Network Threats And Vulnerabilities In Riyadh

Posted on September 19, 2019

Introduction

The development of information systems in organizations has focused more on processing power, high reliability, and memory. However, the primary challenge facing information systems is cybersecurity. Riyadh computers utilize standard operating systems like Linux, Windows NT/2000 and DOS, which are common Human-Machine interfaces. The computers in Riyadh use local access networks, which are a means of remote access and also impose vulnerabilities like insecure communication between PCAnywhere and the control system. Viruses and worms are also threats to Riyadh's information systems. The use of the wireless system is affordable, but natural forces, rogue access points, and eavesdropping are potential threats. There are security technologies such as secure remote access, network access control, critical data encryption, and firewalls that are less implemented. Encryption techniques such as asymmetric and symmetric are the primary forms of preventing cyber vulnerabilities and threats. The paper aims to present a way forward for the use of Riyadh information technologies.

Network Threats And Vulnerabilities In Riyadh

Denial of Service Attack:

The threat occurs when the Channel appears to be busy. The common technique used to perform the attack is Carrier Sense Multiple Access. This threat can either be intentional or accidental. The use of 2.4 GHz is universal to all wireless networks, such as the one used in Riyadh; thus, network interference is possible. The mitigation of the problem is done through the use of the 5 GHz band. Any individual can access the 5 GHz band, which poses a major challenge in mitigation. The detection of retransmission or excess error is through the use of a WIPS alert. It is possible to isolate the device location through the use of a stumbler.

Evil Twin Access Point:

It is a more likely threat to occur since it advertises the name Wireless LAN as a legitimate access point, but the primary objective is to lure users. (National Institute of Standards and Technology, 2024) The identification of the occasionally used Service Set Identifiers of Riyadh is possible via the

use of the KARMA tool. The tool will then choose one Service Set Identifier. Generally, the connection between the access point and the wireless station is not possible. Therefore, it is possible to trick the user into utilizing the phoney access point by placing the evil twin close to the Riyadh area. After the user connects, further attacks such as spreading viruses, extracting usernames and passwords, and creating fake e-prescriptions will not be an issue. However, the cure is an approach that can be used to protect against the Evil Twin attack.

The wireless access and the portable ends are the potential network vulnerabilities in Riyadh. Devices such as laptops and smartphones are portable and can access wired or wireless networks. The devices are capable of infecting the information system in Riyadh, whether inside or outside. The communication system can be safeguarded by minimizing physical access to RJ-45 ports as well as disabling unused ports. The organization should encrypt all the e-prescription files since such sensitive information can fall into unauthorized hands. The Wireless Encryption Protocol commonly used in the Riyadh wireless access points is a very weak protocol. Thus, brute force attacks on the Riyadh information system will be eliminated through the application of WAP2.

Riyadh has various techniques that are used to minimize threats and vulnerabilities in the information technology systems, but the following are additional security technologies that will eliminate the security issues in the organization.

Firewalls:

Riyadh should prevent malicious traffic from unknown sources as a primary step to safeguard the storage and communication system. The use of the network accomplishes the inspection of the network traffic. The pre-defined security policies are the basis for the network firewall to permit access or deny data from any source. The firewall will require every individual to use the Virtual Private Network and an IP address to access the internet since the Network Address Translation can create security zones. The exposure of the organization’s control system to an untrusted network is minimal since the primary firewall objective is to control network traffic. (Joint Task Force Transformation Initiative, 2012) However, the regulation of malicious attacks or unintentional mistakes is impossible because the firewall is the basic step in network securing.

The use of the Secure Socket Layer:

It is a security protocol that will enable physicians to communicate securely via VPNs. The technique has been outstanding in other firms since individuals can access control networks efficiently and securely either when outside or inside the organization. The protocol is essential for administering tasks, performing remote maintenance and sending instructions. The critical aspect of the protocol is sending instructions. The physician uses a very secure network in the two fields. The first is sending an e-prescription to the pharmacist, and the second one is sending diagnostic protocol to a nurse or a specialist.

Authentication/Authorization Systems:

The system uses the privilege level and the user's role before enabling an individual to access a network. The current Riyadh devices have limited memory; therefore, the PLCs and RTUs with limited authentication are the ones used. The organization should adopt a system which mandates an authentication procedure before accessibility. Riyadh uses passwords as a security mechanism, which is not a comprehensive solution. The identification method, such as the use of a certificate and a password, is a standard security protocol. Moreover, the use of the RSA key-based authorization or thumb scanner is more secure than the use of passwords.

References

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST SP 800-30 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1