



Corporate Security on the Internet

By

Shad Mortazavi

Nexus Global Technical Manager

Nexus Management Inc

Corporate Security on the Internet

1

Published in: <http://newsviews.info/techbytes02.html>

NOTE: The information contained in this document is the property of Nexus Management and is disclosed to you on the condition that you maintain the information strictly confidential. You are hereby warned that the information disclosed is subject to change without notice or the assumption of any liability on the part of Nexus Management.

Introduction

In the early days of corporate security, firewalls and proxies were considered a sufficient tool to protect an organization on the Internet. For both the corporate entity and hackers, an Internet connection was expensive, computing equipment was fairly expensive and firewall technology was new and not very well understood.

Those days are over and have been over for a long time. Internet connections are now fast and cheap. Security exploits of all operating systems and security software are available for free on the Internet, and in many cases these are extremely well documented.

The expensive corporate security suite that you spend thousands of dollars on is available in its cracked format from numerous download sites. A skilled hacker will be well versed in the use of your security tool. In some cases this individual will have a test lab, where he or she will test techniques such as Firewalking -a method of discovering devices behind a firewall, Session hijacking- a method of hijacking a TCP/IP connection, to name but a very few, before testing their findings and skills against your system.

Once they find the vulnerabilities they may show off and post these vulnerabilities to a number of news groups, or they may decide to target your organization.

Even if your barrier to the Internet is impervious because you have taken the time and money to implement best practices, you may have your corporate web site, your corporate e-mail system, an FTP site for the download of demo's of your product, sitting within your DMZ. A skilled hacker will know how to exploit these systems, again using well documented and well tested exploits to gain a foothold within your DMZ, and then attempt to gain access to your internal corporate systems.

You may have taken time to invest in an Intrusion Detection Software (IDS) within your DMZ and Internal networks, thinking that if a hacker had access to

your network, you would know about it. You would be wrong; there are ways to evade IDS.

Last but not least, if the firewalls are the front door of your organization, like burglars, hackers will use the windows, they may war dial your organization, or they may gain access to your organization via your new VPN, or by exploiting a remote user sitting at his or her home working on the corporate LAN.

Although you're amateur hackers may not go to such lengths, the professional hacker, be it for money or the intellectual exercise, may go all out to compromise your system.

Like all Tech-Bytes articles the aim of this article is to make you aware of the challenges of corporate security and then to provide you with a number of possible best practices to combat these vulnerabilities. The rest of the article concentrates on some of these good practices.

Good Corporate IT Practices

Before you spend thousands of dollars on security software and hardware, take some time to plan your security strategy, how you are going to enforce security within your organization and identify some good practices that can be followed. These will help reduce the number of backdoors into your environment.

Good corporate IT practice needs to involve your human resources department, representatives of the user community, management, people who understand the business needs of your organization, finance and last but not least your IT department. Some of the key decisions that need to come out of these meetings are:

1. **Policy on Internet Access:** - What resources on the Internet do you give your users access to? Do you give all your users access to every service on the Internet? (Hopefully the answer to this question in no!), or do you make a list of resources and work with H.R and IT to enforce these? It is just as important to define outbound Internet access as it is to control inbound Internet access.

2. **Policy on Instant Messaging:** - IM is a good example of how you can save money on phone bills and communicate with online consumers in real time. Many users will utilize an IM of some form or the other. Unfortunately in most cases these are publicly accessible resources which can be exploited. Consider using your own IM server in your DMZ such as Jabber.
3. **Policy on E-Mail Usage:** - All your e-mail systems should be protected by anti-virus Trend Microsystems and Symantec. This is not always enough and there needs to also be user education. For example, a part of user induction should involve explaining the risk of opening certain attachments that you receive via e-mail. In some instances companies will filter out extensions, only to be bitten by users opening personal e-mail on external web based e-mail systems.
4. **Policy on the Use of Modem:** - Modems are one of the windows into your corporate network. If you need modem access in or out of your network consider housing these modems in your DMZ and shutting off these systems when not in use. When considering modems on the network please do not forget that many laptops will have these installed.
5. **Policy on the Installation of Software:** - All software should be tested, documented and installed by your IT department. Many backdoors are hidden in shareware/freeware software. A special group to keep an eye out for is the screen savers.
6. **Anti-Virus Policy:** - Modern day AV software has the ability to find many backdoors and Trojans that could be used to compromise your network. Ensure that all workstations/servers and applications are protected Trend Microsystems and Symantec.
7. **Remote User Policy:** - It is very important that you keep these individuals well-guarded. They may be using VPN and/or Remote Dial up to access your corporate data. Guidelines for remote users can be found in the first article.

