Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b Option 1

Sandra Davoren
November 2003

Security Considerations for Small Businesses to Achieve Defence in Depth.

Abstract

This paper discusses the security considerations that should be taken into account by a small business to achieve defence in depth. The paper focuses on maintaining the balance between providing a successful IT security solution whilst achieving this on a small budget with the least amount of administrative overhead.

In this paper I discuss the different types of security solutions available today for a small budget and conclude with my recommendations on how a small business can achieve defence in depth.

Introduction

A number of small businesses are left behind when it comes to IT security. They often do not have the staff, skills, time or budget to keep up with the fast changing industry. Trying to maintain the balance between what a business needs to suit its requirements with how much that costs can prove to be a difficult problem.

Below are some issues that should be considered by a small business when planning defence in depth.

1) What is the budget for security?

This is probably the most important factor to consider, which also causes the biggest problem for small businesses today. Security comes at a high price and for a lot of small businesses, the budget often is not there, leaving the business vulnerable.

There are a variety of cheaper alternatives and freeware security solutions available on the market today to help address the problem of budget that many small companies face. These security solutions are discussed below.

When working out the security budget, you need to consider two things;
- What do you need?
- How much will it cost?

2) What data do you need to secure?

Deciding what sort of data you want to secure is very important when trying to balance budget. You need to decide what data you want to secure, what are your 'Crown Jewels', so you can plan a security solution. This could be data such as, information held on database servers accessed by customers over the Internet to make on-line purchases. Such databases may house customer details and credit card numbers and would therefore be a critical area of the business. Other data to secure could be data such as company accounts, staff salary and staff personal information.

3) What security solutions should you put in place?

The key to securing a network is to use a layered approach to security. On its own, one security solution will not have a major effect in securing an unprotected network but used in a layered approach, it will have a much more significant

effect. The chosen solution should be a flexible strategy that allows adaptation to the changing environment we live in.

The main forms of communication small businesses use are e-mail, Internet, telephone and fax communications. The use of e-mail and the Internet, immediately pose a threat in themselves for the reason that as soon as a network is connected to the Internet, it is open and vulnerable to attack. Small businesses are moving towards using Broadband Internet access, which makes the threat of attack, even more prominent.

Broadband users are often assigned unique static IP addresses, to define their computer and/or network on the Internet. As this address rarely or never changes in some cases, unlike with dial up, where your IP address is different each time you dial up, it makes it easier for attackers to find you on the Internet. Additionally with Broadband, you are always connected to the Internet, which gives hackers more opportunity to access your computer as well as being more attractive to them because of the high speed of the connection.

Below are security solutions that are available on the market today for a small business. The idea behind these solutions is to provide a good quality, cheap security solution, requiring little administrative overhead.

A1) Network Firewalls -

Typically the first line of defence, a firewall acts as a doorway into an organisations network, which is used to control access to and from the protected network. A firewall on its own can not fully protect an insecure network but used as a layered approach with other security devices, it can be extremely effective. A firewall rule base or policy is based on a set of rules, which determine what is accepted, rejected or dropped by the firewall. These rules should enforce the businesses security policy.

The 3 main types of firewalls are:

- Packet Filter Firewalls -

  These are the cheapest, fastest and simplest types of firewall on the market. They are often loaded on routers and the disadvantages of these firewalls are they are the least secure, provide poor logging and minimum granulation. For these reasons, this type of firewall is only suitable for a low risk environment.

- Application Proxy Firewalls -

  With these firewalls connections are made to the firewall and then the firewall makes connection to the Internet and visa versa. Proxy firewalls are granular

and have good logging abilities. The disadvantages are they can have slow performance and changes may need to be made on client workstations when using some products.

- Stateful Inspection Firewalls -

These are advanced and secure firewalls that examine the contents of packets rather then just filtering them. These firewalls inspect the connection status of packets, checking that an incoming packet matches up with an outgoing request. A disadvantage of these firewalls is that they are more complicated to configure.

Most modern Firewalls combine all types of Firewall technologies within them.

Examples of firewalls appropriate for a small business are:

- Checkpoint Safe Office 225

This is a stateful inspection firewall designed for a small business with public-facing servers. Some features of this firewall include enhanced firewall/VPN performance whilst also providing a secure, reliable Internet connection.

