;login:

THE MAGAZINE OF USENIX & SAGE
December 2000 • volume 25 • number 8

inside:

SECURITY:

WHY SHOULD YOU ENFORCE A NETWORK SECURITY POLICY?

USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

why should you enforce a network security policy?

by Gary Bahadur

Gary is the Chief Information Officer for Foundstone Inc <*www.foundstone.com*>. He has been performing security assessments for the past 6 years and teaching security training courses for the past 2 years.

<gary.bahadur@foundstone.com>

The purpose of a network security policy is to protect all proprietary and confidential information assets from unauthorized access, disclosure, modification, misuse, or destruction. In any organization, regardless of size, such a policy is a requirement for the secure functioning of the environment. A policy ensures that the necessary protection is enabled for essential business activities to be conducted. A good policy establishes the necessary procedures to enable productivity, security, accuracy, and availability of data and resources.

Organizations frequently mistake procedures for a policy. A policy is the vehicle that implements all security procedures. A policy can define what the parameters are for the organization's security stance and what procedures and low-level details are necessary to enforce it.

No Policy = Get Hacked

This is a pretty bold statement, but all organizational security is derived from policy enforcement or lack thereof. Enforcement of policy is the major problem in most organizations. Too general a policy will allow procedures or actions that should not be permitted. Too restrictive a policy will cause users to break or ignore it. A good policy is useless if management does not support it and enforce its usage. Management can actually be the worst enemy of a good policy. If management does not understand the need for a security policy, you might as well open the doors and welcome the hackers in. This article describes how to set up a usable network security policy that is easily enforceable and can be scaled to support different types of organizations.

When defining a network security policy, the first question that has to be answered is, "To whom does this apply?" The correct answer is everyone. There are many disparate groups in any organization, but one of the things they all have in common is the need for security. It does not matter what type of company it is; one network security policy needs to be applied across the board and adhered to for any kind of security to be in place.

The first group within the organization that the policy has to address is the user community. As power is increasingly placed in the hands of users, their responsibility for security is increased. The policy must spell out what their responsibilities are for securing the organization.

The next groups that need to be addressed by the policy are the system administrators and network administrators. The bulk of security issues concerns the system administrators. As with users, the network security policy must address their roles and responsibilities for security.

Administrators frequently encounter situations in which breaking the policy would provide a convenient and practical way to solve some problem quickly. In any production environment, this may seem a necessary thing to do. When it becomes habit, however, the reason for the policy becomes lost. The security of the network can be compromised very quickly if expedient rather than secure methods are used that fall outside the network security policy. The policy must be flexible enough to address emergency situations yet keep the environment secure.

Test environments are notorious for security weaknesses that can compromise production environments.

One of the great pitfalls of many environments with security policies occurs when administrators set up test environments that do not adhere to the policy. Test environments are notorious for security weaknesses that can compromise production environments.

The third group that is crucial to the success of a network security policy is management. Without management's full support of and adherence to the policy, it will fail. Management that skirts the policy for convenience sets the example for the rest of the organization. A top-down approach to security is necessary to gain buy-in by all users in the organization.

Policy Definition

What makes a good policy? In a UNIX environment, the qualities that make up a good network security policy can also be applied to most other environments. A general policy that can be applied to various network environments must describe all aspects of the environments, from system usage to the configuration of password controls, in detailed procedural documents. As a general rule, a network security policy has to address the following areas:

Roles and Responsibilities

A key aspect of the security policy is the definition of principal roles and responsibilities. Positions such as Security Office, System Administrator, Database Administrator, and Information Security Committees have to be defined by the policy.

System Usage

- An awareness of the importance of security must be disseminated to all users in the organization. Users need to learn system usages' security issues in some detail.
- Users must have authority to utilize the system.
- That authorization must be given by management.
- Management must also define the manner in which the systems can be used.
- The proper use of email has to be specified.
- Users may not use the system for unauthorized activities such as setting up bulletin boards or warez servers.
- Moves between departments or levels usually change user access privileges.
- Information defining the proper usage of the system upon login should be determined in the policy.
- Time restrictions such as automatic logoff, restricted night access, and weekend access should be specified by the policy based on job function.
- The ability of third parties to access internal systems should be clearly defined in the policy. How third parties connect, when they can connect, and what systems and data they have access to should be addressed.
- Methods of connecting to the internal and external systems, the encryption methods that are to be used, and authentication methods need to be clearly described. Access paths can cause numerous problems and should be clearly defined.

Confidentiality

- The levels of confidentiality of information must be defined, and user access to each level must be authorized. Each level should be labelled, e.g, Secret, Confidential, and Public.
- Data networks must be secured through the use of an appropriate combination of controls, including authentication, validation, and logging. Encryption standards for the transmission of data must be implemented to keep it confidential.

- Encryption standards must be established. Encryption can be used for documents both publicly and internally transmitted.
- The policy must state who can disseminate information, what type of information can be disclosed, and where.
- The privacy of user information and company information must be established, in particular, management has to define what privacy rights users will have.
- The policy must describe how user activity is tracked through log files and when management can use logs to follow up on suspicious activity.
- The privacy of email must be determined, and users notified when email can be read by management and what their rights are to personal email.
- Information should be available only on a need-to-know basis.

