Global Information Assurance Certification Paper

How to establish a working IT-Security policy that integrates employees

Abstract

Today it's getting very hard to establish a synergy between security and personnel. Everybody should be able to build a relationship between the IT security a company needs and the personnel within the company. This article will help you to establish a security policy in a professional way. It discusses the different areas of a security policy and who is affected by this and what it means to them.
This article is based on legal issues, security baseline policies from around the world and past experiences.
If you look at the following links you'll find a broad basis of articles from a lot of different sites. All have one common statement:
Security is NOT easy to establish.

Interpol drowning under wave of cybercrime
The former secretary general of international crime -fighting agency Interpol has admitted the organisation lacks the high -tech savvy necessary to fight cybercrime.
http://www.silicon.com/news/500013/1/1021901.html

Part of this article is the following paragraph:
Raymond Kendall told silicon.com in an exclusive video interview published today, that law enforcers have neither the resources nor the ability to deal with crime on the internet.
He said: "We need people who have grown up with this and have been specially trained."

This one sentence really is what we need to think about! There is no way to enforce security without people who really understand security. To get there these people have to be trained. They may not need training in existing operating systems, but they do need training in the area of how today's infrastructure influences IT security and how to administer existing operating systems, to maintain a secure environment.

Another good source for the same information is the following article:

Bush unveils final cyber security plan
Mon 17 February 2003 10:14AM GMT
US on the digital defensive
The Bush administration signed off on Friday the final version of the US strategy for protecting the internet and securing information systems.
http://www.silicon.com/news/500013/1/2902.html
at the top of this article you can read:
"Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society - the federal government, state and local government, the private sector and the American people," President George W. Bush wrote in a letter introducing the document.

Within this one sentence there are a lot of challenges which are simply describe by this sentence. Mainly it includes the need to get a lot of different parties together. To secure cyberspace you will need the help of:

- the government; federal, state and local
- the private sector, which is related to all companies around the world
- all American people. If you transfer this to the challenge of IT security around the world, this must be extended to all people around the world.

Again this short sentence from George W. Bush reflect the real problem. Today you need a common understanding of IT security. This common understanding must be brought in accordance with local law and transferred into regional security policies. Everyone must be able to follow the policy which relates to his profession and usage of IT. To be able to follow a policy everyone must be trained in one way or other. Training can simply be offered by non technical documents or even by deep technical training. The kind of training is dependent on the need the "End-User" has.

Looking at a working solution, to get the needs of an IT department in line with the foundation of well trained an interested employees, you best start by looking at the

Security baselines first

Actual security baselines are found in several well known institutes. These are:

SANS (System Administration, Audit, Network, Security)
http://www.sans.org

ISO (International Organization for Standardization)
http://www.iso.org/iso/en/ISOOnline.frontpage

BS7799 (British Standard)
http://www.thewindow.to/bs7799/index.htm

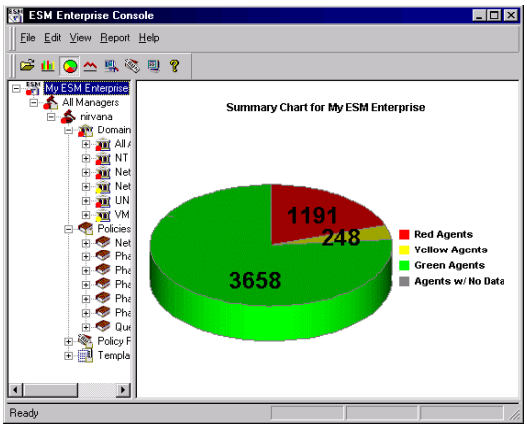
These policies are the baseline for companies who wish to create their own company security policy. This policy includes the hard- and software requirements. These requirements must be divided into the different departments within a company. There is no real way to have one rule which is valid for all departments and employees as there are differing areas of risk within a company. This results in having to create different rules for each of these different areas. But having said that, there is also a set of common rules.

As an example the following rules must be part of a "company wide" policy.

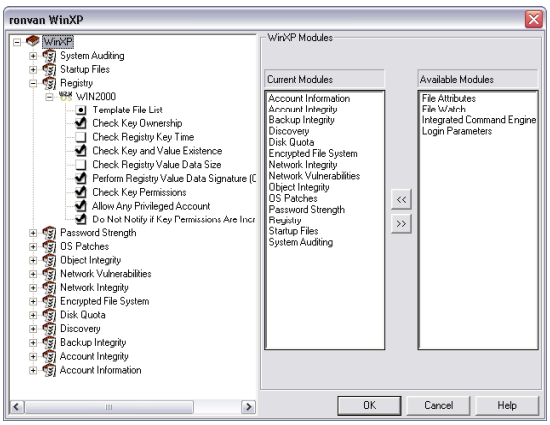
1. the password on all operating systems must be at least 8 character long
2. the password on all operating systems must expire after 30 days
3. normal users are not allowed to install software
4. MS Windows systems are not permitted to have a modem installed.

