Cisco − Network Security Policy: Best Practices White Pape

Table of Contents

Network Security Policy: Best Practices White Paper

Introduction

Without a security policy, the availability of your network can be compromised. The policy begins with assessing the risk to the network and building a team to respond. Continuation of the policy requires implementing a security change management practice and monitoring the network for security violations. Lastly, the review process modifies the existing policy and adapts to lessons learned.

This document is divided into three areas: preparation, prevention, and response. Let's look at each of these steps in detail.

Preparation

Prior to implementing a security policy, you must do the following:

- Create usage policy statements.
- Conduct a risk analysis.
- Establish a security team structure.

Create Usage Policy Statements

We recommend creating usage policy statements that outline users' roles and responsibilities with regard to security. You can start with a general policy that covers all network systems and data within your company. This document should provide the general user community with an understanding of the security policy, its purpose, guidelines for improving their security practices, and definitions of their security responsibilities. If your company has identified specific actions that could result in punitive or disciplinary actions against an employee, these actions and how to avoid them should be clearly articulated in this document.

The next step is to create a partner acceptable use statement to provide partners with an understanding of the information that is available to them, the expected disposition of that information, as well as the conduct of the employees of your company. You should clearly explain any specific acts that have been identified as security attacks and the punitive actions that will be taken should a security attack be detected.

Lastly, create an administrator acceptable use statement to explain the procedures for user account administration, policy enforcement, and privilege review. If your company has specific policies concerning user passwords or subsequent handling of data, clearly present those policies as well. Check the policy against the partner acceptable use and the user acceptable use policy statements to ensure uniformity. Make sure that administrator requirements listed in the acceptable use policy are reflected in training plans and performance evaluations.

Conduct a Risk Analysis

A risk analysis should identify the risks to your network, network resources, and data. This doesn't mean you should identify every possible entry point to the network, nor every possible means of attack. The intent of a risk analysis is to identify portions of your network, assign a threat rating to each portion, and apply an appropriate level of security. This helps maintain a workable balance between security and required network access.

Assign each network resource one of the following three risk levels:

- **Low Risk** Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems.

- **Medium Risk** Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause a moderate disruption in the business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.

- **High Risk** Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems.

Assign a risk level to each of the following: core network devices, distribution network devices, access network devices, network monitoring devices (SNMP monitors and RMON probes), network security devices (RADIUS and TACACS), e−mail systems, network file servers, network print servers, network application servers (DNS and DHCP), data application servers (Oracle or other standalone applications), desktop computers, and other devices (standalone print servers and network fax machines).

Network equipment such as switches, routers, DNS servers, and DHCP servers can allow further access into the network, and are therefore either medium or high risk devices. It is also possible that corruption of this equipment could cause the network itself to collapse. Such a failure can be extremely disruptive to the business.

Once you've assigned a risk level, it's necessary to identify the types of users of that system. The five most common types of users are:

- **Administrators** Internal users responsible for network resources.

- **Privileged** Internal users with a need for greater access.
- **Users** Internal users with general access.
- **Partners** External users with a need to access some resources.
- **Others** External users or customers.

The identification of the risk level and the type of access required of each network system forms the basis of the following security matrix. The security matrix provides a quick reference for each system and a starting point for further security measures, such as creating an appropriate strategy for restricting access to network resources.

System	Description	Risk Level	Types of Users
ATM switches	Core network device	High	Administrators for device configuration (support staff only); All others for use as a transport
Network routers	Distribution network device	High	Administrators for device configuration (support staff only); All others for use as a transport
Closet switches	Access network device	Medium	Administrators for device configuration (support staff only); All others for use as a transport
ISDN or dial up servers	Access network device	Medium	Administrators for device configuration (support staff only); Partners and privileged users for special access
Firewall	Access network device	High	Administrators for device configuration (support staff only); All others for use as a transport
DNS and DHCP servers	Network applications	Medium	Administrators for configuration; General and privileged users for use
External e−mail server	Network application	Low	Administrators for configuration; All others for mail transport between the Internet and the internal mail server
Internal e−mail server	Network application	Medium	Administrators for configuration; All other internal users for use
Oracle database	Network application	Medium or High	Administrators for system administration; Privileged users for data updates; General users for data access; All others for partial data access

Establish a Security Team Structure

Create a cross−functional security team led by a Security Manager with participants from each of your company's operational areas. The representatives on the team should be aware of the security policy and the technical aspects of security design and implementation. Often, this requires additional training for the team members. The security team has three areas of responsibilities: policy development, practice, and response.

Policy development is focused on establishing and reviewing security policies for the company. At a minimum, review both the risk analysis and the security policy on an annual basis.

Practice is the stage during which the security team conducts the risk analysis, the approval of security change

requests, reviews security alerts from both vendors and the CERT mailing list, and turns plain language security policy requirements into specific technical implementations.

The last area of responsibility is response. While network monitoring often identifies a security violation, it is the security team members who do the actual troubleshooting and fixing of such a violation. Each security team member should know in detail the security features provided by the equipment in his or her operational area.

While we have defined the responsibilities of the team as a whole, you should define the individual roles and responsibilities of the security team members in your security policy.

Prevention

Prevention can be broken into two parts: approving security changes and monitoring security of your network.

Approving Security Changes

Security changes are defined as changes to network equipment that have a possible impact on the overall security of the network. Your security policy should identify specific security configuration requirements in non−technical terms. In other words, instead of defining a requirement as "No outside sources FTP connections will be permitted through the firewall", define the requirement as "Outside connections should not be able to retrieve files from the inside network". You'll need to define a unique set of requirements for your organization.

