ISSN No. 0976-5697

Volume 6, No. 6, July-August 2015

International Journal of Advanced Research in Computer Science

REASEARCH PAPER

Available Online at www.ijarcs.info

Advanced Security Policies to protect the Internet resources against the cyber attacks

Prof. (Dr.) Prashant P. Pittalia
MCA Department
SJPIBMCA
Gandhinagar, Gujarat
prashantppittalia@yahoo.com

Abstract: Internet security is the first steps towards protecting the online information against the cyber attacks on Website. Internet security is easily breach by attacker if security policies are not well-designed and implement in the organization or corporate or individual. The major role of the network admin is to proper study of the organization resources and how to implement the security policies to protect against the internet attacks. This paper presents the various security policies which are very important for the secure network. Also the paper inform the key things which network admin has to be in mind when he/she wants to implement the security policies

Keywords: Trojan horse, Authentication, Access Control

I. INTRODUCTION

As the E-commerce comes most of the organization it may be business-to-business, business-to-consumer, customer-to-customer, Government-to-consumer needs to allow their data and information stored in web servers and transmit across the whole world. Networking and Internet concepts in the organization or corporate increase the strength of it, reduce the cost, availability of information 24 * 7. For all such factors is it necessary for the admin of the system to first design the security policy to securely transmission among the various levels and on various devices. The cyber attackers first try with small security breach applications. The cyber attacks like virus, worms, Trojan horse, sabotage, telephone Denial of service, modification of message, and replay and masquerade are exist in the Internet. Installation of some anti-virus or firewall in the organization is not enough to protect against the cyber attacks. With the help of proper designing and implementing the security policy we may control all the resources either it is software and hardware.

II. EXAMPLES OF ATTACKS

A. *Trojan horse:*

It is a worm or virus that may send information back to the originator or may be used by the originator to gain control of a targeted system. Many Trojan horses spread by attaching itself to a useful program. Usually attacks at the application layer. Many Trojan horse programs will attempt to steal user account and password information.

B. *Sabotage*

Sabotage means making damages on a computer system without getting any gain. Discontent staff of fired employee usually commits this.

C. *Telecom Fraud*

Some 70 percent of telecom fraud occurs in and around weaknesses in a carrier's subscription processes. An overwhelmingly typical fraud scheme begins when someone gets hold of a customer's good name and uses it to sign up for service. Add to that, traditional shoulder surfing, and it's easy to see how subscribers lose control of their PINs and other dialing information.

D. *Denial of Service*

In a denial-of-service attack, hackers use automated programs to try to jam a site with bogus requests for service to the point that service is slowed or interrupted for legitimate users. The attempt came as tech-oriented Web sites in Asia were reporting calls from hacker groups in China for denial-of-service attacks to be launched against the CNN Web site on April 18 2008 over the network's coverage of unrest in Tibet.

E. *Laptop/Mobile Theft*

Laptops and other portable devices are frequently lost (stolen or misplaced) in hotel rooms, libraries, airport security counters, coffee shops and taxis. Some estimates suggest that a laptop is stolen every minute and most of them are never recovered.

F. *Financial Fraud*

It means manipulation in the financial activity. The intruder changes the data or it will delete some records to generate wrong information.

G. *System Penetration*

Hacking is part of the system penetration which enters in system & changes the content, check the system is doing and locks or unlocks the port available on the system.

H. *Theft of Proprietary Info*

Financial data, customer lists and R&D are all extremely lucrative and more importantly, extremely private. And much of the fraud is perpetrated by those in trusted positions—employees.

I. *Insider Abuse of Net access*

User of the network access use the illegal website or use pirated software which edged out the virus incidents as the most common security problem. IT security managers don't know whether their systems were compromised from the inside or not.

III. ADVANCED POLICIES TO PROTECT THE ONLINE RESOURCES

A. System Administration Policy

The administrator ensures that the systems are available when needed, that confidential information is only available to those authorized access and that the information is not subject to unauthorized changes. It has to define the users those updates administration policies, users those authorized to grant access and approve usage, users who have system administrator privileges, rights and responsibilities of an administrator. It has to locking down critical files such as registry and configuration files.

B. Physical Restriction

A Physical Security policy document should exist detailing the measures taken to protect buildings as regards disasters (flooding, fire, earthquakes, explosions, power outage), theft, access control, safes, computer rooms & wiring cabinets. It is necessary to define the Areas open to the public, company staff and administrator. It has to define the type of user responsible for destruction of defective confidential disks & tapes and repaired of old servers/disks/tapes. All computing devices should be cleanly installed and labeled. A diagram of what servers are installed where should be available, along with contact persons.

C. Access Control

All users should be authorized. Users should be able to set the privileges of objects belonging to them in their environment. Users should be prevented from deleting others user's files in shared directories. It should be possible to control user access to all objects on the system (files, printers, devices, databases, commands, applications etc.) according to a stated policy.

D. Logon Policy

Each user must be identified by a name or number and belong to a group. Username and group name structure should be standardized enterprise wide (number of characters, composition) if possible. Each user should have only one account on the system. If guest accounts are used, their working environment should be very restricted. When a user is transferred or terminates employment, his account should be blocked or deleted immediately. Procedures should exist whereby the HR administration automatically informs system administrators. A screen lock should be activated after 15mins idle time with password protection. Users should be informed of actions that violate security. Logons should only be enabled when necessary (e.g. Monday to Friday and in between 09:00 a.m. and 05:00 p.m.). It should be possible to specify how many simultaneous login sessions a user may have. It should be possible to set an expiration date for a user account.

