Demystifying Dos/DDos cyber attacks

By Moses Kipchirchir

What are Dos/DDos attacks?

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are types of cyber-attacks that aim to render services inaccessible by disrupting normal web traffic. These attacks occur when systems, networks, or servers are overloaded with excessive requests, causing a breakdown of services. DDoS attacks are particularly destructive, originating from multiple sources and making defence significantly more challenging. In the wake of such incidents, organizations must strengthen their cybersecurity infrastructure to combat these threats.

What are the impacts of these attacks?

When you have been subject to this type of cyber-attack, the outcome essentially is similar: loss of reputation, loss of time or loss of trust. The increasing frequency and sophistication of these attacks adds an extra layer of pressure on organizations to constantly evolve their cybersecurity measures.

> Monitoring detects threats early utilising advanced tools for real-time traffic analysis

Moses Kipchirchir
Associate Director, Technology Assurance
KPMG Advisory Services Limited
mkipchirchir@kpmg.co.ke.

How do you know when you have been attacked?

Identifying a DoS/DDoS attack can be tricky. While a slow or unavailable service is often the first sign, similar network performance issues can also result from genuine traffic increase. Therefore, monitoring for abnormal traffic patterns and suspicious traffic surges is a critical part of identifying an attack. In addition to searching for anomalous traffic patterns, organizations can also employ intrusion detection systems (IDS) and intrusion prevention systems (IPS) to identify attacks. These systems monitor network traffic for suspicious activity and can frequently identify DoS or DDoS attack patterns.

What is the recommended approach for resilience against DoS/DDoS cyber-attacks?

To build resilience against DoS/DDoS cyber-attacks, an approach comprising of prevention, monitoring and mitigation is recommended. Prevention begins with implementation of strong security protocols, including regular software updates, robust access controls, and data encryption. Monitoring detects threats early utilising advanced tools for real-time traffic analysis. Mitigation becomes necessary when attacks penetrate preventive measures. Here, techniques like rate limiting, IP blocking via Web Application Firewalls (WAF), CAPTCHA implementations to differentiate bots from human users, and cloud-based DDoS mitigation and protection services limit attack impact and expedite service restoration. Together, these measures can strengthen our defences against the increasingly prevalent and dangerous threat of DoS and DDoS attacks.

The views and opinions are those of the author and do not necessarily represent the views and opinions of KPMG.