GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Allison Jones
GIAC Security Essentials Certification (GSEC)
Practical v.1.4a Option 1

The Security Infrastructure: A Basic Methodology

Abstract

The key to building a successful security infrastructure is identifying the need to balance two primary objectives: functionality and security. The closer an organization is to impenetrable, the further the organization gets from its functional needs, and vice versa. Therefore, it is essential that all elements work together within the network to create a security strategy parallel to the network strategy. To do this, recognize where the threat lies and what the risks are. In order to guard against these threats, establishing a well-managed and organized network infrastructure is essential. The crucial factors: "Know Thy Environment," "Maintain Thy Environment" and "Secure Thy Environment" need to be identified and assessed. Developing a secure IT (Information Technology) foundation may encompass the ITIL* (Information Technology Infrastructure Management) methodologies, which create a common set of standards for infrastructure development.

The objective of this paper is to develop a basic IT security foundation which any organization can apply and customize to their individual needs. Beginning with the threats, we step through the basics, to the solution and see what can change or evolve within the organization to accomplish the goal of a secure infrastructure. Our conclusion finds that security cannot be implemented as an afterthought, it must be built into the network infrastructure.

Introduction

A solid, secure infrastructure is the foundation to any successful corporation. Whether it is a small network of three computers or a large network of three million computers, the goal is the same: to maintain the integrity, confidentiality and availability of data. Without the foundation securely in place, the corporation will fail over time, not only via security but also via the network management, as the two are, in fact, co-dependent.

A fully secure infrastructure does not actually exist. The only way for that to happen is to pull the plugs on all systems, let go of all the organization's employees and basically close down shop. Security professionals are faced with a dilemma: how to effectively secure the organization as well as retain the necessary functionality that organization requires.

To do this, they must first identify the threats they wish to protect themselves from. Then, they must focus on the three key elements to the development of a secure IT infrastructure:

- Know Thy Environment
- Manage Thy Environment
- Secure Thy Environment

*ITIL (Information Technology Infrastructure Library): ITIL is a library of six compendiums that outline a process-based set of best practices for IT Service Management. (ITIL Essentials, 2001)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

There are many facets to a security infrastructure and many perspectives. Therefore it is wise to note that varying organizations will have varying infrastructures.

The Threat Vectors

When trying to validate a solution, it is essential that you identify the problem, or pending problem. In Security, we look to the threat vector. We can categorize the threats into two broad categories: (1) People and (2) Technology. Implementing a security solution can be costly and it is best to start at the ground level and work your way up. The possibility of compromise for an unprepared organization is a certainty, and the destructive payload will vary, but there most certainly will be a negative outcome. Some of the most effective security tactics begin with the knowledge level of the employees themselves within an organization.

People

People are your first defense, so it is wise to promote awareness of the issues associated with security. Social Engineering is the cause of a multitude of attacks, and can have some of the highest destructive payloads. (See: Social Engineering: http://www.gartner.com/gc/webletter/security/issue1/.) Other issues, such as viruses and worms can cause considerable damage and can effectively be avoided by utilizing a mixture of antivirus software and security awareness tactics.

Among the most destructive attacks are those that originate from internal entities, such as current/past employees. Most attacks originate from outside the organization but the attacks with the most substantial payload can originate from within. While maintaining a certain level of trust is desired, managing and policing internal employees is necessary for a healthy environment.

Building a "human firewall" ([1]PentaSafe, 2002) is an effective strategy used to strengthen and build the physical and intellectual perimeters around an organization. To find information on what level of awareness your organization possesses, PentaSafe has developed an online survey that can assess and advise you of your organization's security awareness. To access this survey visit: https://www.humanfirewall.org/sasurvey/csoregister.asp.

The development, implementation and maintenance of security policies are extremely important to any successful security solution. An organization must have clear, decisive policies that outline all security aspects from physical access, proper use of technology to communicative tactics associating awareness with roles and responsibilities. All employees must be responsible to read and understand the organization's security policies on a regular basis. It is wise to incorporate this into the employees' performance evaluations and the incoming procedure when hiring new employees.

