Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 7, July 2015, pg.27 – 31

RESEARCH ARTICLE

Security Policies for Exchange the Secret Information to Protect against the Attacks on Websites

Prof. (Dr.) Prashant P. Pittalia

MCA Department, Gujarat Technological University

prashantppittalia@yahoo.com

Abstract - Digital attacks may slowdown, effect the cost, reduce the public relations, of the organization or corporate. In today's environment most of the organization having their business through the Internet and they are using their own web server web applications and hardware devices to increase the strength of the organization. At the same time they must have to take care out of the security breach created by hackers or intruders in the web resources. The first step towards the protection of resources against the attacker is to clearly define the organization policies on who, how and when use the web resources and it should be in well-written. Also the policies should be communicated to all persons involve in online accessing the resources of the organization. It is important to aware the employee about the rules and regulation of how to work in online resources and what is important of it, what are the risk associated with it. Here I am explains the usefulness of security policies in the organization as well as the how it improves the strength of organization or corporate. The proposed security policies provide how to make the web resources more secure than normal web resources. It is helpful for the various sectors like banking, finance, retail, medical, education, etc.

Keyword - Virus, Spyware, Authentication

I. POSSIBLE ATTACKS ON WEBSITES

A. Virus

Attaches itself to other software and attempts to spread within the system and to others primarily using e-mail as a transport to spread. It may alter data and files on the infected computer. It is generally attack on application layer.

B. Worm

Spread through a network usually exploiting vulnerability in an operating system or application program. It attacks at the network and application layers.

C. Trojan horse

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.

D. Spyware

Software that may be installed as part of another program. It may also be installed when a user visits a website with malicious code or when an already running process loads and installs it. This program is designed to report on what the user does to the program creator.

E. Adware

Software that may be installed as part of another program. It may also be installed when a user visits a website with malicious code or when an already running process loads and installs it. This program is designed to serve ads, usually in the form of popup to the system user.

F. 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.

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.

II. EXAMPLES OF SECURITY CRIME

A. Fast Flux

A criminal uses advanced technology to ensure that his own terrible website remains "untraceable" to Security agents trying to close him down. They use "fast flux", to hide the location of phishing and spamming sites.

Fast flux networks give attackers some key advantages over the older methods of running phishing and spamming sites. In the past, a phishing site would be linked to a single domain. A phisher would register a fake bank site - say, thefakenatwestbank.com; the site must reside on a machine on the Internet. But once that machine is spotted (from the domain name system or "DNS" records passed around the net, which translate, say, thefakenatwestbank.com into its IP address, say 10.25.25.16) it will be shut down.

Fast flux keeps changing the DNS records (on the orders of one of the machines on the botnet) perhaps every three minutes, thus changing the machine on which the phishing or spam site is hosted. Every machine on the botnet hosts the same site, but trying to shut it down means serially shutting down every single machine on the botnet. This constant "flux" means the botnet's server can't be found, as well as adding a vast new headache to those trying to stop phishing or shut down spammers - who need their sites to stay online to profit.

B. Kifah Maswadi: Sold Pirated Video Games

Maswadi sold pirated Nintendo video games in connection with “Power Player” handheld video game consoles. He had distributed the pirated Power Players in which the consoles connected to a television set with cables; the consoles were pre-loaded with at least 75 Nintendo games. Maswadi sold the game consoles and pirated games to customers in the Eastern District of Virginia and elsewhere through several websites he operated, including: www.powerplayerusa.com; www.powerplayergames.com; www.powerplayerwireless.com; www.gamextera.com; www.wirelesspowerplayer.com; www.marioisback.com & www.gameultimate.com. The indictment also alleges that Maswadi sold Power Player game consoles and pirated Nintendo games in wholesale quantities.

C.VICTOR VEVEA: Distressing e-mails

VEVEA had been found guilty on January 24, 2008 of unlawfully accessing the e-mail account of Bakersfield attorney Michael Kilpatrick for the purpose of sending out harassing e-mails in Kilpatrick’s name. VEVEA gained access to Kilpatrick’s e-mail account and began sending out e-mails in Kilpatrick’s name to government officials and other lawyers in which Kilpatrick purportedly admitted to being a “pervert.” At the same time, VEVEA put up posters all over town, including at Kilpatrick’s children’s school, in which people were told to “warn your children not to be on the street alone” when Kilpatrick was in the neighborhood.

D. Financial Fraud

In Jan 24 2008, French banks Societe General discover an assumed euro 4.9 billion fraud by a futures trader who fooled investors and violate his authority. He used his knowledge gained while working in a different segment of the bank to bypass control procedures and hide his trades from his bosses.

