Global Information Assurance Certification Paper

Name: Victoria England

GIAC Security Essentials Certifications (GSEC) Practical Assignment. Version 1.4b

Descriptive Title:

"Security – What is Enough? What security is enough for a business? This paper outlines what risks, what evaluation and what technology a business should look at before determining what Security Policy should be put in place."

Contents Page

Security – What is enough?
Abstract

"Security" – this can be described as "freedom from risk, freedom from danger and, prevention" "Security" should result in confidence in a system, service or person.[1] The question to ask now is, are you ever free from risk or danger? The quick answer is no, as there will always be new attacks, new viruses and no system is 100% secure. Looking at it from a positive perspective a business can minimise the risk by deploying a detailed, comprehensive and active security policy, which will in turn reduce the risk and threat of danger. This paper will look at the various layers of security businesses have on offer to them today, which will aid the security policy and look at why they should deploy them. Taking a step back, it is important to know what dangers and risks the business is facing, who is the enemy and determine what they want before setting up and running a security policy. Armed with all this information a business can determine what level of security is necessary and determine if they have the budget, personnel, expertise and authorisation to take full advantage of one.

Section 1
Security Policy

A Security Policy is the first line of defence against any attack whether it is social, technical, an internal employee, or a burglar breaking into the building. This is a most important document, as it should outline what to do when you have a breach in security but also how you should go about deploying new technology; what criteria the technology should be tested against and the impact on security when systems are changed. Securing a business is a scary prospect in itself as there is a lot at stake should something go wrong or a system should become compromised; so putting a security policy in place should help remove some of the mysteries and panic that can ensue after or during an attack.

The Policy should outline what systems are critical, what needs protecting, how it should be protected, who should protect this and what the roles and responsibilities are within a business and most importantly within the IT team itself. To explain this point I will use an example of a worm attack on a server. If the server is being compromised by a new unknown attack, for example the SQL worm attack that struck in January 2003 what could be done? Firstly do not panic as this can be counter productive. It would be helpful to know more about the attack, what it is, how it works, what services is uses, in fact anything about it, this will help to stem the attack but perhaps without removing crucial information that could lead to a prosecution against the attacker. The attack needs to be stopped as it is happening and prevent anymore damage taking place, i.e. stem the bleeding, that is another task and could be done in conjunction with the information supplied on the attack/virus itself. At some point either during or after the attack there needs to be an assessment carried out with the aim to determine what, if any damage was

done to the business. A simple calculation for this could be; time spent and money lost as a direct result. The IT department would have to supply information on the time it would take to get the server back online by. This may be hours, or even days but it is important to stress that it is better for the server to be down for longer but fixed than back up after a couple of hours only to be attacked again from the same vulnerability a few hours/days later. The IT team needs to be organised to deal with an attack and this can be documented in the Security Policy. If the Policy is followed by a review of the event this will highlight the difficulties and strengths of the policy and lessons can be learnt.

A Security Policy should be a comprehensive, easily read document that anyone in a company could pick up, read and understand, as they will have to play a part in the Policy. Once the importance of a Security Policy has been determined, the business needs to starting evaluating what is at risk and how to protect those critical assets.

Section 2
Evaluate your Risk.

This is the most important first step to ensuring you are secure. A business needs to evaluate what systems and services are valuable to them and therefore at possible risk before deploying a security policy to protect them.

What are you protecting? Do you have a database full of your customer's details that a competitor would find interesting? Is email business critical and cannot be lost or taken down? Does your business rely on e-commerce? Would it cost money for the website to be defaced or be rendered inoperable? These are all examples of areas of a business that need to be evaluated. As the Internet Security Alliance states

"Identify the adverse impacts when risks to critical assets are realised including financial, reputation, market position, time/productivity. Quantify the financial impact to the greatest extent possible" [2]

