White Paper: Best Practices for Network Security in Small and Medium-sized Businesses

Introduction

Very few businesses can function without a network of computers. Be they Windows or *NIX based, communication is the name of the game. Unfortunately allowing your computers to communicate with each other does have inherent risks, whether that be malware or unauthorised access.

However, if managed carefully a good security policy can dramatically lower the risk of these threats. Being a small business does not shield you from the attention of Cyber-Criminals, depending on your business area it may even make you more of a viable mark.

Getting Started

Your very first task in creating your secure network is to carefully draft a security policy, this policy should contain the rules that your employees must adhere to. You should consider every perceived threat when drafting your policy, no matter how unlikely it may seem. Include policies on the use of removable media, Password Management, Internet facilities and e-mail. Also make your employees aware that all activity will be logged and could lead to disciplinary action.

Plan the Network

Once you have created your first draft, it's time to begin planning the network itself. It may be that you have a network in place already and are reviewing security, if so plan the security from scratch to ensure you haven't assumed that a defence is already present.

The first consideration is, does your network need to connect to a Wide Area Network, be it the Internet or a corporate one? Is it absolutely necessary? If it is, then you should consider whether the WAN is considered secure. Regardless of whether you believe it is or not, you will require a firewall, maybe even two. Whilst many would recommend software firewalls, it is generally better to purchase a hardware firewall. This is simply a dedicated unit for running a software firewall, and most are as easily configurable as Client Based firewalls. The added protection of a hardware firewall is that users will have a harder time bypassing it (Most users will fiddle with any firewall software on their PC). A hardware firewall should be placed at your networks 'entry point', that is the link between your LAN and the WAN. This will help prevent an intrusion getting onto your system at all.

Alternatively you can use client based firewalls, and it would be wise to consider them as an additional measure. Some software firewalls will cause problems when you make changes however. If, for example, your company were to utilise a new bit of software that communicated on port 1078, you would need to configure each and every node to allow connections on that port. With a Hardware firewall located at the Point of Entry this change can be made globally.

A Firewall is not enough

Although firewall manufacturers would have us believe otherwise, it is possible to get through a firewall. Sometimes due to a bug in the code, sometimes due to mis-configuration, so you do need additional defences in place. Setting up a domain is a good way to restrict access to resources, depending on your Operating System there are different methods of doing this. The most popular method, at time of writing, is to use a Kerberos Server. This can be obtained from Microsoft in the form of Active Directory, but there are other alternatives available. Once you have configured your domain you should restrict access on all your network attached equipment to that domain.

This includes any networked printers you may have, many people fail to understand that a networked printer contains a very basic computer. These can be compromised in the same way a computer can. Do not take anything for granted, if it connects to the Network, lock it down.

Restrict Write Privileges

For the purposes of portability as well as data safety, it would be wise to assign your users roaming profiles, and store all their documents on a central server. Deny them write access to their local hard drive (or if suitable, use thin clients instead). This will help prevent users from removing data from the office, especially those users who use laptops. If it is stored on a central server, then it is harder for them to take the data with them without authority. Of course, if you have not restricted the use of removable media then they can quite easily leak your sensitive data. Never use generic passwords or user accounts, maintain user accountability be restricting each user to their own login.

Good Password Policy

Ensure that you define password complexity requirements, and limit the lifetime of a password. Most organisations will require a user to change their password after 90 days, depending on the sensitivity of your work you may need to shorten this. You should also utilise the ability to force a password rotation, many users will change their password back tot heir old password if they can, force a rotation of at least three password and ensure they are alphanumeric.

Users should not be permitted Administrative privileges, employ someone to posses that right (assuming you are not completing the role yourself). The damage a user could do with Administrator rights is horrifying, and may cost your business dearly.

Manage your Data Exchange

Similarly, the leaking of private data should be considered. Disallow access to all E-mail systems except authorised ones. Ideally, you will have implemented a mail server and restricted all E-mail to this server. This will provide you with non-reciprocity (you can verify an e-mail was sent by a specific user), the ability to log all communications and the ability to ensure employees are not mis-using your system. Ultimately your staff are employed to work, not to e-mail family on the other side of the world.

Monitor System Health

The use of Anti-virus should also be implemented, ideally there will be an 'On-access' scanner so that infections can be caught before they happen, and a scheduled scan. The scheduled scan would ensure that your central server is clean, and also check the users Home Directories for anything that has been missed. The use of roaming profiles will also allow you to check their UserData for tracking cookies, spyware etc.

Manage Content

If a connection to the Internet is necessary, implement a proxy server to log and restrict net access. This will allow you to monitor what is being accessed, and to block anything that should not be accessed in the workplace. This may even protect you from legal action, in some areas users are able to sue their bosses for allowing the 'purveyance of obscene material.' It would also be wise to block all Java and Javascript that passes through the proxy, this will help reduce the likelihood of malicious code being executed on an office machine. If an exception is needed, most proxy servers will allow for this.

Ongoing Changes

The most important ingredient for a secure network is educated employees, if they do not know that consequences of running a program they will do it anyway.

Once you have implemented your security precautions, return to your security policy and ensure that it meets the requirement of the network and vice versa. Users should be made to sign a copy of this policy before they are given a user account. If a user is found to be sharing passwords then disciplinary action should follow, you should also make it clear to users that they alone are responsible for any activity that happens under their user account. You might also consider configuring the terminals to display a warning before the log on screen, reminding them that unauthorised access is prohibited. The warning must require user action to continue.

Users should be made to re-sign the policy whenever it changes, and at regular intervals even when unchanged. Some companies set a 6 month time line, others vary. If a user has not signed, do not allow them access to your resources.

Run regular data backups, these may be to magnetic or optical media. You may even consider subscribing to an off-site backup solution provider, but always backup. Backup media should be stored separately to your central server, and should be in a secure location. You should also maintain a copy of the backup in a secure off site location.

Security within reason

Many people are under the delusion that there can never be too much security in place, unfortunately this is untrue. If your security policies are too draconian they will stop your users from doing the work they are paid for, this will result in two things. Your workers will be unable to work, so your business will be less productive, and many users will try to circumvent your security procedures. It is very important to achieve a balance when implementing security, internal users are the most dangerous threat as they already have access to your resources.

You can, however, never review security procedures to regularly. Regularly asess whether your current measures are sufficient, and implement changes as needed.

Conclusion

There are a number of measures that you can implement to secure your network. However these need to be carefully planned and implemented with thought to requirements, future requirements and possible threats. If a system is to be secured it needs to be secured properly, a firewall will be of little benefit if you allow users full access to all your data. Threats can be internal as well as external, disgruntled employees are a SysAdmin's nightmare. Users able to access any website they want will bring trouble to your business, whether it be a malware infection, an employee who sits on Ebay all day or leaks your sensitive data to competitors.

Never allow employees Administrator rights (let alone superuser rights), restrict un-necessary access to the outside world, and ensure your employees know of the expectations laid upon them. Remind all users regularly, and review your security practices even more regularly.

About the Author

Ben Tasker is an IT Manager & Linux Specialist at Virya Technologies. He has substantial experience within the IT Industry, and a keen interest in Network security.

More whitepapers and free resources available at http://www.viryatechnologies.com/