的安全事件比例已經有逐年升高的趨勢。做好「系統層級」、「檔案層級」甚至「內容層級」的資訊安全管控則是防止類似事件發生的唯一方法; 包括帳戶權限、檔案 (資料) 存取權、存取記錄稽核與版本追蹤等等。

多數的資訊安全相關人員普遍認爲類似的機密資料外洩事件防不勝防, 因爲洩密者往往擁有合法權限去讀取機密檔案, 洩密者也可以合法地透過各種管道來傳遞所竊資訊, 這也是防火牆、防毒、入侵偵測、弱點掃瞄等安全機制防範不了類似事件的主因。因此, 對於過往只注重於「網路安全」的管理者而言, 資訊安全的觀念似乎也應該加以修正。不管安全威脅來自於外部或內部,「系統層級」、「檔案層級」管控都是資訊安全的最後一道防線, 也是最緊要的資訊安全管理任務。

相關參考資料

[1] 國家資通安全會報服務中心 http://www.icst.org.tw/

[2] DADO資訊安全教學網站 http://islab.cis.thu.edu.tw/

[3] 資通安全資訊網 http://ics.stic.gov.tw/

[4] 常見網路安全問題剖析 http://www.secucom.com.tw/service/download/column/020206/index.html

[5]「資訊安全」, 作者: 高大宇、王旭正、資訊密碼暨建構實驗室。博碩出版。

[6]「資訊安全入門」, 作者: 賴溪松、葉育斌。全華出版。

[7]「資訊安全理論與實務」, 作者: 陳彥學。文魁出版。

[8]「Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition」, 作者: William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin.