PROTECTING YOUR ORGANISATION FROM DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS

WHAT ARE DDOS ATTACKS?

DDoS attacks are malicious attempts by cybercriminals to render computer services or resources unavailable to legitimate user(s) by using multiple computer systems to overwhelm available resources

PREVENTATIVE OR MITIGATING MEASURES

1 MONITOR AND EXAMINE NETWORK TRAFFIC FOR UNUSUAL ACTIVITIES

Continuously monitor incoming traffic by configuring network perimeter appliances (e.g. firewalls) to detect anomalous traffic types, system capacity overloads and rogue devices connected to the network.

2 PROTECT YOUR NETWORK PERIMETER

Configure firewalls and routers to only accept traffic required for business operations and drop network packets that meet specific criteria (i.e., malformed and spoofed). Other configurations include rate limiting the number of requests a server will accept over a certain time period to prevent volumetric DDoS attacks.

3 INCREASE NETWORK BANDWIDTH

Ensure server redundancy by using a load-balancer alongside multiple servers that can handle increased workloads. If available, enable auto scaling to automatically adjust the resources needed based on demand.

CSA SINGAPORE

SingCERT
Singapore Cyber Emergency Response Team

Follow us @CSAsingapore to stay up to date on the latest cybersecurity news and information.