Denial-of-Service (DoS) Attack Preparation
Maturity Model

ZX SECURITY

A denial-of-service attack is a cyberattack specifically designed to shut down a computer or network, making it inaccessible to its users.

LEVEL 1
Lack of Awareness

The base starting level for an organisation. You are not likely to have a full picture of your IT asset base or have a process for dealing with a DoS attack in place.

1

LEVEL 2
Understand your Ecosystem

You understand your systems and the impact to the organisation if a DoS attack were to occur.

You will have:

- an IT asset inventory
- documentation for key systems
- a patching process
- communication with external service providers

2

LEVEL 3
Planning

You plan what the organisation will do if there was a DoS attack.

This includes a:

- Documented communications plan if an attack were to happen.
- Plan for how the organisation is going to respond to a DoS attack.
- Plan for how the organisation is going to defend its assets.

3

LEVEL 4
Defending the Assets

You ensure all your systems (web, remote access, APIs, email, etc.) have DoS protections in place.

This includes:

- implement DoS mitigations and origin server protection
- conducting performance and load testing of systems
- DoS protection for non-web services, e.g. VPN, Email
- All domains are managed through a single registrar

4

LEVEL 5
Proactive Monitoring and Simulation

You are on the front foot regarding DoS attacks by running through DoS attack simulations and increasing your situational awareness.

Systems are monitored and architected to best use caching technologies offered by your Content Delivery Network or similar.

5

Contact us: www.zxsecurity.co.nz » contact@zxsecurity.co.nz » Level 7, 187 Featherston Street, Wellington