Technology

There are multitudes of technological attacks. From DoS (denial of service) attacks to brute force attacks and the used technology to perform these is varying more and more and becoming easier and easier. (See: Network Security:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

What are you waiting for? http://online.securityfocus.com/guest/5560) Presently anyone, with no technical understanding can acquire and deploy these attacks. Thus, it is wise to wonder at the capabilities of those who have a vast understanding of hacking. How many of your servers inadvertently host the services of an unauthorized outsider?

Figure 1: People versus Technology

How does one avoid these threats or at least minimize them?

Know Thy Environment

A common phrase spoken among security professionals today is "Know Thy System." While this is very true, another perspective goes to a higher level, and is extremely important to retain: *Know Thy Environment*. The first step in any successful project is to know what you have to work with and know all the elements you are responsible to protect. Is the organization small or large? Does it have multiple departments acting as separate subsidiary organizations? Does it operate under central control or does each department have its own agenda? How many servers does the organization hold? What are the perimeters? Thus we have our starting point: *Know Thy Environment*. There are five areas to focus on; *Technology Management, Asset Management, Change Management, IP/DNS Management and Network Management.*

It is essential that these areas be securely in place and managed properly. It is close to impossible to protect an organization where elements of its network are not accounted for. These elements, possibly a rogue server or even a switch, are what predators prey on. These could be open doors to your network and without these fundamental departments/tools in place, you, as the security officer, may not even know they exist!

Technology Management

The Technology Management team rolls out standard builds, patching strategies and keeps up to date on emerging technologies. This is where it all starts and in this team you should find experts in the platforms used by the corporation.

Simplify the environment. Many organizations strive for one thing: customer satisfaction. Therefore some organizations will develop such a wide portfolio of

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

platforms and applications that they are under-educated in all of them. Identify the areas where your organization shines and educate your customers on how you can benefit them.

Otherwise, train your personnel adequately. Have the necessary educated resources on hand to satisfy your vast portfolio. Technology is all about learning and keeping up with the changes, so it is important to constantly strive for higher learning.

Asset/Configuration Management

Here we use the phrase: "*Know what is going on around you"*. The organization's asset management must know all elements of the environment, from firewall to end-user. This may seem difficult for larger organizations, but security professionals *must* have all pertinent information about their charges that is needed at any given time. How can one protect it if they are not aware of its existence or to whom it belongs? What if it is compromised and they don't know who is affected or even where it is physically located?

A properly managed central database that holds the answers to these questions and more is essential not only to security but the efficiency of daily business activities. The goal of Asset/Configuration Management is: "*To identify, record and report on all IT components that are under the control and scope of Configuration Management*." (ITIL Essentials, 2001) It must be one central database for the entire company, so be certain it is expandable.

The Asset Management database can be automated and real-time, tied into an automated tool, such as an IP discovery tool, making it easier to manage and easier to protect. Since this IP discovery tool is tied into the Asset Management database, it can quickly ascertain the validity of any element it finds on the network. If it finds any discrepancies between Asset/Configuration Management database and the discovered element(s), then through that database, the personnel involved can be identified, notified and the problem rectified. All this can be done by automation with little human intervention.

Change Management

The Change Management database and the Asset Management database will tie into each other on a number of levels. The Change Management is the communication point for all the databases and ties into the Asset Management database for information. Here is where we want: "*To ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to minimize the impact of change-related incidents and improve day-today operations.*" (ITIL Essentials, 2001) For example, this is where administrators schedule their changes and application owners are notified. Here is where we avoid mishaps by scheduling changes and getting approval. Change control identifies conflicts and avoids them.

This process must be policed and any personnel making changes to network elements must go through the change process. The process will break down if it is not monitored properly and employees who fail to go through the process must be held accountable. This is one of the most important aspects of the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

organization and many major problems can be avoided as a result of properly designed and administered change control.

