Global Information Assurance Certification Paper

Essential Security Operations Within An Organization

Richard Woon

September 29, 2001

Introduction

It is evident indeed, that the awareness of information security in this day and age is lacking. It is lacking particularly in the digital industry. Failure to understand the source of these security threats prevents most of today's organizations from doing the minimum required to address all the possible threats out there. The subject matter of physical security is well understood by many, this is why in organizations where physical security matters most, it is implemented well enough to address most of the threats at large. In the digital industry however, it is slightly more complicated, as we are dealing with a virtual workspace, where one may not see the entire picture from the physical perspective alone. In order to successfully implement a sound security policy, it is important that the individual is able to see past the physical perspective, understand the digital perspective and come up with a project, which combine strategies applicable to both the physical and digital infrastructure. One of the key areas is to understand the source of these security threats. Understanding these threats is the first step in assisting organizations not only to justify investments required, but also to apply defense in-depth. [1]

Understanding The Source

The source of these threats come from a very organized community based group sometimes called 'computer underground' or 'black hats'. The communication and mentoring methodology within this community is fairly advanced, thus proving the point that there's order within chaos. From experimental hackers to script kiddies, these types represent the very early stage where the primary objective is the satisfaction gained by basically seeing a vulnerability exploited in action. These poses organizational risks since they do not really understand the tools being used. Higher up the chain are the advanced and professional attackers, which are basically very skilled administrators with strong coding skills. The primary objective here ranges from the satisfaction gained from intruding or even monetary benefits and revenge. These highly skilled attackers take pride in their work and spend countless hours studying source codes of applications and protocol stacks documenting all possible exploits discovered. They then begin writing their own application to exploit these holes one at a time, these tools are also distributed into the internet to assist them in a form of distributed use of these tools by experimental hackers and script kiddies.

We have recently seen the wave of worms like 'Code Red' and 'Nimda'. Code Red is a self-propagating malicious code that exploits Microsoft's IIS-enabled systems susceptible to the vulnerability described in CERT advisory http://www.cert.org/advisories/CA-2001-13.html. [9] Nimda is malicious code known as the "W32/Nimda worm" or the "Concept Virus (CV) v.5. This malicious code is known to spread via e-mail clients, network shares and compromised web servers. It is also known to spread via existing backdoors left by variants of Code Red, but mostly systems vulnerability described in CERT advisory

http://www.cert.org/advisories/CA-2001-12.html. The sequence of these events tend to make me ponder on a possibility, that the creators of these worms may actually have a copy of the source codes for the particular type of application, which was the target of the worm. This I can relate back to October 27, 2000 when news reported that a leading software company was hacked and its source code had been compromised.

The damage achieved by these worms to date is deemed critical simply because of the short timed it took to compromise the total number of detected host to date. The internet is driven by applications, the only way to wreak havoc on the internet is a direct attack on these applications. One of the underground society's main goals is to obtain source codes of these popular applications in order to write exploit tools for a direct sequence of attacks.

Understanding Attack Methodologies

Firstly, the types of attacks can be classified into 2 major categories

- Direct Attack Methodology

These are attacks with one goal in particular, where the victim is commonly the unprotected, with virtually no security implementation or an unpatched operating system/service.

- Indirect Attack Methodology

Indirect attacks are slightly more advanced because these are targeted at sites with some level of security. There are two goals, one is to elude the defense before engaging in the Direct Attack Methodology. The frequency of this indirect method is increasing because it aids the attacker in preserving anonymity. An example of this attack would be the 'Smurf' also known as a Distributed Denial of Service attack. For this attack to be successful or impactful, the attacker would need many compromised 'zombie' hosts in its control. This means that the preparation for this sort of attack takes time, from the time the attacker scans the internet for susceptible hosts to plant the 'zombie' application for later use. Once a substantial amount of compromised hosts is available, the attacker would then initiate a distributed attack by instructing all zombies to attack a particular victim or network at the same time. To defend against these attacks, it would also take time to be ready with defense mechanisms in place and also the operational readiness to liaise with upstream providers when an attack of this sort is detected.

Understanding Defense Methodologies

There are 4 primary defense methodologies that can and should be deployed as a part of any security implementation. These defense mechanisms are:

- Perimeter Firewalls
- Intrusion Detection Sensors
- Anti-Virus System
- Auditing and Penetration Testing
- Good Backup and Restore Procedures
- Operations Monitoring, Updating and Reporting

Most of today's implementation covers up to the 2nd level and sometimes the 3rd level of the above described defense mechanisms. This is partly due to the education and awareness process, where probably it was not made clear that you do not install and configure a firewall, an intrusion detection system and just forget about it. Performing an audit and penetration test is equally an important area of operations, not forgetting monitoring, intrusion and virus signature updates and a good reporting mechanism. This in fact is the only way to ensure that the implemented security policy is as good now as when it was first implemented. To relate this situation in physical security is like having a CCTV camera installed, but no one to view and manage the recordings. Some organizations may find difficulty in allocating a resource to do the minimum required in operation, this is where outsourcing the task to a managed security service provider should be considered.

