Cyber security

tips and self-assessment for business

Last year one in five New Zealand SMEs experienced a cyber-attack, so it's essential to be prepared. Our friends at Deloitte have put together this Cyber security self-assessment, to help you reduce the chance of an incident occurring.

What can you do?

There are a range of security measures that can provide enhanced protection, and enable easier detection and investigation of common attacks. We recommend working with your IT provider (where practical) to improve network security and enforce IT security controls that reduce the entry points for an attacker and allow you to investigate incidents.

Deloitte.

NZ6898-1 02/18

Accessibility

	Minimum security	Better practice	Best practice
User account controls Using default user names for administrator accounts makes it easier for an attacker to guess user names to perform brute force (password guessing) attacks.	▸ Username doesn't consist of only numbers. ▸ Remove any unused or idle user accounts. ▸ Remove or disable any user accounts with standard (default) user names e.g. admin, administrator, guest. ▸ Don't share accounts between multiple employees.	▸ Remove domain/local administrator access for accounts that don't require privileged access. ▸ Implement Windows User Access Control (UAC) for standard user accounts to prevent users from executing applications and executable files that aren't legitimate business requirements. ▸ Review user accounts every month to see whether they are still required. Confirm whether any additional user accounts have been added. ▸ Use a standardised naming convention that contains a mix of numbers and letters.	▸ Enforce group policies for passwords to force users to set a password of a minimum of 10 characters using alpha-numeric and special characters. ▸ Force users to change their passwords every 90 days. ▸ Enable auditing and logging for user accounts to help keep a track of user activity. ▸ Wherever you use credentials in your organisation apply two factor authentication.
Password controls Weak password complexity requirements allow staff to set passwords that an attacker can easily guess or brute force.	▸ Change passwords for all users immediately if there's been a recent breach. ▸ Passwords should contain at least 10 characters, using at least three of the below groups: Lower case characters (a-z), Upper case characters (A-Z), Digits (0-9), Special Characters (e.g. * &). ▸ Change passwords every 90 days.	▸ Prevent ability to use previous passwords immediately. ▸ Prevent users from changing passwords more than once a day.	▸ Disable password auto-complete on all web browsers and do not save passwords locally on the machine. ▸ Do not code passwords into your business software. Use an API based solution to retrieve them, as this will help you if you need to reset all company passwords.
Remote access Attackers can get full control over a machine through Remote Access. Secure controls should be put in place to log and limit users who can access the network.	▸ Limit Remote Desktop Protocol (RDP) or Secure Shell (SSH) access to known IP addresses only and those employees who require this access for a business reason. ▸ Implement geo-blocking of IPs outside of New Zealand's range.	▸ Set up site-to-site Virtual Private Networks (VPNs) where applicable (and then limit RDP access to internal IPs only). ▸ The default port for remote access (e.g. 3389/ TCP for RDP) should be changed.	▸ Set up an individual user VPN with 2-factor authentication (suggest using a mobile token). ▸ Use company approved devices to access your business network.
Brute force (systematic password guessing) prevention Even with strong user name and password controls, an attacker may still be able to brute force login names and passwords by using software to make millions of attempts at combinations.	▸ Turn on Windows Server brute force controls that automatically lock user accounts after a number of failed login attempts. This should be done for all accounts, but at a minimum the accounts with remote access enabled. ▸ Specify that accounts should be locked out for 10 minutes after five failed login attempts, before any re-attempts can be made.		▸ Enable SMART authentication to produce a more secure and simpler user experience.

