Cyberspace is a Battle Space

By: Bryant D. Glando

Date Submitted: 24 Oct 2004

CyberSpace is a Battle Space

There is a new battlefield and it is in cyber space. Anything connected to the Internet is in this battle space and everyone who connects to the Internet is an unknowing or knowing participate in this engagement. To understand this battle space, we must understand the environment we are operating in. The first step is to know your business model, your network, and know your employees. The second step is to know the threat and what their intent is. The final step is to develop a mitigation strategy that takes into consideration what you know about your system and processes and what you discovered about the threat. The goal is to provide leadership the information to make a well informed decision to minimize the threat to their information and the operation of their network.

Know Yourself.

To defend your networks you must know your networks and the information that is processed across your networks. To understand ourselves, we need to look at the business process of the company[1]. Once we understand the business process of the company then we need to understand what Information Technology (IT) functions support these processes. The next step is to analyze every piece of computer hardware and every piece of computer software that is used within the company. Finally we have to assess the personnel that work for us, and determine what risk factors exist, and determine what level of computer security training everyone has. By knowing ourselves, we will enhance our ability to defend our network.

Sometimes it is hard to step back and analyze ourselves. However this is a critical factor to assist in defending our networks. Every company has a business model, whether formally or informally. It takes a joint effort between management and IT to conduct the analysis of the business model to understand what functions and processes are in place that makes the company successful.

The initial step in identifying how your company operates is to analyze the internal factors that are a part of the company's business process. Three key areas to analyze are: Leadership, Employees and the Function of each department.

Leadership of the company is critical to understand for it is the driving force that can make or break a company. In order to provide the leadership situational awareness and understanding of a particular cyber threat you need to assess whether you have leadership support or not. Depending upon the leadership style of how the company is run, will enable you to best keep them abreast of any cyber threat. The leadership could be either authoritative, participative or lassie faire. If the leadership has an authoritative style then you might have to build a trust with them in your abilities to approach them directly with a problem, so they take your advice seriously. If the leadership is participative, then you could expect to provide input on a frequent basis on the operations of the network and the risks to the network. If the leadership style is

[1] Wheelen and Hunger, page 9

lassie faire then you would expect to make most decision by yourself or within your department, and expect management to accept whatever you do to mitigate a cyber threat. Why even consider the leadership style of the company? The leadership drives how the company is operated therefore your input as an IT security specialist would contribute to the success or failure of this company depending upon how leadership takes the information that you provide them.

Another internal factor to take into consideration is the employees that work for the company. Some of the considerations when you look at your employees are whether you have any security risks, what are their IT training levels and what level of access does each employee have.

What security risks do your employees poise to your company's operations? Depending upon what your company does, you might require a background security check for each employee and you might require them to sign a non disclosure agreement to not disseminate proprietary information. These two steps will help minimize the risk of the insider threat.

What level of training do your employees have? Do your employees know the do's and don't in regards to IT security? Do they know how to use the various software applications to do their job? "Continuous security awareness is essential in instilling security into the organization's business culture"[2] In addition to having a good program in place to ensure everyone knows the security policies of the company and also knowing how to use various applications you must validate and enforce them. Without validation of your security program and the IT training program then you cannot ensure compliance and hence you jeopardize the information assurance of your company.

Do you control the level of access that each employee has? Every department within the company has a particular function, so does it make sense for someone in shipping and receiving to have access to the financial department's folders? If you do not lock down the access to information stored on your network, then you run the risk that sensitive information might get into the hands of the wrong person. For instance if your company has a competitive salary policy then you want to ensure the privacy of every employee's salary.

The last category for internal evaluation is to know what each department within your company does. Every department has their own processes that feed into the overall business process of the company. Each department has their own special IT requirements in order to accomplish their tasks. It is critical to know what they do and how they interact with one another to identify potential IT security risks. For instance if your company is in the business of selling a product, you need to know how the sales department, shipping and receiving, marketing, financial, and the IT department all function and interact. If your company uses just in time production then it is critical that every department works and interacts with one another smoothly for one kink in the process could delay the process which could result in customer dissatisfaction and of loss sales.

[2] Miles, Rogers, Fuller, Hoagberg, and Dykstra, page 245.

Another area to know about your company is what external factors such as partnerships with other corporations and whether you have a function outsourced. You could have the tightest security within your company however the weakest link might be an external factor. For instance if your company has a partnership with another company in a foreign country, you might have some trusted relationships established. The question you might ask, is how secure is their operations and especially their networks? Could someone use this partnership's trusted relationship as a means to gain access to your valuable information? Another area to look into is whether you outsource part of your business process to be cost effective? For instance if you outsource your maintenance, does that company have the same background security requirements that your company has? It is essential as an IT security specialist to understand and know any external factors that could degrade your company's information and operations.

