DevTech Security Audit

A comprehensive Security Audit and Recommendations Report

Student:

Srikanth Shilesh Pasam - 10387794

Teacher:

Gordon Reynolds

Course:

Computer Systems Security (B9IS103)

Executive Summary

This report is aimed at addressing the concerns of directors and top management in the company, which was regarding the existing course of actions at different levels of the organisation. These levels comprise of the key aspects of an organisation's structure, which include its asset management policies, literacy of IT documentation, networking environment in the company and major internal security parameters of the company. In order to evaluate the efficacy of the above-mentioned key aspects in an organisation, an audit was conducted, which highlighted several laxities in the compliance of the above aspects.

In addition to these aspects, the audit was instrumental in bringing in light several policies regarding IT documentation which needs to be implemented to offer more lucidity in the process. Furthermore, there were some additional security norms too which need proper scrutiny in order to offer mitigation strategies in planning the future course of the company and revamping its policies for the next 12 months in a successive manner of implementation. The concepts which have been widely discussed while highlighting the loopholes in the company's structure pertain to network layer infrastructure as well as principles of cryptographic tools like digital signatures which would serve as an usher of prosperity.

Table of Contents

Overview

The company named DevTech has been surging as a budding start-up company, and the organisational structure of the company has left the top directors and management of the company brainstorming for resolution of the above concerns in the structure. These concerns were primarily pertaining to the rented infrastructure of the company with three other companies which was a major concern as the security parameters were just restricted to fundamental areas like security alarms and lock and keys. In addition to this, other concerns were regarding the hardware capabilities of the company and its inefficiency for pipelining some of its major areas related to software up-gradation in a synchronised manner among different workstations of the company. This aspect also highlighted some major security parameters like encryption of data and significant pathways that were to be taken into consideration for the auditing and recommendation process in subsequent stages.

Furthermore, the other concerns also include the outdated networking paradigms as well as the substitution of shared workstations with cryptographic systems which provide isolated access to each user through private keys without hampering any data. In addition to this, several concerns were regarding the compliance of the IT documentation policies which also required assessment by the first security officer who was delegated with the task of making recommendations on the above and providing mitigation suggestions.

Recommendation in Relation to Security Audit

The process of security audit was performed keeping in mind the existing state of activities performed in the organisation structure which needs to be revamped in order to meet the requirements of directors in the hierarchy. There were several recommendations proposed while auditing the individual aspects of the company's infrastructure which encompassed a wide range of components like hardware, software and digital maneuvering of data. The primary source of recommendation was derived from the very functionality of networking components in the company like switches which incorporated daisy chained topology which was deemed highly inefficient in terms of a local infrastructure where common resources are being shared (El Kamoun, Bahnasse, and Bensalah, 2017). This source leads to the improvisation of the networking capabilities of routers with other corresponding means of topology like star topology or bus topology which are deemed as highly protective means of providing access to diverse communication nodes in local hosting equipment. Moreover, the other concern regarding the networking capabilities included the generating of subnets as the scenario clearly depicted that the company utilised only one subnet under a static Internet Protocol (IP) address which needs to be substituted with masking of subnets followed with the application of dynamic IP that saves lots of time and resources for the company which was earlier not possible in the case of static IP (Zhang and Yu, 2020).

In addition to this, in the case of the DevTech, it is also required by the company to implement more security in their systems such as cryptographic security and server limitations along with providing public key and private keys. In relation to this, it is suggested to the company to utilise strong encryption of data in order to transmit data or information over public networks. In a similar context, it is not necessary that transmitting the data over a public line is safe; therefore, the encryption of data is necessary, and it is the best defence against attackers due to unscrupulous individuals and miss configuration (Gąsiorowski, 2016). The same process is necessary for the decryption of data on the client side. Here are some more major and minor recommendations for the company:

- It is recommended to the company to establish a system hardening process or system hardening standard which is a procedure of securing devices before utilising them and placing them at the workplace. In addition to this, with a good hardening process, the company can decrease the risk of hacker's attacks which is caused by faulty malware protection, unpatched system and default accounts (Lin and Bie, 2018).
- The issue of the company is that the data or information stored in the systems are not updated with anti-virus and laptops and desktops are not backed-up. Therefore, the company needs to back up all the data on regular basis, to be prepared if an unwanted incident occurs.
- It is also recommended to the company to establish a system that regularly checks the rogue devices along with other network devices in order to refute the access until the sanction received. In addition to this, a rogue device can be defined as a portable or attachable device that may connect to the network. In a similar context, rogue devices are such as a laptop of an employee, wireless entrance points and a data switch. Rogue protection will help the organisation by blocking the access to the network until the device checked by a security manager and administrator (Vanjale and Mane, 2018).

