CYBER SECURITY ANALYSIS USING POLICIES & PROCEDURES

ER.ASHAD ULLAH QURESHI, ER.SARVESH RAI

Abstract: Internet provided us unlimited options by enabling us with constant & dynamic information that changes every single minute through sharing of information across the globe. Many organizations rely on information coming & going out from their network. Security of the information shared on the global network gives birth to the need of the cyber security. Cyber security means the security of the information residing in your cyberspace from unwanted & unauthorized persons. Through different –different policies & procedures we can prevent our information from both locally & globally active invade (Hackers).Cyber security is a proactive step to prevent data assets. The policies & procedures, helps us to assess effeteness & ineffectiveness of the security maintained so far by the organizations. Policies & procedures ensures that a standalone PC & a networked PC can be protected in a very effective manner. This paper describes in brief the methodologies'& techniques involved in policies & procedures of along with its benefits & precisions. This paper aims at awareness & creating a security mesh & explains the importance of computer security to deferent organizations.

Keywords: Cyber Security, Cyber Defense, Policies & Procedures, Ethical *Hacking etc.*

Introduction: Cyber security is one of the major issues & commercial Information systems. The growing connectivity of computers through Internet. Increasing number of systems & the exponential growth of size of complexity of the systems have made cyber security a very big problem now days. It is required that organizations to adequately protect their Information assets of following the Policies & different procedures to provide protection from the risks & attack on organizations Database. The protection of our information that it is flowing of networks, this poses a challenge to cyber security. The Lake advantage of IT revolution & its application, the organizations needs to focus on cyber security this will ensure. Protections of its information & systems assets against deliberate branches. As well as failures arising out of negligence & accidents since both equally damaging & their prevention of paramount importance. Computers have now become an initial & indispensable part of our systems. They are used for tasks ranging from routine office work like would processing to complex & operations\al crucial tasks like data fusion & mining. Computers & other Value Added Services (VAS) have become an integral part of our Management & communication systems. With all the advantages of network technology as establishments of networks is inevitable & with these home unprecedented challenges to. Information Warfare (IW) will dominate the 21st century conflict. The battle field will have a number of networks for passage of date in real time. Management of these information systems will be critical for winning the IW. The body between battle field systems of the information system infrastructure has begun to blue, giving the adverting a wealth of non-secure targets in the moss haziness of his moderns, thus, while there have been many benefits of the information revolution, the vulnerabilities' have also increased proportionately.

An Overview of Cyber Security Policies & Procedures

The complete process of Cyber security policies are conducted in major parts. Every aspect of these has a major impact on cyber security of an institution.

A. Vulnerability Analysis

The design & implementation of compile security measured. Depend on the type & complexity of networks for information Computer systems & networks for this purpose are classified as follows:-

(i) Stand-Alone Computers: The security management of stand alone, computers & peer to peer networks. Will be responsibility of authorized persons in whose charge the machine is designated to work.

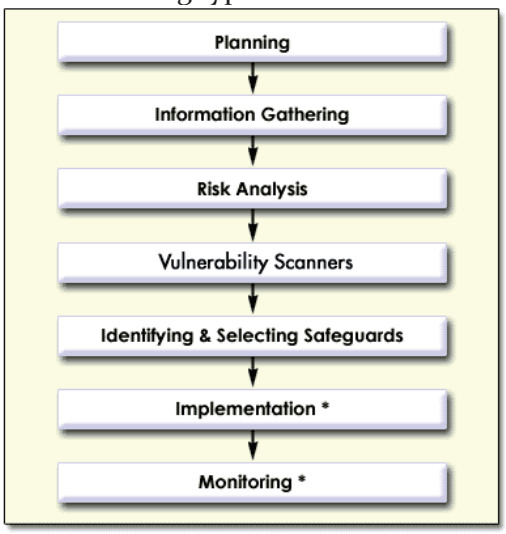
(ii)Computer Peripherals: This encompasses all the peripherals being utilized routinely by the various branches. Which includes scanners, printers, CD writers & Photocopies etc.These machines should be installed in Crypto-Centers, centralized facilities to enable close supervision over transmission.

