Computer forensics investigation plan

Table of Contents

References

Executive Summary

High-Tech Pty Ltd is an Australian organization that deals in computing tools, material, and equipment. The company provides the equipment to the business firms and these firms are also based out of Australia. Due to the non-maintenance and absence of updates since 2010, there are security vulnerabilities that have emerged for the network and system architecture. One such case has been reported recently wherein there are several customer orders accepted in the early 2019 but the customers were not provided with the deliveries.

The report aims to include computer forensics investigation plan for the organization to understand the issue and also covers security policy for the organization.

.

Introduction

Organization Overview

High-Tech Pty Ltd is an Australian organization that deals in computing tools, material, and equipment. The company provides the equipment to the business firms and these firms are also based out of Australia. The company was established in 2005 and has been witnessing rapid growth since then. Currently, there are 250 employees and over 5, 000 clients involved with the company. The headquarters of the organization are in Melbourne and there are four other branch offices in Australia. The organization has always been customer-oriented and has ensured that it works for the customers so that

they are always provided with high-class services and products. The company updated its network architecture with the same purpose in 2010. The post-implementation activities could not be managed well and there were no updated done in these networks since then.

Problem Statement

Due to the non-maintenance and absence of updates since 2010, there are security vulnerabilities that have emerged for the network and system architecture. One such case has been reported recently wherein there are several customer orders accepted in the early 2019 but the customers were not provided with the deliveries. The customers have been charged for these orders. On looking for the information in the database, it was identified that the details are missing from the organization database as well. This is because of the flat network structure due to the absence of the updates. There was also program installed by an employee from the Brisbane office of the organization.

Purpose

The report aims to include computer forensics investigation plan for the organization to understand the issue and also covers security policy for the organization.

Digital Forensic Method & Approach

Utilization & Advantages of the Approach

The use of digital forensics approach for investigating the computer crimes and security issues that have been identified with High-Tech Pty Ltd will provide the organization with numerous benefits.

Digital forensics has been designed to review the digital evidences in no time so that the investigation process is quickly carried out. The primary goal involved in these processes is to discard the irrelevant data and to put the focus only on the evidence associated with the requirements. The utilization of the same in the investigation process will provide the ease of priority in terms of evidences and will provide the ability to come up with the results quickly. The issues that are reported by the organization have a direct impact on the customers. With the timely results of the investigation process, the organization will be able to developed and implement the strategies to control the situation. There are customer orders that have been placed and the customers are also charged for the same. However, they are still waiting on the delivery of these products. Such incidents lead to the deterioration of the customer engagement levels. The use of digital forensics in investigation will determine all of the loopholes so that quick resolution is provided and such incidents do not happen in the future. There are also cases wherein the evidences are piled up and the results are not achieved for a long period of time. The digital forensic tools and approach will determine the relevance of these evidences in association with the case and will retain or discard them accordingly. The accuracy of the overall process will increase in this manner (Kessler, 2012).

There must be specific risk areas associated with the organization that might be more impactful and dangerous as compared to the others. The identification of such areas will be easily done with the aid of digital forensics tools so that the risk control and monitoring can be effectively carried out.

The determination of the effectiveness of the procedure applied can also be done with the aid of the digital forensics tools(Carlton & Worthley, 2010).

Set of Procedures

The primary purpose of the application of digital forensics for investigating the case will be to come up with the reasons behind the occurrence of such issues and the implementation of the control strategies for the same.

The first step shall include the policy and procedure development. The digital evidence that will be involved in this case will be delicate and it will comprise of the sensitive customer information. The cybersecurity professionals are aware of the criticality of the information and are also aware of the need of a formal policy and procedure in place to manage these components. There are strict guidelines and procedures that must be in place to make sure that the gathering of the digital evidence, analysis and storage of the evidence, and the documentation of the results is formally done. There shall also be a high-level analysis that must be conducted to make sure that the digital evidence is securely collected and the rest of the processes are also done as per the norms (Casey, 2013)

