ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Information Security System and Its Different Techniques

Devendra Singh Kushwaha, Dr. Vikash Kumar Singh,Sonal Sharma

Assistant Professor, Dept. of Computer Science, Indira Gandhi National Tribal University, Amarkantak, India

ABSTRACT-The use of computerized information systems has become an integral part of our day to day life. Managing computer and network security programs has become an increasingly difficult and challenging job. One way of enlightening the risks to their computerized information systems is through a risk management programme. Therefore, the objective of this paper is to educate users on how to perform a risk management exercise for their computerized information systems in order to reduce or mitigate information security risks within their information systems and protect vital information assets. This study uses the Operationally Critical Threat, Asset, and Vulnerability Evaluation for small organizations (OCTAVE) , Open Source Security Information Management (OSSIM) system and commercially available software Event Horizon risk management methodology to address these information security risks in small scale industries and users.

KEYWORDS: Information security, Risk management, Information System, OCTAVE.

I. INTRODUCTION

In a networked system, the increasing number of connected devices is multiplying the probability of cyber attacks on both government agencies as well as private sector organizations. This compels the security manager's job to become more difficult and hence is forced to adopt more stringent cyber security solutions in order to secure all the information from unknown sites and users. To maintain all these or monitor them, there are IT Security Specialists who are responsible for keeping all of the technology within the company secure from malicious cyber attacks that try to breach into critical private information or gain control of the internal systems.

The solutions to all the above mentioned problems have been slowly emerging. The three techniques that will be presented in our paper are: OSSIM [6](Open Source Security Information), OCTAVE (Operationally Critical, Threat, Asset and Vulnerability Evaluation) and EVENT HORIZON. Out of these three, OSSIM and EVENT HORIZON are open sources and commercially available solutions whereas OCTAVE is more of a layered based technique. These three solutions are meant to assure control as well as protect the critical assets against information warfare attacks. Before knowing about these techniques first we will know about Information Security, Information Security sometimes shortened to InfoSec [8] is termed as the protection of all elements that constitute an information system from unauthorized users. It is the practice of ensuring that information is only read, heard, changed or broadcasted only by those users to whom it is concerned and no other user or another party have the accessibility.

CIA TRIAD: Information Security guidelines are based on the CIA triad model which stands for Confidentiality, Integrity and Accessibility. CIA triad is a model designed to guide policies for info security within an organization.[5]

Confidentiality: It is nearly similar to privacy. It is the protection of information against theft and eavesdropping.

Integrity: Integrity involves maintaining consistency of the data i.e. the data is protected against unauthorized modification.

Availability: It assures that information is available when needed and to that particular person to whom the information is associated.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Figure.1. CIA Triad

II. RISK MANAGEMENT

Organizations, governments, society, citizens as well as netizens face many threats and risks. None of these four broad groups is excluded from the situation. Ultimately we become the risk takers as well as risk averse depending upon the particular situation we are in. Information is a business asset with varying levels of commercial value and sensitivity. In addition to it, some of the data is personal too and they need to be protected from the risk of being stolen, misused, modified, destroyed, or not being available to those authorized to have use of such information. To be meaningful to the organization, a strategy for dealing with information security risks must be considered in all contexts. So, Risk Management [7]t is a basic management activity that helps the organization to meet its objectives with an understanding of risks so a effective decision making can be applied to control the risks. The risk management is an ongoing activity that aims to continuously improve the efficiency and effectiveness of the organization. It is considered different from other types of management activities as it deals with the uncertainties that an organization faces.

A risk is basically the potential that a given threat will exploit vulnerabilities of an asset or a group of assets, where the assets can be either tangible (software, hardware and data) or intangible (reputation, operations, trust and morale). The assets can also be critical or non-critical.

A risk arises from three conditions:

- Risk factors- existence of threat.
- Exposure of an asset to that threat.
- Vulnerability of an asset-degree to which any asset will suffer a loss.

Two major activities of risk management:

Risk assessment-involves identifying, characterizing and understanding the risk so one can have a better approach towards it.

Risk analysis-is further identification of security risks, determining their magnitude and hence identifying the areas where we need to safeguard.

A. CHOICE OF RISK MANAGEMENT PROCESS

The choice of risk management process depends on the proper understanding and appropriate application of that method in organizational contexts. For small scale organizations (ex: school), this area is very difficult as there is lack of expertise. So in this condition schools or other small scale organizations have to take help from outside.

B. TYPES OF RISK MANAGEMENT METHODS

Depending upon the risk analysis that is carried out, risk management methods can be of two types: qualitative or quantitative.