Password/Account Management

- Password strength is a key security measure in any organization. Standard measures of password strength include alphanumeric, 6+ characters in length, nondictionary words, and special characters.
- Passwords must be changed periodically and should not be written down or shared.
- Procedures should be in place to authorize users to obtain an account and password and to provide for the secure dissemination of the account information.
- Secure initial passwords should be set. Forced password changes should be implemented if the system cannot do it automatically.
- Accounts should follow a predefined scheme for creation, modification, and deletion. Accounts should be disabled when not active.
- Account review should be done periodically to validate all users.
- Unsuccessful account login attempts should be investigated and reported.
- Newer technologies such as token authentication should be explored to increase password security where possible.
- A process for securing vendor software to strengthen weak passwords should be in place.

Application Usage

- Define how encryption should be used for critical application connections or data transfers.
- Virus protection for both applications and the operating system must be established. Updates of the virus-checking software must be timely and efficient. Viruses targeted at email and Web usage are on the rise and should be addressed.
- Software installations by both users and administrators should be authorized and done according to license agreements. The policy should deal with the issue of copyright agreements.
- Application design and usage should follow set security procedures that provide secure operations.
- Proper usages of applications and data for business and nonbusiness purposes should be defined.
- User access to applications should be based on necessity and authorized access. The policy should detail who can access what types of applications and data.
- Developer access to production applications and data should be closely monitored, and records reviewed to restrict the possibility of internal security breeches or unauthorized application changes.

Password strength is a key security measure in any organization.

Remote access through either Internet connections or dial-up connections should be monitored and audited.

Internet Usage

- The business purpose of Internet usage should be clearly defined for both users and administrators. Users should sign an authorization form outlining the rules of proper Internet access..
- Sending data across the Internet will usually be in clear text. The policy should define what types of data can be transferred in the clear and which data should be encrypted.
- Email from and to the Internet should be closely monitored, checked for viruses, and authorized.
- The policy should describe how system administrators monitor Internet usage and track activity, whether authorized or unauthorized.
- All Internet services should be authorized. Administrators and users should not be allowed to start or stop new services without authorization. The policy should address how services are authorized, used, and monitored. Both inbound and outbound servers need to be restricted.

Backup and Recovery of Data

- Data backup and recovery parameters should be set forth in the policy. General outlines such as how often and who performs backup and recovery should be described. Detailed procedures for operating systems and application data can be handled by individual procedural documents.
- User backup of data should be addressed in the policy. Users often have data on desktops that does not get backed up on a regular basis.

Development Process

- The development process should be defined to follow set procedures. Change-control procedures have to be defined as part of the development process.
- Security should be determined before an application is completed. The details have to be developed in the procedures of the development life cycle.

Reporting/Auditing

- Security violations or concerns need to be defined, and the process or chain of command needs to be defined. Problems can include viruses, hacker attempts, system-administration errors, or internal employee problems.
- Audits should address all system areas to report problems such as invalid login attempts, invalid access to production data, hacker activity, or system errors.
- Remote access through either Internet connections or dial-up connections should be monitored and audited. Review of access attempts should be monitored and recorded.
- Log-file collection, backup, and security should be described by the policy. Secure log-server usage should be determined in the policy and the procedures defined by the operating-system documentation.
- The usage of auditing tools and the process of when and how to use them should be part of the policy.
- A process for management review of audit logs and system logs should be determined. Administrator review of the logs should not be the final review of system activity.
- A risk analysis should be performed to determine what systems need to be audited and what security has to be in place, followed by a determination of where to allocate resources based on a risk-classification level.

Operating System

- New services must be closely scrutinized and authorized before being implemented. Services should be based on a business justification. An emergency process should be in place to handle exceptions to the process. The policy does not need to cover each service, just the process for authorization, usage, monitoring, and reporting.
- Users with access to the operating system must be provided with security training specific to operating-system concerns. User training can offset much low-level vulnerability that can compromise a system.
- Installing up-to-date patches and upgrades to the operating system is critical to the security of the organization. Changes to the operating system must be accomplished in a timely and efficient manner.
- Periodically searching the operating system for suspicious files or modification of critical files should be required. The process of file-integrity checking is key to understanding changes in the environment. Monitoring changes is closely tied to installing and utilizing real-time monitoring programs to secure the operating system. The details are left to procedural documents, but the policy needs to determine where and when monitoring of the operating system needs to occur.
- The policy should determine how trust relationships between systems and external connections are secured.
- Reporting at the operating-system level should be determined for administrator usage, activity of users, and potential threats and exception reports of errors or hacker activity.
- Utilization of system monitoring, scanning, and reporting tools should be defined by the policy. Procedural documents can detail which software needs to be used.

Periodically searching the operating system for suspicious files or modification of critical files should be required.

Policy Do's

- Management support of the policy is critical.
- Make the policy general enough to cover all functions of the network.
- Periodically update the policy for changes in the environment .
- Assign enforcement of the policy to a group such as the audit group.
- Require everyone to sign off on the policy when they start working.
- Make the policy easily accessible on the corporate intranet.

Policy Don'ts

- Do not make the policy too detailed or restrictive. Too many details in an overall network policy can cause confusion or backlash in implementing it.
- Do not make exceptions to the policy for individuals or groups.
- Do not tie the policy to specific computer applications or software.

Why Policies Fail

It bears repeating: The number-one reason for policy failure is lack of management support.

Conclusion

Is a good network security policy the end of all your problems? Not likely. But it's a start on a long and never-ending road. A static policy can be just as damaging as a bad policy. A good policy will be a dynamic living document and provide a good framework for the details that follow in standards, procedures, and guidelines. Once the policy is defined, the real work begins with implementation of that policy across various environments. As the saying goes, "The devil is in the details."