10 STEPS

TO HELP PROTECT YOUR BUSINESS FROM CYBER ATTACKS

KIANDRA IT®

Learn more at kiandra.com.au
or call (03) 9691 0500

Penetration Testing

Consider this step one in your cyber security protection plan.
Also known as ethical hacking, it will identify vulnerabilities in a system or network that has existing security measures in place. Step two is taking measures to plug the gaps.

Monitoring

Threat monitoring allows for continuous oversight of any vulnerabilities across your networks to stay on top of incoming threats. Cybercriminals take the path of least resistance, don't leave a door open.

Incident Management

This is a process of identifying, managing, recording and analysing security threats or incidents in real-time. Establish an incident response and disaster recovery plan. Always report an incident to the Privacy Commissioner and notify any affected customers.

User Education

Employees can make or break security. Produce user security policies covering acceptable and secure use of your organisation's systems. Establish a training program with regular testing such as phishing attacks. Start easy with a session on passwords.

Secure Configuration

When building and installing computers and network devices, secure configurations are put in place to reduce vulnerabilities. To maintain these, create a system inventory and define a base-line build for all ICT devices. Beware — misconfigurations are the most common gaps hackers look to exploit.

Network Security

Protects network files and directories from unauthorised access, system changes, misuse and hacking. It's one of the most simple, yet important ways to minimise the risk of data theft.

Home & Mobile Working

Security needs to be rethought in a remote and mobile-working world. Develop a policy and training program to ensure employees know what's at risk. All devices used for work must include a secure baseline build to protect data both in transit and at rest.

Removable Media Rules

Set a company-wide policy to control access to all removable media. Ensure it limits media types, use and all removable devices are scanned for malware before importing into a corporate system.

User Privileges

All users of your systems should only be provided with the privileges they need to do their job. Establish account management processes and limit the number of privileged accounts. Monitor user activity, control access and audit logs regularly.

Malware Prevention

Malware is short for "malicious software"— nasty applications looking to do damage. Establish anti-malware defences such as endpoint detection, response software and application and website whitelisting. Always keep your network up-to-date.