It is becoming more apparent that attacks decreased last year, however the amount of damage done as a result has increased. According to Symantec [4] the overall number of attacks decreased but the number of vulnerabilities rose 81.5% from 2001 to 2002 and those in specific sectors, namely the financial sectors saw an increase in "intelligent" attacks that proved more severe. Armed with this knowledge it is best for the business to take security seriously and take the painful step of evaluating systems and re-evaluating them if time has elapsed and patches have not been kept up to date; security it is not stagnant because the attacks are constantly evolving. Patching is a good first step to ensuring systems and networks are secure against exploits, a university department at California University have even gone so far as to rely on their external router and a patching policy to protect their 800 node network. This is a good example of where patching has almost replaced other security strategies and been successful, the SDSC, is a research organization

at the University, based in San Diego [5]. They have no firewall and according to their sources have had no root exploits in two years. So what is their secret? They have a strict security policy including password management, a stringent patching policy and a packet filtering router at the gateway that for example blocks packets with spoofed IP addresses. The policy they have written demands patching, if someone does not want the IT admin staff to patch a system they own; they are simply not allowed to connect that system to the network. The SDSC have clearly evaluated the risks to them and they are constantly re-evaluating to ensure that the threat does not breach. Hard work and a strict policy of patching are working.

Security is only as good as your weakest link, so in the case of SDSC, if you aim to eliminate the weakest link, that is the servers that are not patched then the job becomes easier. A benefit to deploying this kind of security policy ensures that the SDSC always knows what systems they have, what OS they are running and when they were last updated. This is just as useful to your IT team as it can be to your finance team. The IT team needs to know what equipment they have and what software is running and the finance team needs to know what possible assets a business has.

SDSC would have first determined what equipment they were trying to protect and there are various methods to help determine what systems you have in place and whether they need patching and are therefore at risk of attack. Commercial or freeware such as Nessus can probe a network and compile a detailed list of systems. This can be done by an internal IT administrator or alternatively it may be worthwhile bringing in an independent Security Consultant to perform the task as they will perform an unbiased assessment of the business and even provide suggestions on the way forward. A Security Consultant could perform a Vulnerability Scan on systems that are potentially vulnerable to the Internet. This is often a useful tool when Finance Directors or Managing Directors to not understand the implications of not patching or deploying more security systems, especially if a monetary value can be attributed to the vulnerabilities should an attack occur and assets were compromised and data stolen.

The evaluation process does not start and then stop at the point the Security Policy is established. A vulnerability scan for example should be done on a business at least every six months to highlight any new vulnerability that has not been patched against and any areas where a business is at risk. A scan should also be performed each time business practices change, for example if more users want access to a sensitive system or a new application is being rolled out or users want remote access. In each case, an evaluation and a risk assessment needs to be performed, so the business has a clear idea of the impact of change on security. At this point a decision will have to be made as to whether increased access to systems are given at the cost of reduced security! The users will always want more access and more rights but this cannot always be given when the risk on security is great. The security policy will set guidelines to advise IT departments through the argument of security versus functionality and access and also will set a time schedule when evaluation updates should be performed.

Section 3
What is the threat, who is the enemy?

The risks have now been evaluated and the business knows what systems are in place and what patching needs to be done. Before embarking on an aggressive security policy where the business spends ten's of thousands of pounds on equipment and people, it is worthwhile looking at the enemy itself. It is better to know what you are up against rather than deploy systems and hope that they do the job. If you understand the common strategies and motives of hackers and the tools they use it is possible to form a more effective policy to guard against them.

Firstly: few hackers, in fact (according to Symantec) [4], less than a ¼ specifically target a system, sometimes in information warfare and espionage hackers are aiming to specifically gain access to company confidential information to gain a competitive advantage over that company or just to see what they are up to. However, most of the time "script kiddies" will target a system just to see what they can do. The aim is just to see how far they can get and what havoc they can cause, they are looking for the easy kill [6]. The more sophisticated hackers may design their own tools and leave backdoors so they can come back later to see what has changed and if a server is still available. All types of hackers should be protected against as each one is going to cause some harm to a business. No matter what the skill level of a hacker they all have one aim "to randomly search for specific weaknesses and then exploit that weakness" [6].