- Cisco PIX 501

This is a stateful inspection firewall, which provides a multilayered defence including VPN and basic intrusion protection [1]. This is an ideal firewall for broadband environments, which are always open to attack. The main disadvantage with this firewall is without prior knowledge of Cisco's command line syntax, PIX can be difficult to configure and manage.

A2) Personal Firewalls

As well as using a firewall on your gateway or internal network, another way to provide defence in depth is to install a personal firewall on workstations on the network. Personal firewalls protect the individual computer itself and the data on it rather then the network behind the firewall. A personal firewall is important when using broadband access to the Internet. Some examples of personal firewalls are below.

[1] "Cisco PIX 501 Security Appliance. " Cisco Systems.

- Zone Labs ZoneAlarm

Boasted as one of the best and most widely used personal firewalls. Advantages are that it blocks inbound and outbound connections to the Internet. The commercial version has extra features, which include, e-mail attachment protection, password protection and advanced logging. ZoneAlarm is free for personal use.

- Sygate

This is a popular personal firewall on the market, which has the advantage of blocking inbound and outbound connections to the Internet. Sygate boasts that this firewall is easy to use and configure. Sygate is free for personal use.

- Windows XP

Windows XP comes with its own free built in Personal firewall, which is very easy to use. This is a very basic personal firewall, which will save money if your budget is limited.

B) Intrusion Detection –

Although a firewall will help block attacks from entering a network, it is important to know what attacks are bypassing the firewall. This is where Intrusion Detection comes in. There are two types of Intrusion Detection (IDS), host based and network based. Host based IDS monitor activity on a host, where as network based IDS, monitor activity over a network. In most cases these solutions are based on having host and/or network sensors, which report activity results back to a central core known as the IDS Manager. IDS systems fall at the high end of the cost scale although there are some free intrusion detection tools available. Intrusion Detection systems provide useful and sometimes invaluable information about host and network activity, but for a small business this is one security solution which may not be a priority. To successfully configure and maintain an IDS, takes a lot of effort and comes with large administrative overheads. Some examples of IDS products are below.

- Tripwire

This is a host based intrusion detection tool, which detects file system changes and shows what files have been modified. With Tripwire a snap shot is taken of the original file so that changes can be detected and the file put back to its original state. A commercial version is also available with improved functionality.

- Snort

This is a popular open source network based intrusion detection tool, which is efficient, lightweight and low cost. With snort you have the ability to write and customise your own rules to suit your network and it has good logging abilities. A commercial version with extra functionality is available from Sourcefire

C) Anti-Virus –

Anti Virus solutions are essential, especially in the environment we live in today, where e-mail is a critical means to carry out daily business.
For a small business, the types of anti-virus products I have looked at are ones that are as automated as possible and therefore require little administrative overhead. Some examples of anti-virus products are below.

- Norton Anti-Virus

Norton Anti-Virus solution protects against viruses, worms, Trojans and dangerous malware [2]. The main advantage of this AV product is that is offers automated updates for product software and virus definition files and can be centrally managed with the corporate edition. This is a huge benefit for a small company where resources and time are likely to be few and short.

- Vcatch Anti-virus

This is a free but basic anti-virus tool, which runs on Windows. The software installs itself and automatically updates virus definition files daily. This tool uses an advanced malicious application detection system, which scans all incoming files for suspicious characteristics, which can help detect and block new viruses and worms [3].

D) Encryption -

Encryption is a way to code data, which prevents any non-authorised party from reading or changing it. Encryption could be used to secure information such as customer data, credit card details and company accounts. Encryption can also be used to secure data sent via e-mail so that if the e-mail is intercepted, the data is unreadable. Some examples of encryption products are below.

[2] "Key Features." Norton Anti-Virus.
[3] "Consider These Low Cost Anti-Virus Solutions." Tech Update Security.

- PGP (Pretty Good Privacy)

This is probably the most widely used encryption tool. For home use it is free with a commercial version available for corporate usage. It has the benefit of being simple to use.

- PowerCrypt

This is an encryption tool for Microsoft Windows, which is free for home use. It can be used to send encrypted e-mail attachments, to encrypt multiple files and to compress data to save on disk space.

4) How to address Internet security vulnerabilities?

