Security Architecture and Design

Name

Institution Affiliation

Security Architecture and Design

**What happens when we place the authentication system in your demilitarized zone (DMZ)—that is, in the layer closest to the Internet? What do we have to do to protect the authentication system? What are the implications of doing so for authentication performance for security?**

The demilitarized zone (DMZ), often termed as screened subnetwork or perimeter network, is a logical or physical subnet that parts the LAN from other untrusted networks –often the internet. Services, resources, and external-facing servers are situated in the DMZ. Thus, they can be accessed from the internet, but the remaining part of the LAN remains inaccessible. This gives an extra layer of protection to the LAN because it limits the capacity of a hacker to straightforwardly access data and internal servers through the internet. The main objective of establishing an authentication system is to prevent malicious attacks and unauthorized users from accessing the information. Adding such a layer help strengthen security. Therefore, this closest layer is important because it keeps the malicious attackers away from accessing important data.

The authentication system must be protected from the attacks like guessed and stolen credentials by the utilization of multiple-factor authentication. The best practices must be embraced in order to eliminate the vulnerabilities that are directed to the authentication system. Such vulnerabilities include allowing auto logins, common and weak passwords, and saving critical information on the browsers. Thus, there is a need to put some approaches to eliminate the vulnerabilities surrounding the authentication system and protect it (Schoenfield, 2015). Further, the authentication credentials must always remain hidden from unauthorized persons in the organization, which will prevent these credentials from landing into the wrong persons' hands. The users of the authentication system must learn the basic information regarding the threats in order to identify them easily. For instance, phishing is a common approach the attackers use to gain access to the authentication information. When the users are aware of this technique, they cannot fall victim to the attack.

When the authentication is protected, the security level of the entire system is improved. Further, there is a better performance because the attacks that could pose a serious threat to the system are eliminated, creating an ideal surrounding for operations. The adoption of the best practices related to the authentication system help strengthens security (Schoenfield, 2015). The authentication system's security lies in the hands of the users; if caution is not taken to protect the system, the attackers can eventually identify the credentials and change everything. In contrast, establishing some measures to protect the authentication system comes with other security benefits because the organization is not required to change its system a lot. After all, it is well protected.

Reference

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