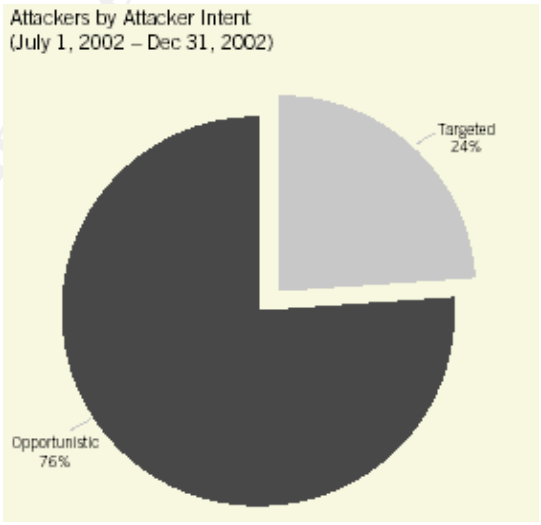

Diagram 1 Symantec Internet Security Threat Report. Attack trends for Q3 and Q4 2002. Volume III Feb 2003. Editor Mark Higgins.

No publicly available host is safe, just because no one knows about your system it does not give it protection just anonymity until it is scanned. Some businesses believe their systems are of no value, i.e. they are not Microsoft, so why should they be probed? Smaller targets are great learning grounds for up and coming hackers, they practice on easy targets before moving onto a more challenging prospects. The consequences of these actions can be great on the small business as they potentially have fewer resources and expertise to cope with these attacks.

The tables below show how small companies (1-499) receive over half the number of attacks that larger companies (5000+) receive in the six-month period July 01 2002 to 31 Dec 2002. This shows how important it is to protect a business no matter how big or how small it is. [4]

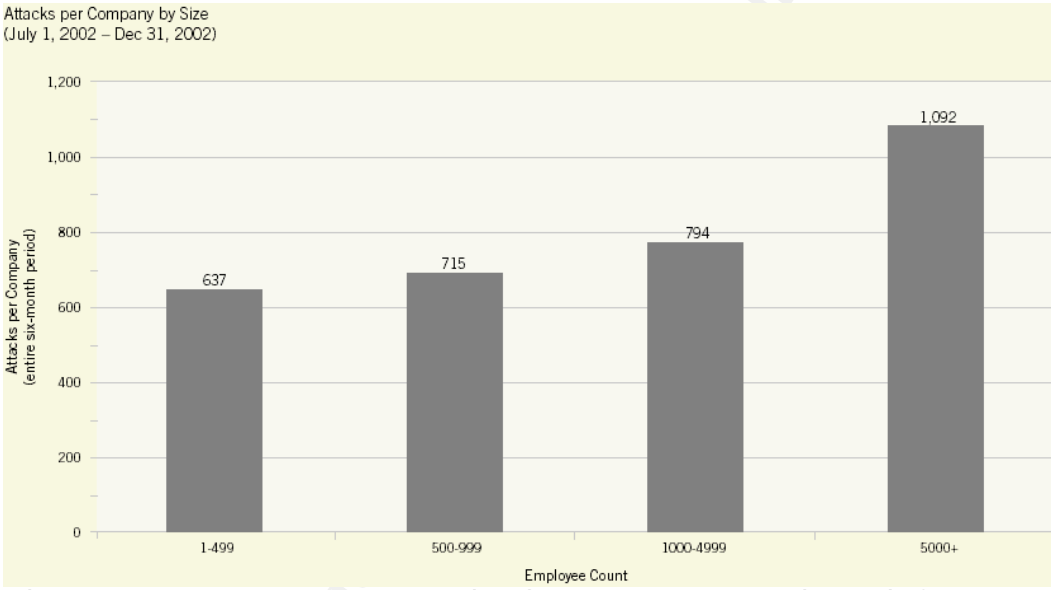

Diagram 2 Symantec Internet Security Threat Report. Attack trends for Q3 and Q4 2002. Volume III Feb 2003. Editor Mark Higgins.