"A vulnerability is a weakness that a person can exploit to accomplish something that is not authorised or intended as legitimate use of a network or system." [4]

Even with extensive security solutions in place, Internet security vulnerabilities are always an issue, with new vulnerabilities being announced daily. Once you have set up and installed a security solution, it is vital that those systems are kept up to date and patched, otherwise security holes will start to appear that can be exploited. An example of a recent exploit was Nimda, which exploited security holes in Microsoft's commonly used IIS webserver. Once infected, Nimda could spread across an entire network rapidly. Whilst the vulnerabilities were known about for some months before Nimda appeared, many businesses did not update their systems and were subsequently infected.

There are many different types of vulnerabilities consisting of flaws in software and protocol designs, weakness in software implementation and weakness in software and network configuration. A protocol design vulnerability is NFS used in Unix based operating systems, which allows a system to share files. Weakness in configuration occurs when default configurations are left on systems. This leaves the system open to exploit not only externally but also internally.

One way to keep up to date on vulnerabilities as they are discovered is to sign up to an Internet security mail group such as, Security Focus's Bugtraq.

There are several freeware tools on the market that can be used to scan systems for vulnerabilities, which could be exploited by attackers. It is important to know your network and know what systems run on your network to ensure they are not vulnerable. One such tool, which can be used to map out a network, is Nmap.

[4] Marcel Dekker.

Nmap can also be used for port scanning to find out what ports are open on your systems, which could be vulnerable. Nessus is another free open source tool, which can be used for vulnerability assessments. Nessus gives you an output of critical to low priority vulnerabilities. Addressing vulnerabilities can be a very time consuming job, especially for a small business. For this reason, it is advisable to address the top 20 critical vulnerabilities first. These can be found on the SANS website http://www.sans.org/top20/
Another way to keep a Windows system up to date and patched is to run 'Windows Update' from Internet Explorer Tools menu.

The major issue with using any of these freeware tools is that they often require a Unix based operating system to run on, their output is often difficult to interpret and installation is not always easily accomplished.

5) Introducing Security Policy.

A security policy is a documented plan for an organisations computer information security as well as physical security. It should contain guidelines and procedures for users and administrators to protect people and information. To avoid a security policy outdating, it should not be technology specific. The policy should be a simple and concise document that anyone even without a technical background can read and easily understand.

A security policy should be used and enforced by organisations security devices.

Security policies have gained a great deal of importance in recent years since the development of the British Standard Code of Practice for Information Security Management (BS7799), which was developed into an international standard ISO17999. This was developed to protect customers and ensure businesses were providing a secure service.

There are 3 main types of policy:

- Local policy – contains information specific to the organisation.
- Issue specific policy – contains specific information such as anti-virus or password policy.
- Procedures and checklists – e.g. standard operating procedures.

A security policy should contain the following type of information:

- Risk analysis –

  Identify what the businesses assets or crown jewels are. What the threat against them is and what the cost of loss of those assets would be.

- Roles and responsibilities –

Details those people responsible for ensuring the procedures in the security policy are adhered to with guidelines of their roles and responsibilities.

- Remote access procedures –

The procedures to be followed by staff for remote access to the internal network. These may include constraints such as authentication and the requirement for a personal firewall to be installed on the machine making the remote connection.

- Password policy –

The procedures to be followed for password security. These should detail how often passwords should be changed, password length and how to store passwords. The standard is that passwords are a minimum length of 8 characters with the use of at least one non-alphanumeric character. Passwords should be changed frequently, I would recommend once a month and stored securely in an encrypted file. Procedures should contain advice on keeping passwords private to the individual and warn of processes such as social engineering to obtain passwords illegitimately.

- Backup procedures –

The procedures to be followed for carrying out critical system backups. These should include details on how often backups should be performed and tested to ensure they work and where backups should be stored. Procedures for disaster recovery (DR) and contingency may also be included here. I would recommend that critical system backups are performed daily and backups stored off site to enable DR.
Since the September 11th terrorist attacks, DR has become more of a priority to all businesses. If critical systems fail, without backups, a business would no longer be able to operate resulting in huge loss of revenue, which would often, be difficult to recover from.

- Vulnerability procedures –

The procedures for vulnerabilities assessments (VA), how often these should be carried out and how to address vulnerabilities. I would recommend that a VA should be carried out every 4-6 months and that the top 20 most critical vulnerabilities be addressed first. All publicised critical vulnerabilities should be patched immediately. To keep up to date with publicised vulnerabilities as they are discovered, I would advise to sign up to an Internet security mail group.

