Information Security Threats, Vulnerabilities and Assessment

Satish Kumar

Abstract—**The majority of government or private institutions\organizations related to business, commerce, finance, education & training, research, health and defense etc have placed their information on computers lying on cyberspace. It is very helpful for the growth of society. The information present on cyberspace is not safe and can be deleted, destroyed, distorted and communicated easily. This may cause financial or social or legal loss to anyone. Information security protects three characteristics related to the information i.e. confidentiality, integrity, and availability. It is cheaper to avoid security breach in earlier stage than to recover from it. Vulnerabilities are weaknesses in system design and may be on client or server side that an intruder can exploit to gain access to a system. In this paper, a study on various security threats and vulnerabilities has been made along with its effectiveness. The role of security assessment is also discussed briefly.**

Index Terms— **Cyberspace, Information Security, Server-Side, Client-Side, Network, Vulnerabilities, Audit**.

I. Introduction

The advent of Information and Communication Technology (ICT) has changed the way we collect, organize, generate, present and disseminate the information. Today, we live and work in globally connected world also known as cyber world. The emergence of ICT has given birth to various new terms such as Internet economy, digital democracy, cyber crime, cyber banking, cyber culture, cyber war, virtual community, e-participation, e-governance, e-commerce, on-line journalism, on-line shopping, on-line gaming etc[1]. The evolution of digital computer and, information and communication technology has changed the working style of people. The information which was earlier processed manually are totally managed through computer. The majority of information that were recorded on paper are being stored in digital form. The availability of Internet has made people dependent on cyberspace. Around 40% of the world population has an Internet connection and there are 3 billion users of Internet world wide[2]. The majority of government or private institutions\organizations related to business, commerce, finance, education & training, research, health and defense etc have placed their information on computers lying on cyberspace. The massive information are available on cyberspace. No doubt, the availability of this information on cyber space is very helpful for society. On the other hand, some criminals for the sake of their own gain are taking advantage of it. The information present on cyberspace is not safe and it can be deleted, damaged, distorted, stolen and communicated over the network to entire world very easily. The criminals are using various tactics to gain unauthorized access to the information.

The number of security breaches suffered by large organizations increased from 81% in 2014 to 90% in 2015 and number of security incidents risen from 66% since 2009[3]. There is shortage of skilled professionals such as security analysis (47%), security engineers & designers (32%) and security auditors (31%) that is negatively impacting the security and integrity of organizations [4]. The average total cost of data breach increased by 23% in past two years [5]. According to the survey conducted by AICPA, one-in-four American is a victim of information security breaches in past [6]. With the number of incidents of information security breaches are increasing, the organizations are investing huge money to get their information protected. There is need of installing effective information security at different level to ensure that sensitive information stored or transcribed in digital form may not be compromised.

II. Information Security

Information security is a strategy used to protect information in electronic format which includes protecting all systems or system devices, storage media and communication channels that carry information of the organizations and the users. It protects three characteristics related to the information i.e. confidentiality, integrity, and availability. Confidentiality guarantees no unauthorized users can view the information. Its breach can allow valuable or private information to fall into the wrong hands; Integrity guarantee that the information is complete, correct and original and has not been altered by any unauthorized user or malicious software. Loss of confidentiality often cannot be recovered. Integrity compromises can cause people to doubt information *i.e.* whether systems and network devices are working properly or not. On the other hand, availability guarantee that information is accessible to authorized users. The interruption in availability can completely disrupt computing operations. The objectives of information security are to prevent information or identity theft, avoid litigation for not securing information, maintain productivity, and foil cyber terrorism [7]. It is cheaper to avoid security breach in earlier stage than to recover from it. There are three ways to mount attack on information [8]: 1) Server-side, 2) Client-side and 3) Network Oriented. In case of server-side attack, the client-side input to the targeted services on server is supplied with maliciously modified data. In case of client-side attacks, the server-side input to the targeted services on client is supplied with maliciously modified data.

Manuscript received April, 2016.

Dr. Satish Kumar is with Panjab University SSG Regional Centre, Hoshiarpur, Punjab, India (a multi faculty prestigious campus of Panjab University, Chandigarh (India)).

A. *Effectiveness*

An effective security policy helps in minimizing security risks, vulnerabilities, and costly breaches. If a security policy reduces or vanishes breaches then it is said that security is effective. This effectiveness can also be viewed in terms of success. For its effectiveness, the support of the top management is not only adequate but there are many factors such as user training, security awareness, proper policy formulation, and policy enforcement that is helpful. The purpose of validating security effectiveness is to ensure the security controls that you have put in place are working as expected and that they are truly mitigating the risks they claim to be mitigating [9]. There are some metrics required for information security monitoring [10, 18]: 1) Investment made in security and it's meaning full results, 2) Managing budget as per proper information security requirement, 3) Number of persons trained in security awareness. The impact of various security factors in terms of fraud loss, audit finding, and security incidents reduction is helpful for effectively managing information security.

