Mohanad Horani

Security Essentials

Assignment 03-1

University of Advancing Technology

Assignment 03-1

Three examples of security controls that are implemented within an organization typically include antivirus software, firewalls, and risk analysis. A security control is defined as a tool that protects the confidentiality, integrity, and availability of information of an organization and meets security for the organization as well (NIST, n.d.). In other words, security breaches and incidents are prevented by such controls (Gerberding, 2018). Not only that, crucial data is also protected when security controls are implemented as well (Gerberding, 2018). Overall, security controls are essential to a network infrastructure.

The first example of a security control that is essential to implement is antivirus software. Antivirus software are programs that help prevent a computer from receiving malware or other computer viruses (Johansen, n.d.). Antivirus software also defends computers against cybercriminals as well (Johansen, n.d.). One reason why antivirus software is necessary includes the rise of new malware (Johansen, n.d.). Not only is it crucial to have an antivirus, but it is also crucial that it is updated frequently (Johansen, n.d.). The main goals of an antivirus are both detecting and scanning for any malware that is a potential threat to the computer (Johansen, n.d.). Some examples of well-known antiviruses include BitDefender, Norton, and McAfee ("Best Antivirus Software 2020," n.d.). Overall, antivirus software has a variety of benefits.

Antiviruses can be implemented in network infrastructures in two different ways. The methods of implementing an antivirus depends on the number of machines available in the workplace, the staff that are available, and the type of server that is utilized (Fuse Technology Group, n.d.). The first type of antivirus is called the “standalone antivirus” (Fuse Technology Group, n.d.). A standalone antivirus involves installing software individually on plenty of machines (Fuse Technology Group, n.d.). This solution is better implemented when there are only a limited number of computers, not many staff members, or not many servers either (Fuse Technology, n.d.). The second option which is more standard is the centralized antivirus (Fuse Technology, n.d.). This option is utilized when there are five or more computers, and tons of servers as well (Fuse Technology, n.d.). The centralized antivirus option allows for updates to be done from one machine and administrators to run tasks all on one computer as well (Fuse Technology, n.d.). Overall, these are the main methods in which antiviruses can be implemented.

The second type of security control that is widely implemented includes firewalls. A firewall is simply defined as a software tool that denies unauthorized access to a certain network that is private (Comodo, n.d.). Firewalls can also help improve the security of computers connected to the internet as well (Comodo, n.d.). In addition, firewalls control which processes can access certain network capabilities as well (Comodo, n.d.). Some other examples of what firewalls can do include but are not limited to the following: manage/control network traffic, record certain events on the network that occur, and enable access as well (Comodo, n.d.). Some instances when a firewall is crucial includes when one browses the internet at leisure, when one connects to a public network, and when a certain program that installed on the desktop must access network functions/capabilities (Comodo, n.d.). Overall, there are various benefits to implementing a firewall.

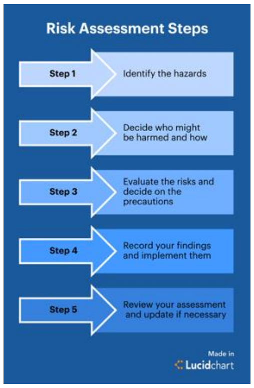
Firewalls can be implemented in a typical network infrastructure in five easy steps. The first method in implementation is to secure the firewall (Skarda, 2019). The reason behind implementing a firewall is if attackers somehow control a network, the business stops functioning completely which is why this step is extremely crucial (Skarda, 2019). This can easily be done by changing all default passwords and updating the firewall for instance (Skarda, 2019). The next step in implementation is to plan IP addresses and zones for the firewall (Skarda, 2019). The third step is to configure access controls. This means determining network traffic for the firewall (Skarda, 2019). The last two steps include configuring logging and testing the setup for the firewall (Skarda, 2019). Overall, these are crucial steps in implementing a firewall.

The final method of implementation that is necessary is risk analysis. Risk analysis is basically an examination of any risks or flaws that the business has (Nohe, 2019). Not only that, risk analysis (also called risk assessment) is utilized in order to organize the priority of any potential hazards that there are for a certain organization (Nohe, 2019). There are also various benefits to risk analysis. For instance, in the long term, costs can be significantly be reduced (Nohe, 2019). Not only that, communication and awareness can be improved/increased and breaches/incidents can be prevented as well (Nohe, 2019).

A risk analysis can be implemented within a network infrastructure utilizing a set procedure. First off, a data audit should be utilized (Nohe, 2019). A data audit sets guidelines for the importance of the data that is being protected as well as the type of data that is being protected (Nohe, 2019). The following six steps should be utilized when performing a risk analysis/assessment: identifying threat sources, identifying threat occurrences, identifying vulnerabilities and ways to prevent them, identifying the chance that such an incident could occur, identifying the outcome/result of the attack, and determining the amount of risk that is presented (Nohe, 2019). When a business is done utilizing a risk analysis, a verification is always essential in terms of double checking the report that was made (Nohe, 2019). Overall, there are no methods in completely elimination security breaches/risks however this is the best method in at least getting a headstart in doing so (Nohe, 2019).

Figure 1- https://www.macworld.com/article/3263722/best-antivirus-for-mac.html

Figure 2- https://www.cbronline.com/what-is/what-is-a-firewall-4900896/



Risk Assessment Steps

Step 1 Identify the hazards

Step 2 Decide who might be harmed and how

Step 3 Evaluate the risks and decide on the precautions

Step 4 Record your findings and implement them

Step 5 Review your assessment and update if necessary

Made in Lucidchart

Figure 3- https://www.lucidchart.com/blog/risk-assessment-process

References

Best Antivirus Software 2020. (n.d.). Retrieved from https://www.trustedantiviruscompare.com/best-antivirus-software?gclid=CjwKCAiA-vLyBRBWEiwAzOkGVMcnOG1S-jloAALSH-5kcDoXKyWxJeCv9svygwivQd1jD9xyWTqAaBoChHsQAvD_BwE

Comodo. (n.d.). What is a Firewall? | Explaining How a Firewall Works. Retrieved from https://personalfirewall.comodo.com/what-is-firewall.html

Fuse Technology Group. (August 1). Anti-Virus is Still Essential for every Organization’s IT. Retrieved from https://fusetg.com/anti-virus-essential-organizations/

Gerberding, K. (2018, March 6). Information Security Controls: Frequently Asked Questions (FAQ). Retrieved from https://www.hitachi-systems-security.com/blog/information-security-controls-faq/

Johansen, A. G. (n.d.). What is antivirus software? Antivirus definition. Retrieved from https://us.norton.com/internetsecurity-malware-what-is-antivirus.html

NIST. (n.d.). security control - Glossary. Retrieved from https://csrc.nist.gov/glossary/term/security-control

Nohe, P. (2019, January 8). How to perform a cyber risk assessment. Retrieved from https://www.thesslstore.com/blog/cyber-risk-assessment/

Skarda, C. (2019, September 13). How to Configure a Firewall in 5 Steps. Retrieved from https://www.securitymetrics.com/blog/how-configure-firewall-5-steps