Public IP/DNS Provisioning

IP/DNS Provisioning is where the distribution and allocation of IP addresses and domain names are managed. If the company is large and without an adequate IP/DNS Management area, it is possible for the company to misallocate or misuse IP addresses. This could mean high financial misappropriation, which results in inflated expenses, which in turn reduces profits. This could also mean that unauthorized persons might use your public or even internal IPs for their own purposes without the knowledge of management.

Public IPs and DNS are not cheap, so it is important that they are managed well. Using internal IPs is a logical way of disbursing a single public IP into multiple internal IPs. This can be done through the use of doing NAT (Network Address Translation) through a firewall. It makes solid business sense to efficiently manage IP and DNS holdings. (See "How Network Translation Works." http://www.howstuffworks.com/nat.htm)

From a security vantage, adequate IP/DNS Management, both public and internal, will result in a clear, organized IP and DNS structure, making it easier to locate discrepancies and deploy treatment tactics.

Network Management

Network Management manages all aspects of the network such as routers, switches, firewalls and so on. This area tracks all these elements in the Asset/Configuration Database. This is also where network diagrams are found and how the network itself is to be maintained. Any additions to the network, such as a router being deployed, must go through Network Management for the necessary approval.

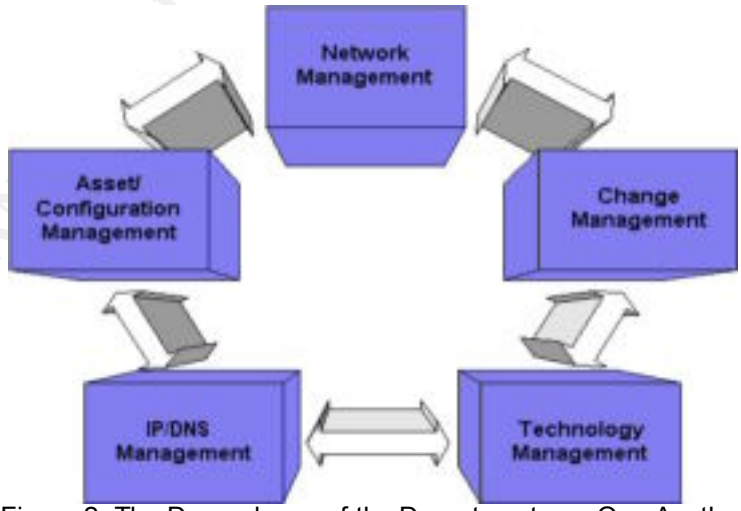

Figure 2: The Dependency of the Departments on One Another

Since all five of these areas are closely tied together, it is imperative that they co-exist functionally and cooperatively.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Maintain Thy Environment

The Operations Center revolves not only around the network but also around the people who use the network. Establishing a well-managed operations center will effectively reduce security issues, but also maximize the efficiency of the daily business operations. The aforementioned departments, Technology Management, Asset/Configuration Management, Change Management, IP/DNS Management and Network Management all fit into this area, as well as other key areas such as the Service Desk, Problem Management and Incident Management. All these areas encompass a large part of efficient management and security of the elements worth protecting.

The Service Desk

The Service Desk is the central point of communication within the organization. It is here that a customer can call with questions or problems. Here is where the organization may provide a single point of contact, not only for customers, but also for internal employees. The service desk begins the service request process, and is the starting point for incident response. Having a single point of contact ensures that when an incident is found, there will be a reduced amount of confusion on whom to contact. The service desk is trained and ready to coordinate the incident and pass it along to all those who need to be aware.

Problem Management

Problem Management focuses on the errors within the IT infrastructure. Problem management is essential because it analyses the current status of the network and attempts to resolve any issues that may adversely affect it. This area operates on both a proactive and reactive stance, effectively reducing negative business affecting situations.