In this world of technology rarely will you find any business operating without some sort of Information Technology? There are two critical areas that you must know in order to safeguard your company's information and operations. The first area is configuration management and the second is data management. When we talk about configuration management, we are talking about software and hardware. The easiest way to manage this is to establish a baseline, and then have procedures in place to add or subtract from this baseline.

Software configuration is important because the majority of vulnerabilities are in software applications. Software configuration starts with the operating system. Knowing the operating system can focus you in on how to defend your network. You might find that your network is operating in multiple environments, which then makes the defense of your networks a bit more complicated. It is easier to focus on one OS vice a mix. Once you determine what your OS is, then the next step is to determine every software application that is being used. This could get complicated for every department has their own unique requirements and could be using a variety of applications. A technique is to start off with a baseline such as a Windows 2000 Operating System, Microsoft Office Professional, and then add to this baseline as you assess each department's requirements. In addition to knowing every application used, you need to know what processes are running at any given time on your network. A good source to assist in the identification of processes running on your network is: www.processlibrary.com or www.sysinternals.com. In the end you will have a good understanding of what applications are running on your networks and where. This will assist in managing the baseline as new applications are added and also assist in fixing problems as they occur.

Hardware configuration is just as critical as software configuration. An approach is to identify your hardware from the outside in. Every hardware component of your local wide area network needs to be identified. Each hardware component could be categorized into services, detection, prevention, and collection. The hardware that provides services is typically servers that are run to provide: web services, mail services, file services, anti-virus updates, and software patches for instance. Hardware components that provide detection, prevention and collection are typically: routers, intrusion detection, and firewalls. A router is the first entry into your network and therefore the most overworked component of your network. A router could be configured using its' access control list to detect hostile IPs, block them, and send the data to a server to log the activity. Since it is overworked, and takes on the brunt of any hostile attack, an IDS is a good component to compliment the router. The IDS could be configured to identify a hostile attack's IP, ports and services and the method of attack (exploit code), deny it (if that capability is turned on and is a part of the IDS), and then log the activity. The firewall is the next line of defense for it could be configured to detect, deny or allow traffic based on the inbound and outbound IP, port, service and what applications are being run. Also an important area of hardware configuration that is typically overlooked is your local Internet service provider (ISP). All traffic should come through this ISP before reaching your LAN. It could be beneficial to know what type of routers they are using, what type of services they provide and what type of protection they have. Although the ISP is configured for their operations they are the gateway to your LAN and do provide the initial detection/prevention/collection. Although this is time consuming, knowing where every hardware component is within your LAN, assists you in identifying problems quickly and will assist in getting your networks operational faster in a time of crisis.

The other area of configuration management is data management. Besides knowing what and where all the hardware and software is, you must know who has access to what. Does your company allow access to everything on your network to all employees? If so, what if a hacker breaks into someone's account, then they have the same access as that employee. Worse yet, it would appear that a legitimate user logged on, extracted sensitive information, and then logged off. Could you detect it? Most likely not, because everyone has access so how could you track them down? So, it is critical to ensure that every person has the right level of access on the network to accomplish their job.

As we can see it is an important process to identify everything possible about your company in order to assist in the defense of your network during a cyber attack.

Know the Threat.

Once you have assessed your business processes and know what your IT structure is that supports these processes; then you must analyze the threat. Your information is worth protecting, for information is power.[3]

To understand the cyber threat, we need to analyze who they are, what they do, when they do it, where they attack, where they are attacking from, why they are doing it, and finally how they do it. Once this analysis is done, we can then match our network defense with the methods of attacks, and determine our strengths and weaknesses, which will allow us to mitigate the threat to our company network.

[3] Kuehl, page 13.

Who is the threat? The cyber threat could be anyone connected to the world wide net, has insider access, or access to your intranet though a trusted relationship. “The depth and breadth of the information infrastructure in the hacking community demonstrates this is not some idle pastime of bored youth”[4]We could categorize the cyber threat into five categories: script kiddy, parasitic, political, and criminal or espionage. Each category of the cyber threat has unique characteristics.

The script kiddy is typically someone who just wants to hack for the fun of hacking and to show off their skills. Their skill sets range from novice to expert. They also like to use scripts to run their attacks for it is easy and requires very little training. A place to get a better understanding of the script kiddy is to attend a Black Hat or DEFCON convention held annually in Las Vegas, www.blackhat.com. In most cases their activity is but a nuisance however it should not be dismissed.