- It’s recommended to the company to set up an Internet of Things (IoT) system which automatically refreshes the servers. In addition to this, IoT devices can be also used as tracking devices such as printers and smart office assistance. Furthermore, can be used to attract the clients and enhance the customer experience along with this it increases the interaction of clients towards the organisation (Khan *et al*., 2017).
- The company should also perform regular testing such as penetration and vulnerability scanning on a customary basis. In addition to this, vulnerability scanning, and penetration testing consist of three major components or security procedures which are automatic vulnerability scan, external penetration testing, and internal penetration testing. In the context of the audit, all the above testing should be executed. Regular penetration testing also helps in figuring out the vulnerability that a hacker or attacker can exploit in a network, computer system, and web application. Therefore, it is recommended to the company to establish a software application or it can be also performed manually (Baloch, 2017).
- The company should also ascertain access or authorisation on the least rights. In addition to this, access to the data should be based on job function and should be limited because this can cause an attack if a rogue administrator leaks the data of the company. In a similar context, the access of the data should be provided to only trusted employees of the organisation. If the company did not implement the controlling system which can lead to result in the security breach, regulatory violation along with this it can also affect the brand image. Furthermore, there is nothing such as full protection, but the company can implement some system such as security controls, a proper review will make less chance of getting threats attacks to the organisation.

- DevTech can also implement a system for safe sending or receiving of information or messages to the client with the help of encryption and decryption. It is necessary for the company to apply data encryption and decryption in order to prevent data breach which can cause a high amount of penalty to the company. In addition to this, DevTech is a freshly established and successful company; therefore, it is necessary to maintain the positive image of the company. By implementing the cryptographic process, it will enable a security system that can be authorized by the specific user (Berti *et al*., 2017).

Implementation of Security Policies

The security policy of a company is a kind of written document in an organisation which describes the ways to protect the organisation from threats, including threats related to computer security and guides to handle critical situations occurring in the organisation (D'Arcy and Lowry, 2019). It is required by the company to regularly update the company policies in accordance with new technology and innovations. In this context, the security policies of the company DevTech are fine, but there are various Information Technology (IT) related issues in policies, such as password protection, secured login, and regular updates and so on. The company is lacking with some policies which are very significant to overcome such permission to allow access to data and monitoring control. Here are some recommendations of policies that are needed to be implemented:

- According to the first policy of the company, the computer and all devices are connected to each other on an internal network; however, this policy is needed to be upgraded, and the company is required to minimise the access of data to very few trusted employees in the staff. In context to this, the more the people access the data higher are the chances of a data breach. According to the minimum access policy, the systems should be connected to a minimum number of networks, and the company should update its firewall and antivirus, along with installing an updated software patch (O'Sullivan et al., 2017).

- In the case of DevTech, it is required by the company to share its password to a minimum number of employees. In this aspect, the company is following the policy, but it needs to be more secure. In a similar context, if a person in staff can access all computers, then a person can steal all the data in the rogue intentions. Therefore, it is necessary to secure all the systems in the company and regularly update the password of all the systems in order to secure the information related to clients and company data. Furthermore, all the systems in the company are required to be secured with password-protected screensavers (Raunio and Sedelius, 2020).
- According to the company policy, it is necessary for all the employees to practise extreme caution when opening an email attachment which can be received from hackers and may contain malicious files or malware. In relation to this, the company should install a firewall in all its systems in order to protect them from viruses. The firewall automatically scans the file and notifies whether it contains a malicious file or not. In addition to this, the company should also restrict the employees if they send their personal emails from the computers of the company. To accomplish this, all the employees should mention a disclaimer in their emails (O'Sullivan et al., 2017).
- According to the company policy, it should be ensured by the company to provide proper training to employees in order to train them about which files should be downloaded on the company system because some software and applications are

pirated, it can also cause data loss which will decrease the value of the company. In addition to this, it can also cause a high amount of penalty if the data loss will not be informed to the clients and users and if the client files a lawsuit against the company. The company should focus on upgrading its security system on a regular basis (Raunio and Sedelius, 2020).

Recommendation on Specific Issues

In the scenario of DevTech, the company is lacking with some issues related to technology and innovation, which are required to be overcome. In addition to this, there are various issues in the company's security policies and network security. In this relation, the above report contains recommendations that are based on the current drawbacks of the company. In a similar context, the company is required to be focused on the use of encryption and decryption process because it is necessary for the sustainability of the organisation. The company has an issue related to its building because proper security is not available in the building, and the gate of the office is locked by a simple key on the door. In this case, the company should hire a personal guard for the night duty and can also apply few security systems in the office, such as CCTV cameras and alarm systems which will notify the owner if the robbery is attempted (Marsaid et al., 2020).