III. INFORMATION THREATS

Information threat is a danger in the form of an event, process, act that exploits vulnerabilities to breach information security. It may cause possible harm to the information, program or database etc., in the form of disclosure, distortion, destroy, delay, denial and distribution. Information security threats now a day are prevalent in myriad form - such as spywares, key loggers, content spoofing, bots, DoS, phishing, and other digital data seeker algorithms. A computer system is made up of two components *i.e.* hardware and software. So, some threats are software oriented and some threats are hardware oriented. Software threats are due to malicious codes or malwares designed to infect a computer system, conceal their malicious actions, or gain something from their deeds. The various program codes of this category are: Infecting malwares (Virus, worms), concealing malwares(Trojan horses, rootkits, logic bombs), Gaining malwares(Spam, spywares, adware, key loggers and Botnets). Hardware threats targets the system hardware or its associate components such as BIOS, USB devices, network storage etc with the help of malicious codes. The information security threat may be internal or external threats. Threats which are internal to the organization and can be control and minimize at organization level are called internal threats. The threats which are external to the organization and cannot be control and minimize at organization level are called external threats. The external threats are generally natural disasters *e.g.* earthquakes, fire, hurricanes, tsunami, uncontrolled mob and terrorist attacks etc. The major perpetrators of internal threats are the insiders. The risk posed to information security is more due to inside rather outside. Any person having proper authority on information system within organization can intentionally or unintentionally steal, destroy, distort and distribute the information compromising the confidentiality, authenticity, and availability of information security. The threat to information in the business or institution is like a plague and a permanent issue that needs to address promptly. The bigger share of threat to information security comes from the insiders to the organization [woods, 2000]. The reason behind this is that they are trusted and either they have some sort of authority on the information system or gain authority through some tactics such as social engineering, shoulder surfing, etc. Their motivation behind this may be revenge, greed, espionage, and ego etc. The insiders can be further categorizing into following [11]: *a*) Annoyed or displeased employees, *b*) Internal hackers may disclose organization vulnerabilities to the outside hackers, *c*) Criminal may join the organization with sole intension to steal information, assets, money, intellectual property etc due lack of security. *d*) The spying agents within organization may supply information to hackers or competitors outside the organization, and *e*) They may act as an aid to the terrorist groups.

IV. SYSTEM VULNERABILITIES

A security risk is called as vulnerability if it is a resource of attack. Vulnerabilities are weaknesses in system (hardware or software) design and may be on client or server side that an intruder can exploit to gain access to a system. The vulnerability in a system on network may be due to design flaws, poor security management, incorrect implementation, Internet technology vulnerability, the nature of intruder activity, the difficulty of fixing vulnerable systems, the limits of effectiveness of reactive solutions, and social engineering [12]. The cause of vulnerabilities are misconfigurations, policy violations, and system flaws[13]. Majority of design flaws are due to software design and there are three reasons behind it[14]: human factors, software complexity, and trustworthy software sources. The human factor includes: forget to add or remove or verify some code(s), finish product in urgency, overconfidence, malice behavior of developer and overlook certain tests. Complexity include: complexity of problem, difficult testing procedure, programming complexity and misunderstanding in design specification. Some developer not uses trustworthy software to develop or test their product. Shareware and freeware may embed hostile code into trusted systems.

V. VULNERABILITY ASSESSMENT

Vulnerability assessment is a comprehensive study of security weaknesses in a system. Its objective is to verify the existence of some sort of vulnerabilities. Security audits, vulnerability scanning and penetration testing are three main security diagnostics [15]. Information security audits measure an information systems performance against a list of criteria. The vulnerability scanning is carried on the system to know vulnerabilities. The penetrating testing is done to determine a) the possibility of gaining the unauthorised access control to a system; b) the Denial of Services (DoS) caused or likely to be caused by overloading the system through packet flooding. Penetrating testing is an effort to gain access to a system either openly or secretly. Vulnerability assessment can be network-centric or host-based [16]. Network-centric vulnerability assessment tools are used to detect the security weaknesses present in the network of a system. Host based vulnerability assessment tools are used to detect the security weaknesses on a host. No network connection is requires in this case. Identifying threats using a vulnerability assessment tool is the first step toward managing or mitigating the information security risk. The security threat assessment tools are used to explore and list exploitable vulnerabilities and gaps *i.e.* Is there exist any mis-configure or un-patched system components. Vulnerability scans are helpful in determining weaknesses or noncompliance of system products with security requirements [13]. Once vulnerabilities are explored and gaps are identified, the necessary remedial actions are taken to gradually mitigate these vulnerabilities to minimize the impact of threats. Vulnerabilities arising from flaws may require system reengineering or design efforts to correct deficiencies [13]. Vulnerability scanning on a system is used to spot the security weaknesses in it. The various vulnerability scanning tools are[17]: port scanners, network mappers, protocol analyzers, vulnerability scanners, the Open Vulnerability and Assessment Language (OVAL), and password crackers. Port scanners are used to ascertain the status of a port. With this user is able to know the various applications running on a system and which among them can be easily exploited. Network mappers are able to identify various systems connected to a network. The task of protocol analyzer is to capture each packet available in data stream, decode it and examine its content. It is also called as sniffer. Vulnerability scanners are used to spot vulnerabilities on a system and alert system administrators about these. The password cracker is used to determine the strength of passwords by using password cracker programs. Open vulnerability and assessment language (OVAL), an international information security standard, is designed to promote open and publicly available security content. It also standardizes the transfer of information across different security tools and services.

