Example of report on justification

Business, Company

TEKLA SOLUTIONS

OPERATIONS MANAGER

JUSTIFICATION REPORT ON THE NEED TO IMPLEMENT ADVANCED SECURITY FEATURES TO PREVENT COMPANY INFORMATION

INTRODUCTION

I intend to dedicate this report to Tekla Solutions where the security of the business will be the main focus in securing the safety of business data. Modern technology has impacted on the state of information systems and rendered them susceptible to both internal and external threats. With enhanced security, the integrity, confidentiality and availability of information stored in company information systems will be preserved. This will ensure that the trust of clients is also preserved translating to more business and continued growth of the company. The purpose of this justification report is to outline advanced methods of ensuring the security of organization data and the clients. This is in order to continue serving the customers as per the company vision and mission, in addition to advanced prevention and, control of crime.

During the preparation of this report, the employees gave full participation in terms of willingness to change the business operations and took part in awareness and training programs. The management coordinated the formation of team members for the drafting and implementation of the report. The steering committee actively participated from the onset of the report in identifying the draft deliverables in the stipulated time frame.

PROBLEM STATEMENT

The proliferation of various technologies continuously puts business data on the risk of attacks. For instance, hackers have continuously devised new ways of detecting weak and vulnerable points on the network. This has enabled them into breaking through and gaining access to business and company data. The report is aimed at exploring the VA techniques in use. It will also be used to look at the computer security solutions and programs that may be applied to an organization. An example is Tekla Solutions to combat information security issues. From a technical point of view, the objective of the report is to develop an all-round computer security solution encompassing the use of software's, policies and programs. The report will involve an interdisciplinary team of members for analysis of the problem and subsequent development of solutions.

METHODS USED

The study utilized data obtained from various sources. Information was obtained from security analyst, management, and staff of Tekla Solutions. The persons concerned were interviewed on the types and frequency of computer attacks in the organization. Prevention and control mechanisms put in place was also profiled. The study included external personnel such as consultants from computer security firms hired, by the organization, to provide their services. The nature of the study involved qualitative and quantitative survey. Quantitative involved the profiling of the frequency and number of attacks in each department of the organization. Qualitative studies involved the feedback from interviews of the staff and consultant personnel on how they dealt with the attack and prevention mechanisms.

The data obtained from the various quotas was analyzed, and the findings made known. The findings and recommendations are essential for Tekla Solutions as they define the course of action in ensuring smooth operations and better productivity.

FINDINGS

The research found various vulnerabilities and computer attacks in the organization. All the findings impacted on the operation of the business and resulted to loss of business among other inefficiencies. Various technologies and programs are found to improve the redundancy to attacks. Other policies and programs guard against misuse of company information, and assets. It is undisputable that technology and internet in general has formed an efficient way of communication. It is central to the business operations of any company as it supports its operations in a cost effective, quick and efficient manner.

Efficient security measures are, therefore, desirable in a bid to improve business operations and maximize profits. Moreover, the privacy of client data is crucial to the success of the company. Building a formidable relationship with the customers will ensure the continuity of the company as well as customer satisfaction. The security programs and policies are intended to guard the privacy of the client, company information, and data. It will also provide the necessary avenue for a true experience of internet connectivity and communication anywhere and anytime.

ANALYSIS

The information obtained has enabled us to give an inference on what needs to be done in regard to computer security in the organization. For the business to develop sound security measures, it must incorporate the following security protocols/policies.

VULNERABILITY TESTING

Given these current status of computer security, vulnerability assessment is required, in the company, to ascertain the state of the system. VA determines the security situation in a system and give recommendations. This process can be done through penetration testing and vulnerability scanning. Penetration scanning takes care of the networks ports that are susceptible to attacks. Vulnerability scanning, on the other hand, is directed to the susceptible hosts and applications, therefore, protecting the system First principles Vulnerability Assessment have four phases that include Architectural analysis, Resource Analysis, Privilege Analysis and Component Analysis. It is true that Architectural analysis probes the contents of the system while Resource Analysis looks at the resources the system utilizes. Privilege Analysis identifies the trust and access issues while Component Analysis probes the software components of the whole system. As stated, vulnerability assessment is always carried out at the deployment stages to determine the state of security. Any instance of hardware or software change including an attack should be followed by VA.

Global threats are associated with thefts of intellectual property and trade secrets which are directed to companies to inhibit competition in economic and military terms. Examples are hacking of company networks through DoS

to cause disruption of services or damage credibility. According to security awareness programs among employees are the critical control measures for a company. Human awareness is an essential practice that ensures that the management of tools and processes and adherence to company policy is successful. However, the method of carrying out the awareness differs with companies and institutions. Each institution has a tailor-made program that suite it staff.

