**Internet-Facing Security and E-Commerce**

Author(s)

Affiliation

Institution

Instructor

Date

**Initial Post**

Hello my fellow peers,

Securing the internet-facing side of an IT system is very important due to the fact that it is the most vulnerable point of attack for malicious hackers. Unsecured internet-facing systems can be easily compromised, allowing hackers to gain access to the system and steal sensitive information, disrupt operations and even cause physical damage (McCollums et al., 2021). By implementing strong security measures, organizations can protect their systems from cyber-attacks and ensure the safety of their data and operations.

SSL is one of the internet –facing security component that an E-Commerce site could implement to protect its Internet facing IT system. Secure Sockets Layer (SSL) is a protocol that enables secure communication between two computers over the internet. It creates an encrypted connection between the server and the client, so that any data transmitted between them is unreadable to anyone else (Pan, 2020). By using SSL, e-commerce sites can ensure that any sensitive information, such as customer credit card numbers and passwords, is kept secure. SSL certificates also provide authentication, ensuring that customers are communicating with the correct server, and not with a malicious one. By implementing SSL, e-commerce sites can ensure the security of their sensitive customer data and provide a more secure online shopping experience.

**Response 1**

One of my peer proposed Virtual Private Networks (VPNs) as the component that E-Commerce site needs to implement since it can be used to securely connect two remote networks together, allowing for secure communications between two different networks (Zimba et al., 2019). This is particularly useful for e-commerce sites since they need to securely send payments and other sensitive data back and forth.

I would like to recommend on a Two-factor authentication as an additional security component to further secure the e-commerce site (Zimba et al., 2019). This would require a user to authenticate the identity by providing two different forms of authentication, such as a one-time code sent to their mobile phone or a security question. This will help to prevent unauthorized access in the E-commerce sites and IT systems.

**Response 2**

My peers proposed and confirmed that, data encryption is equally a viable component that can be used to protect sensitive customer data from being intercepted by malicious actors. Data encryption scrambles data into an unreadable format, making it difficult for unauthorized individuals to access (McCollums et al., 2021).

For further dialogue, I would recommend firewall as an additional security component that an e-commerce site could implement to further secure its internet-facing IT system. Firewalls are used to create a barrier between an organization's network and the outside world, allowing only authorized traffic to pass through (Pan, 2020). Firewalls can also be configured to detect and block malicious traffic, such as malware, viruses, and hacking attempts, as well as allowing organizations to control the type of applications and services that can be accessed.

**References**

McCollums, P., Bakalov, H., Morse, P., Phillips, T., & Day, W. (2021). UC-12 Comprehensive Security Solution for small E-commerce Business.

Pan, C. (2020, October). Construction of intelligent logistics model based on big data. In *Journal of Physics: Conference Series* (Vol. 1648, No. 2, p. 022014). IOP Publishing.

Zimba, A., Wang, Z., & Mulenga, M. (2019). Cryptojacking injection: A paradigm shift to cryptocurrency-based web-centric internet attacks. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 40-59.