To be able to continually comply with these 4 requirements necessitates a lot of different checks that have to be automatically executed and always at the same time and with the same base settings. To fulfill this task you require software which is able to deliver this functionality. One product that fulfills these requirements is Symantec Enterprise Security Manager (ESM). More information can be found at: http://www.symantec.com/product/
With ESM you have the possibility of defining the required software settings such as password settings and/or user-id rights as well as registry key settings. Another function of ESM is the ability to check the version of a file. This enables you to check your operating systems for compliance with your security policy. One of the advantages of ESM is that it is possible to check compliance with a security policy from one central point and from a single console.

It is very important to note that ESM is NOT an administration tool. ESM is a very powerful tool which has the ability to create reports to determine whether the company is complying exactly with their own security policy. This allows them, if they require it, to obtain a security certificate from the one of the companies mentioned above.



You are able to show your are in accordance with the security policy in different ways. One is the diagram shown on left hand side. Other possibilities are HTML or Crystal based reports. These functions are fully integrated in ESM. The report data can be also exported to an SQL database. This functionality allows you export data to all of the commonly used reporting tools.
So called “policy runs” are either started manually or scheduled. The input for each policy run can be customized so that it is possible to check different settings at different times and to carry out very intensive scans at a time of low normal workflow. You are also able to create policies for a department or location that has special requirements. ESM checks settings on MS Systems as well as on Unix, VMS, AIX Systems and on IBM mainframes running z/OS (former known as OS390).



After you’ve finished establishing security baselines you need to define related:
Responsibilities.

Having established security baseline checks does not mean

that you have established IT-security. You still need to define WHO is responsible for the adherence to the rules which have been set up? If you say: everybody; I would say that you are right but who ensures this?

The step of establishing a “Security policy” is not difficult. For this purpose you can make use of tools like “Symantec ESM” to check the adherence of the system settings with your policy. The difficulty is getting all employees to comply with this policy. Usually a security policy takes away or restricts rights that personnel have already been delegated. The result is that these people are usually unwilling to accept the new policy. This comes down to the question: Who is able to establish a security policy? Is it the Security officer? Can it be the Security Administrator? Neither is true. The one and only person in a company who should be able to establish a security policy which is valid for ALL employees is the President and/or manager of the company. The reason for this is presented in the following scenario:

I’m in charge of all the IT-personnel working in the development department and it is my job to create a security policy. I have done this in a professional way and created a security policy which must be adhered to by ALL employees otherwise the protection I want to establish against threats is not complete. I have been able to ensure that the people working in MY department meet the requirements of the security policy but is this true regarding to all the other employees? Do they have to follow a policy I’ve written? The answer is NO, because I’m NOT directly in charge of them.
Who then is able to establish a security policy? The only person who is able to do that is the President and/or Manager of the entire company. If he enforces the policy everyone has to follow this policy. If the President and/or Manager establishes the policy, it will be highly likely that also he will follow his own guidelines.
Another positive aspect of that is that he, as a manager, will make sure that the resources for establishing a good security policy will be made available. This relates to the money as well as the manpower to

Put the policy into practice

The most important step in putting a policy into practice is, that you have to involve all the employees who have to adhere to the new security policy. How can you do that? The one and only way to do that is good training. This training must start before you put the security policy into practice.
Training should have several steps. The first mandatory step is to explain to all, why a security policy has now been established. If this step is omitted then the security policy will not get the attention it should receive. If you are able to make absolutely clear why the security policy had to be created and why the individual has to follow the policy, you are very likely to be successful. To make this happen you should establish training which is divided into different steps. Each of these steps should explain a part of the entire security policy the individual has to follow. This means that you may have to split the training. Remember, each individual has a different role in the company. Your policy should also have different sections for the individual roles employees have within the company. Symantec Education Service offers an awareness

program that can be used to introduce employees to a security policy. One key topic within this training is Social engineering. For me that is really one of the key points when I speak about securing data which is important to the company. Looking at the following article shows one issue when you discuss "social engineering" and "is the employee really guilty".

Social engineering: Are people really this gullible?

