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

Jasu Mistry
Security Essentials
Version 1.2d

Developing Security Policies For Protecting Corporate Assets

1. Introduction

The Digital revolution of the 21st Century has not been achieved without its consequences. Real time business requirements and economic drivers have forced rapid changes to the methods used to conduct business-to-business and business to client communication. The Internet has now become a convenient and economic deployment medium for global business.

With the ever-increasing number of connections and growth of the Internet, security has become an issue for not only for the corporate environment but also for home user. This has never been more apparent then after the Code Red worm incident. All user populations were affected.

Security assurance and user-friendly sites are required if businesses are to be successful at attracting customers to their Internet sites. It is therefore important to be able to understand the business requirements and be able to translate these into a public network presence with security in mind. A security policy is derived to provide guidelines on how to best conduct business with security, confidentiality, integrity, and accessibility in mind.

Security is a vast area; therefore it is not possible to cover all aspects in the scope of this paper. The paper will focus on some aspects of a security policy with an aim to protect assets from risk.

2. Scope of possible policies

Security policies govern the steps and procedures taken to protect business assets and confidential information from intrusion via the use of technology or physical intervention. When considering the possibility of transacting business over public networks, the goal should be how best to protect corporate assets, data integrity and confidentiality.

Business assets can be considered to be and include items such as valuable and sensitive data that needs to be kept secure and confidential. For example financial data, client information or employee contract details. Business critical hardware such as routers, switches, network cables, firewalls, file servers, desktops, laptops, modems and backup systems are equally important to protect.

Software distribution should be strictly controlled to avoid misuse and/or tampering. Security policies are an ideal method of achieving this.

© SANS Institute 2000 - 2005 Author retains full rights.

A major aspect of a security policy is the use of passwords to protect business systems and users. Generally this would be the primary step towards protecting information.

It is commonplace to use written material within the business environment. It is essential that the responsibility lie with all employees to avoid sensitive information from being distributed to unauthorised persons. Guidelines set out in the security policy should ensure and address this.

3. Assessing the Risks

First the business needs to establish what assets it needs to protect and why. A 100% security guarantee cannot be given, but it is best practice to identify insecure components and try to protect them from known risks and attack.

Businesses face risks from software and hardware misuse from its employees (1). Internet facing connections provide threats of hackers and crackers who can launch spoofing and denial of services attacks using a list of known vulnerabilities and techniques, thus making a business site unavailable to its employees and clients. Threats from viruses, worms and Trojans are also a major concern.

Malicious attacks such as bombs and theft of hardware or natural disasters like fire, flood and earthquakes cannot be ruled out.

Dangers also exist from internal users who do not take security seriously since it is not fully understood and appreciated.

4. Areas of Investigation

"Best practice" procedures should be used to protect corporate assets from risk. The rule of thumb for any policy should be "whatever should not be accessed is prohibited". A controlled copy of the security policy should be made easily available to all employees. Administrators and departmental managers should ensure that correct procedures are implemented and adhered to, showing their support and the importance of security policies.

Policies should conform to all existing rules, regulations and laws appropriate to the organisation in question.

Clear, precise and readily available policies together with acceptable tools will give employees the power to make sound decisions. (1)

Areas to be examined are:

- Auditing and its use to identifying vulnerabilities

© SANS Institute 2000 - 2005 Author retains full rights.

- Administrators policy
- Password Policy
- Backup and recovery Policy
- Computer user policy and user training
- Network Policy
- Remote access policy
- Physical Security Policy

"Best practice" procedures should incorporate incident handling in the event of business attacks.

4.1 Auditing and its use to identify vulnerabilities

Regular auditing of systems is an important aid in understanding system weaknesses. Test the infrastructure by conducting regular penetration tests. Check Audit logs and reports and ensure that necessary actions are taken for any discovered vulnerabilities.

When audit logs are analysed, review them against the security policy and if need be update it. Example of this is if too many log failure attempts are discovered on the security event log, then trace user who was unsuccessful in logging on the system and verify if it is a genuine systems user. Check to see if the security policy is set to lock accounts after a specified number of log on attempts. If not, then carry out risk analysis assessment to the business and if need be review and change the policy.

Protect audit logs; e.g. by making use of wormdevices or one time write able CDS, so that they are not tampered with, as these are the only system records to show any events that have occurred and may be required for legal investigation.

4.2 Administrators Policy

Systems administrators play an essential part in implementing security policies. System and Security Administrators need to work closely together to carry out their jobs satisfactorily. If they are not aware of security policies systems could be compromised. The principle of the least privileges should be followed, however, at the same time employees should not be stopped from delivering their objectives.

This principle is very important when configuring operating systems and loading software, ensuring that unnecessary services are not loaded. Always maintain and follow configuration procedures and keep abreast of the latest vulnerabilities. Apply operating systems hardening procedures to protect it from known security loopholes.

Administrators are also responsible for implementing access controls to directories, databases and password policies. Administrators should enforce passwords

© SANS Institute 2000 - 2005 Author retains full rights.

changes for newly issued ID's, any compromised passwords and timely disabling of discontinued User ID's. Re-use of passwords should not be allowed. System administrators must change and maintain system and software application passwords regularly and keep these passwords safe by making use of password protecting tools such as "Info Keep".