(iii)LANS: the security management of LAN will be the responsibility of the systems Administration of the LAN. The decision of system admits of the network beginning from the clients through the wireless links via the hubs/route/ other across on network devices, till the across point of the WAN.

Information systems are composed of heterogeneous components interacting thorough some form of communication medium. The assorted security & protection required for their holes in information systems & provide an overall assessment of system integrity.

B.Vulnerability Analysis Risk Management

Vulnerability analysis and risk as assessment needs to be carried out periodically to identify security problems from compliance to lay down security policy. All vulnerabilities deleted during analysis must be brought formally the notice of the controlling authority & corrective action initiated immediately. These vulnerability tools are of following types:



Risk Management.

(a)Audit Trials: to carboy out a system audit of generate of audit report specifying weaknesses of notices unauthorized activities of areas to be addressed.

(b)Intrusion Deflection: To detect unauthorized access to networks.

(c)Penetration testing/ Detection: To test the strength of our networks anoints any unauthorized intrusion for cyber attack.

(d)Event Log: To generate a log of all activities taking place on the network at specified frequency in order to (maintain) monitor the network.

The full registers of security threats to computer network can be addressed under the following heads:-

(a)Physical Threat: this is by way of contact by unauthorized persons with the network server, work stations cabling, jacks of computer, usage by unearth persons of data displayed LAN server or the screen or the screen of a work station which is logged on to the network or the of components or work station.

(b)Electronic Threat: this is affected by intro of topic bombs, Trojan house or virus programs, manipulation of files, alteration of size, file corruption, changing of password, access control software security, breaking codes of encryption by systematic hacking, taping of interconnecting electronic cabling etc.

Network communication is another area of security concern this concern consist primarily of the following two types of attacks – “Capping” of ‘spoofing’ wire tapping provides with risk for attack on any systems which uses telephone or wire communications. Spoofing is pretending to be a server or peer. There are multiple kinds of spooks that can be employed. A program can be put in place to replace the login program of gather usernames of & password. Another spoof can be implemented between servers, where one server identifies it to another server for routing of communication. It the fourth server begins using the spoofing server, all information routine through it can be captured.

(c)Procedural Threats: threaten occur due to lack of LAN documents, faulty maintenance documents, improper classification of data of irregular assignments. Permissions, locality of policy & standard ordered procedures (SOPs) on LAN / security, lock of security training to the users& operators, not earmarking clear cut responsibility not nomination a qualified LAN administrator.

(d)Cyber Attacks: Growing numbers of networks of reliance of computer based system for war

fighting have made us vulnerable to cyber attacks by adversary securing endpoints without impacting efficiency of system performance demands a highly flexible solution that task into account the necessity of cyber security measures of the dynamics of our specific work environment.

Scope & benefits

Cyber security is conducted in four major aspects those are entitled for their respective scopes & benefits & they are as follows:

(1)Vulnerability Analysis

(2)Cyber Security Policy

(3)Areas of Breaches in Computer Security & Measures to overcome them.

(4)Damage & Disaster Management.

A.VULNERABILITY ANALYSIS

The design and implementation of computer security depend on the type and complexity of computer system. Commonly, the types of information or computer system and networks for information/computer system and networks for this purpose are classified as follows-:

(a)Stand alone computers-: the security of standalone computers and peer-to-peer networks will be the responsibility of officers or executives in whose charge and department the machine is designated to work.

(b)Computer Peripherals: This encompasses all the peripherals being utilized routinely by the various branches to inclusive fax machines, scanners, printers, CD writers and photocopies etc. These machines should be installed in crypts centers, centralized facilities/branches to enable close supervision over transmission. This equipment should be held on the personal charge of an office.