8. **Policy on Commissioning new external services:** - If you are going to commission a new external service over the Internet, research the security of the organization fully and ask for a guarantee of security.
9. **Policy on User Names and Password:** - Make sure that passwords are changed as frequently as possible, at least every 2-3 months. When users leave the organization the account must be rendered unusable/ or deleted immediately. Consider the use of a password cracker such as John the Ripper, LC3 and/or Brutus to check the strength of your users passwords. Refrain from the use of the Admin/Supervisor and/or root accounts.
10. **Policy on Physical Security:** - Store your core computing equipment, in a secure room and/or cabinets, with restricted access via keys, numeric pads, swipe cards and/or bio-scanners. If your data is very sensitive deploy alarms and security cameras.
11. **Patches, Updates and Hardening:** - This is a golden set of rules for the system administrators. Never deploy a system without patching it with the latest security patches, service packs and/or updates. Once you have built a system, make sure that it is only running services that you expect it to be running. Have a daily look at security sites such as Security Focus and Eye-on-Security.

The Security Audit

Again before you spend thousands of dollars on equipment, consultants and software, take time to run vulnerability scans. There are two powerful tools that can be used to check for vulnerabilities. Please take great care when using these tools and always get permission if using these tools to check vulnerabilities on other peoples systems

- Nmap: - This is a very powerful port scanner, with the ability to fool some of the weaker firewalls. It has the ability to sweep a range of network addresses making it an ideal tool for initial assessment.
- The Security Administrator's Integrated Network Tool (SAINT): - A wonderful indispensable tool for checking the security vulnerabilities on networked systems. It offers an explanation of the vulnerabilities and good organization of data for report writing.

Make it a habit to run these audits on a regular basis, on your internal network, external network and DMZ. Whenever you build a system or update a system run a scan against the system to make sure that you have not inadvertently opened up a port or picked up a vulnerability. Keep a record for future comparison.

Constantly look through sites like Security Focus and Eye-on-Security to make sure that you are aware of new exploits. Update your tools to reflect the change. If there is an announcement of a major vulnerability, update your tools, run your scans and patch your systems where appropriate.

Once you are happy with the state of your system you will want to implement change control to keep the systems in order, you may also consider using a tool like:

- Trip Wire: - This will allow you to keep an audit of your critical configuration and system files. Enterprise wide configuration of this type of product is the subject of next month's article.

Last but not least, perform password audits of all systems on a regular basis. Work with HR to make sure all user accounts E-mail, Print and File, Intranets are current.

The Security Infrastructure

One of the keys to a secure infrastructure is to present as many challenges to the intruder as possible.

However, the minute you decide to create a DMZ, with the purpose of giving remote users access to the company intranet, you open up your organization to possible exploits.

One possible construct for securing your network and creating a secure DMZ is to make full use of Stateful Packet Inspection engine and a Proxy in series. The logic behind this is that both security gateway technologies are subject to exploits. Many of the exploits such as the 'man in the middle attack' and 'session hijacks' used for attacking Proxy servers are detected by the Stateful Packet Inspection, and Proxies are impervious to Firewalls. In addition the use of a

caching Proxy server can give you a 30% performance gain on your Internet browsing.

Good firewalls that you may want consider;

- Checkpoint Firewall-1:- Very good industry standard product with an excellent reputation.
- Cisco PIX 500:- Again an Industry strength long-standing product.
- Astaro: - A good product with good reviews, good web based GUI and great performance.
- Microsoft ISA: - A great improvement on the previous versions of the product with built in IDS.

Good Proxies:-

- TCP/IQ: - A great product, very visual, with the ability to log all connections and to view all the data passing through the proxy in real time.
- OSTIS Win proxy: - Product with some very good features, including AV scanning, content filtering, banner blocking. A very visual product.
- Squid Web Proxy: - Has been around forever. A choice for many ISP's due to its amazing speed and efficiency, a great product, if configured with security in mind.

Within your DMZ, Consider securing all web based applications using SSL/TLS. This will ensure that transactions involving user names and passwords are encrypted.

Mail Services such as POP3 /SMTP and IMAP can be secured using SSL, as can Instant Messaging. Implement User Secure FTP to secure FTP transfers.

At the very least place Anti-Virus on all your systems, Symantec and Trend Micro produce good products. They have specific products that are well suited for Proxies and Firewalls. You would also be well advised to trip wire your systems.

If you use Telnet for administration consider switching to SSH. If you need to provide your external users with remote access consider using a VPN client to

secure the transaction. There are many VPN clients available, SafeNet, SSH (In pilot, Linux version coming soon). Major advantages of VPN's include;

- Eliminate the use of modems (Modems are a big security risk)
- Encrypt all data transmissions
- Allow remote working from any location, regardless of distance,

The installation and management of VPNs can be a complex procedure with a high cost of ownership. You may wish to consult an external company for your needs. Nexus Management Inc. has extensive VPN knowledge and experience.



As depicted by diagram 1 (click to enlarge), you may want to deploy multiple IDS's to check activity outside your firewall, your DMZ and internal network. Distributed and

Enterprise wide IDS is considered one of the holy grails of Security and will be covered in next months articles.

One IDS worth considering is Snort. To compliment this IDS, you may use tools like Snortsnarf and/or ACID to manage the data collected by snort.

Conclusion

Security is about being alert to all potential threats. It is about taking the minimum number of risks, and careful planning of your security infrastructure. It is also about establishing good policies and maintaining those policies.

Security is one of the most challenging areas of IT and also one of the most interesting and rewarding areas.

If you are interested in further information on this market, please contact Nexus management at +207 319100