The next step in the procedure will be the evidence assessment. The clear understanding of the case will be necessary to be obtained and therefore, the classification of the cybercrime shall be done in this step. There are different forms of cybercrimes that may take place. For instance, in this case it is possibly malware attack. There may be other forms, such as identity theft, data breach, or eavesdropping that may occur. The initial analysis shall determine the type of the cybercrime so that the pertinent idea around the

same may be developed. The source and integrity of the information shall be determined before including it in the digital evidence. The most important phase of the procedure will be evidence acquisition. The detailed information shall be recorded and preserved. It shall include the specifications of the software and hardware involved, network information, and other security details. The policies around preservation of data integrity shall be applied so that the acquisition is done in a secure process. The data from all the possible sources shall be acquired and stored in the investigator system.

The next step shall include the examination of the evidence. The evidence shall be stored in an adequate database and shall be classified correctly. There are different methods that may be used to investigate and examine the digital evidence that is collected. The use of automated data analytics tools may be done to identify some of the important keywords and the associated patterns behind the occurrence of the cybercrime. There are data sets that are tagged with date and time which are used by the investigators to gain information on the attack. The analysis of the filenames may also be performed to understand the creation of specific information and have information on the transactional information. There are different areas that may be analysed, such as cloud databases, cloud networks, social media, and so on. The files that are available online also comprise of the information around the dedicated servers and computers from where they might have been uploaded. The examination of all of these factors and information is done.

The investigation logs are very relevant from the documentation aspect and these are used to prepare a formal report. All of the steps conducted are

included in the report supported by the data sets and the details of testing, retrieving, and storage is also covered. The primary aim of the investigation process is to ensure that the information is correctly presented. The information is therefore documented in detail and the archiving is also done to avoid the risks in the future (Casey, 2019).

Digital Forensics Requirements

Resources & Skill Sets

The Information Security Officer will be the manager of the entire activity and will carry out the development and implementation of the policy and plan. The definition of the strategies and the guidelines and the determination of the security policies will be done by the resource. The experience and skills will be needed to accomplish the task and there shall be soft skills as leadership and communication with technical expertise necessary (Provataki & Katos, 2013).

The resources in the core forensics team will include the Computer Forensics Expert, analysis panel, data engineer, and technical expert. These shall have the analytical, creative thinking, technical, and monitoring skills.

Software & Hardware

There are digital forensics tools, such as SANS SIFT, FTK Imager, ExifTool, etc. available and one of these may be used for conducting the computer forensics investigation.

Network security and analysis tools shall also be used along with the automated analytical tools. The tools will be accessed through the computer systems and there shall be networking peripherals also used.

Approach – Identification & Acquisition of Data/Evidence

The initial step will incorporate the arrangement and methodology improvement. The digital evidence that will be associated with this case will be fragile and it will involve the touchy client data. The cybersecurity experts know about the criticality of the data and are likewise mindful of the need of a formal strategy and technique set up to deal with these segments. There are severe rules and methods that must be set up to ensure that the social occasion of the digital evidence, investigation and capacity of the evidence and the documentation of the outcomes is formally done. There will likewise be a high-level examination that must be directed to ensure that the digital evidence is safely gathered and the remainder of the procedures are additionally done according to the standards.

The following stage in the strategy will be the evidence appraisal. The clear comprehension of the case will be important to be gotten and in this manner, the arrangement of the cybercrime will be done in this progression. There are various types of cybercrimes that may happen. For example, for this situation it is perhaps malware assault. There might be different structures, for example, wholesale fraud, information rupture, or listening in that may happen. The underlying examination will decide the sort of the cybercrime so the appropriate thought around the equivalent might be created. The source and honesty of the data will be resolved before incorporating it in the digital evidence. The most significant period of the system will be evidence procurement. The nitty gritty data will be recorded and protected. It will incorporate the particulars of the software and hardware included, network data, and other security subtleties. The strategies around safeguarding of

information trustworthiness will be connected with the goal that the obtaining is done in a safe procedure. The information from all the potential sources will be gained and put away in the agent framework (Schatz & Cohen, 2017).