(c)LANs-: The security management of LAN will be the responsibility of the system administrator of the LAN. The decision of the system administrator of these networks shall cover the length and breadth of the network beginning from the clients through the wireless links, via the hubs/routers/other access or network devices, till the access point of the WAN (if the subject network is connected to the WAN).

B.CYBER SECURITY POLICY

Cyber security policy covers the following issues-

1. Safeguarding of classified and confidential information: Classified and sensitive confidential information shall be safe guarded at all times. Necessary safeguards in terms of passwords and authentication systems shall be applied so that such information is accessed only by authorized persons and retains its content integrity.

2. Safeguarding of information and information systems [IS] resources: Information and its resources shall always be safeguarded against sabotage, tampering, denial of services, espionage, fraud, misappropriation, misuse and release to unauthorized person. this shall be accomplished through the continuous employment of safeguards consist of administration, procedural and physical means.

3. Networking of different information systems [ISs]: When IS managed by different administrators are interfaced of networked, compatible accreditation requirements will be evolved. The details will include description and classification of data, clearance levels of the users, designation of the administrator who shall resolve conflicts if any and safeguards to implement before interfacing the IS.

4. Internet Access: A networked computer will not be connected or used to access the internet. Stand- alone PC's not having important data can only be used to access internet wherever the competent authorization has accorded such permissions. No information of value will be passed using internet as a media. These PCs should be on the charge of an officer like manager or other administrative post who use PC for internet. The downloaded data should be scanned before copying it on a CD. Internet PCs too should have updated licensed antivirus. Adequate differential measures need to be taken while reconfiguring to internet PC for use on internet and vice-versa.

Following are the important points to be followed-:

(a) Software downloads should be avoided. However necessary, only download from trusted sites inet.com that certify their downloads.

(b) All articles and other documents .pdf or word should be downloaded and then scanned before opening.

(c) Internet browsing should only be done from a user account which has limited rights rather than an administration account which has rights for installing and running .exe files.

Areas of Breaches in Computer Security

1. Personal Security**:** User Responsibility-User Accounts on official computer systems are to be used only for official purpose & not to be used

for personal activities. Unauthorized use of the system may be in violation of the company Law, constitutes theft can be punishable under some circumstances, therefore, unauthorized use of the official computing system & facilities may constitutes grounds for prosecution/disciplinary actions.

2. Physical Security: Physical protection of premises housing the computer hardware& software system & data contain therein, is absolutely essential. This requires batter techniques then those for conventional office security & document.

3. Biometric Security: Biometric Systems are based on unique characteristics of human being. These provide extra protection for PCs & laptops. These can also be used to control access to sensitive area like the operational rooms. Fingerprint locks are an invaluable tool for high security centers.

4. Chassis-Lock: Chassis lock should be used to avoid change of password though removal & reinsertion of CMOS battery.

5. Software Security

Only licensed & proprietary version of the software shall be used. In a regular patch management should be ensured for reducing operating system & antivirus vulnerabilities.

6. Database Security: The need for security arises once the Databases house information that can be accessed across the network. Security of Databases, need to be taken into act while conceptualizing & creating them. Entry into Databases needs to be rigidly controlled. Access right must include who can access what classified information & who can read, modify, create, delete, take print outs & for what duration the access be allowed. Management of Database will always rest with the central agency which develop or introduced it for use.

7. Communication Security: Elaborate interests already exist on security in communication media of various hues. There will be no exceptions in this regard for data networks. Briefly, security for communications which carry data networks will be as follows:

(i) Within in a LAN data should flow with customized software based secrecy depending upon the content classified document.

(ii) Between adjacent WAN nodes an additional hardware based secrecy system will be used for encryption of the channel/media.

8. Network Security: Security measure use to ensure network security is largely software based. These includes

(i)Methods must be instituted to prevent unauthorized access to network/system implemented through system administrator by means of authentication procedures.