E. Data Storage Policy

This policy informs how the data stored so easily track of database records. Each record in the database table should contain at least following information, which helps in data tracking. Created UserId, Modified UserID, Date of record creation, Time of record creation, Date of record updating, Time of record updating, Company Id (In case of multiple branches)

F. Accountability and Audit

Audit trail logs and programs/utilities must be protected. They should only be accessible by security personnel. System administrator activity (especially use of *su* in UNIX) should be logged. Unsuccessful login attempts should be logged (and possibly notified). Important events should raise an alarm (high priority message) automatically. Logs should be kept on read-only media if possible. Logs should also be forwarded to a especially secure machine instead of locally on each machine, if possible. Avoid storing logs on shared file systems. Programs scanning audit logs can help detect attacks as they occur by recognizing unusual behavior, suspicious patterns, or atypical error messages. Audits should be run regularly on the system (once per year, once every 3 months). New servers are installed and prepared by their system administrator. Then they should be audited and certified to one of the sensitivity levels by security staff.

G. User Management Policy

The user management policy set out how user accounts and privileges are created, managed and deleted. It includes how new users are authorized and granted appropriate privileges, as well as how these are reviewed and revoked when necessary, and includes appropriate controls to prevent users obtaining unauthorized privileges or access. It might also include recording of user activity on information systems and networks. The purpose of this policy is to establish a standard for the administration of computing accounts that facilitate access or changes to Organizational data. An account consists of a user ID and a password; supplying account information will usually grant access to some set of services and resources. This policy is applicable to those responsible for the management of user accounts or access to shared information or network devices; information can be held within a database, application or shared file space. This policy covers departmental accounts as well as those managed centrally.

- Issuing Accounts: The owners of organization data are takes decision regarding access to their respective data. Account setup and modification will require the signature of the requestor's supervisor. The identity of users must be authenticated before providing them with account and password details. Passwords for new accounts should NOT be emailed to remote users UNLESS the Email is encrypted. The date when the account was issued should be recorded in an audit log. All users of accounts with access to organization data must sign the required documents that are kept in their personal file under the care of the Human Resources department.

- Managing Accounts: All accounts will be reviewed at least annually by the data owner to ensure that access and account privileges are corresponding with job function, need-to-know, and employment status. Any temp or guest accounts with access to organization computing resources will contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized department heads. Assign the roles to the staff of an organization instead of individual rights according to their category.

- Shared Accounts: Use of shared accounts is not allowed. However, in some situations, a provision to support the functionality of a process, system, device or application may be made. Each shared account must have a designated owner who is responsible for the management of access to that account. The owner is also responsible for the above mentioned documentation and for establishing and maintaining the account name and password in the organization password database, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.

- Administration of Password Changes: The identity of users must be authenticated before providing them with ID and password details. Whenever possible, organization passes should be used to authenticate a user when resetting a password. Password change events should be recorded in an audit log.

- Application and System Standards: Applications developed at organization or purchased from a vendor should contain the security precautions. Passwords must not be stored in clear text or in any easily reversible form. Role-based access controls should be used whenever feasible, in order to support changes in staff or assigned duties. Systems should allow for lock-outs after a set number of failed attempts (5 is the recommended number). Access should then be locked for a minimum of 5 minutes, Lock-outs should be logged.

- Device Distribution and Used Policy: In today's E-commerce the organization provide resources like Pen Drive, Laptop, Removable Hard disk drive, CD, DVD, Mobile etc. to the employee. It is necessary to aware the employee of how & when to use it, for example, if the organization has provide the laptop then it should be protected preferable with biometric authentication or password and all information are stored in encrypted form. Also maintain all activity perform by the employee, wherever he/she connect with organization network with laptop. If organization provides mobile it has to track all outgoing/incoming call, SMS, MMS and application stored in it. Within an organization campus Mobile or Laptop users should not be allowed to On Bluetooth, On Infrared or use USB cable for accessing the network without administrator permission. Limit business data exposure by defining what can and cannot be copied onto each device and how that data may be stored, modified, deleted or shared with others.

IV. CONCLUSION:

It is necessary to implement the security policies before start the online business or accessing the online information through the Internet. It is also important to inform the employee about the security policies in organization and take a signature on policy document related to them. This paper contributes a detailed description of the security policies needed for the organization, corporate and individuals. The paper helpful for admin of network to decide policies and implement in organization..

REFERENCES

[1] http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf
[2] http://research.microsoft.com/en-us/um/people/fournet/papers/an-advisor-for-web-services-security-policies-sws05.pdf
[3] C. Basile, A. Cappadonia, and A. Lioy, "Network-Level Access Control Policy Analysis and Transformation," IEEE/ACM Transactions on Networking, vol. 20, no. 4, August 2012
[4] C. Basile and A. Lioy, "Analysis of Application-Layer Filtering Policies With Application to HTTP," IEEE/ACM Transactions on Networking, vol. PP, no. 99, December 2013
[5] A. Liu, "Change-impact analysis of firewall policies," in 12th European Symposium On Research In Computer Security, Dresden, Germany, September 24–26 2007
[6] Guide to Computer Network Security, By Joseph Migga Kizza, 3rd Edition, Springer
[7] Cyber Security Management: A Governance, Risk and Compliance Framework By Dr Peter Trim, Dr Yang-Im Lee, Gower Publishing Ltd.
[8] Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Eric D. Knapp, Joel Thomas Langill, Syngress