This requires some research to be done at the initial stage to determine the quality of service and credentials of these managed security service providers. Also bear in mind here that if you're planning to outsource your security implementation, make sure you have a methodology to validate their work. This can be achieved by engaging another security consulting firm to perform an adhoc audit and penetration test to see the level of response in the event of an incident. Justification of having a dedicated resource for security operations may be difficult for some organizations, but this is where the approach needs to be handled with care. The best way to address this is a detailed proposal covering from risk analysis to cost of investment be developed sending a clear message as in 'Is the value of the data in the organization worth the required investment?' [2]

Operations Must Come After Deploying Security Measures

This is a subject most often left behind in any implementation. The term 'operation' should mean as much here in a security implementation as with any industry, unfortunately this isn't the case. This is also the reason why I've personally seen several firewalls at sites where they haven't been logged on for at least 6 months to a year. Based on the CSI/FBI 2001 Computer Crime and Security Survey, the following emerging trends have been confirmed over the previous years [4]:

- Organizations are under cyber attack from both inside and outside of their electronic premises.
- A wide range of cyber attacks have been detected.
- Cyber attacks can result in serious financial loss.
- Defending successfully against such attacks requires more than just the use of information security technologies.

We are pretty much aware of the first 3 points above, but the 4th point should raise an eyebrow at least. Why is this statement so ? This is simply because new attack methodologies are appearing by the day, and only with a good security operations can one hope to stand a chance defending the organization. Emphasis is required in the development of a comprehensive approach to information security, embracing both the human and technical aspects, which includes proper funding and training. [5]

Computer consultants practicing information security need to emphasize this need to end-users and customers. It is more than just closing a sale for a firewall or intrusion detection system. It is the responsibility of the security practitioner to ensure that the organization seeking the solution to protect its information and service is made well aware that implementation without the 'Operational' aspect is to have partial protection for a short period of time. It is therefore my conclusion that the role of the security consultant is more than just providing the solution, but to deliver the understanding that would help the organization achieve defense in-depth. [1]

To have a successful security operations in an organization, the security teams needs the support of the

organization in terms of training and resources for a start. They then need to be empowered with the responsibility and accountability to develop a security policy. It is this unit within an organization that will work closely with the security vendor or consultant to determine what's best for the organization. The responsibility of the security vendor or consultant is to highlight key areas of concern and it is the responsibility of the operations team to map the organizations' requirements and processes to address these key areas of concern. The security operations must also validate any information provided by any consultants or security vendors. This is the basis of how a security policy should be developed.

How Many Incidents ?		1 to 5	6 to 10	11 to 30	31 to 60	Over 60
	2001	33%	24%	5%	1%	5%
	2000	33%	23%	5%	2%	6%
	1999	34%	22%	7%	2%	5%
	1998	61%	31%	6%	1%	2%
	1997	48%	23%	3%	n/a	n/a
	1996	46%	21%	12%	n/a	n/a
How Many From The Outside ?		**1 to 5**	**6 to 10**	**11 to 30**	**31 to 60**	**Over 60**
	2001	41%	14%	3%	1%	3%
	2000	39%	11%	2%	2%	4%
	1999	43%	8%	5%	1%	3%
	1998	74%	18%	6%	0%	3%
	1997	43%	10%	1%	n/a	n/a
	1996	n/a	n/a	n/a	n/a	n/a
How Many From The Inside ?		**1 to 5**	**6 to 10**	**11 to 30**	**31 to 60**	**Over 60**
	2001	40%	12%	3%	0%	4%
	2000	38%	16%	5%	1%	3%
	1999	37%	16%	9%	1%	2%
	1998	70%	20%	9%	1%	1%
	1997	47%	14%	3%	n/a	n/a
	1996	n/a	n/a	n/a	n/a	n/a

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Scurity Instatute

Based on the survey results illustrated above, it is evident that internal threats are equally important when implementing a security policy. The results show that in Year 1998, Under incidents 1 to 5 times, 70% of attacks originated from the outside, this figure dropped to 37% in Year 1999, 38% in 2000 and 40% in 2001. This means that successful attack threats from the outside is growing as compared to successful attacks from the inside, this should give us an insight of the progress in attack methodologies of the underground community. Implementing a sound security policy to protect the organization from external and internal threats can only be achieved with sufficient emphasis of the organization on its security operations. Nobody can implement a security policy without participation from the organization itself. Security Operations within an organization needs to be empowered with the responsibility and the ability to act and react accordingly in order to be the least prepared for handling an incident when and if necessary.

Why is 'OPERATIONS' So Important

The objective here is to touch on the relationship between a particular type of attack, which is linked to a secondary agenda. This is very difficult to ascertain, but we need to defend against these attacks due to the impact of the potential secondary agenda. The idea is not only to defend our organization against this attacks but also to prevent our organization from being the used to attack other organizations. If all internet hosts can act accordingly to prevent the primary agenda for this case study, we would not be seeing any large scale DDOS (Distributed Denial of Service) as we've seen in February 2000 when several massive DDOS against internet sites like Amazon.com, eBay and ZDNet [3] to name a few. The start phase of a DDOS

attack is the development of zombie hosts. Typically universities and small to medium sized organizations with connections to the internet are prime targets. It could be because small to medium sized industries do not take security seriously and are therefore susceptible to exploits like buffer overflow, and these are the types of attacks that are used to employ zombie hosts. Without a strong host and network based intrusion detection system, it is almost impossible to detect an attempt to compromise a host. Even if there are network based intrusion detection in place, the underground community is already working on methodologies to bypass these network based IDS by using tools that modify buffer overflow attacks to evade signature based intrusion detection systems.

