Global Information Assurance Certification Paper

The Basics of an IT Security Policy

By Jack G. Albright
March 25, 2002

GSEC Practical Requirement V.1.3

Table of Contents

Purpose

This paper is intended to address the importance of having a written and enforceable Information Technology (IT) security policy, and to provide an overview of the necessary components of an effective policy. The reader will gain an understanding of the basic processes, methodologies, and procedures needed to initiate the development of an organization-wide IT Security Policy.

When developing an IT Security Policy you should keep in mind the 'defense in-depth ' model. In other words, you should not be relying on one principal means of protection (or layer), instead, you should develop your security program so that it provides multiple layers of defense. This will ensure maximum protection of your data and resources and will minimize the potential for compromise.

Please keep in mind that we can only protect ourselves from known and existing exploits. We are all possible targets of zero day exploits! However, an effective IT security program will be enable you to detect anomalies in network traffic and take the necessary steps toward mitigation. (i.e., proactive v/s reactive).

What is an IT Security Policy?

An IT Security Policy is the most critical element of an IT security program. A security policy identifies the rules and procedures that all persons accessing computer resources must adhere to in order to ensure the confidentiality, integrity, and availability of data and resources. Furthermore, it puts into writing an organization's security posture, describes and assigns functions and responsibilities, grants authority to security professionals, and identifies the incident response processes and procedures.

Note: The security-related decision's you make, or fail to make largely determine how secure or insecure your network is, how much functionality your network offers, and how easy your network is to use. However, you cannot make good decisions about security without first determining what your security goals are. Until then, you cannot make effective use of any collection of security tools because you simply will not know what to check for and what restrictions to impose. [1]

What Determines a Good IT Security Policy?

In general a good IT Security Policy does the following:

- Communicates clear and concise information and is realistic;
- Includes defined scope and applicability;
- Makes enforceability possible;
- Identifies the areas of responsibility for users, administrators, and management;
- Provides sufficient guidance for development of specific procedures

- Balances protection with productivity;
- Identifies how incidents will be handled; and
- Is enacted by a senior official (e.g., CEO)

Development of a security policy should be a collaborative effort with security officials, management, and those who have a thorough understanding of the business rules of the organization. A security policy should not impede an organization from meeting its mission and goals. However, a good policy will provide the organization with the assurance and the "acceptable" level of asset protection from external and internal threats.

What are the Components of a Security Policy?

A key point to consider is to develop a security policy that is flexible and adaptable as technology changes. Additionally, a security policy should be a living document routinely updated as new technology and procedures are established to support the mission of the organization.

The components of a security policy will change by organization based on size, services offered, technology, and available revenue. Here are some of the typical elements included in a security policy.

Security Definition – All security policies should include a well-defined security vision for the organization. The security vision should be clear and concise and convey to the readers the intent of the policy. In example:

> "This security policy is intended to ensure the confidently, integrity, and availability of data and resources through the use of effective and established IT security processes and procedures."

Further, the definition section should address why the security policy is being implemented and what the corresponding mission will entail. This is where you tie the policy to the mission and the business rules of the organization.

Enforcement – This section should clearly identify how the policy will be enforced and how security breaches and/or misconduct will be handled.

The Chief Information Officer (CIO) and the Information Systems Security Officer (ISSO) typically have the primary responsibility for implementing the policy and ensuring compliance. However, you should have a member of senior management, preferably the top official, implement and embrace the policy. This gives you the enforcement clout and much needed 'buy-in'.

This section may also include procedures for requesting short-term exceptions to the policy. All exceptions to the policy should be reviewed and approved, or denied, by the Security Officer. Senior management should not be given the

flexibility to overrule decisions. Otherwise, your security program will be full of exceptions that will lend themselves toward failure.