III. PROPOSED E-COMMERCE SECURITY POLICIES FOR ONLINE BUSINESS:

Organization uses the security policies as per their requirement. Here I am discussing the E-commerce security policies which are essential to every organization, regardless of size, location, and mission or the product or service produced.

A. Insurance policies

Insurance Policy defines which E-commerce issues are covered under the policy. Organization has to collect the E-commerce data and its associated risks to decide the insurance policy. Insurance companies might cover following.

1) The loss of intellectual property.
2) Damage or loss of goods during shipment.
3) Some costs due to credit card fraud or nonpayment.
4) The cost of prosecuting criminals or any cost of paying for information that leads to the capture of a criminal.

B. Wireless Security Policy

To access the enterprise resources remotely the VPN must be used. Apply strong authentication and the encryption of sensitive data wherever it is stored. All wireless devices should be registered with their IP address and Physical address to confirm by the admin before accessing the organization data. Also the physical boundary is decided to accessing the information. Admin is alert if someone accesses the data outside the boundary and sensor application will find the physical location of the device. Most of the organization provides the wireless connectivity for 24hrs a day, 365 days a year. The attacks are done mostly during the organization non-working days and out of organization time schedule, so wireless accesses should be disabling during that time and day.

C. Privacy Policy

Privacy policy defines what is private and what is not private when working with the organization resources like hardware, software, company property. Privacy is addresses by the laws and regulations. This policy defines what information is collected and what are not, what information can or cannot be disclosed, for what purposes the data was collected, to whom the information may be disclosed.

D. Authentication Policy

Authentication policy decides how the user is accessing the information. It should be decided by the organization that E-commerce data is accessible by single-factor authentication or two-factor authentication. Most of the E-commerce sites are using password based authentication. The password may be cracked if it is week, so it is preferable to use the biometric characteristic for the authentication. Fingerprint, Face recognition, Hand geometry, Palm print, Iris recognition, Signature and Voice recognition are various biometric characteristics used at various applications in organization. PINs and passwords are vulnerable to being forgotten, given away, observed by others or otherwise obtained. Cards can be stolen and /or forged. Combining the operations with a biometric system will improve both usability and security.

E. Disposal and Destruction Policy

The disposal and destruction policy defines when and how to free the important material. Sensitive printed documentation or old storage devices thrown away can be collected and examined by your competitors, your enemies, and the government. It is a serious threat to security. Shredding and burning are often solutions for both printed materials and storage devices. The low level formatting of a storage device prevents all known concepts of data trace recovery.

F. Classification Policy

Organization can benefit from the use of a classification system. A classification system sorts and labels every resource with its value, importance, sensitivity, cost, and other concerns in order to guide the implementation of security and prescribe processes of management and use. Assigning classification labels, such as public, private, sensitive, internal only, confidential, proprietary, etc., helps Employees understand how to use and handle resources properly. This policy helps to defense against social engineering and other information leakage attacks. If employees know how to communicate through E-mail, Chat, Mobile and Phone, then most socially guided attacks through those mediums will fail.

G. Change Management Policy

Organization needs to install new software, updating existing software, updating device drivers, updating patches and modifying configuration to provide more security. The security is at risk if change is not monitored or controlled. A change management policy imposes a procedure to evaluate, test, and approve changes before they are allowed into the production environment. Organizations should adopt the rule that no software is ever installed before it has been tested and approved. This will prevent most internal causes of downtime and security failures.

H. Storage and Retention Policy

It is needed to store and maintain the information of an organization. Data, such as customer information, financial history, auditing data, etc., must often be retained for years or indefinitely. It is important to plan out the technology, storage location, and security of the process of backing up and storing this information. If technology changes then long-term storage can have

problems. Be sure to keep a working media device, backup software, and compatible OS software in storage along with all stored backup media.

I. Language Policy

It defines which languages are supported by the E-commerce applications. Today most of the E-commerce websites pages are developed in English language. It should be difficult for person who is expert in other than English language to use the E-commerce website for doing the transaction. If website is provide in Multilanguage than it should be increase the number of customers.

J. Information Policy

Information policy determines the kind of information collected, created, organized, stored and accessed. It is used to cover all the information within a organization. It identifies the perceptive information and steps to protect it from intruders. Each employee must be aware about the sensitive data that comes in to his/her control.

1) Perceptive Information: All the information in the organization is not sensitive. It is identified and aware the employees of the organization about it are important which comes into their control. Business transaction records, product design, patent information, payment information, Budget information are considered as perceptive information.

2) Storing and Marking Perceptive Information: The information should be stored in paper as well as in computer files. To store the information required some level of protection, which makes the information very secure. Using strong encryption/decryption techniques the files, folders and drive should be stored in computer. So in case of unauthorized access or stolen of laptop the data should not be accessible to the attacker. Using header and footer in the Microsoft word you can mark the information.