What's Next After Operations

Security operations within an organization should have the following objectives or mission statements. The need for operational excellence goes without saying, so the best method is to empower and to be made responsible. This will spawn the efforts required to be at best while in command of the console.

- To be aware of all possible information security threats. This will spawn the need for training and education of the operation team.
- To be able to map key areas of concern for the particular organization and relate the type of defense strategies to employ i.e. encryption. This will initiate risk analysis studies building the basis of justification for investment requirements of any security solutions.
- To be able to react when there is an incident. This will spawn the need to do research, including running/experimenting with attack tools and understanding signatures of packets, and keeping in close contact with local CERT bodies and Internet Service Providers. This will also push the operation towards research on current security best practices in development of an incident handling process. Best practices guide in terms of networks and systems can be obtained from some of these sites. These sites also contain materials which help in justifying best approach methodologies from the management standpoint. [8]
    - http://www.cisco.com/warp/public/126/secpol.html
    - http://www.cert.org/security-improvement/modules.html
    - http://bsp.cio.gov/list.cfm
- To ensure that the security policy is built around these steps: [6]
    - Harden/Secure (To patch and harden all operating systems)
    - Prepare (To prepare audit methodologies)
    - Detect (To have network and host based IDS deployed)
    - Respond (To develop an incident response procedure)
    - Improve (To research and keep up with current threats, deploying new defenses when required)

To develop policy checklist is one good way of ensuring that your organizations' policy is adequate to take on today's available threats. A very good reference and samples of checklist can be obtained from this book.

The Cert Guide to System and Network Security Practices by Julia H. Allen. Addison-Wesley. [6]

- To be empowered to constantly conduct internal audits, using common open-source based attack tools or commercial audit tools to ensure constant strength of the applied security policy.

- To contribute back to the community by sharing information with local and international CERT bodies on new or suspicious findings.

- To ensure proper documentation of all processes and incidents in a database for future references and investigation evidence when and if required.

- To be aware of the country's law on computer crime. This will initiate the process of determining the types of information required for evidence in the result of legal proceedings.

Conclusions

What does this tell us end of the day ? Is there no way to protect ourselves ?

Well it only stresses the earlier subject on 'Operations'. Without operations, meaning a dedicated team and resource spending time doing research and constantly keeping aware of the threat development out there, it simply isn't sufficient. Successful deployment of defense-in-depth [1] depends heavily on operations. The value of an organizations' data cannot rest alone on solutions provided by internet security companies and technologies. It is also clear that organizations need to play their role in validating information such as those derived from security vendors and consultants

as some of the information are based on surveys conducted several years ago, and may not be currently applicable. Initiative has to be the driving factor of the organizations' security operations team. The future direction of attack methodologies are moving towards a distributed architecture, which makes it virtually impossible to apprehend these attackers. Therefore our only hope in this day and age is the defense approach that we're employing in our organization. It may not suffice entirely as these threats are truly persistent beyond one's imagination, but it will have to do compared to ignorance.

List of References

1. The SANS Institute. Presented by Stephen Northcutt during the SANS/NISER 2001, Kuala Lumpur. Track: SANS (GIAC) Security Essentials.

   http://www.sans.org/giactc.htm.

2. The SANS Institute. Presented by Stephen Northcutt during the SANS/NISER 2001, Kuala Lumpur. Track: SANS (GIAC) Information Security Kickstart. http://www.sans.org/giactc.htm

3. Ed Skoudis. "Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses". Reading: Prentice-Hall, 2001.

4. Richard Power, Editorial Director, CSI. Computer Security: Issues and Trends. Volume VII, No. 1, Spring 2001. 2001 CSI/FBI Computer Crime and Security Survey. Computer Security Institute. http://www.gocsi.com/prelea/000321.html

5. Patrice Rapalus, CSI Director. 2001 CSI/FBI Computer Crime and Security Survey. Computer Security Institute. http://www.gocsi.com/prelea/000321.html

6. Julia H. Allen. The CERT Guide to System and Network Security Practices. Reading: Addison-Wesley, 2001.

7. Cisco Systems. Network Security Best Practices. http://www.cisco.com/warp/public/126/secpol.html

8. CIO Council. Federal Best Security Practices. http://bsp.cio.gov/list.cfm

9. Carnegie Mellon Software Engineering Institute. CERT® Advisory CA-2001-13 Buffer Overflow In

IIS Indexing Service DLL. http://www.cert.org/advisories/CA-2001-13.html

10. Carnegie Mellon Software Engineering Institute. Cert Security Practices. http://www.cert.org/security-improvement/