Security Risks And Vulnerabilities In IT Network Systems And How To Manage Them

Prepared By

Student’s Name

Instructor’s Name

Institution

Date

Business websites and web applications are significant assets for any business that owns one. Every company works extremely hard to protect its site against any security attack. This is done by analyzing security risks and vulnerabilities that the system might face. (Joshi and Singh, 2017) Network security risks are a significant problem when not identified in time; hence, one may realize when the damage is beyond repair. This paper focuses on some network security risks and vulnerabilities and points out the methods, tools, and techniques used to solve them. Computer Viruses are a common network security risk. They work by inserting their code that multiplies the virus itself, thus modifying other system programs. The system is said to be infected by the virus if the replication succeeds. They come in various forms and work in different ways. Viruses can delete valuable data and corrupt files, thus affecting the company's regular operations and leading to big losses. The worst-case scenario can happen where the viruses can delete everything from the hard drive. (Jones and Ashenden, 2005).

Protecting software and systems against computer viruses can be done by: Educating the staff on viruses and encouraging them not to open email attachments before scanning them, avoid clicking any advertisements that may pop up on their screens, scanning files they share among themselves or even from outside the company before opening them and installing anti-viruses from trusted providers.

Hackers are another network security risk. They are computer experts who can gain access to your network and computer system by using their technical knowledge. Their intentions are purely for malicious reasons. Some of them access the system to steal data and expose the trade secrets to the competitors of the company or even the entire world. To prevent hackers from accessing the data, high-security measures have to be put in place. Outdated software also causes the risk to the organization. They may slow down the whole network, thus making it hard for any work to be done. They can also lead to crashing down the site, and when the system is down, they may lose many customers who try to access the software. To prevent such cases, regular software updates need to be carried out. Lack of awareness among employees can pose a great threat to network security. Some employees can expose a system to vulnerabilities without knowing. These could involve clicking attachments and sharing the company's files on insecure networks. All employees have to be educated on network risks and how to prevent them. Misconfiguration of firewalls or operating systems is also a risk to any organization’s software. Firewalls prevent unnecessary traffic from entering the network. If the firewall is misconfigured, blocking traffic from entering the network won’t be possible. The actors can utilize the opportunity to attack the network. To ensure that the firewall is well configured, penetration tests need to be undertaken to determine the effectiveness of the security control.

**Computer programs and systems that help manage and audit risk and security issues.**

The Nmap tool is used for port scanning. The ports are tested to determine their state. There are six port states which are recognized by Nmap, namely open, closed, filtered, unfiltered, open filtered and closed filtered. (Pinkard and Orebaugh, 2011). An open state indicates that an application is active, which means accepting TCP connected or UDP ports. Finding an open port is usually the main goal during port scanning. Typically open ports are an avenue for security attacks. Attackers usually want to exploit open ports while system administrators aim at closing and protecting them with firewalls. Once an open port is found, it's easy to close it, thus reducing security risks.

Nessus is a tool used to scan vulnerabilities in a system. It works by raising an alert in case of any vulnerabilities that hackers can access any computer connected to a network. Though Kali is used for penetration testing, the Nessus tool is highly recommended to be used hand in hand with Kali Linux as an operating system. (Rogers, 2011). OpenVAS (Open Vulnerability Assessment System) is an open-source vulnerability scanner used to test the system and identify security holes. This is done by getting and analyzing data from a database with over fifty thousand test plugins.

**Analysis of security breaches and issues**

Security breaches and issues are a significant concern in many organizations. In order to prevent or stop security breaches and issues, the first step is to identify the root cause of the issue. Some of the causes of security issues include human error, which can be done by anyone, including using weak passwords, giving out sensitive passwords, and sending information to wrong recipients. Other causes are malware attacks, theft of data-carrying devices and the presence of old unpatched security vulnerabilities. After identifying the causes of the risks, the organization has to gain more visibility in its IT environment by staying current on any data breaches. Lastly, Cybersecurity has to be made a priority, and this can also be done by training employees on Cybersecurity.

**Legal, social, ethical and professional issues faced by information security professionals.**

Legal issues involve setting are rules that prohibit particular behavior in Information Technology; These rules are derived from ethics, which are socially acceptable behaviors. Information security professionals most of the time have access to personal and confidential information pertaining to individuals and companies' networks and systems. It gives them the power to do anything with the information they have access to. The professionals can, however, abuse that power given to them intentionally or non-intentionally. (Whitman and Mattord, 2011). Privacy of customers' information needs to be protected in any way possible.IT associations and organizations had to come up and address the legal, ethical, social and professional side of the job. However, the challenge still exists because there is no requirement for all the IT security personnel to register and be part of those organizations. (Shinder, 2005). The guidelines are essential because, during training, the specialists only focus on the technical parts of the job and forget that the skills can be misused.

**References**

Jones, A. and Ashenden, D., 2005. *Risk management for computer security: Protecting your network and information assets*. Elsevier.

Joshi, C. and Singh, U.K., 2017. Information security risks management framework–A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, *35*, pp.128-137.

Orebaugh, A. and Pinkard, B., 2011. *Nmap in the enterprise: your guide to network scanning*. Elsevier.

Rogers, R. ed., 2011. *Nessus network auditing*. Elsevier.

Shinder, D., 2005. Ethical issues for IT security professionals. *URL: www. windowsecurity. com/articles*.

Whitman, M.E. and Mattord, H.J., 2011. *Principles of information security*. Cengage learning.