RESEARCH ARTICLE OPEN ACCESS

Remote Access and VPNs

Azhar Ushmani

ABSTRACT

The competitive business environment demands that companies take all possible measures to address customer needs and maintain satisfaction. Remote access allows employees to work from anywhere to deliver services and increase productivity. However, remote access also requires effective security measures to prevent compromises to company data and operations from potential cyber threats. The article discusses the importance of remote access and security for maintaining customer satisfaction and employee productivity in a competitive business environment. Corporation Techs is planning to adopt remote working for its employees, and to ensure safety; it will need a VPN (Virtual Private Network) to secure connections. Virtual Private Networks (VPNs) are secure, encrypted connections between two or more sites over the public internet. VPNs allow remote users to access a company's network and resources online. The article recommends SSL/TLS VPN technology over IPsec VPN, as it is more flexible, less expensive, and platform-independent. The VPN solution should also accompany a VPN policy, regular backups, and updates to enhance security. Finally, multifactor authentication should be used to increase the checks before granting access to the organization.

Keywords:- Remote access, VPN, Internet of things, Data science, Big data

I. INTRODUCTION

In the current competitive environment, companies must ensure that there are all possible measures to address the customer's wants and maintain their satisfaction with the services they deliver. Remote access allows users to work from any location to provide services to the customers and keep their satisfaction with their products and services. Remote access also increases the employees' satisfaction with the convenience and flexibility of their work schedules.

This satisfaction allows the employees to be more productive in delivering the company's mission to make the company more effective and reliable. Langer (2017) notes that the desire to work remotely and under flexible terms is one of the characteristics of Generation Z employees that supports their productivity in the current organizational spaces. Corporation Techs has adopted the move as most of its employees will start operating remotely to execute their roles at their convenient locations.

In this delivery, the company will require adequate security to ensure no compromises to its operations and ensure they are more competitive in its delivery to its clients. The essence of security is that the internet connection between the users and the company is insecure, given the many threat agents targeting the companies (Schenfield, 2015).

The security of these connections is essential for maintaining that there are no compromises to the company's data and operations. Therefore, the links need protection to ensure attackers do not compromise them and the companies maintain delivery to their clients. Besides the firewalls, the company will require VPNs to secure these connections.

II. OVERVIEW OF VPNS

A VPN (Virtual Private Network) is a secure, encrypted connection between two or more sites over the public internet. A VPN can securely connect remote users and other locations within a company's network. All data passed between your company and its partners stays within the secure VPN tunnel with a VPN. This protects information from eavesdropping, man-in-the-middle attacks, or misrouted data packets. The VPN is a standard solution to allow remote users to access the network and its resources through the internet. Once a VPN connection has been established, the user's computer appears to be part of the corporate network, allowing access to file servers and other network resources.

III. VPN RECOMMENDATIONS FOR CORPORATION TECHS

When deploying the VPN technology, Corporation Techs will maintain that manageability and security are primary considerations. The company is deploying a VPN for the first time. Therefore, it needs the expertise to manage the VPN and maintain a secure

and safe organization free from attacks between VPN connections. Companies' standard VPN implementation technologies include Internet Protocol Security (IPsec) and SSL/TLS VPN. The SSL/TLS VPN will be the most effective technology since these VPNs provide connectivity through the secure sockets layer (SSL) protocol (Stewart & Kinsey, 2021).

According to Stewart and Kinsey (2021), SSL/TLS VPNs are more flexible because they can encapsulate information at layers six and seven of the OSI model. IPsec VPNs require the client machines to have special software to connect to the machines in the organization. This requirement complicates their management since the administrators must manage the organization's client machines and servers or computers.

These requirements also complicate the security since the security will depend on the measures maintained by the remote users or the client computers to protect them against potential security threats. The users are the primary cause of the security issues since they are the weakest links in the organization's security (Johnson & Easttom, 2021). According to Solomon (2019), users could ignore the policies established by an organization, be forgetful, or commit some errors when executing their operations.

These mistakes increase the security vulnerabilities in an organization. The company will consider SSL/TLS technology, which is less expensive and platform-independent. In this case, the company does not face costs for managing another software. Platform independence eliminates non-uniformity in the versions of the operating systems running on different devices. Also, fewer firewall rules support SSL/TLS technology running, making it reliable for the company to execute the desirable security needed to maintain remote access (Stewart & Kinsey, 2021).

IV. ADDITIONAL RECOMMENDATIONS

Since the company will be relying on the VPN to provide the required remote security, ensuring that the VPN provider offers redundancy to maintain security is essential. The chosen solution should be after considering all the necessary factors, such as the security requirements that match the organization's size. The VPN solution should also be accompanied by a VPN policy to guide the employees on the measures to observe when using the VPNs to provide the organization's security.

A VPN policy will reduce the organization's vulnerabilities since a guide will be available to remind the users of the measures they should observe to make the company's operations effective. The company should also enhance its authentication to ensure multifactor authentication increases the checks before granting access to the organization. It also increases the chances that an attacker will be caught.

More importantly, Stewart and Kinsey (2021) note that the company needs regular backups and updates to enhance its security. Updates provide the latest security definitions to protect the organization from the latest and emerging known threats. Backups will ensure the company has a restore point if there is a service disruption to minimize the loss from security events.

V. CONCLUSION

In conclusion, remote access is essential for modern businesses to maintain customer satisfaction and employee productivity. However, it also poses security risks that must be addressed to protect the company's data and operations. Implementing VPN technology is crucial in securing these remote connections, and Corporation Techs should consider SSL/TLS VPNs due to their flexibility and lower costs. To ensure the effectiveness of the VPN solution, the company should also have a VPN policy in place to guide employees on the proper use of the technology. Additionally, the company should enhance its authentication process, regularly back up data, and implement updates to protect against emerging threats. Companies must proactively protect themselves from cyber threats in today's digital landscape. By implementing VPN technology and following best practices, Corporation Techs can ensure that their remote access solutions are secure and effective, allowing them to maintain their competitive edge in the market.

REFERENCES

Johnson, R., & Easttom, C. (2021). *Security policies and implementation issues* (3rd ed.). Jones & Bartlett Learning.

Langer, A. M. (2017). *Information Technology and Organizational Learning: Managing Behavioral Change in the Digital Age*. CRC Press.

Schoenfield, B. S. (2015). *Securing systems: Applied security architecture and threat models*. CRC Press.

Solomon, M. G. (2019). *Security Strategies in Windows Platforms and Applications*. Jones & Bartlett Learning.

Stewart, J. M., & Kinsey, D. (2021). *Network Security, Firewalls, and VPNs* (3rd ed.). Jones & Bartlett Learning.