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 (Security 401)"
at http://www.giac.org/registration/gsec

Enterprise Security Management (ESM): Centralizing Management of Your Security Policy

Scope:

This paper will define Enterprise Security Management (ESM). It will discuss motivations for implementing ESM. It will also look at security policy development and overview some of the items that security policy should contain. The different types of ESM product suites found on the market today will be highlighted. As well, ESM architecture and some of the tools usually integrated in ESM suites will be discussed.

Discussion:

Introduction

In today's environment, computer networks are vulnerable to threats from both inside and outside the organization. As enterprise networks expand nationally and globally to include Internet access, intranets, extranets and e-commerce activities. Corporations seeking to manage and enforce security policies must choose from hundreds of security point products that offer little, if any, overlapping functionality. [1] Within the network infrastructure, security point products include firewalls, intrusion detection systems (IDS), virus detection systems, and Public Key Infrastructure (PKI) and Virtual Private Network (VPN) solutions. Important corporate information is being distributed across a variety of different systems. Networks, in turn, will have security point products - most of the time from various vendors - with different security attributes and settings. Administrators are faced with the task of coordination, implementation and monitoring of security attributes across varied, dispersed infrastructures. The dynamic nature of corporate networks means that they are no longer defined by physical boundaries, but instead by enterprise-wide security policies. [2] Administrators must account for the logical boundaries of an infrastructure, including extranets and remote access. Enterprise Security Management is the process of controlling configuration, deployment, and monitoring of security policy across multiple platforms and security point products.

Security Problems and Threats

Security problems and threats are a major reason for using ESM across an organization. Threats can come from internal or external to the company. More organizations are finding that despite their use of Internet firewalls, an even bigger threat to corporate data is created by disgruntled or temporary employees. [3] They may consist of loss of data, unauthorized services running on servers or the introduction of viruses into the workplace.

An administrator can use an ESM suite of products (a list of products is provided in Appendix A) to make sure anti-virus software is installed and updated across all servers and workstations on the network. Some internal security problems may also be: users not setting screensaver passwords, administrators leaving backup media unprotected and workstation BIOS passwords not set.

© SANS Institute 2000 - 2005, Author retains full rights.

External threats may occur from hackers using attacks such as denial of service or packet spoofing attacks. Many organizations are susceptible to the notion that having a firewall is enough to protect their data. However, we will see that having a firewall, alone, does not equate to having a detailed, maintained enterprise security policy.

First Step: Developing a Security Policy

Enterprise Security Management begins with security policy. Incidents such as the Melissa and ILoveYou viruses, and the Distributed Denial of Service (DDos) attacks against Yahoo and other sites made many organizations re-evaluate their current security implementations. In response to the many security threats that exist, corporations look to make sure their security policy is adequate and enabled across the enterprise.

The process of implementing an ESM solution can be complicated. Listed are some steps to take when developing the security policy, before ESM deployment can begin.

- Identify critical resources
  - Identify requirements
- Perform Risk/Threat assessment
  - Identify high-risk areas
- Develop security policy

Identify Critical Resources: The critical resources of the corporation (i.e. servers, applications, existing security point devices, etc.) should be identified and documented. This will provide the company a baseline of assets that need to be addressed in the security policy. Will the solution be required to provide coverage for legacy systems, etc.?

Perform Risk/Threat Assessment: A risk/threat assessment should be completed to identify the corporation's current security posture. The output of this step should provide the company a detailed listing of the assets requiring protection and their value. During the risk assessment, determine and prioritize which business-critical systems, applications, communications devices, etc. are most vulnerable.

Develop Security Policy: Based on the information from the risk/threat assessment, the company can develop its security policy. Procedures are developed concerning both physical and logical controls. Physical controls may include: controlled access to server rooms, storage of backups in secure locations, etc. Logical controls may include: password policy, time restrictions on network usage, restricting user logins to specific workstations, etc.

Security Policy

Security policy should outline the rules of computer and network usage and must be adhered to by the entire organization. It should at a minimum address some the following issues:

© SANS Institute 2000 - 2005, Author retains full rights.

- Network access
- Password usage
- Network usage
- Policy enforcement
- Support

Network Access:	Guidelines regarding who has access to the network. Which resources will be restricted, which resources will be available to users.
Password Usage:	Guidelines regarding password attributes. These may include password length, requiring unique passwords and use of complex passwords (requiring use of a combination of alphabet, numeric and/or special characters).
Network Usage:	Guidelines on how the network and its resources will be used. Delineation of what is acceptable and non-acceptable behavior for those using the network.
Policy Enforcement:	Guidelines on what will be done when violation of the policy occurs.
Support:	Guidelines to designating who will be responsible for administering the policy. This may be a group or team that will maintain the security policy and assure it is adhered to.

Authentication, identification, protection from viruses, data backup and using a firewall to defend against attacks are important components of that policy. [4] However, how does an administrator implement this policy across the entire organization -- which may encompass different systems, platforms and architectures?

ESM Architecture

ESM solution suites can be complicated to architect and deploy. Some solutions, such as e-Security's Open e-Security Platform (OeSP) solution and BMC's Control-SA solution, use agents to configure and monitor security policy on managed assets. Managed assets may be security point products like firewalls, IDS or VPN equipment. Servers, such as application, database, web and legacy systems (mainframes, mid-range) are resources that can also be managed. The BMC Control-SA agents communicate with a server, which houses a central database of security information for the entire enterprise. The agents provide real-time data back to the server. If security policies are changed locally on the managed asset, they are replicated immediately to the central database. Administrators can also add/modify security policy at the enterprise level (central server) and have those changes propagated to all managed resources (via agents).