The parasitic hacker is someone who wants to steal your resources. They want your bandwidth, storage capacity, and CPU power for their activities. Typically they will use this for sharing their MP3 files, movies and pornography. Because they steal resources from your network operations they could degrade if not completely shut down your network processes.

The political hacker wants to make a statement for whatever message they want to get across to the world. Typically their method of attack is by defacing a web page, redirecting a web link to their own, establishing chat channels using your resources (also parasitic in nature), or using your services to conduct mass emailing. This could have a significant impact on your company’s reputation and also degrade your network services.

The criminal hacker is someone who wants to steal information for a profit. They could steal personal information from your employees or customers and use it for identify theft. If your company maintains credit card information, they could steal them for use or sale. The impact to your company’s reputation is at stake, and also the assurance of information processed on your network.

The hacker that conducts corporate espionage or espionage for another country could fit into the category of the criminal hacker; however they could be assessed as the most dangerous depending on your company’s functions. Corporate espionage is a reality, and if your company has valuable information that someone else wants then you could expect a hostile cyber attack to gain that information. For instance if your company is taking bids on a major government contract, and someone is able to steal that information, then they would have an unfair advantage over anyone bidding on the contract. Another example is if your company has put three years into research and development of a new product and is about to put it into production, and if someone stole this information they could make a similar product and get it to market before yours. The impact to your company is critical for it could put you out of business, especially if your company relied upon that product for future success and longevity.

[4] Adams, page 159.

Once we understand the threat and what their intentions are, to further analyze the threat, we need to understand how they get into our networks. To do this we look at various phases of a cyber attack. The phases are: the initial target identification, target assessment, the exploit, the actions within the target network, and then covering any trace of their activity. A good source to understand the details of these phases is: "Security Warrior", by Peikari & Chuvakin.

The initial target identification is driven by the hacker's motive. If the hacker for instance is looking to steal corporate information from a competitive company then the target identification is quite easy. If the target is more general such as find all networks that are associated with the government, then the hacker has some work to do. The hacker has to find the network he is going for, and then determine how to gain access to that network. Some methods to find the target is as simple as doing a google search for that organizations name. Once you find the company you are looking for, then you conduct further searches to find out as much information about that company as possible, such as what partnerships do they have (could be a weak link in their defense), what is their organizational structure, and who their employees are (could use social engineering to gain access to the network). So the first step is to identify your target.

Once you identify the target, the next step is to assess the target. Target assessment is trying to find out everything there is about the network so you can identify vulnerabilities. Typically this is done through scanning and probing. As the hacker scans and probes they will discover the target network. The discovery is no more then identifying the network map (the domain, IPs, all network nodes), what OS, what services they are running, what ports are open, what applications they are running and what are all of the hardware components down to the network interface cards that are used. After the hacker has determined everything they can about your network, then they have to probe deeper to find what hardware or software application is vulnerable to give them access to your network. Once this is complete they can move onto the next phase which is the exploitation phase.

During the exploitation phase the hacker has to take the identified vulnerabilities found during the target assessment phase and either find an exploit or write an exploit for that vulnerability. If the hacker has to write an exploit that exploit is typically known as a zero day exploit because no one knew that particular vulnerability existed. This is very resource intensive and requires skills commensurate to the task (identifying a vulnerability that has not been identified before, writing the exploit code, testing it, and then using it on a target). In most cases the hacker can find an exploit for a vulnerability that is known to the community but has not been patched on the target network. The hacker has to take into consideration everything he found during the target assessment phase and match it up with his chosen exploit. For if the exploit is very noisy (it lights up the target's IDS's) then you might not want to use it, unless it is a smash and grab (get in fast, get what you want, and get out). Before launching his attack, the first step is to get pass the router access control list, therefore the attacker has to find an IP that is trusted and spoof it. Once you get past the router, then you have to avoid any detection by an IDS (most IDS are signature base, so if you know what the signature is for your exploit, modify the code so the signature is changed). The next step is to get pass the firewall. One method is to come through a trusted port, such as port 80 which is normally turned on for web traffic. Once you're in, run the exploit against the vulnerable system which gains you a foothold into that network. As you can see, it takes someone with decent skills to gain access to a network, especially if the network defenders are up to speed.