NZ6898-1 02/18

Common attacks and security suggestions

Data protection

	Minimum security	Better practice	Best practice
Backups (data and configuration) Backups can help rebuild a system after an attack; however, there are often damaged or missing files when an incident occurs. Attackers can also modify or delete an unsecured backup, making recovery impossible.	▸ All important information and systems should be backed up regularly. ▸ Backup the database dump file and server image in multiple locations. ▸ Turn on notifications to confirm that backups have been successful.	▸ Regularly backup/transfer files on to a storage facility that is not attached to the internet. ▸ Backups should be kept for 90 days before being overwritten.	▸ Important data (e.g. Database files) and configurations should be backed-up daily and verified weekly. ▸ Backups should be verified at least once a month (verification should include file size, file integrity and date stamp).
Patching/Anti-virus protection A patch is a piece of software designed to fix holes or improve vulnerabilities in existing software and systems. By not patching, the network is left vulnerable for an attacker to exploit with ease using already defined scripts.	▸ Ensure Anti-virus updates, exclusions, scheduling of regular scans, and device coverage is in place and appropriate. ▸ Confirm Windows patching is automated and/or performed regularly and reliably if using a manual process.	▸ Critical security patches should be deployed as soon as they are released.	▸ Regularly check that anti-virus and operating system patches have been successfully installed. ▸ Regularly update your business applications (including web browsers) to address security vulnerabilities.

Deloitte.

NZ6898-1 02/18

Incident response and recovery

	Minimum security	Better practice	Best practice
Logging Without logging, investigating an incident can be challenging and can make it difficult to investigate the extent of damage and/or data loss, and determine the cause of an attack.	▸ Ensure that all Windows Security Event Logs are turned on, enable log archiving and keep logs for as long as possible for all Windows servers. ▸ If you are using Microsoft Office 365 for email, the mailbox audit logs should be enabled. ▸ Extend logging retention on the firewall to three months or the maximum the firewall device can support. ▸ Confirm the following logs (Security, Remote Connection Manager, RDP, Local Session Manager) are functioning correctly for all Windows servers.	▸ Implement centralised log collection and/or check logs regularly for: failed login attempts, remote access from unknown/ international IP addresses, unknown actions by privileged accounts, port scanning of sensitive services, and unusual network traffic flows. ▸ Regularly archive/transfer logs on to a secure/offline server.	▸ Implement a Security Incident and Event Management (SIEM) platform or a modern machine-learning security monitoring platform to alert if any unusual and suspicious activity takes place.
Disaster recovery Without a disaster process, it can be hard to resume business operations and recover data.	▸ Establish formal security expectations with IT providers and agree on roles and responsibilities. ▸ Establish an incident response process plan that includes who within your business can make decisions and a requirement to preserve data in the case of a security incident.	▸ Arrange to be supported if an incident occurs, which may include a cyber insurance policy backed by a strong incident response partner and/or a security and incident specialist who is on call. ▸ Practice your incident response plan with tabletop exercises, as it's vital that the response team knows what to do if an incident happens.	

Employee awareness and education

	Minimum security	Better practice	Best practice
Staff awareness Humans are often the weakest link in IT systems. By raising staff awareness, common social engineering/attack techniques can be avoided, as staff are able to better identify threats.	▸ Raise staff awareness about common social engineering techniques by sending out emails periodically reminding them to be vigilant. ▸ Outline steps that staff should follow if they detect a cyber incident or social engineering attempt. Establish a mailbox (possibly supported by your IT provider) for them to send suspicious emails to so they can be checked by an expert.	▸ Implement and communicate an acceptable use policy so staff are clear on the use of your business' technology and information.	▸ Conduct regular cyber security training sessions for new and existing staff to keep staff up-to-date on common attacks and trends. ▸ Consider a "phishing simulator" that regularly sends staff fake phishing and malware emails to test and report on their awareness (gamify the learning).

Assessing vulnerability

	Minimum security	Better practice	Best practice
Vulnerability audit Even after regular security upgrades, patching, and testing, new and existing vulnerabilities may appear over time. It is important to test the controls that are in place, and to regularly check for vulnerabilities.	▸ Perform an automated vulnerability scan every 12 months.	▸ Undertake a penetration test by an independent third party. A penetration test is a process by which security experts will attempt to "hack" your systems and identify vulnerabilities.	▸ 'Run tools' to inspect processes running on workstations and servers (e.g. Windows Process Explorer to determine whether they are legitimate). ▸ Proactively identify and check for new and emerging cyber security threats and vulnerabilities. Your IT provider may be able to assist in implementing controls to prevent identified threats.

NZ6898-1 02/18