Data/Evidence Analysis Phase

The analysis phase of the process will be a critical stage. The evidence will be put away in a sufficient database and will be arranged effectively. There are various techniques that might be utilized to research and analyse the digital evidence that is gathered. The utilization of robotized information analytics apparatuses might be done to distinguish a portion of the significant watchwords and the related examples behind the event of the cybercrime. There are informational indexes that are labelled with date and time which are utilized by the specialists to pick up data on the assault. The investigation of the filenames may likewise be performed to comprehend the formation of explicit data and have data on the value-based data. There are various zones that might be broke down, for example, cloud databases, cloud networks, social media, etc. The records that are accessible online additionally include the data around the devoted servers and PCs from where they may have been transferred. The examination of these elements and data is finished.

The investigation logs are applicable from the documentation viewpoint and these are utilized to set up a formal report. The majority of the means led are incorporated into the report bolstered by the informational indexes and the subtleties of testing, recovering, and capacity is likewise secured. The essential point of the investigation procedure is to guarantee that the data is

effectively introduced. The data is consequently recorded in detail and the chronicling is likewise done to keep away from the dangers later on.

In the case of the networks, there will be a lot of information available from the network logs. These logs will be easily accessible and will provide the details of the transactions and the user activity over the network. The transactional details from the network will be used to determine the specific users that accessed the networking resources at the time of the attack.

The server information will provide the information on the distribution of the resources and the initiation of the malicious applications and systems. The data sets tagged with date and time information attached to the server will also be obtained. The information from the specific computer systems and machines will also provide system logs to understand the user access details and the changes that may be purposely carried out.

The exchange of emails and the associated information may provide the details of the chain of the users involved in the process. The cloud database and network will be used to acquire the information around the customers involved in the security attack and the internal users that may be involved in the same.

Social media is one of the major agents that are being used as a threat agent in the present times. It may be used to capture the information on the interaction between the customers and the employees of the organization. Also, the involvement of malicious intent through the data shared, posts accessed, and information posted may be acquired(Federici, 2013).

Security Policies

There are certain security steps that High-Tech Pty Ltd and other organizations must make sure so that the management of security is effectively carried out.

The security policy shall include the four major areas as basic security, technical security, physical security, and administrative security.

There were flaws in the basic security of the organization as there were no maintenance and update activities conducted on the network channels. Also, the installation of the firewalls was not correctly done. It led to the emergence of security vulnerabilities and the attackers could give shape to the security attacks with much ease. The basic security shall be the initial point of security in the security policy. The basic controls, such as firewalls, passwords, implementation of the information security plan and authentication measures shall be ensured. The firewalls and proxy servers are some of the controls that filter the content and block unwanted access to the information. Passwords are the basic security measure that shall be implemented for all the applications (Kumar, 2016).

There are technical security controls and measures that shall be applied next. Numerous technical and logical security controls have been developed with the increase in the security risks and attacks. The implementation of the anti-malware tools shall be done so that any of the malicious activity and attempt is nullified and the information sets and the applications are kept protected at all times. The anti-denial tools and network-based intrusion detection/prevention systems shall also be installed so that the network-

based security attacks are prevented. There are encryption algorithms and automatic backup tools available which shall be used and applied. The encryption of the data sets will make sure that malicious access is violated and the backup will keep a copy of the data sets in another location. Access control and authentication tools, such as biometric tools for recognition shall be used along with the multi-fold authentication systems.

Physical security is also necessary so that the employees or other entities unauthorized to enter the organization or specific areas are prohibited from doing so. The physical identity checks and the use of automated identity checkers at the entry and exit points shall be ensured. The secure areas, such as server and data rooms shall have numerical and biometric based recognition systems to keep the access secured. There shall be security cameras and surveillance tools also installed.

The administrative security controls shall also be applied by the development and implementation of the information management security plan. The security status shall be reviewed and there shall be audits conducted at regular intervals. It shall be ensured that the information security officer keeps a track of the maintenance and update activities and the security vulnerabilities are treated(Lakshmi & Begum, 2011).