After the hacker has gained access to the target network then they have to gain enough privileges to explore elsewhere within the compromised network. In most cases the system that was vulnerable might not be the target of choice, but what the hacker really wants is the account logins, or information stored in a database, or something else. In order to move elsewhere, the hacker will download their favorite set of tools. These tools might include a buffer overflow (to elevate his privileges to admin), a tool to scan for other vulnerabilities, a tool to map the network, a tool to crack accounts, and so on. So once they are in, they will download their tools, elevate their privileges, find the system that contains the information they want, then gain access to that system, then finally do what they wanted such as: deface your company's web page (inserting their code), steal valuable company information, corrupt your data, or even shut down services that are critical to your operation. Once they complete this phase of their operation, they will typically try to cover their tracks.

The hacker will typically try to cover their tracks through all phases of the attack. For instance when they conduct target identification, they might come from a different IP then their actual IP or even use a local library's internet access under the pretense of research. During the target assessment phase, they can use various tools such as Nmap (www.insecure.org); to scan your networks and make it look like they are coming from a different IP. As they conduct deeper probing of your network to find vulnerabilities, they can come from different IP's and also probe on ports that there is heavy traffic on such as port 80. Once they gain access during the exploitation phase, they typically try to conceal their tracks by hiding processes that are running, shutting down processes such as system logging, and also running tools such as a log cleaner to change or delete logs of their activity. Finally when they extract data they might package the stolen files into a zip and rename that zip file as a jpeg extension and pass it through port 80 so it looks like regular web traffic. Why do the hackers try to conceal their tracks? If caught, they could be prosecuted and with a conviction be sentenced and or pay a fine.

Develop a Mitigation Strategy.

After you assess who the threat is, what their intentions might be, and how they conduct their attacks, then you must determine what actions you can take to mitigate the threat to your network and the valuable information processed on it. To do this you would have to determine what the risk to your company's network is. The risk assessment has to have a detection phase, collection phase and a prevention phase. To know that you are being attacked, you must be able to detect it. To determine who, what, when, where, why and how, they attacked your network, you must collect data on the attack. Finally, to stop the attack and the loss of valuable company information, there has to be a prevention phase. Without these phases, you can not mitigate the threat to your company's network operations, data, and information.

To start off the risk assessment, the leadership (management) needs to drive the process. Without their buy in, you will not get the resources (time, money, training, and equipment) to produce an effective mitigation strategy. Once you can prove that your company's information is valuable and there is a cyber threat to this information, then you can get the proper guidance from management to develop a mitigation strategy. Sometimes management needs to get the hard cold facts such as knowing the average loss per incident for research and development is: $404,375 in order for them to support your mitigation strategy.[5]

The detection phase is critical in the mitigation process for if you do not know that you are being attacked, then how do you mitigate it? The detection phase starts with identifying when your network is being scanned and probed. Because there is so much noise out there, the scanning and probing might get lost in the noise. However, to assist in identifying when your network is being targeted; you need to know what is normal network traffic on your LAN and also what is happening in the rest of the world. A method to assist you is shown at http://securitywizardry.com/radar.htm. You might discover that everyone is being hit with some automated script or a worm and not just your company. This doesn't mean that you will not be attacked, but it will assist in determining if you are being targeted. In the detection phase, your router, IDS, firewall and system administrators are the key components to detecting a cyber attack. Increase router traffic could indicate an attack is imminent. Increase port activity detected by your IDS might also indicate an imminent attack. If your firewall starts to get overload with traffic, might also indicate an attack. Finally an astute system administrator might discover an attack in progress when someone logs onto the network that should not be there, or that has privileges they should not have. It is easy to see that deciding what to detect, where to detect and how to detect is not a simple task. However, it is critical to identify the attack, before, during and after, in order to develop methods to prevent it in the future and also assist in recovering what was loss.

If you do not collect the data on an attack, then you do not have the means to bring those who stole company information to justice. The collection of data is critical for determining who, what, when, where, and how they attacked you. The collection of data starts from the router logs, IDS logs, firewall logs, and any system logs for services that might be running. This data can assist in tuning your sensors to detect the attack if they use the same exploit, and also assist in recovering data loss and or bring those who hacked into your network to justice.

[5] Wired Magazine, 09/2004, page 55

After you have detected an attack, collected data on the attack, the next step is to prevent the attack from happening again. The prevention phase might be as simple as blocking a port or an IP, or using a vendor hot fix to patch a vulnerable system, or as difficult as rebuilding your entire network. The blocking of an IP or port is easy and quick, however if the attacker is persistent and wants what is within your network, they will come from another IP and also use a different port to launch their attack. By using a vendor patch, you can fix the problem fairly fast and cheap, but what if a patch is not out yet, or the vendor patch breaks other systems within your network? Before applying a patch you might have to test it to ensure the patch does not break other systems in the network. If there is no patch for a vulnerable system, then you might have to consider taking the system offline until a patch is developed. What if your entire network is compromised such as every account has been hacked and you can not guarantee the protection of any information stored on your network? This might require you to rebuild the entire network by creating new accounts and purchasing new hardware and or software. There is no doubt the threat has the advantage of time over the defenders, especially if they use a new exploit which has no patch. The prevention phase is where you have to get management buy in for critical resources in order to prevent the loss of company information or services.

