Network Security Needs: Comparing Wired and Wireless LANs

Introduction

Network security is a critical component in the design and implementation of any IT infrastructure. As threats evolve, understanding the distinct vulnerabilities in different network types becomes essential. Both wired and wireless LANs have unique security needs, but the openness of wireless environments often exposes them to greater risk. A detailed comparison helps clarify which setup demands more stringent security measures.

Security in Wired LANs

Wired LANs typically offer a controlled environment where access is physically limited. Since devices must connect via Ethernet cables, unauthorized access is more difficult without physical presence. Standard security measures like firewalls, access control lists (ACLs), and port security help manage internal threats and unauthorized access attempts. According to Forouzan (2012), wired LANs benefit from inherent physical security, making them less susceptible to external interception.

However, this does not mean wired LANs are immune to threats. Insider threats, unsecured endpoints, and poor configuration can lead to vulnerabilities. Still, these threats are easier to monitor and manage within the confines of a secure facility.

Security in Wireless LANs

Wireless LANs, on the other hand, transmit data through radio waves, making them inherently more vulnerable to eavesdropping, spoofing, and unauthorized access. Because wireless signals can extend beyond physical boundaries, attackers can attempt intrusion without

needing physical access. Therefore, wireless networks require advanced encryption protocols such as WPA3, strong authentication mechanisms, and regular monitoring for rogue devices (Stallings, 2020).

Additionally, the dynamic nature of mobile users and Bring Your Own Device (BYOD) policies complicates wireless security. Without robust protections, attackers can exploit misconfigured access points or weak passwords to compromise the network.

Conclusion

While both network types demand security planning, wireless LANs require more stringent measures due to their susceptibility to remote attacks and broader attack surface. Enhanced encryption, authentication, and continuous monitoring are essential to securing wireless environments effectively.

References

Forouzan, B. A. (2012). *Data communications and networking* (5th ed.). McGraw-Hill. https://books.google.pt/books/about/Data_Communications_and_Networking_Globa.html?id=8IVvEAAAQBAJ&redir_esc=y

Stallings, W. (2020). *Network security essentials: Applications and standards* (6th ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/network-security-essentials-applications-and-standards/P200000003333/9780137561650?srsltid=AfmBOoofKjpD-dm1iXoVHWQq0XvUgb2yfBh3sEOWZgFwoPeCbmzWwDGq

Word Count: 311