FIREWALLS

A small business such as Tekla Solutions may implement firewall in order to protect individual PCs on the network. Firewalls are available as either software or hardware components. Software firewalls are installed on each computer, but this choice may be expensive for a small business since it requires regular updating and maintenance.

Hardware based firewalls protect all computers on the network and does not require individual administration on each PC. Rather integration of the hardware firewalls with software controls provides comprehensive security that may include VPN support, antispam, antivirus, content filtering and antispyware. A firewall provides a number of security measures for Tekla Solutions business operations and is recommended. First it supports the changing business needs by allowing integration and deployment of new applications. Thus advanced application layer security is guaranteed for a wide range of application such as VoiP, multimedia programs, video and email.

Next it provides a controlled access to the company resources thus security and privacy is enhanced. Firewall blocks unauthorized applications or

information from accessing the network. Thirdly, blocking unauthorized applications will prevent the loss of enormous employee productivity time and influential company data. Employee conduct in the workplace will be strictly adhered to, therefore, increasing productivity.

According to Mansfield-Devine, 2010 multi-factor authentication is another policy that uses two factors; what the user has and what he/she knows. The policy is true and effective in securing and accessing system resources and networks.

In addition, content delivery networks via the Clouds guards the network resources against DDoS attacks elastic and scalable resources mechanisms. It is noted that the dispersed geographical hosts delivers better service to the end users as well as efficiently distribute the load of DDoS attacks

Finally, the best firewalls improve business resilience by preventing loss of business due to disruption of critical applications and services resulting from security breaches. Information in the internet is better managed by use of a firewall. Users without advanced security features will find requests and alerts unmanageable and, therefore, require a firewall to prevent them from the business network. There are easy to install and cost effective firewalls that are tailor made for small businesses .

SECURITY POLICIES

Information security programs and policies are essential components of an organization's security. In the formulation of these programs and policies, certain relevant standards are used. A security program or policy determines the standard to be used. For instance ITU-T and IEEE are bodies of standards that cover all fields in telecommunication and computer and electronic

industry respectively.

The company used the National Institute of Standards and Technology standards in the formulation of its information security program and policy. Security of information systems for an organization is an valuable exercise that poses significant implications on the operation of personnel and security of assets. Security controls are the fundamental parameters that define the managerial, operational and technical safeguards and counter measures deployed to an organization's information system. The fundamental aim of NIST standards is to aid in the development of policies that preserve and restore the confidentiality, integrity and availability of information within the system

An example is that NIST issued the FIPS 140 to coordinate the necessary standards for hardware and software cryptographic modules. They are used in agencies and department, in the US federal governments. The requirements stipulate the cryptographic modules, the documentation at the highest level, and aspects of comments contained in the source code. FIPS 140-2 has definitions for four levels of security. From these levels, the first level imposes limited requirements while the fourth level has more stringent and robust requirements. The scope of the requirements includes cryptographic modules, ports and interfaces, authentication, finite state model, physical security operational environment and cryptographic key management. Tekla Solutions can best formulate its policies using the NIST standards to ensure compliance and effective security solutions.

CONCLUSIONS

Technology has changed the way people communicate with each other. Business conducts their operations more efficiently through the use of computers and internet. However, the privacy of the company and customer information is crucial to the continuity of the business. In this age where computer attacks have intensified, there is a need to develop efficient security prevention mechanisms and protocols. This includes vulnerability assessment and testing to determine the state of computer networks, implementation of firewalls and antivirus software's, and development of security policies as per the NIST standards. Business entities using more than one computer in a network to share files and data are susceptible to attacks and as such, need more advanced security procedures. The information in this report provides the framework for basic security measures that can be implemented to change the security state of the company. The manager of the implementation team will review each mechanism and tailor it suit the requirements of each department. The manager will also oversee the awareness of the security protocols through training and distribution of the policy documents to ensure compliance.

Reference

Ciampa, M. D. (2011). Security+ Guide to Network Security Fundamentals. Cengage Learning.

Mansfield-Devine, S. (2011). DDoS: threats and mitigation. Network Security. Springer .

Sandhu, R. H. (2009). Identification and Authentication. In Computer Security Handbook. John Wiley & Sons.

Serrano, J. H. (2012). Vulnerability Assessment Enhancement for Middleware for Computing and Informatics. Computing And Informatics. Springer.