User Access to Computer Resources - This section should identify the roles and responsibilities of users accessing resources on the organization's network. This should include information such as:

- Procedures for obtaining network access and resource level permission;
- Policies prohibiting personal use of organizational computer systems;
- Passwords;
- Procedures for using removal media devices;
- Procedures for identifying applicable e-mail standards of conduct;
- Specifications for both acceptable and prohibited Internet usage;
- Guidelines for applications;
- Restrictions on installing applications and hardware;
- Procedures for Remote Access;
- Guidelines for use of personal machines to access resources (remote access);
- Procedures for account termination;
- Procedures for routine auditing;
- Procedures for threat notification; and
  Security awareness training;

Depending on the size of an organization's network, a more detailed listing may be required for the connected Wide Area Networks (WAN), other Local Area Networks (LAN), Extranets, and Virtual Private Networks (VPN).

Some organizations may require that other connected (via LAN, WAN, VPN) or trusted agency's meet the terms and conditions identified in the organization's security policy before they are granted access. This is done for the simple reason that your security policy is only as good as the weakest link. For example, If Company 'A' has a rigid security policy and Company 'B' has a substandard policy and wants to partner with Company 'A', Company 'B' may request to have a network connection to Company 'A' (behind the firewall). If Company' A' allows this without validating Company 'B's' security policy then Company 'A' can now be compromised by exploits launched from Company 'B'.

When developing a security policy one should take situations such as this one very serious and develop standards that must be met in order for other organizations to be granted access. One method is to require the requesting organization to meet, at a minimum, your policy and guidelines.

Security Profiles - A good security policy should also include information that identifies how security profiles will be applied uniformly across common devices (e.g., servers, workstations, routers, switches, firewalls, proxy servers, etc.). The

policy should reference applicable standards and procedures for locking down devices. Those standards may include security checklists to follow when adding and/or reconfiguring devices.

New devices come shipped with the default configuration for ease of deployment and it also ensures compatibility with most architectures. This is very convenient for the vendor, but a nightmare for security professionals. An assessment needs to be completed to determine what services are necessary on which devices to meet the organizational needs and requirements. All other services should be turned off and/or removed and documented in the corresponding standard operating procedure.

For example, if your agency does not have a need to host Internet or Intranet based applications then do not install Microsoft IIS. If you have a need to host HTML services, but do not have a requirement for allowing FTP, then disable it.

Additional information for securing some vendor devices can be found at the following web sites:

- http://www.microsoft.com
- http://www.cisco.com
- http://www.sun.com
- http://www.novel.com

Passwords - Passwords are a critical element in protecting the infrastructure. Remember, your security policy is only as good as the weakest link. If you have weak passwords then you are at a higher risk for compromise not only by external threats, but also from insiders. If a password is compromised through social engineering or password cracking techniques, an intruder now has access to your resources. The result will mean that, you have just lost confidentiality and possibly the integrity of the data, and availability may have been compromised or in progress.

The policy should clearly state the requirements imposed on users for passwords. Passwords should not be any of the following:

- Same as the username;
- Password;
- Any personal information that a hacker may be able to obtain (e.g., street address, social security number, names of children, parents, cars, boats, etc.);
- A dictionary word; or
- Telephone number

These are some examples of passwords not to use. You should force users through automated password policy techniques to require a minimum of eight

characters, use of a combination of symbols, alpha charters, and numerals, and a mixture of uppercase and lowercase. Users should be required to change their password at least quarterly. Previous passwords should not be authorized. Lastly, an account lockout policy should be implemented after a predetermined number of unsuccessful logon attempts.

Another tip to consider is that you should be logging all successful and failed logon attempts. A hacker may be trying several accounts to logon to your network. If you see several 'failed' logon attempts in a row and then no activity; does this mean the hacker gave up or did he "successfully" logon?

E-mail – An email usage policy is a must. Several viruses, Trojans, and malware use email as the vehicle to propagate themselves throughout the Internet. A few of the more recent worms were Code Red, Nimda, and Gonner. These types of exploits prey on the unsuspecting user to double click on the attachment thereby infecting the machine and launching propagation throughout the entire network. This could cause several hours and/or days of downtime while remedial efforts are taken.