Quantitative: It draws upon methodologies used by financial institutions and insurance companies which are suitable for large information systems infrastructure supported by strong human and financial resources. Ex: ALE (Annualised Loss Expectancy), LRAM (Livermore Risk Analysis Methodology). The main constraint of this

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

risk management method is they are very expensive and require high expertise in this field. Because of this, schools and other low scale organizations offered.

Qualitative: It involves the assessment of the effects of identified risk factors and the creation of priorities that can be used to decide on how to solve the potential risk factors. They are simple and hence are considered better than quantitative method as the risks are expressed in terms of descriptive variables. They are based on judgment and intuition. They are complex and pose serious problems in secondary schools due to complexities. Ex: Hazard and Operability study (HAZOP), Failure Mode and Effects Analysis (FMEA) and CCTA-Risk Analysis and Management Method (CRAMM). Not all techniques require strong expertise or are complex. Technique like OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) which is a layered based technique provides easy, cheap and viable means of achieving the same objectives. It has also been found to be the most appropriate one as not much knowledge is required in the field of information risk management. Hence OCTAVE is always recommended for small scale organizations.

III. OCTAVE

The goal of security engineering is to have modernized systems protect themselves and not to increase the vulnerability of existing systems. Present practices which are going on in information system assets is to identify and control persons who may have access to the assets through the physical security of installations and manual procedures for user identification and access control. As more systems require distributed processing and communications across sites. These physical manual methods are no longer adequate. The OCTAVE approach is a framework that enables organizations to understand, assess and address their information security risks from the organization's perspective. OCTAVE is not a product, rather it is a process-driven methodology to identify, prioritize and manage information security risks. It is intended to help organizations: Develop qualitative risk evaluation criteria based on operational risk tolerances. Identify assets that are critical to the mission of the organization. Identify vulnerabilities and threats to the critical assets Determine and evaluate potential consequences to the organization if threats are realized Initiate corrective actions to mitigate risks and create practice-based protection strategy.

IV. INFORMATION SECURITY

Concern about security systems

Many organization CIS are supported by local area networks (LANs), which are normally connected to the Internet to provide access to the web. Personnel with baseline computing knowledge and skills administer these CISs. Administrative computers, holding vital and sensitive school information relating to educators, learners, creditors and financial records, are also part of these LANs. Educators and learners access these facilities, especially, when browsing the web and accessing e-learning material. The extent to which these information systems are secured is a matter of conjecture. There exists the need to encourage and educate information system users in secondary schools to regularly undertake risk management exercises, in order to reduce the exposure of critical information assets to risks from internal and external.

Solution to the impending problem

This implies that organization should conduct information security risk management exercises to assist the school management to explore various information security mechanisms that could be implemented in order to sustain these CISs. However, most organizations (colleges or schools) neither have expertise nor financial resources to perform risk management exercises. Therefore, there is a dire need for schools to be guided or assisted in performing risk management exercises, utilizing the risk management methods that have the potential to educate users and management on how to manage risks in data.

Process 1: Identifying critical CIS assets and their protection requirements.

A collaborative team will comprise mainly of the regular users of the CISs in any association lead by the researcher. The users of the CISs in the collaborative team know where different Information assets are located and will provide all the required information about the information assets at their organization. Each team will then examine the security status of each identified critical asset taking into account the immediate environment of that asset. Organization information security policy and other related policies will be studied if they are availed. During this process the team

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

leader will assist the other members on how to collect the necessary data and record this data on the worksheets assets for the schools' CISs. By participating in this process, users of CISs will be provided with an opportunity to learn to identify critical assets based on given information about a group of information systems assets.

Identifying problem to critcal CIS asset

Here checking of data take place, monitoring factors come in account, to know the system variation and any change in the system and surveillance monitoring

. The team further examines who accesses the asset, how it is accessed, when is it accessed, why is it accessed in that way, what security breaches are likely to take place and their effect on the confidentiality, integrity and availability of the information stored in that asset. The team leader will also observe how the systems are being used and then interview system users. Users of the CISs should be able to identify threats to critical assets.

