BURSTEK™
The World's Choice for Internet Security.

What is Internet Security?

Author: David Heiler
Burstek IT Department

Many companies today market their products with "Internet Security" on the cover and claim that if you just buy their product, it will solve all of your computer security needs.

They promise to harden your systems against intrusion by Cyber Criminals and protect you from the latest virus outbreaks.
All you have to do after buying their product is install it and go about your daily activities secure in the knowledge that the "Security" company has your back.

As nice as this sounds, it is just not the case in the world we live and work in. Search the Web today and you will be able to find countless articles related to security breaches, from stolen data to virus outbreaks that interrupt access to websites and cost businesses thousands of dollars to recover from.

With such an abundance of information available and every company involved claiming to protect its customers, how do you ensure that you are protected. In order to answer this question you must ask yourself another:

Would I know if my systems were compromised and if so, who gained access, how did it occur, when did it happen, what systems were compromised, and what data was stolen

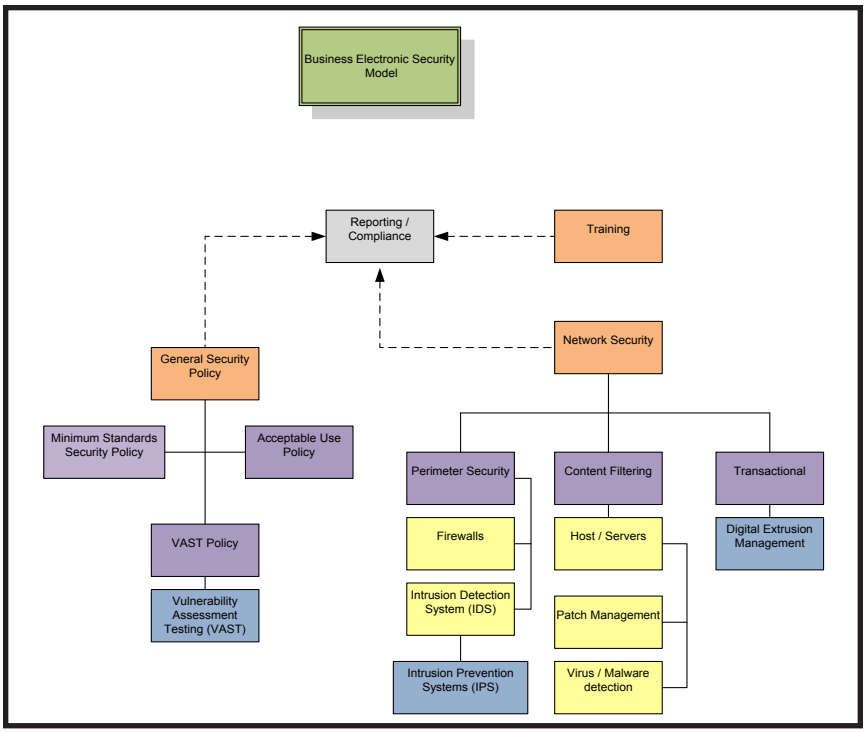
The question is simple and can only result in a yes or no answer. If you answered yes then congratulations. You are among only 25% of business worldwide that can. If you answered no to any part of that question don't feel bad, you're not alone.

Businesses spend thousands of dollars or more each year on security for their networks but rarely do they get what they expect. They may have the most expensive security applications and appliances that money can buy and a whole department of security professionals to watch over it all only to have an employee navigate to a malicious website that takes control of their PC allowing the hacker to bypass all those expensive intrusion prevention measures. The question then is asked, "Well if I have an anti-virus application, am I not protected?"

Maybe. The question should have been, "how do I try to mitigate it even getting to that point?" You may have an anti-theft device on your car but that doesn't mean you would leave it unlocked overnight. You take the extra precaution to ensure that the vehicle is safe while it's unattended. The same care should be taken with your network. Just because you have an anti-virus application on your network shouldn't mean that you can roam the internet freely. As a rather famous person once said, "An ounce of prevention is worth a pound of cure"

The Business Electronic Security Model

As the name implies, this is a model to help you identify the areas of your environment that you need to focus on. The model is broken down into four major sections that require specific methodologies to ensure security across your infrastructure. If anyone piece is neglected it will have an adverse effect on the rest of the environment as you will see.



Section I – The General Security Policy (GSP)

This is the first step in any process, to ensure that whatever comes next follow the guidelines of the organization. The General Security Policy (GSP) is similar to a company's General Policy in that it sets the framework for how everything else is governed. The GSP may contain information about physical building security as well as the infrastructure. This is not the detailed section of the policy but it should present a mandate for technology just as a Company Emergency Policy requires a policy for a building fire or other disaster.