How is Hacking done?

Hacking is generally not personal, people scan the Internet for weaknesses and then exploit them, and these methods are usually automated and require little interaction from the hacker themselves. Initially a hacker needs to build a database of IP addresses, once this information has been gathered, which is often the most time consuming part of the process, the IP addresses are scanned for weaknesses. Hackers keep the database of IP address to use in the future when new vulnerabilities appear as they will then test the IP's for the new weakness. Monitoring software on an Internet connection can give a business an idea of the number of scans that are performed over a period of time to show how often it occurs. This will give insight into how vulnerable a business could potentially be and also what scans hackers are using and possibly give insight into what they are also looking for when scanning.

Here are list of the Top 20 Scans in 2002, here you can see where the greatest number of scans are aimed at: 29.5% are aimed directly at the Microsoft SQL server, which indicates that when this is installed on the default settings it is potentially a vulnerable server and therefore if a business uses this software, checks would need to be done to ensure the server was patched and hardened to protect it as much as possible. This information can be useful to look at when evaluating a business to ensure that all vulnerability scans are done against these threats and more.

Top 20 Scans
(July 1, 2002 – Dec 31, 2002)

Scan Type	Percent of Total Scans
Microsoft SQL Server	29.5%
HTTP	16.5%
FTP	13.3%
Netbios Name Service	13.0%
HTTPS	4.0%
SSH	3.2%
SMTP	3.1%
RPC (tcp)	2.5%
SubSeven	2.0%
Netbios (139/tcp)	1.8%
Netbios (445/tcp)	1.7%
SOCKS (1080/tcp)	1.3%
CDE Subprocess Control	1.1%
57/tcp	1.0%
Telnet	0.9%
Squid Proxy	0.9%
LPD	0.8%
135/tcp	0.6%
DNS	0.6%
1524/tcp (Ingreslock)	0.4%

Diagram 3 Symantec Internet Security Threat Report. Attack trends for Q3 and Q4 2002. Volume III Feb 2003. Editor Mark Higgins.

The best way to protect yourself from hackers is to protect the business, the systems and network from the common exploits, the "easy hacks", this will rule out a vast number of hackers getting into and taking down your business. It is best to ensure that Operating Software installations are not the default installation. A shocking statistic from a Honeynet Investigation done between April and December 2000 showed that seven default installations of Red Hat 6.2 were attacked within three days of connecting to the Internet. Using this statistic is can be estimated that the life expectancy of Red Hat 6.2 default installation is just 72 hours! [9] In addition, a business should only run the services that it needs, why have ports open on a firewall that are not used? Hackers trying to initiate an attack could use these. During the evaluation stage of a business, the services that are commonly used and needed will be highlighted; it is then the administrators job to lock down all other services and

if these services are needed it will soon will become apparent as users will be wondering why they can't access a system.

The most common techniques of attack and scanning methods vary year on year. In 2000 a Honeynet Experiment [6] revealed the most popular scanning method detected was the SYN-FIN scan, this searches an entire IP range for specific ports; a great way of gathering information that could be used to attack a business. This reflects the tactic of focusing on a single vulnerability, and scanning as many systems as possible for the vulnerability [9]. In 2003 this may not be the most popular method so businesses always have to be aware and have up to date information on threats and vulnerabilities. Some businesses deploy their own Honeynet experiments to trap hackers; this is a useful tool for a number of reasons; the information gained can be used to update a security policy and protect systems from common attacks; it could be used to trap attackers and the information used could form a legal case and ultimately a prosecution against the attacker. In addition Honeynets can divert attention from the real LAN/WAN and prevent attacks on the business systems and the business itself.

So having evaluated the risks, looked at the threats a business now has to design a Security Policy and determine what level of protection is needed.

Section 4
What level of protection should you take?