"Info Keep" helps to store complicated (difficult to remember) passwords without writing them down. "Info Keep" creates the triple DES encrypted file, this is password protected and cannot be opened without the Info keep program.

Encryption of files needs to be implemented to protect business sensitive information and SAM files.

It is important for policy to be implemented using company-approved virus checking software, installed on all servers, desktops and laptops. Restrictions should be placed on users transporting data onto the network from external sources (disks and external downloads). All viruses checking software should be regularly updated with the latest virus definition files.

Taking regular successful backups and storing backup media onsite and offsite in safe locations gives administrators an ability to carry out a recovery process if required. Backup media must be protected from damage and unauthorised personnel. It should be clearly labelled and regularly tested for integrity. Periodically create and update emergency repair disks and store in a safe place with backups.

System Administrators are privileged to certain business confidential data. Administrators need to be aware that maintaining confidentiality is part of the job and must be strictly adhered to.

4.3 Password Policy

Passwords do not imply privacy but allow authorised users to gain access to required applications, files and e-messages. Weak passwords have no value and will not perform its task. Passwords need to be stronger in the case of critical systems or when administrative level access is used.

When remote users are allowed access through a firewall, implement one time password generating tools for firewall authentication. Protect such tools and software used by administrators by encryption or other similar method. Limiting and monitoring consecutive unsuccessful password logon attempts is useful. Encryption of passwords should be used when transmitting data between external networks.

Vendor-supplied passwords should always be changed before establishing communication on networks. All users should be responsible for any activities carried out under their individual ID's and passwords. Use strong passwords by

© SANS Institute 2000 - 2005 Author retains full rights.

substituting alphabetic letters with numeric and signs, using first letter of phrase or sentence to form a word, thus deriving non-dictionary words.

4.4 Backup and recovery Policy

Businesses rely on good backup recovery procedures for recovering critical systems and data. It is important that this function is considered and carried out with no weakness in the policy. Backups should give management an assurance that if any part of the of the infrastructure fails, then it can be recovered using backups.
All backed up data must be clearly labelled and kept in a secure place. Always use available tools to carry out backups and to check its integrity. Depending on the critical nature of the business, it may be necessary to build contingency plans for hardware failure. Make use of high availability firewalls with "full fail over" capability or use RAID arrays for hard disk failure.

Protect hardware from power failure by making use of uninterrupted power supply units or generators and protecting all devices from malicious interference.

4.5 Computer users policy and user training

Although employees are given PCs so they can deliver the task that they are assigned, it must be understood that these PCs are company property and must not be abused for personal use. Computer resources are expensive and so offensive material must not be downloaded and stored on business PCs.

Company provided email systems should only be used for business purposes and care needs to be taken of any material sent via email. The company is liable for an employee's action (3).

Spam, mass mailing lists, playing games or engaging in online chat groups should be prohibited.

Desktop and laptop users must make use of business loaded anti virus software to check all data on their PCS, downloaded data or data transferred via disks. Data loaded onto the network servers or sent outside the company must be virus checked. Users must not be allowed to disable such software. Administrators can maintain better control of PC's by implementing group policies as per departmental functions so that users cannot tamper with configurations.

Always make sure that the latest updates/patches for all operating systems and application have been installed thus ensuring any known vulnerabilities have been taken care of. Software and tools provided by Systems Management Servers can be used to audit all PCs.

It is important to make users aware of the security policy and the risks that a business can run into if they are not followed correctly. Educate users by regularly sending emails, holding awareness sessions and putting posters on notice boards.

© SANS Institute 2000 - 2005 Author retains full rights.

User education cannot be taken lightly after the ”ILOVEYOU” virus, which only required one user to open that email message and attachment to flood email servers and gateways.

4.6 Network policy

Using dissimilar network components and layered approach, a satisfactory good infrastructure design can be achieved. Differing technologies and platforms make it increasingly difficult for hackers to break into a system using a single vulnerability.

Exchange of information to or from external sources should be routed through a single gateway. This minimises the risk of information related to internal networks being disclosed. By implementing policy using filtering rules will allow or deny access by source and destination address, helping restrict access to networks by unauthorised personnel. Routers translating internal RFC1980 IP addresses can be used to add another layer of security for attackers to overcome via public/private routing network issues.

Application proxies on Demilitarise Zone (DMZ) allow all secure connections from internal to proxy server, which reduces the risk of internal to external routed traffic.

It is essential to maintain all operating systems and software applications with the latest update/patch. All changes should be documented. A back out plan should be considered in the event of problems. Follow “best practice” procedures by testing upgrades prior to implementation in test environment.
Make use of vendor provided tools to audit and monitor user activities. Administrators must use the principle of least privileges when assigning access on functional and departmental based policies, making auditing and monitoring easier. Always take time to analyse logs for any vulnerabilities in a system. It is best to know system weakness rather than be surprised by intruders.

