RANSOMWARE MATURITY MODEL

A type of malicious software designed to block access to a computer system until a ransom has been paid.

1 LACK OF AWARENESS

The base starting level for an organisation.
You are not likely to have an understanding of your internal and external IT assets or have a Ransomware response plan in place.

2 UNDERSTAND YOUR ECOSYSTEM

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

You have an inventory of IT assets and have documented the expected impact of a Ransomware attack on each asset.

You are aware of the information you collect and store and whether this information is private or personally identifiable.

3 PLANNING AND COMMS

You plan what to do if there were a Ransomware attack and how to mitigate its impact. This level includes a documented communications plan for if an attack were to occur and how the organisation will respond to a Ransomware attack.

4 DEFENDING THE ASSETS

You ensure all your systems have Ransomware protections in place.

This includes a defence strategy broken down into the different stages of a Ransomware attack, with security controls to prevent an attacker:

- Gaining access to the network
- Moving laterally and elevating their level of privilege
- Extracting private data from your systems
- Corrupting or stopping backups
- Deploying the Ransomware agent and encrypting files

5 PROACTIVE MONITORING AND SIMULATION

You are on the front foot regarding Ransomware attacks by running through simulations and tabletop exercises. Systems are monitored for abnormal activity and you regularly test restoring from backup.

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

ZX SECURITY