The CIA triangle principle is the most important thing in the cyber security field. Confidentiality, Integrity, and Availability together are a security model for organizations used to protect their data and keep the data away from unauthorized access.

One of the security design approaches is network security, which according to (Pawar & Anuradha, 2015) is protecting the network from unauthorized access, misuse, modification, and denial of service. Denial of service (DoS) and distributed denial of service (DDoS) attacks affect the availability of systems by consuming network bandwidth with abnormal traffic. Stateful firewalls track packets for the active connections and keep track of the new packet while they compare them with previous ones which are in session tables (Trabelsi et al., 2018). Advantages of a stateful firewall such as not just inspecting the data packets, however, data characteristics, channels, and behavior; with the log of the behavior of attacks and learn how to prevent those attacks in the future, on the other hand, it has disadvantages such as their software need to be up to date, otherwise, vulnerabilities may be compromised and it can be fooled to allow harm connection (Fortinet, N.D.).

The second security approach is software security, Denial of service could be related to applications besides the network infrastructures. Authentication system is one of the security design implementation considerations whereas brute-force aims to get user passwords, however, repeat that many times could be turned into denial of service attack, therefore lock the account after 3-5 failed attempts can help to prevent the attack (Nsrav, N.D.)

In conclusion, offline backup, cloud storage, failover, and disaster recovery could be used to ensure data, application, and system availability besides the security approaches which include network security, software security, and the human factor, therefore no one magic solution will succeed in cyber security challenges.

References

Fortinet. (N.D.) Stateful vs. Stateless Firewalls. Available from: https://www.fortinet.com/resources/cyberglossary/stateful-vs-stateless-firewall [Accessed 16 September 2021].

Nsrav. (N.D.) Denial of Service Software Attack. Available from: https://owasp.org/www-community/attacks/Denial\_of\_Service [Accessed 15 September 2021].

Pawar, M. & Anuradha, J. (2015). Network Security and Types of Attacks in Network. *Procedia Computer Science* 48: 503-506. Available from: https://www.sciencedirect.com/science/article/pii/S1877050915006353 [Accessed 15 September 2021].

Trabelsi, Z., Zeidan, S., Shuaib, K. & Salah, K. (2018). Improved Session Table Architecture for Denial of Stateful Firewall Attacks. *IEEE Access*, 6:35528-35543. Available from: https://ieeexplore.ieee.org/abstract/document/8395423 [Accessed 16 September 2021].