Investigation and implementation of network security

Student’s Name

Institution

Date

**Introduction**

Security of internet and system are some of the key in issue business. The revolution of network, threats and computer system have risen over the last few years. Studies have indicated that the issues of security are essential to enterprise and therefore, without data and hardware security, the information could be exposed. According to Salah (2018, p. 32), computer and system threats have increased due to advanced technology. Most systems are being targeted by either hackers or authorized entry to access and therefore, it is important to ensure that the system is protected from any unauthorized access. Therefore, this paper analyzes the security threats and the types of threats which businesses and companies are usually exposed to and methods, which can be used to solve the problem.

The first defense of any system or computer to any kind of security threat is firewall. Most internet users are concern about the internet connection and therefore, strict network connection usually weakness the network. According Ossi (2018), access to internet creates a lot of vulnerability into the system and therefore, it is important to ensure that the system is protected before connecting it to the network. Again, when the effectiveness of the network security is being done, it is important to assess the firewall platform and its impact to the network connection. A business network can only be regarded as secure when it is already been secured against any threats. Without implementing proper security then the network is still not secure.

As stated by Ahmad (2018 some of the threats to network are virus, hackers, unauthorized access by either employees or external attacks. These threats are usually get entry into the system based on the vulnerability, which are created by uses. According Kumar & Malhotra (2015)., system users create vulnerability which occurs as a result of recklessness the end user. It is also happened as a result of lack of enough information regarding the threats and therefore, users unknowingly open loopholes into the system, which are actually utilized by hackers to gain easy access to the system.

Without adequate protection or network security, the businesses, government and individual information are at risk. Network security is the process or techniques where digital information is protected from unauthorized access. The main goal of internet security is to protect the confidentiality, privacy and integrity of the information. Business leaders or government implement strict and power network security to protect government information from being accessed. With this in mind it is appropriate to protect information from threats and vulnerability for the business to be able to achieve its full potential. Studies also discovered that vulnerability can arise from poorly configured hardware, router, poor network design, end user carelessness and inherent technological weakness. It is therefore, important to disable any unnecessary services from router and also limit the access to the router by ensuring that the system has a strong password.

**Network Security and protection**

The purpose of security is to protect assets. With the growing technology and the involvement of different sectors such as e commerce, personal computer, and internet, the concern about security is high. Most data are kept within personal computers must be protected and the best way to offer protection to these data is by ensuring that the system is well setup and clear policies are also designed to protect the management of the network. Network security is therefore the most important component in the provision of security to the system. It ensures that information which is stored cannot be accessed by any one. It simply makes it difficult for any access to the system (King, 2014, p. 32). It is securing any information, which can pass through the netw0rk. The network security is referred to the hardware, software, operational producers, accountability, measures and control to the system. Network security for it to be successful, it must prevent the access or any entry into the system. For network security to be successful it has to prevent the information from getting loss. In network security there must be accountability, privacy and confidentiality.

In real world network security involve prevention detention and response. If the prevention techniques were perfect there would be no need to require detection and prevention. There are so many techniques, which are used to protect the system. Besides firewall, there are encryptions, passwords which are used to provide proper security to the system. Security of the network can be achieved only through proper installation of firewalls, which is at the entry and exit point of any system. The firewall prevents entry and exists of information without authorization. Therefore, firewall is a component which must be installed at the any network to prevent any entry to the system.

**Implementation of network security**

The network security can be implemented in there levels on the network infrastructure. It can be implemented at the backbone, servers, and at the computer. At the backbone level, the network security is installed at router, gateway, and switches to prevent any unauthorized access to the system. When using CISCO router, the network security is configured in two levels to prevent any access to the system. This is to ensure that the entry point to the system is protected and it becomes difficult to gain entry into the system or the network. The switches also should be configured with strong passwords or key to prevent any entry and therefore, installation of network security is necessary to be done at the entry point to ensure that the system is protected. Besides installation of security at the gateway and switches, it is important to install strong firewall hardware and set software as well. This will limit access to the system to ensure that unauthorized person does not get access to the network. In some cases, the security is also deployed at the gateway to ensure that the system is fully protected. However, it would be important to ensure that there is a clear security policy, to prevent the data from being accessed.

