Network security:

A guide for small and medium businesses (SMBs)

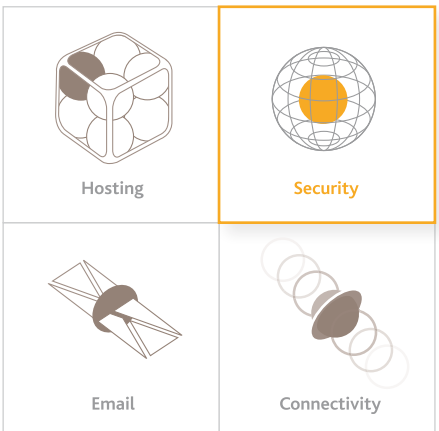
A Star Technology White Paper

March 2008
www.star.net.uk

Summary

Network security is essential as it helps to prevent threats from damaging your business. Business use of the Internet has rapidly increased and organisations are becoming more reliant upon IT infrastructure to operate their business.

This paper provides a summary of key issues, threats and risks SMBs need to consider along with how to combat these to ensure network security. It reinforces the importance of planning and the benefits of working with an IT security specialist.



Introduction

Network security is an essential part of the network, preventing the many threats from damaging your business.

"Star's broadband solution has opened up a world of online resources to our staff, enhanced internal communications and dramatically improved IT support."

Graham Parker, IT Manager, PDSA

Business use of the Internet has rapidly increased and organisations are becoming more reliant upon IT to operate their business infrastructure. According to the DTI Security Breaches Survey (2006), 1 in 6 businesses could not operate without decreasing the cost of Internet connections and 88% of businesses that have a connection now utilise broadband as their main connection to the Internet.

However, the Internet brings with it a series of added security threats. Your Internet connection is a two-way street, your computers and networks can be visible on the Internet 24 hours a day. Just as you can effortlessly access the Internet so too can the rest of the connected world and they are able to access your computers and network with similar ease.

Although computers have been subject to attack from viruses and worms for many years, businesses assume this security risk is well under control. However, virus writers are now using more covert methods to deploy their attacks and penetrate networks, which often lie undetected until damage occurs. The MessageLabs Intelligence: 2007 Annual Security Report states that average virus levels for 2007 were 1 in 117.7 (0.8%) emails and although virus levels rose and fell throughout the year, September reached the highest virus levels in 18 months, with 1 in 48 emails containing a virus or Trojan. The report also states that 2007 saw cyber-criminals changing their tactics and favouring the method of including links to malicious web sites hosting the malware code, rather than attaching the malware itself. Further analysis revealed that the proportion of email-borne viruses that contain malicious links has increased from 3% at the beginning of 2007 to approximately 25% by December 2007.

The curse of spam

In today's sophisticated business environment, spam is increasingly being used as a delivery mechanism for viruses, spyware, phishing and hackers. Over the past few months, there has been increasing evidence that spammers are using virus-writing techniques to improve the chances of getting their message across. At the same time, resourceful virus writers have latched onto spammers' trusty mass-mailing techniques in an effort to wreak widespread digital mayhem.

According to the MessageLabs Intelligence: 2007 Annual Security Report, the overall trend for spam remained fairly stable with 84.6% of emails intercepted being identified as spam. However, the proportion of spam that is new and previously unknown has increased; it is more sophisticated and difficult to stop when using traditional anti-spam software and appliances.

Failing to plan = planning to fail

"…the average cost of a security breach is up 50% from 2 years ago at £12,000 per incident…"

A single attack can be devastating, with all your valuable data wiped out, confidential information stolen or corrupted, your entire network made inoperable, or access to vital for your business operations shut down. Many analysts believe the prime reason for rapid spread of these attacks is because network security can be significantly lacking. Network security is an essential part of the network, preventing the many threats from damaging your network and business.

The DTI Information Security Breaches Survey (2006) revealed a number of interesting findings with overall businesses being more aware of the importance of security and the implications of a breach. Of those companies surveyed the median of security breaches is 8 per year, 62% of businesses have been the victims of a security incident, of which, 29% was due to accidental systems failure and data corruption and 52% due to premeditated malicious incidents. Demonstrating the growth in security attacks, the average cost of a security breach is up 50% from 2 years ago at £12,000 per incident, resulting in 3-6 days of downtime, not to mention damage to reputation, loss of revenue and breach wof confidentiality.

When a crisis emerges, knowing how to react and respond is critical as it can result in either success or failure and ultimately determine whether or not your business is able to survive. The ability to anticipate potential threats is a key part of the planning process.