- Anti-virus procedures –

The procedures to be followed for configuring and updating anti-virus (AV) software and virus definition files. I would recommend that AV software is updated each time there is a new software version available and that virus definition files are updated weekly and as soon as any major virus outbreak is announced. AV software should be configured so that users can not disable it and regular virus scans of the hard drive scheduled. I would also recommend that AV software be installed on any machines used for remote access to the internal network.

- Firewall policy –

This should detail the type of traffic and services allowed through the network firewall as well as information on how often the firewall should be audited. The firewall audit should be compared against the security policy for any breach in policy. I would recommend a network firewall be audited every 4-6 months. Always have a procedure for exception to the policy for unique circumstances, specifying who will give permission for exceptions and take responsibility to review and follow them up.

- Data protection procedures –

The main difference between one business and its competitor is its data. Procedures should include steps to be taken to stop sensitive data being shared with competitors and other staff. I would recommend that sensitive data be encrypted and signed agreement is sought from staff to adhere to these procedures. Data protection also applies to personal data, such as e-mail.

- Security breaches –

A guideline as to what constitutes a breach in security, what actions should be followed if this occurs as well as the consequences. I would recommend advice on how to deal with the media and other third parties in the event of a major security breach are included in this section.

- Physical security –

The procedures to be followed for physical security, including physical access to the building. Security passes or swipe cards could be used for physical access to add an additional layer of security. Laptops, desktops and other security devices should be locked down and secured. I would also recommend that no unauthorised modems be connected to the network, which will reduce the risk of unauthorised entry to the network through unknown points.

Conclusion

I have discussed to some extent the considerations that should be taken into account when planning defence in depth for a small business. Although you can never entirely defend a network from attackers or provide an unbreakable security solution, you can build a good defence by providing a layered security solution. I have discussed some options for providing such a layered solution on a small budget including utilising freeware tools available on the market today. While such tools are cheaper to procure, they may be more expensive in terms of human resources and administrative overhead, therefore this should be considered when planning a security solution.

My recommendation for a small business is to use a layered approach to security. In order of importance, I would recommend as a priority that a desktop AV solution and network firewall be introduced first if budget is limited. There are some all in one solutions available on the market, such as Symantec's all in one solution which combines AV and content filtering. I would also recommend signing up to an Internet security mail group to stay up to date with the latest vulnerabilities and to patch all systems against critical vulnerabilities. Finally it is imperative to have well documented processes and procedures, which can easily be followed by all staff as part of a security policy.

Securing a network is not a case of having the most expensive tools but more a case of having a well thought, well planned, up to date security solution, which will provide Defence in Depth by using the most appropriate tools for the environment.

References

Cole, Eric, Fossen, Jason, Northcutt, Stephen, Pomeranz, Hal. Sans Security Essentials with CISSP CBK V2.1 Volume 1. USA: Feb 2003. 347-361 & 650-673.

Network Security Fundamentals. Atlanta, USA: Internet Security Systems Inc, November 2001. 184-191.

"Product Review Zone Alarm Personal Firewall." 30 July 2002. URL: http://www.theguardianangel.com/product_review_zonealarm.htm (20 Oct 2003)

"Making Open Networks Trustworthy." URL: http://smb.sygate.com/products/spf/spf_ov.htm (20 Oct 2003)

Muchmore, Michael W. "Windows XP's Built-In Firewall." PC Magazine. 26 Feb 2002. URL: http://www.pcmag.com/article2/0,4149,2230,00.asp (22 Oct 2003)

Cody, Larry. "Small Business Firewalls." A Smooth Solution to a Big Problem. 5 Aug 2002. URL: http://download.smoothwall.net/pdf/20020508.asn.pdf (22 Oct 2003)

Geroski, Ray. "Consider These Low Cost Anti-Virus Solutions." Tech Update Security. 25 June 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2872106-2,00.html (24 Oct 2003)

Dekker, Marcel. "Security of the Internet." CERT Co-Ordination Centre. 1997. URL: http://www.cert.org/encyc_article/tocencyc.html (24 Oct 2003)

"Freeware Security Software." URL:http://www.freestuffer.com/software/security.html (24 Oct 2003)

"Cisco PIX 501 Security Appliance." Cisco Systems. URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b18.html (24 Oct 2003)

"Key Features." Norton Anti-Virus. URL: http://www.symantec.com/nav/nav_9xnt/features.html (24 Oct 2003)