Usually one of the first devices thought of when discussing security is a firewall, this is to be expected when they have been around for a long time, in fact they are the oldest Internet Security sub-Industry [7]. They are the main defence of the perimeter, guarding the gateway to stop intruders/hackers getting past, they help to stop and stem the "physical" attacks. A firewall is a useful tool, it can block attacks, it can help protect a business to a certain extent, it can connect offices together and it can create logs from which useful information can be gathered about traffic flows, user activity and scans performed by potential attackers. All useful tools, but there are many more devices and systems available, which can be used in conjunction with a firewall. Ideally a business would use multiple devices and create layers of security.

The best attack to take when designing the security policy for a business is the layered approach [8]. A large proportion of businesses today, especially in the SME market place only have firewalls, they feel that they are too small and insignificant to be attacked and do not have the available budget for anything more. Security does not necessarily have to be expensive and flash, a lot of is based on vigilance, time and some knowledge.

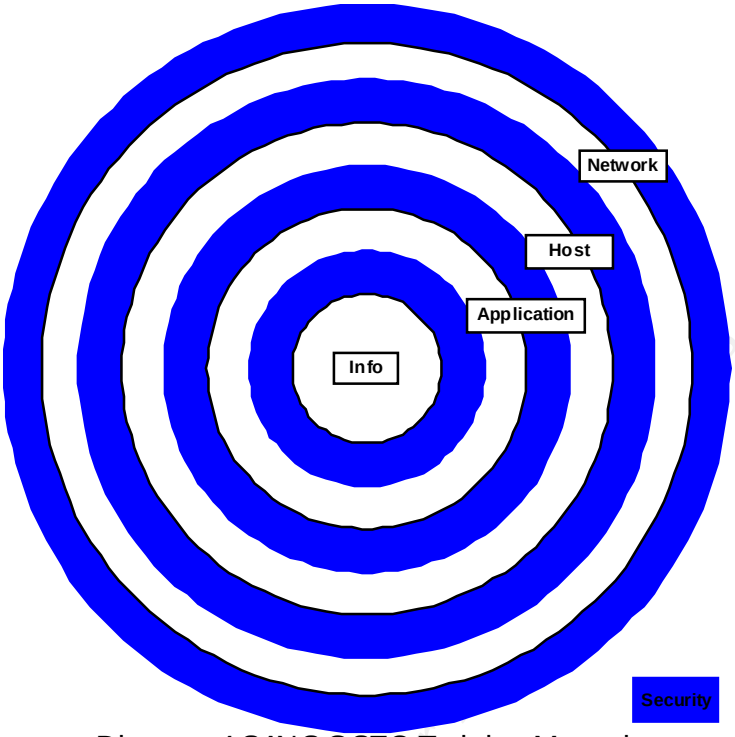

Diagram 4 SANS GSEC Training Manual

The diagram above depicts the SANS layered approach to security the blue circles are layers around the data, systems, services and networks that require protecting. In the traditional 'one firewall' approach there would only be one blue circle and that would go around the network, when looked at like this it shows how vulnerable the systems are within the perimeter of the firewall.

There are many ways both complicated and expensive to implement the 'layered approach' to security but it does not have to be this way. Simple actions can be taken, as long as they in compliance with the overall security policy and kept up to date and monitored. Below are some examples of 'layers' that could work together and work towards the goal of protecting a business.

Firewall:
There are many advantages to having a firewall; one of which is to connect two or more networks together for example a private network and the Internet. An advantage of having a firewall at the Internet Connection point is to funnel all traffic through the firewall to the private network. This ensures that as long as all traffic flows through this device an attack can only ever occur in one place where it can be viewed monitored and logged. The firewall stems the 'brute force' attacks such as Denial of Service attacks, by blocking and registering the source IP address(s). The firewall can also log all of this activity for reference, should the information need to be used in a prosecution. Some firewalls are useful when more intelligent attacks are taking place, such as hijacking http connections, as long as the firewall is capable of inspecting

data streams it will detect suspicious activity and again log the information. The firewall is a useful tool but it is not fail safe, it is a configurable device; it takes some skill to set up so unfortunately the firewall is only as secure as its configuration. The configuration should be planned and designed to meet the needs of the business. Once configured it should be checked by at least a second person to ensure no simple mistakes have been made. It is very easy to mistype a port number for example; if an administrator accidentally opened 0023 instead of 50023, this would result in telnet access from the Internet! On the flip side, problems can occur when there are too many administrators on the firewall; a large number of admin users can add complexity when a firewall should be as simple as possible.