A small/medium business will need network security if it has:

- A connection to the Internet
- An internally hosted website or any website that handles e-commerce transactions
- Employees that require remote access to the network
- Data that is held in business systems

Network threats and risks

Back in the mainframe age, network security was simple – it meant locking the computer room, only allowing access to authorised individuals. This is no longer the case and the nature of the threat facing small and medium business networks has expanded dramatically.

The threat no longer comes through a single entry point like the ubiquitous floppy disk, but from multiple entry points to the network, such as the Internet gateway, Virtual Private Network (VPN) links, remote access servers, email, wireless Local Area Networks (LANs), handheld devices and even employees.

The security threats facing small business networks can be broken down into the following categories:

Viruses and Worms

Often spoken of in the same breath, viruses and worms are subtly different creatures. Like its counterpart in nature, a computer viruses' primary function is to replicate and 'infect' healthy files in its host computer and then spread its infection to other healthy computers. Typically, a virus will replicate itself and try to infect as many files and systems as it can. There are many types of virus, some mostly harmless, some very harmful. Either way, because they have to be eradicated to stop them from spreading, they are always bad news. Viruses originally used to spread via infected floppy disks but these days they are more typically spread via email or file downloads, which accounts for the speed with which the entire world can be affected by a single outbreak. Users unknowingly open a file or run an application, without realising that it has been infected, this causes the infection to spread to other files or network resources.

A 'sub-species' of the computer virus is the worm. Like other viruses, it too is a self-replicating programme. However it doesn't necessarily infect other programmes. Instead it proliferates across networks and the Internet, typically using your email address book to send infected emails, but there are other transmission methods. Once on your Local Area Network (LAN), worms can damage data or cause computer crashes. Users can quickly damage entire networks by unknowingly downloading and launching dangerous computer worms.

MessageLabs Intelligence: 2007 Annual Security Report highlights that the introduction of more advanced products and services to address virus concerns is improving however, it is getting easier for virus writers and cyber criminals to inflict their wares upon Internet users predicting a year of virus growth for 2008.

Trojan Horses

As you might expect, a Trojan horse is a small program that sneaks in under the guise of being useful or entertaining and bides its time until it is ready to reveal its purpose. Trojans can destroy files, but they are more commonly used to create a back door for hackers to access and control your computer or to take part in an attack on a remote computer. They can give full access to the computer, including access to file system and even real-time keystrokes but do not replicate like viruses and worms.

Blended Threats

Blended Threats are a breed of attack, heralded by the Code Red and Nimda worms. They combine the methods of viruses and Trojan Horses to exploit the weaknesses in operating systems and applications using multiple attack methods to get past network defences, such as email, web sites, IRC, IQ, Instant Messenger and network protocols. They can spread very quickly because they employ so many vectors. This is also their Achilles Heel as this provides anti-virus programs more of a chance of detecting them.

Spyware

Evolving from the anti-virus industry, Spyware is a new and rapidly growing threat. Many businesses are unaware that downloading potentially malicious software from compromised URL's can make them vulnerable to adware, spyware, phishing and virus attacks. This creates a brand new market for today's generation of virus writers. Three quarters of businesses in the UK have no protection against spyware and in 2006 this resulted in 1 in 7 malicious software incidents being related to spyware (DTI Security Breaches Survey, 2006).

Botnets

A botnet is where a group of computers are linked together and usually being controlled by a central source with the aim of deploying Internet based security attacks in the form of viruses, Trojans, spam, phishing, etc. MessageLabs Intelligence: 2007 Annual Security Report rates the StormWorm botnet as one of the most significant incidents where over two million computers were used in this attack.

Phishing

Phishing is another relatively new threat that has experienced tremendous growth where cyber criminals will attempt to fraudulently obtain confidential information, passwords or financial details via email. MessageLabs Intelligence: 2007 Annual Security Report states that 2007 was the first year where the proportion of phishing attacks within emails overtook virus and Trojan levels.

Unauthorised network access

This is where a hacker enters the network and tries to gain information (such as passwords or access to data). This might be done without the owner of the network even knowing that anyone has gained unauthorised access to the network. Hackers breaking into your network can view, alter or destroy private files.

Unauthorised network use

Business networks are often used for non-related tasks by employees who access non-business related web sites, send and receive personal email, use Instant Messaging applications and share personal files over the network. According to the DTI Security Breaches Survey (2006), 41% of companies surveyed had recorded incidents of web misuse through employees accessing inappropriate web sites and 36% had cases of excessive web surfing. Not only does this waste valuable bandwidth and reduce employee productivity but can potentially provide an avenue for virus, phishing and spam attacks. The growth in social networking sites such as Facebook, and MySpace are increasingly being used by virus writers and cyber criminals to release potentially damaging network threats to the public and unsuspecting businesses.