In addition to this, the company should also restrict the employees that they are not permitted to take laptops at their home because if important data is stored in the laptop of employees, then it can be dangerous for the organisation. In relation to this, it can also cause leakage and breaching of client information along with which, the company secrets can also be unleashed. Moreover, the company should also make a pantry area for the employees because if they are having lunch on the desk, this ct can also affect the property of the company, and if the food is spilt on the laptop, it might be destroyed or lose some data. It is also recommended that DevTech should upgrade its firewall and antivirus software on a regular basis. The company directors have expressed their concern about malware attacks and data loss. In addition to this, the directors are also concerned about IT security because it can affect productivity and system usability (Daniellou, 2020).

Conclusion

In the scenario of the DevTech, the company is lacking with some issues related to technology and innovation which are required to be overcome. In addition to this, there are various issues in the company's security policies and network security. In this relation, the above report contains recommendations that are based on the current drawbacks of the company. In a similar context, the company is required to be focussed on the use of encryption and decryption processes because it is necessary for the sustainability of the organisation. The company has an issue related to its building because proper security is not available in the building and the gate of the office is locked by a simple key on the door. In this case, the company should hire a personal guard for the night duty and can also apply the security system in the office such as CCTV cameras and alarm systems which will notify the owner if the robbery is attempted (Marsaid et al., 2020).

In addition to this, the company should also restrict the employees that they are not permitted to take laptops at their home because if important data is stored in the laptop of employees then it can be dangerous for the organisation. In relation to this, it can also cause leakage and breaching of client information along with this, company secrets can also be unleashed. Moreover, the company should also make a pantry area for the employees because they are having lunch on the desk, this act can also affect the property of the company, and if the food is spilled on the laptop it might lose some data. It is also recommended to the DevTech to upgrade their firewall and antivirus software on a regular basis. The company directors have concerned about malware attacks and data loss. In addition to this, the directors are also concerned about IT security because it can affect productivity and system usability (Daniellou, 2020).

Bibliography

Baloch, R. 2017. *Ethical hacking and penetration testing guide*. New York: CRC Press.

Berti, F., Pereira, O., Peters, T. and Standaert, F.X. 2017. On leakage-resilient authenticated encryption with decryption leakages. *IACR Transactions on Symmetric Cryptology*, pp. 271-272.

Daniellou, F. 2020. Developing Human and Organizational Factors in a Company. *In Human and Organisational Factors*, pp. 41-43.

D'Arcy, J. and Lowry, P.B. 2019. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal* 29(1), pp. 43-45.

El Kamoun, N., Bahnasse, A. and Bensalah, F. 2017. Evaluation of the Scalability of the Protected Multipoint Dynamic VPN by IPsec in a WiMax Network. *International Journal of Computer Science and Network Secuirty* 17(12), pp. 108-109.

Gąsiorowski, J. 2016. Managing security in electronic banking–legal and organisational aspects. *In Forum Scientiae Oeconomia* 4(1), pp. 123-124.

Khan, A., Pohl, M., Bosse, S., Hart, S.W. and Turowski, K. 2017. A Holistic View of the IoT Process from Sensors to the Business Value. *International IoT BDS,* pp. 392-394.

Lin, Y. and Bie, Z. 2018. Tri-level optimal hardening plan for a resilient distribution system considering reconfiguration and DG islanding. *Applied Energy* 210, pp. 1266-1279.

Marsaid, R.H.J., Huda, M., Lydia, E.L. and Shankar, K. 2020. IMPORTANCE OF DATA SECURITY IN BUSINESS MANAGEMENT PROTECTION OF COMPANY AGAINST SECURITY THREATS. *Journal of Critical Reviews* 7(1), pp. 251-252.

O'sullivan, P.J., Harpur, L., Willner, B.E. and Stern, E.H. 2017. Differential security policies in email systems. *U.S. Patent* 9, 742-743.

Raunio, T. and Sedelius, T. 2020. Decision-Making in Foreign and Security Policies and EU Affairs. *In Semi-Presidential Policy-Making in Europe*, pp. 127-128.

Vanjale, S.B. and Mane, P.B. 2018. Multi Parameter Based Robust and Efficient Rogue AP Detection Approach. *Wireless Personal Communications* 98(1), pp. 139-141.

Zhang, Y.L. and Yu, J. 2020. The Application of GABP Neural Network Algorithm in the Aspect of Security Assessment of Computer Network. *In Journal of Physics: Conference Series* pp. 24-25.