'Social engineering' is the phrase on many a security expert's lips. But what does it mean? Basically it means computer users are more likely to fire-up a virus if it arrives in an email offering smutty pics of pretty ladies.
http://www.silicon.com/leader/500013/1/2876.html

Nudey pics of Britney Spears you say? Excellent... Oops, I did it again...

The above is exactly what will happen and did happen as part of one kind of social engineering. I'm sure there is one email which you will remember. This was called the "love letter". The subject line was: "*I love you*". For sure, who does not want to know by whom he is loved?
The real reason why this worm was able to spread so fast was the subject line. Warning about the existence of a new mail attack did not really resolve the problem. What does is tell us? You can simply use something someone likes and you will get his attention regardless of previous warnings. Most times this will work. This has nothing to do with any kind of criminal energy. This is purely curiosity

Another way of doing social engineering is related to the question:
What do I need to do to get hold of important company related data?
What is security related? Some examples:

- hardware like firewalls, computers, including decommissioned machines that still have an installed included hard disk.
- Files on a removable medium like floppy or CD
- a combination of User-Id and password.

How can I be successful in obtaining this information or resources?

Here is an example of a training session which demonstrates social engineering:

With the approval of the companies management I walk through the companies offices and introduce myself to the employees as the new security officer. After having done that I go back some hours later to one of these employees and ask them about their satisfaction with their computer environment and also ask about problems they have had in the past using implemented software applications. You will most certainly get answers back regarding problems an employee has had. From then on you have a real "attack" point from where to start. You promise that you will help her/him to avoid this kind of problem in the future, either by explaining how to avoid this problem or by changing the settings of the software. Then you ask exactly what she/he did when the problem occurred, and of course, you need to try to recreate the problem. To remember the steps for the future you ask the

person to allow you to do all the steps by yourself. Where do you think I would like to start?
I personally start by rebooting the PC. I explain the reason for that. I explain, that I do that only to get a clear picture of what is happening. This step will show me as a very profession person because I do not believe in anything I'm told, I check everything. The first thing, after reboot, I ask for is the User-Id and the related password. You think I will not get it? You're wrong. In more then 90% I will get the combination. Next I type in the UserId and password. From then on I know a very important combination: I know a User-Id and a matching password. I will stay for a while at the side of the employee and work with him to recreate a problem she/he had in the past. I will also show him, which could be much better for me as an criminal, how to create backups of files with important and company related data. I also explain that the reason for creating backups is so that these files can be restored in the case of a hard disk crash and that if this kind of situation should occur the backup will be very important for the company. Maybe she/he will be one of the only people having a backup. If that situation should occur her/his boss will be very proud on him. This normally is enough to destroy any kind of uncertainty in regard to my intentions. After having done the backups I will take them with me to store them away in a secure place. When I leave to employees desk, most the time, we have not been able to recreate a problem she/he did have. But, because I trained him how to create backups, I leave a happy employee.
This is because I gave him the impression that I helped him. I'm also very happy because I got what I wanted: a working User-Id / password combination and possibly a lot of interesting data about the company which I can sell. This is a example of social engineering. I'm quite sure that this will work in most cases.

To avoid social engineering and detrimental situations you have to carry out a security awareness program.
This will teach employees what security issues are, what they can do to help the company be secure and, by that, he will get a very important employee. This is because she/he will learn that she/he IS a major component of the companies security.
A good sample of a working security awareness program is:
The Symantec Security Awareness Program
http://www.symantec.com/education/learn_more.html

It offers structured training on security awareness. This training must be adjusted to the need of each company using it otherwise the students will not accept it as THEIR policy. Also an amusing way of learning should be established. This should be accompanied by gifts. After each session a short test should be completed. This test is evaluated and the winner of each test can win a prize. After completion of the whole training, there is another and final test. The winner of this final test should be offered a special price. This

could be a weekend at a hotel or something similar. If you establish this kind of training then everybody in your company will know the contents of the security policy they need to know about. Also they will be willing to follow the rules.
Do you think that is not necessary? I will show you a few issues which, I'm sure, will happen WITHOUT a good awareness:

Virus definitions not up to date, files are not scanned	High risk of virus infections. Lost of productivity
E-Mail attachments are opened	High risk of recurrent virus infection
Intensive Internet usage and file download	Reduced band with and lost of productivity
Reduced password strength	Increases possible network attacks
Unable to detect social engineering	A lot of ways are opened to attack the company: physically and logically

Hopefully you now understand why it is important that every employee needs a good understanding of security and what is expected of him.

The following link will show you another site where you can find useful information regarding awareness.