Identifying vulnerabilities in computing

The team will physically inspect all computing facilities concentrating on hardware, systems software and specialized application software configurations. Malware and simple Vulnerability scans will be performed on selected workstations and the network. All identified vulnerabilities in the computing facilities will be documented. Visible threats to the assets will also be documented. The team will also examine the databases, and network infrastructure in the schools. The team leader will educate the other team members on the implications of the shortfalls identified. After completing this activity, users of CISs should be able to identify and describe vulnerabilities in their CISs assets Development and strategies to rectify the problems of security. The team will assess risks using the information gathered in the first three processes. A qualitative risk metric will be used to guide the team in this process. Risks or threat sources are identified, analyzed and their impact on concerned information systems evaluated too. The matrix uses qualitative descriptive terms, high, medium and low as determined by the collaborative team. The risks are categorized according to their impact on the operations of the schools. The team then recommends on what treatment should be adopted. Based on these findings, the team will develop a protection strategy based on the identified risks that each school could implement. Upon completing this process, each participating user is expected to perform simple risk analysis and come up with a protection strategy for an affected asset.

V. PEN SOURCE SECURITY INFORMATION MANAGEMENT (OSSIM) SYSTEM

Functionally the OSSIM package is divided into four components: Server, Framework & Framework-D, Agent and, Databases. The functional interaction among them is illustrated in Fig.

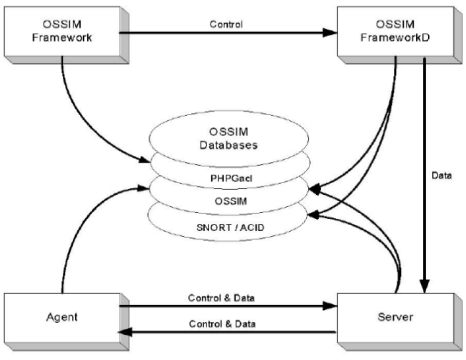

Figure.2 Functional Interaction among different Components of OSSIM

Verification, Integration, Risk Assessment may be OSSIM's most valuable contribution at this time. Using its correlation engine, OSSIM screens out a large percentage of false positives, enables to perform a range of tasks from auditing, pattern matching and anomaly detection to forensic analysis in one single platform and offers high level state indicators that allow guiding inspection and measuring the security situation of network. OSSIM is a distribution rather than a product. The OSSIM aims at intercommunication, making these processes integrate with each other. OSSIM

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

general system description can be seen at its website. OSSIM integrates a number of powerful open source security tools in a single distribution. These include: Snort, Nessus, Ntop, Snortcenter, Acid, Riskmeter, Spade, RRD, Nmap, POf, Arpwatch, etc. These tools are linked together in OSSIM's console giving the user a single, integrated navigation environment.

VI. REVERSE ENGINEERING OF OSSIM

The current OSSIM code comprises of 60,000 plus lines and involves six different programming languages. Reverse engineering of a software system is the process of analyzing a program in an effort to create a representation of the program at a higher level of abstraction than source code. It is the set of procedures for design recovery. This activity has been performed with aim to extract data, architectural and procedural design information from the existing OSSIM code. Mainly, three issues are addressed in this process i.e. abstraction level, completeness and directionality. The abstraction level of a reverse engineering process refers to the sophistication of the design information that can be extracted from source code. Ideally, the abstraction level should be as high as possible. Therefore, the reverse engineering process has been performed with capability to derive procedural design specifications, program and data structure information, object models, data flow models and UML diagrams. As the abstraction level increases, more information is provided that will allow easier understanding of the code. The completeness of a reverse engineering process refers to the level of detail that is provided at an abstraction level. Generally, the completeness decreases as the abstraction level increases. Emphasis is on the amount of analysis performed by development team to improve completeness.

The directionality of reverse engineering process is one-way, if all information extracted from source code is provided to the software engineer who can then use it during any re-engineering activity. The directionality is two-way, if the information extracted is fed to a re-engineering tool that attempts to restructure or regenerate the old program. At the program level, internal program data structures have been reverse engineered as part of an overall reengineering effort. At the system level, global data structures (e.g. files, databases) have been reverse engineered to accommodate better database management paradigms. Two major activities performed during Verification, Integration, this reverse engineering sub-phase are: internal data structures, and database architecture.
Internal data structures: Reverse-engineering techniques for internal program data focus on the definition of classes of objects. The program code has been analyzed with the intent of grouping related program variables. Abstract data types have been identified in accordance of data organization within the code.

Database architecture: A database allows the definition of data objects and supports some method for establishing relationships among objects. Therefore, reengineering one database schema into another requires an understanding of existing objects and their relationships. Information has been extracted to perform a series of transformations for mapping the old database structure into a new database structure.