ESM suites include the capability to send alerts to a central console, as well as external interfaces. In fact, Control-SA and Tivoli's SecureWay suite integrate into Enterprise Management architectures,

© SANS Institute 2000 - 2005, Author retains full rights.

like BMC Patrol and Tivoli TME10, respectively. Other functionality integrated into the solution may be: Single Sign-On, Workflow and Report generation. These capabilities are discussed in the next section.

ESM suite components

Once the security policy is established, the actual ESM solution can be developed. Traditionally, ESM suites focus on one of two critical areas in the IT infrastructure: (1) user administration and management, including tasks such as single sign-on; and (2) risk assessment activities, such as vulnerability and threat assessment of critical network systems. [5] ESM suites may include some of the following tools:

- User Administration
- Single Sign-On (SSO)
- Reporting capabilities
- Vulnerability assessment
- Alert Management

User Administration: Policies concerning user access control management. This includes password policy management. Most suites use role-based management to administer users. Role-based administration involves assigning sets of access rights to groups based on job function. This makes administration easier and more efficient. It also provides for a more granular user security policy.

Single Sign-On: Implements single sign-on within the organization. Single sign-on (SSO) solutions are a central element of all the market-leading ESM products in the user/policy administration space, and often represent a requirement that drives an overall ESM project. [6]

Reporting capabilities: Reporting tools enable the administrator to search for information about users, groups, resource security configurations, etc. They also provide capabilities to query log files and ESM centralized data stores (in some products).

Vulnerability assessment: ESM risk assessment tools, such as ISS System Scanner or NAI CyberCop make sure corporate security policy is complied with. These tools scan hosts, compare current security settings against an organization's security policy and report any deltas.

Alert management: Most tools provide for centralized event management. When security policy is violated, events can be captured and displayed on management consoles. Tools also can be configured to generate alerts and notify the appropriate personnel.

Implementing an ESM tool suite to administer security policy and security point products can be a time-consuming, but worthwhile project. ESM provides administrators with a centralized means of organizing, implementing and monitoring security policy.

© SANS Institute 2000 - 2005, Author retains full rights.

Conclusion

About two-thirds of computer break-ins originate among individuals within the organization. [7] Security threats abound, both internal and external, in the commercial and government sectors. The leading problem most security professionals face today is the management and maintaining of consistent security policy across diverse systems and infrastructures. As we have seen, it is important for organizations to develop and implement an enterprise security policy. But how do administrators make sure that the security policy is being followed? How are security policies effectively monitored?

Enterprise Security Management suites enable organizations to efficiently deploy, configure and monitor security policy across diverse platforms, products and environments. ESM suites may be deployed differently. Most, however, use management agents to interact with security point products. This enables administrators to configure and monitor policy on those products. Management of users, password policy, Single Sign-On, alert management and reporting are some of the capabilities provided by ESM tool suites. Enterprise Security Management solutions offer security administrators a centralized means of maintaining security policy, while allowing users the access to resources they desire.

© SANS Institute 2000 - 2005, Author retains full rights.

Appendix A: **List of ESM vendors and products**

Security Policy Management

Axent Technologies
http://www.axent.com
Product: Enterprise Security Manager

BindView Development Corporation
http://www.bindview.com
Product: bv-Control and bv-Admin

BMC Software
http://www.bmc.com
Products: BMC Control-SA

Computer Associates
http://www.ca.com
Products: eTrust product line: e-Business Security Management suite

e-Security Inc.
http://www.esecurityinc.com
Product: Open e-Security Platform (OeSP) suite

Evidian
http://www.evidian.com
Product: AccessMaster suite

Tivoli
http://www.tivoli.com
Product: Tivoli SecureWay suite

Vulnerability/Risk Assessment

Intrusion.com
http://www.intrusion.com
Product: Kane Security Analyst

Internet Security Systems (ISS)
http://www.iss.net
Products: ISS Security Scanner

Network Associates Inc.
http://www.nai.com

© SANS Institute 2000 - 2005 Author retains full rights.

Product: CyberCop Scanner

© SANS Institute 2000 - 2005, Author retains full rights.

References

[1] Cisco Systems, Inc. "Cisco Secure Scanner Overview." Cisco Secure Scanner User Guide, Version 2.0. 29 June 2000. URL. http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csscan/csscan2/cssug/overview.htm (9 Dec 2000).

[2] Tec-gate.com. "Enterprise Security Management." URL. http://www.tec-gate.com/checkpoint/firewall-1/sec_ent.html (14 Dec 2000).

[3] DePompa, Barbara. "Firewalls Deter Outside Attacks – But Users Need More Security." 1 September 1997. URL. http://www.internetwk.com/supp/security0901-1.htm (14 Dec 2000).

[4] DePompa, Barbara. "Firewalls Deter Outside Attacks – But Users Need More Security." 1 September 1997. URL. http://www.internetwk.com/supp/security0901-1.htm (15 Dec 2000).

[5] Gardner, Dale. "ESM, ASAP!" June 2000. URL. http://infosecuritymag.com/jun2000/juncoverstory.htm (17 Dec 2000).

[6] Gardner, Dale. "ESM, ASAP!" June 2000. URL. http://infosecuritymag.com/jun2000/juncoverstory.htm (17 Dec 2000).

[7] BMC Software. "INCONTROL for Security Management" November 1999. URL. http://www.bmc.com/products/incontrol/security.pdf (17 Dec 2000).

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.