Warnings should not be turned off and the log files should not be ignored, as they are both useful tools that can help prevent and stem attacks. Warning settings should only be for events that are potentially damaging and logs should be managed to only include useful information, otherwise administrators will be reluctant to view and track them especially if the job is excessively laborious. Maintenance needs to be performed on a firewall; software updates and patches should be done as quickly as possible, the monitoring of connections should be logged and complied ready for evaluation if necessary and the firewall policy should be reviewed and updated on a regular basis to ensure the configuration still complies with the business needs but at the same time is still securing the business from attacks. By doing all of this a business ensures that the device is up to date and patched, everything necessary is logged and examined for any suspicious activity and that should any changes need to be made they are compared against the security policy before being done.

A firewall can only protect what it can see, if connections, such as dial-ups bypass the firewall then hackers can attack using these and do not have to go round or through the firewall, it therefore reduces the time it takes to perform a successful attack and exposes the network to uncontrollable vulnerabilities. An important point to make with a firewall is that it should always comply with the Security Policy, as the policy is the basis of the firewall configuration. A firewall is one line of defence, and ideally should form part of a 'Security Package'; a number of defences working together to secure all areas of network and business.

I have discussed using layers of security to encompass the whole business; this philosophy could be attributed to just one layer that is using different devices and methodologies for the defence of just one layer. A business could layer firewalls of different makes for example; a primary firewall such as a Nokia Checkpoint in conjunction with a Cisco PIX, and these could both be used in a layered set-up to supply a business with two lines of defence. If the firewalls are from different vendors there is less chance of an attacker successfully knowing the vulnerabilities of both, therefore providing more protection that just one. A second layer firewall is generally hidden behind the primary firewall and will often provide a surprise for the hacker if they manage to penetrate through the first firewall.

IDS (Intrusion Detection System):
There are two types of IDS, network and host IDS. In an ideal world a business would use both types to ensure that all traffic no matter whether it is on the private LAN/WAN or situated on the Internet Connection is monitored. However for smaller businesses this is not feasible. IDS looks at samples of traffic and assesses the type of traffic that is flowing past it. The IDS detects suspicious activity by comparing the traffic flows and packet structures against a database of signatures. Should the IDS detect suspicious traffic it would log the event but it will not block the traffic. Some IDS systems are intelligent enough to work in conjunction with a firewall so that should any dubious traffic go past the IDS it will request that the firewall blocks the traffic, but the majority of IDS systems are there just to monitor and log. Administrators have the ability to configure an IDS device so that limited traffic types are monitored. The device can be tailored to suit the requirements of the business and target specific areas of the network. Host IDS can be placed on every PC in an office to determine what traffic is flowing around a network and in addition, to determine what a user does on a daily basis. They can run silently without the user knowing but they can be processor intensive on the machine especially if the software is not configured properly. IDS's are not fool proof, there are intelligent attacks that can spoof them, some attacks send packets that are so small they bypass both the IDS and the firewall therefore rendering them useless, however the majority of traffic is captured and logged. As with all software and systems that are reliant on up to date information to work effectively, time has to be spent updating the IDS signatures. With IDS it is important as the monitoring of traffic flows is reliant on a database of signatures and without this the hackers could sneak past the IDS and through into the network.

