Running head: Network security 1

Network security

Students Name

Institution Affiliation

Network security 2

Windows firewall is a basic part of a company's network. Even though a firewall is a basic feature for security, it should not be solely relied on. Windows firewall is meant for preventing attackers that come from outside the network. It is not applicable when the attacker is from within the network. Attackers may exploit vulnerabilities in the firewall itself since it is a software. This happens when the windows firewall is not managed properly. For instance, failing to install updates for security firewall system on the given period of time. The firewall configuration settings can cause vulnerabilities if they are not configured well. For instance, having dynamic routing can cause security to reduce due to loss of control. Many companies forget to switch off dynamic routing creating vulnerabilities in their systems. Having a poorly configured firewall is a waste of time since it makes work easier for attackers to exploit the company's systems (Naik, Jenkins, 2016, August).

Fewer advance windows firewalls only check the data point of origin and it's destination before approving it. This information can be manipulated by an attacker to trick the system approves it to the network. Also, attackers use Distributed Denial of Service to penetrate through the system security. The main purpose of using Distributed Denial of Service is to stop or slow the operation of the company's services. Windows firewalls can detect Distributed Denial of Service attack but can be drained by protocol attack. Windows firewall cannot serve as a security measure for all the threats present. However, they can only serve as a basic measure for a security network to safeguard the business (Khedr, Gulak, Vaikuntanathan, 2016).

Data leaks are one of the security threat in infrastructure as a service. Data leaks occur because of the large amount of data being stored in the platform. This makes it be targeted by attackers. Authentication bypass causes leaks of data in the platform. Weak passwords and poor management of security certificates causes authentication bypass. This is caused by poor data access and encryption of the data in the platform.

Network security 3

Encryption of data is one of the security measures taken by infrastructure as a service. Encryption is the main method of protecting data. Managing encryption keys is important as well in securing the platform's data. They also encrypt the whole network so that any data passing through the network is encrypted. Both the infrastructure as service providers and the clients should perform vulnerability check regularly. There is a control on access of data from the infrastructure as service providers. Multiple security layers have been implemented to cope on security measure by the infrastructure as a service provider. Lastly, staff training is important. Both infrastructures as service providers and the clients should have thorough training on its staff.

Data security is the most important issue when it comes to computer security. There should be dedicated systems that store the data in the platform. There are some items that need to be implemented by the infrastructure administrator. One of the items is a firewall which should control the flow of data in a network. The firewall should be configured in such a manner that it allows access exception and disallow for the public. This will prevent public access of network to the public thus minimizing any threat in the platform. Windows firewall and configuration settings should be configured in such a manner that it prevents all the suspicious threats from penetrating through the network. All data stored in the system should be protected by anti-virus. Anti-virus check should be performed on the boundaries of the network, communication systems, servers, workstation, and emails. Data encryption, session, and filtering of content help in protecting data in and out of the network. Computers should utilize the use of virtual private networks(VPN) as well. All the computers that use virtual private network must have the latest and up to date anti-virus. Staff must act with responsibility and integrity while using the platform (Tebas, Roberts, Muthumani, Reuschel, Kudchodkar, Zaidi, Boyer, 2017).

Network security 4

Reference

Tebas, P., Roberts, C. C., Muthumani, K., Reuschel, E. L., Kudchodkar, S. B., Zaidi, F. I., ... & Boyer, J. (2017). Safety and immunogenicity of an anti–Zika virus DNA vaccine—preliminary report. New England Journal of Medicine.

Naik, N., & Jenkins, P. (2016, August). Enhancing windows firewall security using fuzzy reasoning. In 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) (pp. 263-269). IEEE.

Khedr, A., Gulak, G., & Vaikuntanathan, V. (2016). SHIELD: scalable homomorphic implementation of encrypted data-classifiers. IEEE Transactions on Computers, 65(9), 2848-2858.