Recommendations

There are numerous recommendations that the organization shall consider so that these risks and cybercrimes do not take place. There are numerous risks that occur due to the lack of user awareness. The users, that is, the customers and the employees shall be trained on the security policies and

practices. The users shall be asked to put strong passwords on their accounts and applications. The information on the malicious and suspicious links shall be provided to the users. The possible threat agents and their information shall be shared with the users so that the frequency of such risks may be controlled.

The encryption algorithms are being improved with every passing day. The latest encryption algorithms shall be used so that the occurrence of cryptanalysis attacks is avoided. Encryption may also be used in the process of access control and authentication. The maintenance and update of the security policies and controls is extremely essential and it is recommended that the same is conducted at regular intervals. Digital forensics is gaining a lot of popularity and there are integrated digital forensics tools and controls that are available in the market. Instead of using the standalone tools for analysis, data gathering, etc. the integrated tools must be used. These will provide the ability to carry out the digital forensics activities in a better manner.

There are insider threats and attacks that have become a common occurrence. The employees of the organization shall be provided with security, operational, and ethical trainings so that the occurrence of such risks is avoided. The employees shall be made aware of the possible implications of the violation of the violation of the ethical principles and security norms. The audits shall cover the employee actions as well. The scanning of the logs shall also be done to determine the activities performed by these employees. The basic security will be the underlying purpose of security in the security strategy. The basic controls, for example, firewalls,

passwords, usage of the data security plan and authentication measures will be guaranteed. The firewalls and intermediary servers are a portion of the controls that channel the substance and square undesirable access to the data. Passwords are the basic security measure that will be executed for every one of the applications.

There are technical security controls and measures that will be connected straightaway. Various technical and consistent security controls have been created with the expansion in the security dangers and assaults. The execution of the anti-malware tools will be done as such that any of the malicious movement and endeavor is invalidated and the data sets and the applications are kept secured consistently. The anti-denial tools and network-based interruption recognition/counteractive action frameworks will likewise be introduced so the network-based security assaults are avoided. There are encryption algorithms and programmed backup tools accessible which will be utilized and connected. The encryption of the informational indexes will ensure that malicious access is abused and the backup will keep a duplicate of the informational collections in another area. Access control and authentication tools, for example, biometric tools for acknowledgment will be utilized alongside the multi-crease authentication frameworks.

Conclusion

The security attacks and risks that took place at High-Tech Pty Ltd were because of the security vulnerabilities in the organization and the inability to manage the information security and the technical systems. The company did not succeed in maintaining and updating the network resulting in the flat and unrestricted architecture. It is possible that the users from one office

easily access the systems of other office without proper access control in place. Computer and digital forensics will provide the ease pf investigation in the cybercrimes that took place in this case. The primary purpose of the application of digital forensics for investigating the case will be to come up with the reasons behind the occurrence of such issues and the implementation of the control strategies for the same. It is also essential that the organization enhances its existing security controls and policies.

References

- Carlton, G. and Worthley, R. (2010). Identifying a Computer Forensics Expert: A Study to Measure the Characteristics of Forensic Computer Examiners. *Journal of Digital Forensics, Security and Law* .
- Casey, E. (2013). Triage in digital forensics. *Digital Investigation* , 10(2), pp. 85-86.
- Casey, E. (2019). Maturation of digital forensics. *Digital Investigation* , 29, pp. A1-A2.
- Federici, C. (2013). AlmaNebula: A Computer Forensics Framework for the Cloud. *Procedia Computer Science* , 19, pp. 139-146.
- Kessler, G. (2012). Advancing the Science of Digital Forensics. *Computer* , 45(12), pp. 25-27.
- Kumar, R. (2016). Cloud computing and security issue. *International Journal Of Engineering And Computer Science* .
- Lakshmi, V. and Begum, S. (2011). Security Issues & Controls in Cloud Computing. *Indian Journal of Applied Research* , 1(5), pp. 38-40.
- Provataki, A. and Katos, V. (2013). Differential malware forensics. *Digital Investigation* , 10(4), pp. 311-322.

- Schatz, B. and Cohen, M. (2017). Advances in volatile memory forensics. *Digital Investigation* , 20, p. 1.