3) Transmission of Perceptive Information: The information is transmitted via the fax, e-mail, mms etc. To protect the information it should be passed through encryption/decryption techniques. Deleted information may be store in the recycle bin. The other entity may misuse the recycle bin data. So provide the facility which will not allow the unauthorized person to access it.

K. E-mail Policy

Most of the chances to leak the information of organization are through the E-mail. The organization need to create its own email service to track all corporate Emails. Employees are restricted to send information to selected Email addresses according to their role and responsibility. Employees are not allowed to forward or send email to public email services like Yahoo, Zapak, Gmail and Windows Live Hotmail etc. As the employee is relived from the organization his/her account is automatically disable for further processing.

1) Internal Mail Issues: Employees of the organization are not allowed to pass illegal information with a network. Also they are restricted to number of email. Personal email saved in different folder. It also dictates deletion of e-mails after a certain amount of days.

2) External Mail Issues: Each outgoing mail should be checked by the administrator. The policy should say that which information is allowed for outsider and how securely it is transmitted to the outside users. Also it tracks about the information coming from outside to within organization. Also employees are instructed on compressing attachments to save bandwidth.

Incident Response Policy: This procedure should detail which actions should be taken in case of a security incident. It is regularly monitored for security breaches. When a breach is detected, one must know how to react. That is the aim of this procedure. The reaction to an incident aims to protect and restore the normal operating condition of computers, services and information. The goal or purpose of this policy is to minimize downtime, reduce loss, and improve availability.

L. Incident detection: quick assessment

It helps in find out the source of theft. E.g. Accidental administrator damage/mistakes, accidental disclosure of internal or confidential documents, attack from the Internet, attack from the telephone network or attack from inside the corporate network. Also check the effect of it on system. It decides where the problems occur, extent of damage.

*1) Immediate action: limit damage: I*f a serious attack or disaster occurs, the Management Responsible and Technical Responsible should decide on the immediate action necessary to eliminate the threat or limit damage. Start an event log: Document every single action taken, events, evidence found (with time & date).Possible immediate actions are:

- a restore of information,
- The concerned client, server, or network can be isolated from the network or shutdown.
- Attempts are made to minimize the damage without affecting user services
- An immediate copy of all logs/data could be made to tape or other offline storage.

2) Detailed situation analysis: Set priorities, decide what to do. Determine the extent of damage. E.g. analyze the system(s): what files have changed? What programs/accounts were added or modified? If modifications are found, check for these

modifications on similar systems. Try to confirm exactly what happened. Notify administrators, management and law enforcement authorities as required.

M. Software Policy

It defines the precaution taken during purchasing or maintaining the software. An organization has to purchase or develop the E-commerce application such a way that it does not use any third party controls in it. Because it may be possible that third party control may make your system vulnerable. Also there is need to check that the test data should not be your actual data. Delete or disable the unnecessary users provided in software. The default Password of Operating System software, Database software, or Application software should be changed once it is installed on computer. Users may not duplicate any licensed software or related documentation for use elsewhere. Developmental and operational software should be run in different operating environments. Source code and configuration files should be protected from unauthorized viewing and changing. If possible then do not provide the source code on operational systems.

IV. CONCLUSION

The Web servers are secure with the proper installation and configuration of hardware and software. It protected against cyber threats, vulnerable, and several types of potential attackers. It is necessary for the organization to regularly identify the current cyber attacks and which are the countermeasures use in various cases. Also It is very important to understand the security policies and apply the appropriate policies to protect the devices and resources against the cyber threats.

REFERENCES:

[1] Sari Stern Greene, Security Policies and Procedures: Principles and Practices. Prentice Hall
[2] Sandy Bacik, Building an Effective Information Security Policy Architecture. CRC Press
[3] Computer Crime Research Center, "Cybercrime is in a state of flux", March 29, 2008, http://www.crime-research.org/articles/cybercrime0308/
[4] http://www.gamepolitics.com/category/dmca?page=3#.VZiGIPkirIV
[5] http://www.bakersfield.com/news/2008/02/14/paralegal-sentenced-for-sending-harassing-messages-from-attorney-s-e-mail.html
[6] http://www.marketwatch.com/story/socgen-takes-71-billion-loss-on-rogue-trades
[7]http://www.esecurityplanet.com/trends/article.php/3861026/US-Oil-Companies-Targets-of-Tenacious-Cyber-Attacks.htm 9 December 2009
[8]www.datasecuritypolicies.com 5 January 2010
[9]www.watchguard.com/docs/whitepaper/securitypolicy_wp.pdf 11 January 2010