A couple of things you may want to address in your policy are content filtering of email messages. Filtering out attachments with extensions such as *.exe, *.scr, *.bat, *.com, and *.inf will enhance your prevention efforts. Also, personal use of the email system should be prohibited. Email messages can and have been used in litigation (Microsoft anti-trust case). This includes all email messages both personal and business. Additionally, some institutions archive email messages indefinitely (Federal Government). Those messages are subject to the Freedom of Information Act (FOIA) requirements. Just think how embarrassing it would be if several email messages with vulgar content were released to a law firm or the media. This could have significant negative publicity for your organization.

Internet – The World Wide Web was the greatest invention, but the worst nightmare from a security standpoint. The Internet is the pathway in which vulnerabilities are manifested. The black-hat community typically launches their 'zero day' and old exploits on the Internet via IRC chat rooms, through Instant Messengers, and free Internet email providers (hotmail, yahoo, etc.). Therefore, the Internet usage policy should restrict access to these types of sites and should clearly identify what, if any, personal use is authorized.

Moreover, software should be employed to filter out many of the forbidden sites that include pornographic, chat rooms, free web-based email services (hotmail, Yahoo, etc.), personals, etc. There are several Internet content filtering applications available that maintain a comprehensive database of forbidden URLs. The following are being provided for additional information.

- http://www.superscout.com

- http://www.telemate-software.com/internet_monitoring_software.htmhttp://www.symantec.com

Anti-Virus - Anti-virus software is a 'must' in the detection and mitigation of viruses. The policy should identify the frequency of updating the virus definition files. The policy should also identify how removable media, attachments to email, and other files should be scanned before opening. Your anti-virus software should be configured to automatically scan all incoming and outgoing files. If a virus is found you need to identify what action should be taken (e.g., clean, notify administrator, deny access to file, etc.). Anti-virus vendors include:

- Mcafee (http://www.mcafee.com)
- Norton (http://www.symantec.com)
- Computer Associates Innoculate IT (www.ca.com/innoculate)

Back-up and Recovery – A comprehensive back-up and recovery plan is critical to mitigating incidents. You never know when a natural or other disaster may occur. For example take the 9/11 incident. What would have happened if there were no off-site storage locations for the companies in the World Trade Center?

Answer: All data would have been permanently lost! Back-ups are your key to the past. Organizations must have effective back-up and recovery plans that are established through a comprehensive risk assessment of all systems on the network. Your back-up procedures may be different for a number of systems on your network. For example, your budget and payroll system will have different back-up requirements than a miscellaneous file server.

You may be required to restore from a tape back-up, if the system crashes, you get hacked, upgrade hardware, and/or files get inadvertently deleted. You should be prepared. Your back-up and recovery policy (separate document) should stand on its own , but be reflected in the security policy. At a minimum, your back-up recovery plan should include:

- Back-up schedules;
- Identification of the type of tape back-up (full, differential, etc.)
- The type of equipment used;
- Tape storage location (on and off-site);
- Tape labeling convention;
- Tape rotation procedures;
- Testing restorations; and
- Checking log files.

Intrusion Detection – A Network Intrusion Detection System (NIDS) is a system that is responsible for detecting anomalous, inappropriate, or other data that may be considered unauthorized occurring on a network. Unlike a firewall, an NIDS captures and inspects all traffic, regardless of whether it's permitted or not. Based on the contents, at either the IP or application level, an alert is generated [4]

Intrusion detection tools will help assist in the detection and mitigation of access attempts into your network. You need to make the decision through the risk assessment process of whether to implement network or host based NDIS or a combination of both. Additional standard operating procedures should be derived form the policy to specifically address intrusion detection processes and procedures. Following are some examples of NDIS systems:

- ISS - (http://www.iss.com)
- Cisco - (http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/)
- Snort - (http://www.linuxsecurity.com/feature_stories/using-snort.html)
- Zone Alarm – (http://www.zonealram.com)

Remote Access - Dial-up access to your network will represent one of your greatest risks. Your policy should identify the procedures that one must follow in order to be granted dial-up access. You also need to address whether or not personal machines will be allowed to access your organization's resources.

