Securing Remote Network Access

Student’s Name

Institutional Affiliation

Securing Remote Network Access

In today’s internet environment, it is much easier to work from home and easily access company data and resources at one’s convenience. However, this convenience of connectivity and accessibility comes with significant risk since the internet is filled with numerous threats that could compromise the work and place sensitive company data in jeopardy. Stallings (2013) reports that network security should be paramount since, today, cybercrime is arguably the most prevalent crime and perhaps the toughest to combat since it can be conducted remotely and covertly. Remote access presents both an opportunity for working conveniently from home, especially in these tumultuous times of the COVID-19 pandemic outbreak. However, remote access could leave the company vulnerable to attacks that could lead to significant losses. This essay discusses two vital methods of securing remote access to company data and resources, namely Virtual Private Network (VPN), which are commonly used in business today.

**Virtual Private Networks**

Virtual private network (VPN) is a widespread technology that provides confidentiality, secrecy, and comprehensive access security to network users. Stewart and Kinsey (2020) explain that VPNs are often fortified with proxy servers and overlay networks, strengthening the tunneling process to bolster security further. While individual users mostly use remote access VPNs, the corporate network utilizes a site-to-site VPN that connects two networks, for example, to facilitate collaboration between enterprise branches in different geographical locations. However, for employees attempting to connect to a company network and access its resources and data, remote-access VPNs can be sued to connect the employee device and the company intranet away from the office. Stallings (2013) highlights that VPNs cannot anonymize online connections completely but considerably boost security and privacy. Using various security protocols and authentication methods, VPNs can provide reasonably secure connections for corporate use.

Stewart and Kinsey (2020) explain that VPN is the most common security option for most businesses since they allow online privacy and anonymity, two critical needs with remote access. VPNs also offer data encryption using disguising features that safeguard online activities. VPN is also preferred since it is relatively low-cost and is user friendly. For example, at my workplace, Cisco AnyConnect VPN is used since it is among the best with efficiency due to ease of integration with other software and Cisco solutions and enterprise-level technical support. While VPNs offer numerous pros, they also have some cons. Stewart and Kinsey (2020) claim that the main concern with VPN is customer data security, with some vendors opting to log VPN transactions and sell client data to third parties. Some VPNs also have a leakage problem which affects the security of company remote access communications.

**Privileged Access Management**

Privileged Access Management (PAM) is a technology that can help bolster remote access security. PAM is a technology that allows for safeguarding, regulating, and monitoring of access to company resources via privileged accounts (Chapple, 2020). PAM tools and technologies ensure constant oversight that lessens the risk of unauthorized access to company resources with the added ease of detecting suspicious activities. Stewart and Kinsey (2020) report that privileged users, mostly in big corporations, are targeted by cybercriminals for their capacity to access sensitive and highly valuable company information. In recent years, over forty percent of data breaches involved hacking of privileged identities (Stewart & Kinsey, 2020). With PAM, many privileged accounts can be hosted on-premises, with each cluster having different configurations that allow for controlled access to company data and network resources. Privileged accounts present a severe threat to company networks, with credentials theft rising exponentially in recent years, which is a primary concern of corporate IT divisions.

While different PAM models offer varied benefits related to security, monitoring, and control of access, they also have disadvantages such as tediousness and time consumption for recurrent access verifications and secure individual privilege account re-establishment (Stallings, 2013). PAM can also prove to be costly for dedicated solutions with added complexity for end-users. Seemingly PAM is less user-friendly in comparison to VPN hence the latter’s popularity in the corporate world. While having improved in recent years, the enterprise PAM system is still marred by user unfriendliness with a subsequent need for configuration and management expertise (Stallings, 2013). Also, substantial IT resources are needed to facilitate setup and long-term maintenance.

**Conclusion and Recommendations**

To secure access to remote workers, it is advisable to use a method that best suits the particular company. While PAM can help with multi-level security controls, its complexities make it difficult for employees to work efficiency; thus, it would be advisable to use a robust enterprise VPN solution to secure remote access to company resources. However, due to VPN limitations, it would be wise to add other remote access security measures such as developing a cybersecurity policy for remote workers with network border protection. Chapple (2020) suggests having added encryption layers, especially for the firewall and communication channels. Additionally, employee cybersecurity training can help prevent threats from human error, such as social engineering. For example, today, malicious attackers are tricking people through psychological manipulation to run a phishing attack, primarily via unsolicited emails. Training staff can help them detect and avoid such attacks thus preventing major network breaches.

References

Chapple, M. (2020). *Access control, authentication, and public key infrastructure* (3rd ed.). Jones & Bartlett Publishers.

Stallings, W. (2013). *Network security essentials: Applications and standards* (4th ed.). Prentice Hall.

Stewart, J. M., & Kinsey, D. (2020). *Network security, firewalls, and VPNs* (3rd ed.). Jones & Bartlett Learning.