4.7 Remote Access Policy

As the number of dial up modem users rapidly increases, the number of vulnerabilities also increases. To enable administrators to give controlled access to dial up users, Remote Access Dial In User Server (RADIUS) should be implemented. SecureID or Safeword Token access through a firewall provides one time session authentication access to networks. If data is being transferred remotely, use data encryption to minimise the possibility of data being comprised.

User on internal network should never to able to dial out of the corporate network whilst on a LAN; i.e. avoid a scenario of breaching the public and private network via a modem.

Remote access policy can stipulate to users not to release dial-up numbers to unauthorised users. Audit, monitor and publish figures, by user name, of those who spend excessive hours on the Internet. This can help stop abuse of Internet

© SANS Institute 2000 - 2005 Author retains full rights.

privileges, making users more aware that their activities are being monitored. Remote Access policy should also provide guidelines for implementation of standard client configuration.

4.8 Physical Security Policy

Physical security of buildings, servers, transportable media (disks, tapes), laptops, desktops and any network components connected to internal data networks is equally important.

Firstly, secure access to the building via a reception area and allow access to authorised users by ID badges and swipe card access machines. Make use of CCTV or tools like Van Eck Radiation/TEMPEST or electromagnetic pulses (2). 24 hour monitoring by a reputable Security consultancy should be considered.

Protect equipment by housing it in purpose built data centres, monitored by some of the above-mentioned tools, controlling access and monitoring usage. Keep communication hardware in lockable cabinets where only authorised users are allowed access.

When transporting media such as backup tapes and hard disks, due care must to be taken to use special sealable containers that will protect the media from damage and cannot be tampered with. Always keep backup tapes onsite as well as offsite in secure locations.

Laptop hard disks should be encrypted and password-protect the bootable protocols (netbios password).

Many users leave printed material on their desks and rubbish bins. Inside attackers are always looking for such opportunities. Store printed material in lockable cupboards or shred unwanted material. Enforce and operate a ”clean desk” policy.

Control all visitors to the site and warn employees of “Social Engineering”. People use telephone, faxes, e-mails or personal influence to try and get what they want. Individuals must safeguard against such attacks.

5. Conclusion

The expansion of networks globally has allowed business to be conducted via the Internet. Current trends suggest there are clear indications that security needs to be considered very seriously by any business that has access to the Internet. The Internet has become an important topic and it is important to society, business and government agencies (1).

At the same time crime continues to increase as threats of economic espionage, technology oriented terrorism and information warfare becomes sophisticated. Each system connected to the Internet is subject to attack. To protect the business

© SANS Institute 2000 - 2005 Author retains full rights.

from problems associated with the Internet, some technical issues relating to security have been discussed in this paper.

Physical security is equally important to be managed and controlled. A high number of security breaches occur as a result of an internal hack. This can be as a result of easily available access to keys to locked devices and lack of physical security controls. Social Engineering is very common and often overlooked due to internal employee relationship or friendships.

No site is absolutely secured but giving guidance and making employees aware of security issues can only help to protect it. Security policies are there to let the employee know the do's and don'ts.

Policies make decision-making and responding to emergencies easier. They must not be too ridged that they stop employees from performing their role. Regular review of policies, staying vigilant through testing, monitoring, upgrading and updating can only provide a better secure site for their employees and client (4).

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

© SANS Institute 2000 - 2005 Author retains full rights.

6. References

1) Dr. Gerald L Kovacich (1998), Information Systems security officer's Guide, Butterworth-Heinemann (USA)

2) IT Security Cookbook – 8 Physical Security – Latest update June 2000 http://www.boran.com/security/IT1x-8.html

3) Michael R Overly (1999), e-policy how to Develop Computer, E-mail and Internet Guidelines to protect your Company and its Assets, SciTech Publishing inc. (USA)

4) Developing an Internet Usage Policy - April 14, 2000
Understanding Email Security Threats – March 31, 2000
Human Resources and Information Technology: A Joint Security Partnership – May 10, 2000
Ten Steps to Protect Your Enterprise from DoS Attacks – March 27, 2001
URL: http://enterprisesecurity.symantec.com

5) How to Develop a Network Security Policy An Overview of Internetworking Site Security URL: http://www.sun.com/software

6) Security Overview URL: http://www.sun.com/security

7) An Overview of Corporate Information Security
Combining Organisational, Physical & IT Security by Sean Boran December 13, 1999 URL: http://securityportal.com

8) Security Planning by Christopher Benson, Inobits Consulting (Pty) Ltd
Security Threats - Microsoft Solutions Framework
URL: http://www.microsoft.com/TechNet

9) About Info Keep by Michael Koszenski as the author and creator of Info Keep
http://www.infokeep.net

10) Security Best Practices for Internet Service Providers. Presented by: Internet Service Provider Security Consortium "Security Best Practices" Task Force

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

ICSA.net – 27 September 1999 Version 6.

11) Information Security management – Part 1: Code of practice for information security management – BS7799-1: 1999 - Part 2: Specification for information security management systems – BS7799-2 1999. http://www.c-cure.org

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