Incident Management

Incident Management is a security strategy that is essential to any organization. All organizations will face security incidents, and will need to plan to react effectively. Incident Management deals with resolving incidents on a reactive basis, working with Problem Management to minimize incidents on a proactive basis.

Another part of Incident Management is the Incident Response Team. This team may consist of management from multiple areas within the organization, managed by a security professional. It is this team that responds to incidents, and a clearly laid out escalation plan needs to be implemented. For example, a routine Nessus[15] scan compared to an earlier Nmap[14] report shows some discrepancies. After some investigation it is decided that it is very likely that this server has a root kit* in place. It is therefore escalated to the Incident Response Coordinator who notifies the pertinent personnel of the issue and it is resolved thereof. Another example, a DDoS** attack begins, the situation is escalated to the Incident Response Team.

*Root Kit: A tool or set of tools/methods used to hide the presence of an unauthorized intruder.
**DDoS (Distributed Denial of Service): Similar to the DoS (Denial of Service) attack except that the data packets originate from multiple sources, usually coordinated by the original malicious hacker with the intent of drowning the server in requests so that it can no longer accept packets from legitimate sources, effectively stopping the server's service.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Patching and Updates

Applying the recommended patches and updates is part of routine administrative responsibility. Patching strategies should originate from Technology Management and the system administrators or the operations center are the ones to apply the patches. It should be stressed that this is an essential activity and should be incorporated into the performance evaluations of those involved.

Many OS vendors have developed methods of updating and patching systems that require less and less effort. Sun has recently developed patch analysis tools: "Patch Manager[21] and PatchPro[21]." Microsoft has simplified the update and patching process by way of rolling all the recommended modifications up into "service packs", for example where *SP3* (Service Pack 3) is the current version for Windows 2000. Linux Red Hat uses a program called "up2date[22]" which will retrieve the latest software packages from Red Hat. Numerous other vendors have developed similar tools to facilitate the patching and update process, leaving little to excuse the lack of patching and updating on a system.

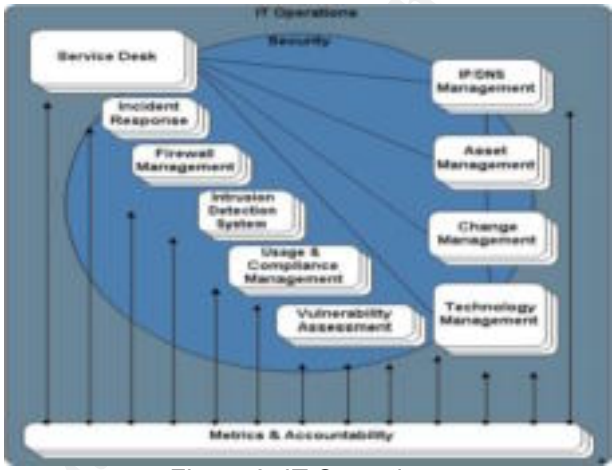

Figure 3: IT Operations

*Keep in mind that these are only the basic elements of a managed environment. An organization may have numerous departments within the IT infrastructure, the ones previously mentioned are simply a starting point to the IT infrastructure. All these departments are inter-related with security. Security plays a role in every aspect of the organization, from the IT department to finance.

Secure Thy Environment

Defense in Depth provides for multiple levels of defense. A firewall is not enough. Physical security is not enough. In order to achieve an adequate level of systems security, many levels must be protected and monitored. All of these levels are equally important. The following is a basic overview of security areas.

Physical Security

Physical security of an organization may encompass numerous aspects. Of note are the need to: Identify and secure locations that need to be physically

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

secured, establish access control policies, and secure all sensitive documentation. ITIL notes this as the "clear desk policy" where all documents are secured at the end of the working day. (ITIL Security Management, 2002) Be sure to secure equipment. Be prepared for power failures by securing power supplies, utilizing alternate power supplies such as the UPS. Ensure that cables are safely and properly installed to minimize cable issues. Keep all equipment well maintained.