So how do we tie in the detection, collection, prevention processes into a mitigation strategy? The easiest way is to develop a scenario and run through it with management. For instance, if a new vulnerability is announced by Microsoft, the first question is so what? Does this vulnerability impact our networks? If so, what is the risk to our network? The scenario could look like this:

Step 1: Vulnerability is announced. It is important to know everything about this vulnerability, such as what OS is associated with it, what hardware if any is tied to it or what software application is vulnerable, what ports could be used, and what services. A good source to be up to date on what the latest vulnerabilities are: http://isc.sans.org, www.sans.org/top20, or http://research.pestpatrol.com.

Step 2: Determine what is the impact to your network? If you do not use the hardware or software that is vulnerable then the risk assessment would be minimum. However you still need to be aware of it, for what if one of your partnership companies uses the hardware or software that is vulnerable? It could provide them a backdoor into your network.

Step 3: Determine if there is an exploit written for this vulnerability? If you can identify the exploit as it is released in the wild, you might be able to develop the necessary signatures for your IDS or vulnerability scanners to detect this exploit, and also start the development of a patch to protect your vulnerable systems. "Over the past six months, the average time between the announcement of a vulnerability and the appearance of associated exploit code was 5.8 days".[6] With this fact, it is critical to make this assessment earlier in order to develop a mitigation strategy before your network is attacked.

[6] Granneman, page 3

Step 4: Determine if there is patch for this vulnerability? If so, then conduct testing, and patch as soon as possible.

Step 5: Determine if you can detect when this exploit is being launched against your network. Develop the signatures for your sensor packages to detect when this exploit is run against your network.

Step 6: Present your recommendations to management, and lay out a plan of action.

Step 7: Execute your mitigation plan, and monitor whether it is successful or not.

There is no doubt there is a new battle space out there and it is cyberspace. In today's business world, we are use to having information at our finger tips which gives us a competitive advantage over those that do not have access to the same information in a timely manner. By assessing our company's business model, knowing what IT supports it, identifying potential cyber threats to our company, and finally developing a mitigation strategy, we can minimize the risk to our network and protect the company's well being. One element by itself is not enough to ensure this. As an IT security specialists, it is our function to provide the leadership situational awareness of a cyber attack, understanding of this cyber attack, and to convey the so what factor to the leadership so we can properly develop an effective mitigation strategy to protect the company's network and valuable information within.

Bibliography

Adams, James, “The Next World War, Computers Are the Weapons & Front Line Is Everywhere”, Simon & Schuster, New York, NY, 1998.

Granneman, Scott, “Fueling the Fire”, http://www.securityfocus.com/columnists/271

Kuehl, Dan Dr., “Information Operations: The Hard Reality of Soft Power”, Information Resources Management College, National Defense University, www.iwar.org.uk/iwar/resources/jiopc/io-textbook.pdf

Jensen, Jesse, “Wanted For Stealing Intellectual Property, Notably Email Addresses and PowerPoint Presentations”, Wire Magazine, 09/2004.

Miles, Greg, Rogers, Russ, Fuller, Ed, Hoagberg, Matthew P. and Dykstra, Ted, “Security Assessment, Case Studies for Implementing the NSA IAM”, Syngress Publishing Inc., Rockland MA, 2004.

Peikari, Cyrus & Chuvakin, Anton, “Security Warrior”, O’Reilly Media Inc., Sebastopol, CA, 2004.

Wheelen, Thomas L., & Hunger, David J., “Strategic Management Business Policy, Edition 7”, Addison Wesley Longman, 2000.

http://isc.sans.org, “SANS – Internet Storm Center – Cooperative Cyber Threat Monitor And Alert System – Current Infosec News and Analysis”

http://www.processlibrary.com, “ProcessLibrary.com – The online resource for process information!”

http://research.pestpatrol.com, “eTrust PestPatrol – Center for Pest Research”

http://www.sans.org/top20, “SANS Top 20 Vulnerabilities – The Experts Consensus”

http://securitywizardry.com/radar.htm, “Talisker Computer Network Defense Operational Picture”

http://www.sysinternals.com, “Sysinternals Freeware”