**Security Policy**

Security policy is an important measure which is taken to prevent the access to the system. The best way to protect a system is derived a policy which can protect the system from unauthorized access. An organization can derive policies regarding login and accessibility of the system. The security policy can be including login password strength, active status and how clients can be able to log to the system and stay active after certain duration. The network administrator must come up with security policy to prevent people from login to the system. The policy would be able to prevent the system from external attack such as hackers and therefore, it is important to ensure that there is a proper security system based on the policy. For instance, the system can be set to require string password such word and letters, and at least eight. This is to make sure that nobody can easily guess the password and use to access a system.

**Biometric and password**

Mostly entries are protected using biometric and password. It is important to ensure that the password is strong. The personal computer, server, and other electronic devices should be protected using passwords; it is upon the network administrator to design the kind of passwords allowed and the biometric devices which is applicable. The biometrical could be figure print, eye and other allowed system. It is therefore, important to ensure that every employee has a unique passwords and clear policy for login. The passwords are set at the server and configured for every end user could be best way to ensure that the system is protected. It is also required that users should change their passwords often at specific time and any user who failed to change the password would be lockout. It is some of the policies which should be included as part of the network policy to protect the system.

Security decision making

There are some mistakes, which business leaders usually make which affect a company badly. It is required of an individual to take his or her time before deciding on what to do or any action to take. Studies have indicated that decisions which are made in rush always lead to poor choices and therefore, it is important to take time before deciding on what to do (Michael, 2014). Jeff Miller, the director in charge of training and development for human resources and business performance solution highlighted that leaders usually make quick decision without consideration other key factors. This affect the company’s performance since such decision was made without thinking of the alternative. It is also important to note that avoid making decision can also hurt the reputation of business. And therefore, it is required for a business leader, manager to make quick and appropriate decision without delaying because such delaying may hurt the company.

**Recommendation**

Network security is an important factor for enterprises. It is therefore, important to ensure that the system is protected using policies, hardware and software to safeguard the integrity of the data. Security implementation should be done at the entry point and within the system to ensure that any network is protected from any unauthorized access. It is therefore recommended for enterprises to deploy some of the latest security system which require the use of bio for access to a building or a system. The firewall should e deployed as well at the entry and exists to make sure that the system is protected. In real world network security involve prevention detention and response. If the prevention techniques were perfect there would be no need to require detection and prevention. There are so many techniques, which are used to protect the system. Besides firewall, there are encryptions, passwords which are used to provide proper security to the system. Security of the network can be achieved only through proper installation of firewalls, which is at the entry and exit point of any system. The firewall prevents entry and exists of information without authorization. Therefore, firewall is a component which must be installed at the any network to prevent any entry to the system.

**Conclusion**

Network and network security are essential for businesses and other enterprises. Without network security the information is exposure and this can hurt a company. Most companies have sensitive information, which should be protected. Therefore, it is important to ensure that such information is protected using various standards and policies. The network protection can be informed of hardware, software or policy application to ensure that the data and any other information about the company are protected from access.

# Bibliography

Ahmad, N. (2018). Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of. 2-31.

King, T. (2014). CompTIA Security+ Exam: Devices, Media, and Topology Security. 2-3.

Kumar, A., & Malhotra, S. (2015). Network Security Threats and Protection Models. *Technical Report – CSE-101507* , 2-34.

Ossi, V. (2018). 2 EVALUATION OF FIREWALLS AND RESEARCH. *Degree Programme in Information Technology* , 5-38.

Salah, A. (2018). Design and Implementation of a Network Security Model for Cooperative Network. *https://www.researchgate.net/publication/50367393\_Design\_and\_Implementation\_of\_a\_Network\_Security\_Model\_for\_Cooperative\_Network* , 2-35.