Compliance and Usage Management

Though it is fundamental, security awareness can only go so far. Establishing set policies for the usage of the organization's assets is essential. Utilizing tools to maintain and monitor compliance can greatly increase the success of not only the security solution, but also the overall business success.

Tools for URL and Email Filtering, such as WebSense[2] and SurfControl[3], watch incoming and outgoing web and email traffic, and censors non-work related materials, such as entertainment web sites and pornography. Studies have shown that there are significant increases in cases of employee addiction to personal Internet use. (See: Websense's Employee Misuse Survey: http://www.websense.com/company/news/pr/00/102600.cfm.) Filtering can decrease these incidents and increase productivity.

Encryption

This is the process of encrypting data so that it is undecipherable to unauthorized parties. Encryption attempts to ensure the integrity and confidentiality of data. It is used to verify the authenticity of the person transferring the data as well as prove that the data was actually transferred from that person (non-repudiation). It is important that sensitive transfers be encrypted not only to hide the transfer from prying eyes, but also to prove the transfer is authentic and valid.

Many organizations are still using tools such as telnet and ftp (file transfer protocol). These communication transfer methods are unencrypted and the chances of the transfer being hacked are high. SSH (secure shell) offers an encrypted mode of communication and provides much of the same services as telnet and ftp. (See: OpenSSH, http://www.openssh.com)

Another mode of secure communication is to employ the use of VPNs (Virtual Private Networks). VPNs offer a secure method that organizations use for private secure communication over the public Internet. This method is employed for the reasons that it can reduce costs, which are incurred by installing telephone wire, cable and so on needed to implement a private network. (See: Virtual Private Network Consortium for info and a list of vendors, http://www.vpnc.org/.)

Authentication

Organizations have been applying physical authentication for centuries, from medieval passwords to today's retina scans. Yet the process of applying system authentication is a relatively new concept. Authentication in itself deals with validating that data has originated from its stated source, as well that the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

individual attempting to access a secured system or area is who they state they are. One of the most common methods of authentication is employing passwords, yet emerging technologies like biometrics* are quickly becoming popular.

Password cracking is becoming easier to perform therefore it is essential to have policies that enforce strong passwords. Passwords should have set minimums, such as six characters or more and encompass more than one type of character, employing letters and numbers, special characters and even ASCII. Policies should also enforce that the passwords be changed on a regular basis, for example, once a month.

Another method to avoid password cracking is employing the use of one-time passwords via smartcards. This method reduces the chance of an attacker gaining access to the network through password cracking/guessing. It also reduces the 'social engineering hacker', as the password will not be based on personal experience.

Every security professional should note that they are not only trying to achieve a secure environment, but also retain the necessary functionality their users require. Therefore it can be difficult to implement password policies that demand changing passwords often or carrying smartcards. Implementing an authentication procedure should go hand in hand with an awareness campaign. It does little good to change passwords every month when the users are writing their passwords on sticky notes and hiding them under their keyboard, or using the name of their dog as a password. With this in mind, each organization must assess its own strengths and weaknesses and create a customized authentication atmosphere.

Many companies offer managed authentication packages that can control authentication policies. Novell[4], eToken[5], CryptoAdmin[6] are all such companies that offer authentication packages. Novell offers a range of authentication features, ranging from biometrics, enforcement of strong password policies and automatic lockdowns after a period of inactivity. Both eToken and CryptoAdmin provide smartcard solutions, with eToken also encompassing VPN, network logon as well as other authentication techniques.

In order to assess the strength of password, tools such as LC3/LC4 for Windows and Crack for UNIX can be utilized. These tools attempt to decrypt encrypted passwords and if successful, and will notify the administrator of the fact.

Intrusion Detection Systems Management

Intrusion Detection Systems work to identify possible breaches in the network, or a pattern of attacks, successful or not, that are deemed of interest to the organization. When applying Intrusion Detection Systems it is best to use both host based and network based systems on a real-time basis. This Defense in Depth strategy assures better coverage when monitoring unauthorized attempts to access both the network and the system.