Active attacks

There are several sorts of active attack, each with different goals. Some attacks are meant only to disrupt an online service for other users. Known as 'denial of service' attacks, their one aim is to prevent others from using a particular service. The nature of the attack can range from crashing a web site to flooding an Internet link with bogus data so that there is no bandwidth available for legitimate use.

While no data is compromised, the consequences can be quite serious, as many e-commerce sites rely on service availability for their revenue. Other attacks are meant to take over servers, so that data can be stolen or modified or so the server can be used to launch other attacks. These attacks typically exploit operating systems or applications that are poorly configured or have vulnerabilities caused by software bugs. Common targets are web servers, mail servers and DNS servers because they are not protected by firewalls or other security products.

Top 10 cyber threats for 2008

The SANS Institute is a worldwide organisation that focuses on computer and online security. Each year they undertake an annual piece of research with the aim of identifying key security risks and providing this information to the world to assist in improving security measures.

1. Increasingly sophisticated website attacks that exploit browser vulnerabilities
2. Increasing sophistication and effectiveness in botnets
3. Cyber espionage efforts by well-resourced organisations to extract large amounts of data for economic and political purposes
4. Mobile phone threats, especially against iPhones, Google's Android phones, and voice over IP systems
5. Insider attacks
6. Advanced identity theft from persistent bots
7. Increasingly malicious spyware
8. Web application security exploits
9. Increasingly sophisticated social engineering to provoke insecure behaviour
10. Supply chain attacks that infect consumer devices

Source: http://www.computerweekly.com/Articles/2008/01/14/228890/sans-institute-reveals-top-10-cyber-threats-for-2008.htm. © Reed Business Information 2008.

The elements of good security

Security threats are more than just a distraction. An attack directed at financial, personal records or business critical applications is potentially devastating. Even indiscriminate attacks can result in the loss of valuable data, high repair costs, negative publicity, legal liability and the loss of hours or even days of productivity. Security vulnerabilities can also potentially damage a company's reputation.

Spending money on security is notoriously difficult to justify in traditional cost/benefit terms: you spend a lot on security and in the best-case scenario nothing ever happens! However, it is important to remember that reactive security spending is usually greater than that on proactive measures, after allowing for rectification costs. It seems that companies have to suffer a significant breach of security before they take the issue seriously.

Another major hurdle to overcome is a misconception about the nature of effective network security. In reality, it is a management problem with a technology solution. Security isn't a check-list of do's and don'ts – it is a discipline covering the entire business infrastructure. Installing a firewall is a start but it is not enough. A firewall is a specialised piece of security equipment designed to address only one part of the security puzzle. Given the many types of security threats, companies put themselves at great risk by implementing a 'point' product such as a firewall thinking that they are safe.

The need for a multi-layered approach

With businesses expecting an average of 8 security incidents per year (DTI Security Breaches Survey, 2006), the requirement has never been greater for a fully managed, multi-layered security system that intercepts potential threats before they enter your business.

When it comes to security, a multi-layered approach, which protects against both internal and external threats works best. The Nimda virus was specifically designed to bypass firewalls. The damage it caused could have been prevented by the integrated use of a firewall and an intrusion detection system.

A multi-layered security approach is where security solutions are overlaid or overlapped providing a much stronger and resistant layer of security for your business perimeter.

"Another major hurdle to overcome is a misconception about the nature of effective network security."

With a multi-layered approach, even if an intruder is able to bypass one access point, overlapping layers of security ensure that the break-in will be stopped by another mechanism. So, preventing and combating the array of network security threats requires a variety of security solutions and best practices, including: firewalls, anti-virus protection, virtual private networks (VPNs), content filtering, reporting, vulnerability assessments, intrusion detection and software maintenance. Together these provide a secure perimeter for your company network. It is equally important that all the security layers you put down are not only interoperable but can be centrally managed.

Acceptable use policies

Three quarters of companies with an email misuse policy require employees to read and acknowledge they have read it (DTI Security Breaches Survey, 2006), which assists in defining and communicating acceptable usage.

It is critical that your staff know what they can and cannot use the network for. The production and delivery of an 'Acceptable Use Policy' to all staff reinforces the fact that your company has a clear-cut, written security policy that can be understood and adhered to by all employees.

Such a policy reinforces the idea that every employee plays a pivotal role in the security of the company's data. The policy should outline security goals and provide information on issues such as password protection, remote access, use of personal software and so on. Some larger companies make computer security rules as part of their standard HR policy that each employee is required to sign. It is not uncommon for larger companies to instigate disciplinary procedures against anyone who violates it more than twice. While it might seem draconian to small companies, it is one method to ensure a very high compliance rate.