The whole issue of remote access causes heartburn for security officials. You can lock down you're your perimeter, but all it takes in one remote access client dialing into the network (behind the firewall) who has been compromised while surfing the Internet with that Trojan ready and willing to start looking for other unsuspecting prey. Next thing you know your network has been compromised. Following are some examples to include in your policy:

- Install and configure personal firewall on remote client machines (examples, Norton or BlackIce Defender);
- Ensure antivirus software, services packs and security patches are maintained and up-to-date;
- Ensure modems are configured to not auto answer;
- Ensure file sharing is disabled;
- If not using token or PKI certificates, then username and password should be encrypted;
- If possible push policies from server to client machines; and
- Prohibit the use of organizational machines from being configured to access personal Internet Service Provider accounts.

Auditing - All security programs should be audited on a routine and random basis to assess their effectiveness. The security officer must be given the authority, in

writing, by the head of the organization to conduct audits of the program. If not, he or she could be subject to legal action for malicious conduct. Random and scheduled audits should be conducted and may include:

- Password auditing using password cracking utilities such as LC3 (Windows) and PWDump (Unix and Windows);
- Auditing user accounts database for active old accounts (persons who left the agency)
- Penetration testing to check for vulnerabilities using technical assessment tools such as ISS and Nessus;
- Social Engineering techniques to determine if you can get a username or password from a staff member;
- Simulate (off hours) network failure and evaluate your incident response team's performance and readiness;
- Test your back-up recovery procedures;
- Use Tripwire or similar product to monitor your critical binary files;
- Configure your Server OS to audit all events and monitor several times a day for suspicious activity;
- Use a port scanner (Nmap, Nessus, etc.) within your network to determine if your system administrators catch the traffic and take appropriate action.

These are just a few examples of the things to audit. The extent of your auditing will depend on the level of your security program.

Awareness Training - Security Awareness training for organizational staff must be performed to ensure a successful program. Training should be provided at different levels for staff, executives, system administrators, and security officers. Additionally, staff should be retrained on a periodic basis (e.g., every two years). A process should be in place for training newly hired staff within a certain time period. Staff completing training should be required to sign a written certification statement. This signed statement helps the security officer and management enforce the organization's security policies.

Trained staff can help alleviate some of the security burden from security officers. Trained staff can and often do provide advanced notification of suspicious events encountered on their machines which could prevent a worm or other Trojan from propagating throughout the entire network.

Conclusion

I hope this paper provides you with a better understanding of the importance of an effective IT Security policy. Security polices are crucial to ensuring the protection of organizational assets. From polices, standards and procedures are developed that are enforceable. Without formal policy, standards and procedures will be ad-hoc and staff will have no accountability.

There are standards published by the National Institute of Standards and Technology (NIST) and the International Service Organization (ISO) that should be followed when developing a security policy. This will ensure your policy is in alignment with current standards. Lastly, your policy should not be placed on a shelf collecting dust. They should be living breathing documents that all staff are aware of and follow.

References

[1] Fraiser, B, "Site Security Handbook", September 2000. http://www.cis.ohio-state.edu/cgi-bin/rfc2196.html

[2] Information Security and Disaster Recovery, IT Security Policy and Implementation http://www.network-and-it-security-policies.com/

[3] International Standards Organization, ISO/IEC 17799:2000(E), Information Technology, Code of Practice for Information Security Management, 2000

[4] Wreski, Dave and Pallack, Christopher, Network Intrusion Detection Using Snort, June, 2000 http://www.linuxsecurity.com/feature_stories/feature_story-49.html

[5] Goncalves, Marcus and Brown, Steven, Check Point Firewall 1, "Administration Guide, 2000.

[6] SANS Institute, Basic Security Policy, Security Essentials, Network Security, Vol. 1.2

[7] Bowden, Joel, "Security Policy: What it is and Why – The Basics", August 14, 2001 http://rr.sans.org/policy/sec_policy.php

[8] Bug Traq: FAQ http://www.securityfocus.com/frames/?content=/forums/bugtraq/faq/faq.html

[9] Microsoft Windows Security, http://www.microsoft.com/security/default.asp

[10] NT Security, http://www.ntsecurity.com/security-news.asp

[11] SANS Institute, http://www.incidents.org

[12] Zone Alarm, http://www.zonealarm.com

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event