Host based intrusion detection systems concentrate on monitoring individual

*Biometrics: The study of biological differentiators, where in the security field it may be used for authentication, for example fingerprint or retina scanning.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

systems. They monitor the log files for the system or for an application and can notify the administrator of any irregular activity. Some examples of host based intrusion detection systems are ManTrap® by Recourse Technologies[7] and TripWire[8].

Network based intrusion detection systems monitor the network traffic. These systems will send an alarm when they detect patterns of traffic that they identify as a scan, or as an attack such as a DoS (Denial of Service) attack. Examples of network based intrusion detection systems include ManHunt™ by Recourse[7] Technologies and SNORT[10].

When an intrusion has been found, follow the Incident Response procedures set by the IDS Management area. If a system has been compromised, there are certain incident response steps to follow. It is essential that the IDS Management area has the necessary authority to pull the plug on any element it deems as compromised.

Firewall Management

Firewalls are a form of perimeter defense where they can eliminate unwanted intrusions via a ruleset of who to allow and who to deny. There are many different types of firewalls, ranging from packet filtering firewalls, stateful inspection firewalls to proxies.

As security is enhanced, functionality decreases. Similarly with firewalls, as security increases, speed decreases. That is what differentiates packet filtering, stateful inspection and proxy (See Figure 4). A router for example, uses packet filtering, which is fast and will enhance security, but it can be fooled because it checks the fields in the packet, not the data content. Stateful Inspection, like GTA's Gnat Box, tracks the packets and logically assesses the session. This form of firewall is better for its security tactics, but is slower than packet filtering. Finally proxies, such as Novell's Bordermanager[4] capabilities, go through each level of the protocol stack, then back up, to communicate the data. Proxies are secure firewall alternatives although their process of tearing down and building back is time consuming. Therefore it is much slower than the less secure packet filter. (See: Facts About Firewalls, http://www.netguard.com/subpages/about_facts.htm)

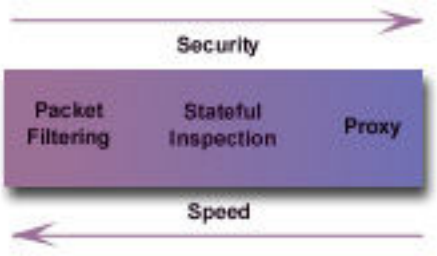

Figure 4: Security versus Speed

Simply having a firewall is not nearly enough, but it is an essential starting point to a security structure. Employing the use of a firewall is the least an organization can do for security measures. Yet a firewall is fallible. If the policies are not firmly in place, firewalls can effectively do nothing against certain attacks. The firewalls guarding the systems are directly dependent on the administrator's

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

competencies. Therefore, set guidelines on which of the organization's allow/deny policies are essential.

Also, firewalls themselves should be monitored regularly, with logging policies properly in place. Without the logs, the organization has no idea what potential threats are attacking, as well as what traffic is passing through the firewall. Logs should be maintained and monitored, and set to alert the administrator if unusual or suspicious activity is noticed. Checkpoint[11], Cyberguard[12], and Gnat Box[13] are all firewalls that vary in options and capabilities.

Vulnerability Assessment

Vulnerability Assessment is the process of scanning, investigating and gathering information on a system or network's security weakness. Vulnerability Assessment can be a port scan, an ethical hack or a combination of multiple strategies. One of the core elements of an anti-hacking strategy is performing routine vulnerability assessments as well as assessing the vulnerabilities of new servers before they go into production mode. Vulnerability assessments should be done using a multitude of tools, or by hiring a third party firm to assess your vulnerability status. Performing these scans can be done in-house without too much trouble, and can be fairly inexpensive to implement. Training a range of individuals, with a range of backgrounds can lead to a very effective vulnerability assessment team. Open source tools such as Nessus[15] and Sara[16] are cost efficient but can require a fair amount of know-how. On the whole, they are excellent products and can adequately assess the vulnerability status of a server. NMAP[14] is a tool that performs port scans, OS detection and more. It is recommended because it is a tool frequently used by malicious hackers to expose holes in prey networks. Many vendors supply vulnerability assessment tools and it is up to the organization to decipher which tool(s) would best suit their needs.