VII. EVENT HORIZON

Lanifex Intrusion Detection Workbench, marketed under Event Horizon (EH), is a network security solution that offers intrusion detection monitoring of network via a single web- interface. Fig.4. shows the security roadmap of EH. Event Horizon's primary objective is to add value to the intrusion detection process by providing a range of tools which primary objective is to add value to the offer effective management of large amounts of data gathered from enterprise networks. The solution services and functions including Intrusion Detection, Integrity includes a wide range of Checks, Incident Management, and Managerial Reporting. The distinctive benefits of EH include: use of a single web-interface for remote IDS management, consolidation of all security to incidents to a single database for central analysis and management, use of encryption for secure inter-system connection, and storage management features, help security and network analysts to be more efficient and productive through filtering and automated scanning of network incidents and services. Prominent features of EH are: Analyses, Audit Administration, Sensors and Log Management, Incidents, Alerts and Traps, Reporting, Integrity Check and Inspection Although both the security solutions, mentioned and discussed above, cover a wide domain of difficulties currently addressed post and focused by researchers and experts in this area, however, preventive measures from external attacks is still a hot issue. Moreover, false positives and false negatives are required to fix at minimum level. Customized report generation is another challenge to meet. The intent is to develop an indigenous system that could be economically tailored to desired needs As EH is a commercial product,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

so it is not possible to modify or improve its functionality without the consent of vender, despite of the fact that source code is provided. Every time a high cost would be required to upgrade the system once becoming a client of any commercial product and spending a handsome amount at the time of first purchase. On the other hand, being an open source, architecture of OSSIM is more robust and scalable proving it a true candidate to incorporate intrusion prevention capability.

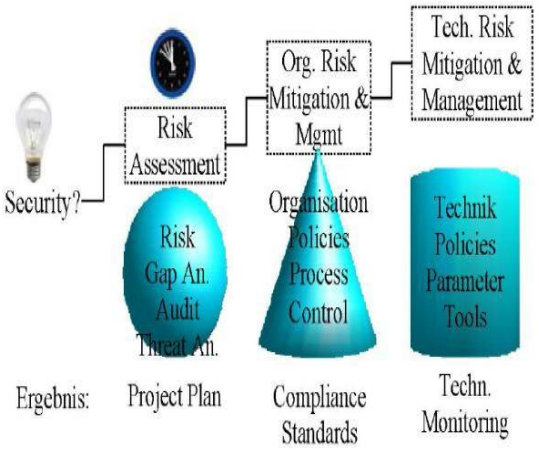

Figure.3 Security Roadmap of EH

VIII. CONCLUSION

Information security is difficult because it is one of the few things that touch every layer of an IT infrastructure - physical, network, application, and operating system - and there is no simple solution to implementing information security in a complex environment. What is needed is a total security knowledge management solution that seamlessly integrates all the numerous entities that abound in a present environment. Users want systems that save time and money. The best possible solution must meet user wants, the rules and regulations related to privacy, as well as, the statutory and constitutional requirements regarding the types of information that can be obtained and how it is to be used. The right solution will be applicable across the system but also applicable in other modes of a system and designed to accommodate diverse user/stakeholders and permit customization for specific applications. It will facilitate communications, improving the security effectiveness of current processes and guaranteeing that threat information will be disseminated in the proper format. At the appropriate time and to the necessary personnel to make effective security decisions. Technology solutions must not only strive to meet these objectives but provide users - government, airports, airline industry, and travelling public - the most complete, secure. private, scalable, implementable, cost effective, and flexible design possible. A complete solution will protect the data in transit, determine what data is allowed in and out and protect the endpoint servers from direct contact with the masses, while allowing easy and secure access to the data.

REFERENCES

1. A Proposed Preventive Information Security System M.M. Anwar*, M.F. Zafar* Z. Ahmed* [doi 10.1109_ICEE.20074287288]
2. Information Security Risk Management in Small-Scale Organisations: A Case Study of Secondary Schools Computerised Information Systems (Moses Moyo, Hanifa.Abdullah, Rita Nienaber -School of Computing Science, UNISA)
3. Information Systems Security-Airport Environment in an D. L. Wilson Transportation Security Research & Development Laboratory FAA William J. Hughes Technical Center Atlantic City International Airport, NJ [doi 10.1109_ccst.20021049241].
4. EventHorizon:http://jila.colorado.edu/~ajsh/insidebh/schw.html,http://casa.colorado.edu/~ajsh/s ingularity.html.
5. CIA:http://en.wikipedia.org/wiki/Information_securit y#Key_concepts.
6. OOSIM:http://en.wikipedia.org/wiki/OSSIM
7. Risk management: http://en.wikipedia .org /wiki / Risk _ management
8. Infosec:https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/2013%20Global%20Information%20Security%20Wrkforce%20Study%20Feb%202013.pdf
9. http://www.iss.net
10. http://www.ossim.net
11. "Engineering Principles for Information Technology Security". csrc.nist.gov.