Promotional/specialty trinkets

> *Awareness relies on reaching broad audiences with attractive packaging techniques. Messages or motivational slogans can easily serve as refreshers on promotional or specialty trinket items, such as: Badge holders, biometric devices, calendars, coffee cups, first-aid kits, flags, frisbees, golf tees, greeting cards, magnets, mousepads, notes and note pads, postcards, security screensavers, and t-shirts.*
> http://csrc.nist.gov/ATE/materials.html

Looking at the information found on the web site you will find a lot of additional information you can use to build up awareness. It starts with one of the most important steps: Motivation.

- **Motivational slogans**
  - Security is everyone's responsibility!
  - SECURITY is not complete without U!

Isn't that something you will agree without any doubt? Have you ever done something good without being motivated? If not, how can you expect that anyone else around the world is doing a good job without being motivated? If you are able to motivate every employee you will, for sure, be successful in getting a secure company.

Next there are lot's of links to useful material you can use to carry out your awareness program.

Don't forget that awareness is tightly combined with social engineering.

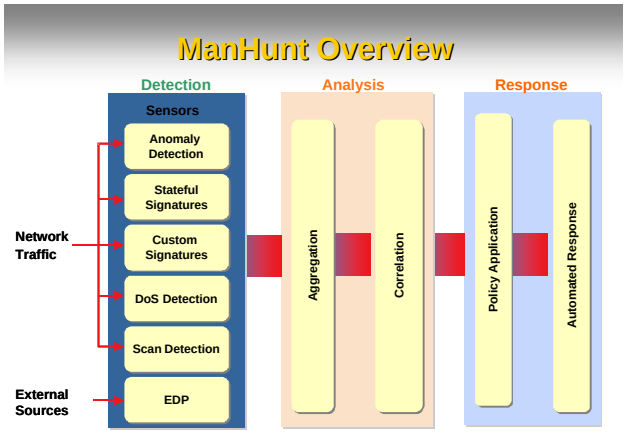
What's next?

Having done the security awareness training will not free you up from doing additional training and checks. Be sure that every employee will follow the guidelines he was trained on. But, as you know, people forget! What must be done to prevent that? There must be someone, preferably a security officer who checks for the observance of the security policy. This is a MUST. If you look around your company you will most certainly find PCs that are not locked or switched off, even if no one is around. This kind of carelessness must be followed up. There is definitely not an easy way of doing this. This is because you have to change the way people work. This again will restrict them in what they do want to do and what they did for a long time. But, it must be done. Perhaps a better way to remind employees from time to time about what they have to do can be achieved by sending short emails with a reminder or with some goods for the desktop. These can be mouse pads or "post it" labels with a simple printed message e.g. "Don't write down your password on this label" or "Don't forget to lock your desktop" etc. This will help to keep in mind the message they have learned.

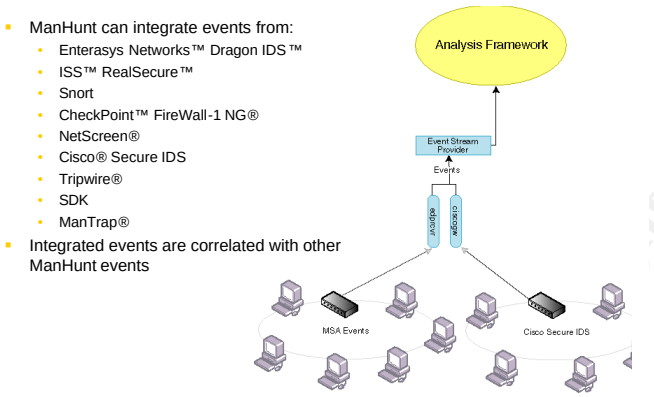
When you get to this stage, you feel secure. Is this true? Let us see what you do have:
You have a security policy which describes your hardware and software environment and perhaps the outfit of your office building. This includes furniture, heating, air conditioning, fire extinguishers etc. This is physical security. There is also another physical boundary which is part of your security policy and surely defined. This is the "firewall". This firewall prevents your IT environment from attacks from the internet. The firewalls log file and other log files should be monitored all day, preferably 24 hours x 7 days. These log files are the source for all actions you will take to protect your data. Have you ever thought of the enormous amount of lines a log file contains? I'm sure the people working with log files do their very best, but I'm also absolutely sure that they will not find all the potential attacks. What can be done to help them to

React and respond in the right way?