Training

Educating your staff on security basics through proper training is important. HR has a role to play in security too, because experts say that most security breaches can be avoided through adequate staff training that nurtures a security culture within the company. For example, staff should be taught to use strong passwords, not to leave their machines open when they are away from their desks, to not automatically open email attachments and so on.

Strong passwords

You should encourage staff to create passwords that are not likely to be easily guessed by co-workers. A combination of letters, numbers, upper and lowercase characters is recommended. You can make it easy for your staff to comply with security requirements by providing password creation guidelines and recommendations for password date changes.

"It is critical that your staff know what they can and cannot use the network for. "

Firewalls

A firewall is a piece of hardware or software that places a barrier between you and your network and the Internet – it is usually the first security mechanism deployed at the point of external entry and exit to the company network.

A firewall can protect servers and works stations from direct attack from the Internet, as well as hiding internal network resources so that they cannot be detected. Firewalls can also authenticate internal and external users so that their identity can be verified and logged before granting access to network resources. A firewall works by examining each packet of data sent to your computer or network and deciding, based on pre-defined rules whether or not to let it through. It also blocks attempts by unknown programs such as Trojans, from communicating with the Internet. It can further protect your systems by restricting the surfing activities on your network.

However, a firewall won't protect your system against viruses. Software firewalls traditionally run on top of your operating system. Hardware firewalls are easier to use and install and are usually faster than their software counterparts and tend to be more reliable. Both types of firewall need to be carefully configured in order that the permit 'good' and deny 'bad' network traffic.

There are other IT provider managed solutions available including; virtually managed firewalls and MPLS solutions which are very popular with small and medium sized businesses because they are managed an maintained by a third party. MPLS-IP-VPN or Multi-Protocol-Label Switching -Internet Protocol -Virtual Private Network is an alternative to traditional IPSEC (Internet Protocol Security) Virtual Private Networks and prevents the need to purchase multiple firewalls and leased lines for inter-site connectivity solutions.

Anti-virus protection

Another essential security mechanism is anti-virus protection. There are two types available; generic virus-detection software and scanning software. Scanning software is the most common. It checks your system for known viruses, examines incoming files and warns of infection. It also typically runs in the background, checking and monitoring files as they are opened, executed and installed. Some software also checks email as it downloads. Scanning AV products depend on virus signature files for detection and these files need to be updated regularly if they are to be effective.

Generic virus detection software works in a different way. Using a technique known as heuristics, it monitors your system for virus like behaviour and checks programs and files for modifications. This type of software can even pick up on previously unknown viruses and so is less dependent on frequent signature updates, which are essential for AV scanning products.

As so many viruses and worms are now email-borne, it also makes sense to consider using a managed email security service, such as that provided by Star, powered by MessageLabs, to transparently scan your incoming and outgoing email for infected emails and attachments. That way, you can be sure that your incoming and outgoing email is completely free of infected emails.

Internet level scanning

With virus writers using email as their main deployment method, Internet level scanning as a solution to intercept unwanted viruses, spam, web malware and harmful content has grown significantly.

Internet level email services complement but don't replace measures taken on the computer and network server. However, such services have the benefit of always being up to date and don't rely on the user regularly updating their anti-virus software on each computer. Managed services aren't confined to virus protection, Star's range of Internet level scanning services powered by MessageLabs provides a range of fully managed and monitored services that intercept viruses, spam, spyware, web malware and offensive images and content.

System updates

It is very important to keep all of your servers and computers updated with all the latest security patches. If you use Windows, you should frequently check Windows Update for new Critical Updates, which seem to occur all too regularly.

Track your security logs

It is important to regularly review network access to see who has been trying to gain access to your servers and when they have been doing so. For example, a remote access attempt that is continually denied could point to a hacker trying to breach your firewall. Treat every concern as a possible threat and always be cautious.

Seek specialist advice

The growth in the sophistication of technology and the broad range of security products and solutions has encouraged many small and medium sized businesses to pass responsibility for security to third party specialist providers. Speaking to your IT provider is a good place to start as they can undertake a security assessment of the potential security risks within your organisation and recommend solutions that can reduce internal and external security threats to your business.

About Star

Star is the largest independent business to business Internet Services Provider in the UK, serving over 500,000 business users. Star has over 13 years experience in providing practical Internet-driven services for UK small to medium sized businesses (SMBs).

By listening, understanding and responding to the needs of SMBs we develop solutions to tackle IT issues. Security, hosting, connectivity and email have been brought together to provide the broadest range of integrated business ready technology services. Star focuses on developing and delivering products that fulfil the needs of small and medium sized businesses whilst providing outstanding and dedicated customer support.

Star
The Business ISP

For further information call: 0800 138 4443
email: info@star.net.uk visit: www.star.net.uk

Ref: WP 2008 | Network Security