VI. CONCLUSION

The cyberspace is so vulnerable that the information present on cyberspace can be attacked easily causing loss to anyone. No doubt the availability of millions of digital information hosting devices on cyberspace has made huge advantage to the society world-wide but some elements in society who might take advantage to gain; financially, politically; from such infrastructure by causing damage to others on the expenses of small or no cost. Security threats are due to security vulnerabilities. The previous year’s survey reveals that the numbers of information security breaches are increasing day by day. There is shortage of professionals dealing with security related to information. There are so many factors, apart from support from top management side, to make information security effectiveness. If an organization takes some remedial steps then such attacks can be avoided. One more way of ensuring information security is assessment of security by organizations on routine basis. Security audits, vulnerability scanning and penetration testing are three main security diagnostics the organizations must follow.

REFERENCES

[1] Christian Fuchs, Internet and Society: Social Theory in the Information Age, Routledge Research in Information Technology and Society (2008).

[2] Internet Live Stats - Internet Usage & Social Media Statistics http://www.internetlivestats.com/internet-users/

[3]http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html; 2015 Information security breaches survey.

[4] https://www.isc2.org/giswsrsa2013/; “The 2013(ISC)^2 Global Information Security Workforce Study Survey 2013”.

[5] https://securityintelligence.com/cost-of-a-data-breach-2015/; ‘2015 Cost of a Data Breach Study: Global Analysis’.

[6]http://www.aicpa.org/press/pressreleases/2015/pages/aicpa-survey-one-in-four-americans-victimized-by-information-security-breaches.aspx

[7] M. Ciampa, Security + Guide to Network Security Fundamentals, Chapter-1(Introduction to Security),Third Edition, Course Technology, Cengage Learning(2009).

[8] A VLADIMIROV, K GAVRILENKO, A MICHAJLOWSKI, Assessing Information Security: Strategies, Tactics, Logic and Framework, IT Governance Publishing , IT Governance Limited (2010).

[9] A. Caballero, Information Security Essentials for IT Managers: Protecting Mission-Critical Systems (Chapter 14), Computer and Information Security Handbook(Ed. By J.R Vacca), Elsevier(2009).

[10] R. S. Poore, Information Security Governance(Chapter-8), Information Security Management Handbook, 6th Ed.(H.F. Tipton,M. Krause), Auerbach Publication, Taylor & Fransis Group, 2007.

[11] Marcus K. Rogers , Internal Security Threats, Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management, Vol. 3, pp 3-17, Ed. (Hossein Bidgoli)Wiley (2006).

[12] Pethia, Richard D. Information Technology—Essential But Vulnerable: How Prepared Are We for Attacks; http://www.cert.org/congressional_testimony/Pethia_testimony_Sep26.html.

[13] S. M. Price, Developing and Conducting a Security Test and Evaluation, Corporate Governance, Information Security Management Handbook, 6th Ed.(H.F. Tipton,M. Krause), Auerbach Publication, Taylor & Fransis Group, 2007.

[14] J. M. Kizza, Guide to Computer Network Security, Computer Communications and Networks(Series), (Chapter-4)Computer Network Vulnerabilities, Springer-Verlag London 2009.

[15] www.isag.com/; Internet Security Advisor Group.

[16] M. SANTANA, ELIMINATING THE SECURITY WEAKNESS OF LINUX AND UNIX OPERATING SYSTEMS(CHAPTER 6), COMPUTER AND INFORMATION SECURITY HANDBOOK(ED. BY J.R VACCA), ELSEVIER(2009).

[17] M. Ciampa, Security + Guide to Network Security Fundamentals, Performing Vulnerability Assessment(Chapter 9),Third Edition, Course Technology, Cengage Learning(2009).

[18] Herrmann, Debra, Ben Rothke, Robert Slade, Ralph Spencer Poore, Jeff Davis, Todd Fitzgerald, Stephen Fried, Jeff Misrahi, and Brian Geffert. "Outsourcing Security", Information Security Management Handbook on CD-ROM 2006 Edition, 2006.

[19] Price, Sean. "Developing and Conducting a Security Test and Evaluation", Information Security Management Handbook Sixth Edition, 2007.