1. Minimum Standards Security Policy – This, along with the Acceptable Use Policy will be the foundation on which you build your security operation. In the Minimum Standards Security Policy, items such as minimum password age, complexity, automatic lockouts, etc, are described. Failure to implement this policy will result in a non-uniform approach that costs a significant amount of resources but accomplishes very little.
2. Acceptable Use Policy (AUP) – This is where you will define how the business systems will be utilized and for what purpose. For example, you might say that users are not permitted to use their PC's for personal use except during their lunch hour. Be careful with this policy. While it might seem easy to just "Restrict Everything to Business Use" you may increase your costs when you try to ensure compliance.
3. The Vulnerability Assessment Testing (VAST) Policy – This will state how and when you will check your environment for potential weaknesses. This could include specific tests run again the network and even the hiring of an outside company to try and gain access to your data.

Section II – Network Security

Now that you have a completed GSP, you can start to address the security of the network. Essentially, if you described it in your GSP here is where you implement it.

1. Perimeter Security – Consists of your Firewalls, DMZ's, and even Data Room security. Nothing would be worse than having what you would consider a bullet proof perimeter only to discover that a member of the cleaning crew walked into your data room that night and pulled the hard drives out of your servers.

   Intrusion Detection Systems (IDS) – These are devices and applications designed to identify unauthorized access to your network. They may also be tasked with preventing the access once identified.

2. Content Filtering – You've done it. You have created a comprehensive Policy and your perimeter network is so secure an ant wouldn't even be able to gain access unless he received permission. Not so fast grasshopper. So you have a nice secure house. All the doors and windows are locked, only you and your family have the keys, you're safe. Well, little Sally brings her friend over from school one afternoon while you're at work and suddenly things are missing or broken.

Little Sally has no idea how it happened and although you suspect, it's rather pointless now because the damage has already been done even with your security. How to prevent this from happening? Simple. Little Sally can only bring home friends that you have already approved.

Welcome to Content Filtering. By implementing this widely overlooked but simple solution you throw a significant roadblock directly in the path of would be hackers and many times, the cost of one of these solutions is less per user than your anti-virus. Not only does Content Filtering reduce your exposure to malicious websites, but it can also help protect you from legal liabilities. Oh and let's not forget, if they are accessing their favorite social networking site, they are not doing the job you are paying them for.

Host / Servers – Although Internet browsing from servers is normally frowned upon, you would be hard pressed to find a Server Admin trying to bring a failed application back on-line at the server console that had not used the server's browser to search for a possible solutions. Again, why take a chance.

As important as it is, Content Filtering is only one piece of the puzzle. Keeping the servers and host machines and their application properly patched with security updates and a managed anti-virus solutions all combine to help provide a significant deterrent.

3. Transactional – This is another area often overlooked until too late. Transactional security deals with the access of the data and/or network resource itself. File security and resource permissions are a good start but how about the users who do have legitimate access to the data? Have they sent an e-mail to a customer with financial data or other confidential information attached? Did they take a spreadsheet home on a USB drive to do some after hours work? You may have secured the data when its one your network, but how about when it's not? A comprehensive security policy will address Digital Extrusion's as a fundamental security practice.

Section III – Reporting and Compliance

The network is secure. You have addressed the issues in all of the previous items and sit down with your CIO and proudly state this fact. Your CIO looks at you calmly and simply states "Prove it. Show me every website that you visited and on what machines you gained access."

Obviously this is not a problem because you are reading this and included reporting as part of your General Security Policy guidelines.

When designing your Security Policy you must make provisions for proper reporting. Without it, you will not be able to ensure that the configurations and applications that you have chosen are working as anticipated. Also keep in mind that reporting is just that, a report. If you ask an application to show you all the times that it blocked FTP access to your website it will certainly do that but what about access that was granted? Why was Tom accessing the Marking FTP site when he is in the Production group?
The same goes for compliance reporting. If your security policy states that only company authorized applications may be installed on the computer system how do you make sure that is the case? Do you run a report once a month? Once a week? What it a user brought in his tax program to complete his income tax return and as soon as he was done he uninstalled it? Would your compliance reporting tell you this?

Section IV – Training

Of all the previous topics, this one is by far the most important. Without the proper training how can your employee's be expected to help keep your business secure? Security is the responsibility of every employee and any employee can easily dismantle your hard work by simply writing their password on a piece of paper and taping it to the bottom of their keyboard.

Conclusion

As you can see, security is a multi faceted topic and is not something that can be accomplished by any one single store purchased application. While each of the topics presented in this short paper can be expanded on considerably, the goal was to provide you the user with a high level overview of how to secure your network. Every network is different and will have its own unique challenges but if you adhere to the principles in this document than you will be that much closer to a safe and secure network.