(ii)Use of non repudiation feature through the use of digital signature procured through company channels for accountable document transactions.

(iii)Registered audit should be carried out to ascertain breaches in security on the LANs.

Damage & Disaster Management

Computer related disasters can occur in form of data & information theft, intentional or unintentional corruption or loss of data by persons, damage due to fire or other natural calamities.

A. Firewalls

Firewalls shall be used by all WAN/LANs Servers. The WAN/LAN administrator will provide firewalls. The default PC Windows firewall should be enabled. Firewall will be used as under

(1) All inward & outward traffic must pass through the firewall

(2) Type of traffic to be passed & persons permitted to originate such traffic will be defined by the local security considerations.

(3) Firewalls must be made immune to penetration by institutions of Intrusion Detection System.

(4) Enforcement of strong authentication.

B. Authentication System: In order to make the system trusted, strong authentication is essential. Numerous systems of authentications are available for use.

C. Encryption System: Encryption of classified data & messages during storage/transactions is an essential & important element of security.

D. Capability Restoration: Capability is an important facet since it restores the information systems to their correct configuration after a mishap. Information system must embody automated restoration capabilities & other redundancy options.

E. Data Backup: Data backup is an important ingredient of infallible capability restoration strategy. Information system infrastructure must cater for other information systems crises management teams (ISCMT) as part of the

management organization. These teams would be responsible for providing the security framework to the information systems, assist in implementation of security infrastructure, carry out periodic vulnerability analysis, react on security related incidents & help on restoration of information system during crisis/emergency.

References

1. *C. Sudhakar, B. Vasu, V.Ramachandra Prasad, N. Bhaskar Reddy,* Effect of thermophoresis Particle Deposition ...; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 2 Issue 1 (2013), Pg 51-53
2. S.Shah, B.M.Mehtre,"A Reliable strategy for Proactive Self Defence in Cyber Space using VAPT Tools & Techniques", IEEE 4th International Conference on Computational Intelligence & Computing, ICCIC,2013,Madurai,India.
3. W. LanFang and K.HaiZhou, " A research of behaviour based penetration testing model of the network". IEEE International Conference on Industrial Control & Electronics Engineering, Aug 23-25, 2012,Xi'an, China.
4. Jatinderdeep Kaur, integrability and *L1*-Convergence of Mixed; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 3 Issue 1 (2014), Pg 96-98
5. S Turpe, J.Eichler, "Testing production systems Safely: Comman precautions in Penetration testing", IEEE Academics and Industrial Conference, Sep 4-6, 2009, Windsor.
6. A.Austin and L.Williams, "One technique in not enough: A comparison of vulnerability discovery techniques".IEEE International Symposium on Empirical Software Engineering and Measurement, Sep.22-23,2011, Guenther, Ruhe.
7. *Babar Vijay Y, Raut Yogesh G, Khot P.G.,* Queuing theory and Patient Satisfaction: An Overview of Terminology ; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 2 Issue 2 (2013), Pg 147-153
8. A Kurilo, N.Miloslavskaya and S.Totstaya, "Ensuring Information Security controls for the Russian banking organizations."ACM Conference Sin'09, October 6-10, 2009, Gazimagusa, North Cyprus.
9. Open Web Application Security Project, https://www.owasp.org/ index.php/ Category: Vulnerability.
10. A.P.Dhana Balan, R.Buvaneswari, totally Feebly Continuous Functions; Mathematical Sciences international Research Journal ISSN 2278 – 8697 Vol 3 Issue 2 (2014), Pg 584-586
11. Audit your website security with Acunetix Web Vulnerability scanner, https://www.acunetix.com/vulnerability-scaccer/.

* * *

Ashad Ullah Qureshi/Tilak Ganj Sagar MP/
M.Tech Scholar/RGPV/asadullah31@rediffmail.com
Sarvesh Rai/Bada Bazar Sagar MP
/Asst.Professor/RGPV/sarvesh.s51@gmail.com