First of all you need to get away from the thousands and thousands of lines of information and reduce it to a summary. This summary must be meaningful, which means: data must be correlated and then one "incident" must be shown. This "incident" is the summary of maybe hundreds or thousands of log records, which by themselves do not mean anything and are seen as absolutely normal data flow. But all these events in total are a denial of service attack. One possible kind of solution is a network based intrusion detection system which is able to analyze the data flow of packets on the wire.
Lets look at the Symantec solution ManHunt.
ManHunt is a network based intrusion detection system which is able to analyze traffic on a switched network with a bandwidth up to 1GB and more. The difference to other



solutions is the way it detects an attack. Other systems start the detection by looking for signatures. To do this, they have a list of signatures and check them against the data they find within a packet or in more than one packet, if the original data string was divided up into many packets (fragmentation).



Doing it this way means that data will have to be repeatedly checked against known signatures which is of course very time consuming. ManHunt has a different approach. ManHunt looks for **Protocol Anomaly** first and then, if necessary, it uses other methods of finding an attack. The diagram shows the complete workflow of ManHunt. As you see there are a lot of helpful steps. It starts with detection which is then followed by analysis which then results in a response. The response can be configured freely for the actions which have to be taken. This could be sending emails, firewall hardening or whatever you can think of as a necessary response. This tool helps the employees who have to analyze log files by decreasing the amount of data they have to process. The following diagram shows some external resources which can also be integrated into ManHunt.
Having said that I need to add that collecting data from other platforms and applications gives you a complete picture of what happens or has happened in your network. Only with this kind of insight are you are able to decide whether your network was attacked or not. Also, with this view of your network, you can create a precise security model, which includes all of your hard and software components.
The software can be included by using a policy management tool (Symantec Enterprise Security Manager), Vulnerability Assessment Tools (Symantec Vulnerability Assessment) and Host based intrusion detection systems (Symantec Host Intrusion Detection System). Each of these components has a special task in the complete picture of an “up to date” IT security model.

Conclusion

Lets try to gather all the above facts and see what the outcome is:

1. Technology
    a. hardware
    b. software

    There is up to date hardware and software available which is able to help you to make your network secure. You need to manage the installation and administration of all the different platforms. This is a

real challenge. You have to coordinate all the different options and settings for each of the systems and applications you have. Being able to do this is a major step towards a secure environment.
To get help for this step you may need additional software, which is able to deliver data and configuration settings to all the different sites and collecting information from all the different sites at the time it is needed. If you are lucky the software you are using can be administered and monitored from one central point. This helps you to save time and money and not to forget: reduces your TCO.
Products I mentioned above, which can be used in that way, are:

Symantec Enterprise Security Manager (check for Policy compliance)
Symantec Policy Vulnerability Assessment (check for known vulnerabilities)
Symantec Host Intrusion Detection System (look after systems settings and watch the logs for not allowed actions)
Symantec ManHunt (network based intrusion detection system)

Finally there should be a central point of view (GUI) for all of the above solutions and also for every 3rd party vendor who do want to send their own data to a central console. To get this done you may have a look at Symantecs new solution. This is called the Symantec System Management Console (SSMC) which is based on SESA (Symantec Enterprise Security Architecture), the underlying architecture which allows the exchange of data in a common, open way.

2. Personnel
    a. Training
    b. Control
    c. Understanding

    Most of all, security is related to the way employees handle their work. You can install the best hardware and software in the world but if your employees do not understand how to handle security, there is no way to get the installed hard- and software, working properly. If you want to get your investment handled well, you need to get all of your employees to meet the needs of your security policy. The best way to get there is to:
    - give them good training and let them understand the security policy
    - let them understand that they are part of the security plan
    - make them feel important
    - make security enjoyable

Finally the conclusion is:

Without the synergy between mankind and technology, there is no real security, at all.

List of references

Interpol drowning under wave of cybercrime
http://www.silicon.com/news/500013/1/1021901.html
date 10.01.2001, by Mark Graham

Bush unveils final cyber security plan
http://www.silicon.com/news/500013/1/2902.html
date 17.02.2003, by Robert Lemons
Social engineering: Are people really this gullible?
http://www.silicon.com/leader/500013/1/2876.html
date 13.02.2003, by Silicon.com

Symantec
http://www.symantec.com

The BS7799 / BS 7799 Security Standard
http://www.thewindow.to/bs7799/index.htm

The ISO17799 Toolkit.
http://www.iso17799-made-easy.com/

NIST (National Institute of Standards and Technology) / CSRC (Computer Security Resource Center)
http://csrc.nist.gov/ATE/materials.html

SANS (SysAdmin, Audit, Network, Security)
http://www.sans.org

ISO (International Organization for Standardization)
http://www.iso.org/iso/en/ISOOnline.frontpage

The Symantec Security Awareness Program
http://www.symantec.com/education/learn_more.html