AV (Anti Virus):
An additional method of protection is to use Anti Virus software. This can be deployed with the aim of inspecting email, protecting PC's and also protecting servers. There are many ways to deploy AV, which matches the many ways that viruses can attack. Viruses predominantly come through email and generally as attachments, the best way to stop a infected email getting onto a LAN and even reaching a user is to catch it either at the mail server on the LAN or by the upstream provider filtering the emails before they reach the LAN. This provides both incoming and outgoing protection for a business. Another way to protect is to use Anti Virus software on PC's, this can constantly check downloads for viruses to ensure a PC is clean and not holding infected data. The same theory applies to server based AV, it protects the server from viruses, the software can detect virus-infected files transmitted to and from servers, while scanning for viruses that may already exist in other server locations. Once detected, the infected file can be automatically cleaned, quarantined, or deleted. As with firewalls and IDS, these systems are only as secure as the administrator, if the AV updates are not done when new viruses are released, the business is exposed to that form of attack, to overcome this the software can be automatically updated and

software vendors often include automatic updates as part of the software package.

Education:
I have discussed a few types of hardware and software security technologies that can be deployed, there are many more but these give an indication as to how seriously security needs to be taken and why too much security is never enough. In addition to technologies, basic training for the end users needs to be done. Each user that is using email, services and the Internet needs to know how to prevent a breach of security and how to act should a breach have already taken place. Users need to be taught the importance of strong passwords on their machines, and being able to memorise the password. They need to know not to give out their password to anyone, even an administrator as hackers often use social engineering tactics to get username and password information, users often feel they cannot question the authority of the person pretending to be an IT administrator but they should question as these tactics are often used to try and break into a company. The business needs to include sections in the Security Policy about acceptable use of the Internet, for example when and what can be viewed during business hours. The policy should encompass sections on downloading from the Internet as there is often no need for a user to be downloading, so restrictions should be put in place. An email policy, including disclaimers, content and none business related use should all be documented. All users should be aware and have read the sections of the Security Policy that directly relate to them to ensure they understand the business drivers behind the policy and also what the restrictions are.

Section 5
Conclusion:

"Security – what is enough". No matter how many devices are deployed across a network there will never be enough security to ensure a business is 100% secure. A combination of technology, knowledge and education will provide layers of security to ensure as much protection as possible is achieved. The only way to protect a business from the Internet is not to be connected to it at all! This is not feasible in today's market, so the best to approach security is in a practicable, methodical and realistic way. Never makes assumptions about hackers and viruses, base a Security Policy on fact and knowledge and ensure it fits into the strategy of a business and has a realistic and working practice to it.

Bibliography:

1 – http://dictionary.reference.com/search?q=security

2 - Internet Security Alliance 'Common Sense Guide for Managers' July 2002

3 6th March Computer Weekly 2003.

4 – Symantec Internet Security Threat Report. Attack trends for Q3 and Q4 2002. Volume III Feb 2003. Editor Mark Higgins.

5 - The Power of Patches – Patching systems isn't easy? But it's essential to your network's security. Rik Farrow. http://www.spirit.com

6 - Know your Enemy – The tools and Methodologies of the Script Kiddie. Honeynet Project (http://project.honeynet.org) July 2000.

7 - Firewalls: are we asking too much? Frederick M. Avolio. http://www.spirit.com

8 - SANS Training "GIAC Essentials……."

9 - Know Your Enemy: Statistics – Analyzing the past……. Predicting the future. Honeynet Project (http://project.honeynet.org) July 2001.

Other Sources

a) CSI – Computer Security Institute April 7th 2002. "Cyber Crime bleeds U.S corporations, survey shows; financial losses from attacks climb for third year in a row.

b) STSC CrossTalk – Security often sacrificed for convenience. Oct 2002. http://www.stsc.hill.af.mil/crosstalk/2000/10/hernan.html

c) Firewalls and Internet Security, the Second Hundred (Internet) Years. By Frederick Avolio, Avolio Consulting Inc. http://www.spirit.com

d) Building Internet Firewalls. Elizabeth D Zwicky, Simon Cooper, D Brent Chapman. 2nd Edition.

h) January. February, March 2003 Computer Weekly Editions.