The security team should review the list of plain language requirements to identify specific network configuration or design issues that meet the requirements. Once the team has created the required network configuration changes to implement the security policy, you can apply these to any future configuration changes. While it's possible for the security team to review all changes, this process allows them to only review changes that pose enough risk to warrant special treatment.

We recommend that the security team review the following types of changes:

- Any change to the firewall configuration.
- Any change to access control lists (ACL).
- Any change to Simple Network Management Protocol (SNMP) configuration.
- Any change or update in software that differs from the approved software revision level list.

We also recommend adhering to the following guidelines:

- Change passwords to network devices on a routine basis.
- Restrict access to network devices to an approved list of personnel.
- Ensure that the current software revision levels of network equipment and server environments are in compliance with the security configuration requirements.

In addition to these approval guidelines, have a representative from the security team sit on the change management approval board, in order to monitor all changes that the board reviews. The security team representative can deny any change that is considered a security change until it has been approved by the

security team.

Monitoring Security of Your Network

Security monitoring is similar to network monitoring, except it focuses on detecting changes in the network that indicate a security violation. The starting point for security monitoring is determining what is a violation. In Conduct a Risk Analysis, we identified the level of monitoring required based on the threat to the system. In Approving Security Changes, we identified specific threats to the network. By looking at both these parameters, we'll develop a clear picture of what you need to monitor and how often.

In the Risk Analysis matrix, the firewall is considered a high−risk network device, which indicates that you should monitor it in real time. From the Approving Security Changes section, you see that you should monitor for any changes to the firewall. This means that the SNMP polling agent should monitor such things as failed login attempts, unusual traffic, changes to the firewall, access granted to the firewall, and connections setup through the firewall.

Following this example, create a monitoring policy for each area identified in your risk analysis. We recommend monitoring low−risk equipment weekly, medium−risk equipment daily, and high−risk equipment hourly. If you require more rapid detection, monitor on a shorter time frame.

Lastly, your security policy should address how to notify the security team of security violations. Often, your network monitoring software will be the first to detect the violation. It should trigger a notification to the operations center, which in turn should notify the security team, using a pager if necessary.

Response

Response can be broken into three parts: security violations, restoration, and review.

Security Violations

When a violation is detected, the ability to protect network equipment, determine the extent of the intrusion, and recover normal operations depends on quick decisions. Having these decisions made ahead of time makes responding to an intrusion much more manageable.

The first action following the detection of an intrusion is the notification of the security team. Without a procedure in place, there will be considerable delay in getting the correct people to apply the correct response. Define a procedure in your security policy that is available 24 hours a day, 7 days a week.

Next you should define the level of authority given to the security team to make changes, and in what order the changes should be made. Possible corrective actions are:

- Implementing changes to prevent further access to the violation.
- Isolating the violated systems.
- Contacting the carrier or ISP in an attempt to trace the attack.
- Using recording devices to gather evidence.
- Disconnecting violated systems or the source of the violation.

- Contacting the police, or other government agencies.
- Shutting down violated systems.
- Restoring systems according to a prioritized list.
- Notifying internal managerial and legal personnel.

Be sure to detail any changes that can be conducted without management approval in the security policy.

Lastly, there are two reasons for collecting and maintaining information during a security attack: to determine the extent to which systems have been compromised by a security attack, and to prosecute external violations. The type of information and the manner in which you collect it differs according to your goal.

To determine the extent of the violation, do the following:

- Record the event by obtaining sniffer traces of the network, copies of log files, active user accounts, and network connections.
- Limit further compromise by disabling accounts, disconnecting network equipment from the network, and disconnecting from the Internet.
- Backup the compromised system to aid in a detailed analysis of the damage and method of attack.
- Look for other signs of compromise. Often when a system is compromised, there are other systems or accounts involved.
- Maintain and review security device log files and network monitoring log files, as they often provide clues to the method of attack.

If you're interested in taking legal action, have your legal department review the procedures for gathering evidence and involvement of the authorities. Such a review increases the effectiveness of the evidence in legal proceedings. If the violation was internal in nature, contact your Human Resources department.

Restoration

Restoration of normal network operations is the final goal of any security violation response. Define in the security policy how you conduct, secure, and make available normal backups. As each system has its own means and procedures for backing up, the security policy should act as a meta−policy, detailing for each system the security conditions that require restoration from backup. If approval is required before restoration can be done, include the process for obtaining approval as well.

Review

The review process is the final effort in creating and maintaining a security policy. There are three things you'll need to review: policy, posture, and practice.

The security policy should be a living document that adapts to an ever−changing environment. Reviewing the existing policy against known Best Practices keeps the network up to date. Also, check the CERT web site for useful tips, practices, security improvements, and alerts that can be incorporated into your security policy.

You should also review the network's posture in comparison with the desired security posture. An outside firm that specializes in security can attempt to penetrate the network and test not only the posture of the network, but the security response of your organization as well. For high−availability networks, we recommend conducting such a test annually.

Finally, practice is defined as a drill or test of the support staff to insure that they have a clear understanding of what to do during a security violation. Often, this drill is unannounced by management and done in conjunction with the network posture test. This review identifies gaps in procedures and training of personnel so that corrective action can be taken.

Related Information

- **More Best Practices White Papers**

Updated: Apr 08, 2002 Document ID: 13601