Anti-Virus

Anti-virus (AV) protection is a necessity in any organization. From antivirus software that is located on the server, to antivirus software located on the end-user's system. Using a mixture of both will substantially lower the risk of intrusions by viruses, trojans or worms and provide a form of Defense In Depth required in a solid security solution. Some antivirus software outfits include Symantec (Norton[17]), Trend[18] and McAfee[19].

Auditing

Effectively controlling the elements in your organization can directly depend on your auditing technique and tools. There are many tools that can aid the auditor's plight, such as NMAP[14] and ethereal[20].

Auditing is well worth the effort, it can identify the organization's weaknesses, and find system/network compromise or employee misuse. It is essential to investigate these and work to develop strategies that avoid these issues on an ongoing basis. (See: A Guide To Understanding Audit in Trusted Systems, http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-001-2.html, 1 June 1988)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

These are but a portion of all the aspects of a complete security solution. Others include Penetration testing, web server security, the use of routers and bridges, emerging technologies and so on.

Metrics and Accountability

The ability to measure the effectiveness or non-effectiveness of your solutions is essential. Evaluating whether or not your policies are being followed leads to the strengths and weaknesses in the human aspect of your security solution. It can also account for your weaknesses in the technology aspect of your organization.

It is wise to incorporate the maintenance of servers within the system administrators' performance evaluations – including patching and keeping up to date on recommendations of Technology Management.

Another element is accountability. Your configuration management database should be continually maintained and contain accurate and up to date information on who is responsible for individual elements on the network. With this, it should be that responsible party who is accountable for on-going maintenance such as updating the platforms and applying recommended patches.

Law Enforcement

Working with a representative of your local law enforcement agency will not only benefit your organization, but also all users of the Internet. Many organizations do not like to advertise that they have had a compromise of some sort. Yet, if they do not notify the authorities, the attacker will not be caught. Therefore, establishing a relationship with a representative from a law agency may help to lower the profile while still persecuting the criminal.

It is advisable to follow the corporate legal guidelines and work with your organization's legal department to develop the policy and process of escalating hacking attacks to law enforcement authorities. Following a defined and clear process can be the difference in catching an attacker and letting the attacker get away.

Summary

Most organizations are concerned with a vast array of issues. Within the IT department, they desire cost efficiency and timeliness of investment into IT undertakings. Resources, human and technological need to be rationalized and accountable. Organizations want secure technological environments that are both functional and reliable, in addition to wanting a return on investment as well as positive results. This is difficult to do in the realm of security. Without security, the organization will fail, but how does the security professional foretell the future when it has not yet come to pass? The decision-makers need to understand firsthand the risk, and the consequences associated with those risks. Risk analysis is key here. Another astonishing factor is that many organizations do not have the fundamental foundational elements, such as Asset Management and Change Control, firmly in place. Some organizations do not have a firm grasp on their network perimeters, or how many servers are operating within their environment.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Implementing a security solution does not only encompass firewalls and vulnerability assessments, but also the tools and the reorganization necessary to first implement the core-managed areas within the organization. Cooperation from all the departments is a must, as well as the assignment of necessary authority and accountability. ITIL gives a common sense approach to the IT infrastructure, and helps to develop a common perspective on the actual makeup of the infrastructure. Security cannot simply be implemented on an efficient level without first organizing the organization. Security is at its best in multi-level, expandable and adaptable situations. Defense in Depth begins at the core network areas and must be assimilated into the entire organizational structure in order to succeed.

*Please note that the tools mentioned in this document encompass only a portion of the utilities available. They are mentioned only to provide a starting point to the search for the right tool/vendor for an organization. A security solution must first assess the organization's network status, business needs, etc, including the tools/vendors currently used by the organization, and then customize the security solution to their specific needs and expectations. A tool may better benefit one organization than another organization and vice versa.

