Name: Huong Quach

Date: 06/24/25

Exploring attacks on availability: DSoS

BLUF

Attacks on availability are intended to disrupt corporate operations and critical services by preventing authorized users from accessing systems, networks, or data.

What is an attack on availability?

When fraudsters purposefully prevent legitimate users from accessing systems, networks, or data, this is known as an attack on availability (National Cyber Security Centre, 2025). The CIA Triad's availability principle, which guarantees dependable access to necessary resources for authorized users, is directly broken by these attacks. Availability attacks are frequently carried out using techniques like ransomware, distributed denial of service (DDoS), and targeted network interruptions.

Recent example of DDoS attack

The record-breaking DDoS attack that Cloudflare reported in September 2023 is a noteworthy recent example. One of the biggest DDoS incidents ever documented, the attack peaked at around 201 million requests per second (RPS) (Cloudflare, 2023). DDoS attacks use massive botnets made up of compromised devices to overwhelm targeted systems with traffic.

Serious service interruptions result from this enormous load, which blocks legitimate customers from accessing services.

DDoS mitigation strategies

Businesses frequently use traffic filtering and scrubbing services to protect against Distributed Denial of Service (DDoS) attacks, one of the most prevalent availability threats (DDoS Mitigation: Strategies, Providers, and Solutions Explained, 2025). By distributing traffic among several servers, content delivery networks (CDNs) like Cloudflare or Akamai lessen the load on any one system. Rate limitation can stop servers from receiving too many requests, while IP reputation lists can stop known malicious sources. Furthermore, traffic can be dynamically redirected to servers that are accessible by using anycast routing, which lessens the effect of localized overloads (NIST, 2024).

More implications

Attacks on availability have broad ramifications. They can lead to serious financial loss, damage to a company's brand, legal repercussions, and a decline in consumer confidence. Disruptions to critical infrastructure could jeopardize vital services and public safety (Fortinet, 2023). Organizations must put defenses like traffic filtering, rate limiting, load balancing, redundancy, and specialist DDoS prevention solutions in place to lessen these dangers.

References

DDoS Mitigation: Strategies, Providers, and Solutions Explained. (2025, April 3). DataDome. https://datadome.co/guides/ddos/mitigation

Fortinet. (2023). What is a DDoS Attack? DDoS Meaning, Definition & Types. Fortinet. https://www.fortinet.com/resources/cyberglossary/ddos-attack

National Cyber Security Centre. (2025). A Guide to Ransomware. Www.ncsc.gov.uk. https://www.ncsc.gov.uk/ransomware/home

NIST. (2024). Cybersecurity Framework. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

The Cloudflare Blog. (2023). The Cloudflare Blog; The Cloudflare Blog. https://blog.cloudflare.com/