Resources

Pink Elephant Inc., ITIL IT Service Management Essentials Ver 5.1, Burlington: Pink Elephant Inc., 1 Aug 2001

Cazemeir, Inq. Jaques A./Overbeek, Dr. Ir. Paul L./Peters, Drs. Louk M.C., Security Management (ITIL), Carleton: The Stationary Office, March 2002

Zimmerman, Scott C. "Secure Infrastructure Design". 1 Jul 2002. http://www.isalliance.org/resources/papers/Secure_Infrastructure_Design.pdf (1 Aug 2002.)

Scalet, Sarah D./Berinato, Scott, "The ABCs of Security", 20 Feb 2002 http://www.cio.com/security/edit/security_abc.html (23 Jul 2002)

Berinato, Scott, "Finally, A Real Return on Security Spending, 15 Feb 2002 http://www.cio.com/archive/021502/security.html (26 Jul 2002)

Gallagher, Patrick R. (Jr.), "A Guide To Understanding Audit in Trusted Systems", National Computer Security Center, 1 Jun 1988, http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-001-2.html (28 Jul 2002)

Avolio, Frederick M., "A Multi-Dimensional Approach to Internet Security" May 1998, http://www.avolio.com/MultiDimensional.html (28 Jul 2002)

The SANS Institute, "Essential Security Actions: Step by Step." 1999 http://www.sans.org/newlook/resources/esa.htm (1 Aug 2002)

References continued…

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Tyson, Jeff, "How Network Translation Works."
http://www.howstuffworks.com/nat.htm (3 Sep 2002)

Gartner Inc., "Social Engineering: Exposing The Danger Within" 22 Oct 2001
http://www.gartner.com/gc/webletter/security/issue1/ (4 Sep 2002)

Websense Press Release, "Landmark New Survey Shows Employee Internet Misuse Goes Beyond Porn, But Employer Balance is Needed"
http://www.websense.com/company/news/pr/00/102600.cfm (4 Sep 2002)

Tatone, Daniel "Network Security: What are you waiting for?" 7 May 2001
http://online.securityfocus.com/guest/5560 (4 Sep 2002)

NetGuard Inc. "Facts About Firewalls"
http://www.netguard.com/subpages/about_facts.htm (5 Sep 2002)

Graphics

The author (Allison Jones) created all graphics (figures) used in this document.

Products/Organizations listed in document:

[1] PentaSafe (http://www.pentasafe.com)
[2] Websense (http://www.websense.com)
[3] SurfControl (http://www.surfcontrol.com)
[4] Novell (http://www.novell.com)
[5] eToken (http://www.ealaddin.com/etoken/default.asp?cf=tl)
[6] CrytoAdmin (http://www.cryptocard.com/)
[7] Recourse Technologies (http://www.recourse.com/index.html)
[8] TripWire Inc, (http://www.tripwire.com)
[9] Cisco (http://www.cisco.com)
[10] SNORT (http://www.snort.org)
[11] Checkpoint (http://www.checkpoint.com)
[12] CyberGuard (http://www.cyberguard.com/HOME/home.cfm)
[13] Gnat (http://www.gta.com)
[14] NMAP (http://www.insecure.org/nmap)
[15] Nessus (http://www.nessus.org)
[16] Sara (http://www-arc.com/sara)
[17] Symantec: Norton (http://www.symantec.com/nav)
[18] Trend (http://www.antivirus.com)
[19] McAfee (http://www.mcafee.com)
[20] ethereal (http://www.ethereal.com)
[21] Sun (http://sunsolve.Sun.COM/pub-cgi/show.pl?target=patchpage)
[22] Red Hat (http://www.redhat.com/docs/manuals/RHNetwork/ref-guide/up2date.html)

© SANS Institute 2000 - 2002 Author retains full rights.

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS