certnz

Ten critical controls 2019.

CERT NZ has summarised the ten controls that would mitigate, or better contain, the majority of information security incidents that we've analysed so far.

CERT NZ's ten critical controls for 2019 are intended to help you decide what to spend your time and money on. They're based on the incidents that we've seen to date, as well as other sources that we have privileged access to. This includes the global CERT network, and international data feeds. We update the list every year based on the data we receive.

We'll publish more details about the importance of each control on **www.cert.govt.nz.** We also explain how to implement them there.

This is not a complete list. We recommend you continue with your own best practices, like maintaining an effective password policy.

Report anything that breaches, or almost breaches, your defences to us — even if you don't need help. Your reports give us rich data that we use to assess the current threats facing New Zealanders.

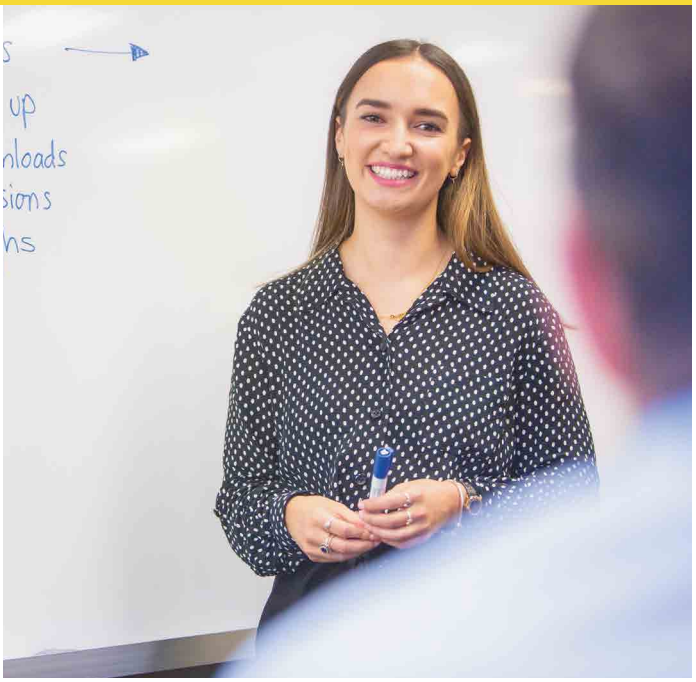
New Zealand Government

Ten critical controls 2019.

1. Enforce multi-factor authentication (MFA)

Credential dumps and credential harvesting attacks are common. They give attackers access to large numbers of usernames and passwords. Protect your business systems and data by enabling MFA on all privileged or remote access systems. This includes VPNs, administrative consoles, webmail and published applications like Citrix.

We saw several phishing campaigns focused on credential harvesting in 2018. One example was the Office365 campaign. In the cases we saw, enabling MFA would have prevented unauthorised access to the accounts with leaked credentials.



2. Patch your software

Keep software, like operating systems and applications, up-to-date. It's one of the most simple and effective steps you can take to secure your environment.

We've seen many organisations attacked by malware that exploits known vulnerabilities. Applying patches would have helped them avoid these attacks.

3. Disable unused services and protocols

Keeping your systems up-to-date isn't always enough to keep attackers away. Older services and protocols often have their own vulnerabilities. Leaving them on your network gives attackers more opportunity to breach your network. To mitigate this, scan your network for services and protocols that are:

- no longer used, or
- known to be vulnerable.

If you identify any, carry out remediation based on your findings. The recent WannaCry incident demonstrated what can happen when attackers exploit out-of-date protocols.

4. Change default credentials

Security is sometimes overlooked in the rush to get a new piece of technology into production. A key step to take for any new application or device is to change or remove all default credentials. This prevents an attacker gaining access to your network by using known usernames and passwords.

We continue to see organisations compromised by attackers using unchanged default credentials.

5. Implement and test backups

Backups are critical for recovering from incidents like ransomware. Store your backups offline, and test them often. Organisations often need to restore data from their latest backup in response to threats like ransomware.

We've seen organisations lose data and incur significant operational costs because they didn't have up-to-date, well-maintained backups.

6. Implement application whitelisting

Two of the most common ways to infect a user's workstation with malware are through email clients and web browsers. To prevent this, identify a list of applications that your users need. Make sure they can only execute approved applications.

Most malware incidents reported to CERT NZ are thought to have originated from:

- opening malicious email attachments, or
- drive-by downloads.

Whitelisting the approved applications will help protect the system from these attacks. It's a key security control for your network.

7. Enforce the principle of least privilege

Grant users the minimum level of access and control in your network that they need to do their job. Remove their accounts when they're no longer needed. This will limit the damage that intrusions into your network can cause. We also recommend enforcing separation of privilege. When a user requires administrative privileges, use a separate account.

We're aware of incidents where users held unnecessary administrative privileges. Attackers were able to exploit their accounts to make unauthorised changes to the environment.

8. Configure centralised logging and analysis

Storing and securing your logs in a central place makes log analysis and alerting easier. Logs are a key part of understanding what happened in an incident. Configuring alerts for key actions can help you detect abnormal behaviour, and tell you what to investigate. Without good logging, it's very difficult to discover the nature and extent of a compromise. This makes your efforts to contain and recover from an incident much harder.

Logs weren't available for many of the incidents reported to CERT NZ. This meant it wasn't possible to do a complete post-incident investigation.

9. Implement network segmentation

Proper network segmentation relies on the implementation of other critical controls, in particular:

- disabling unused services and protocols, and
- enforcing the principle of least privilege.

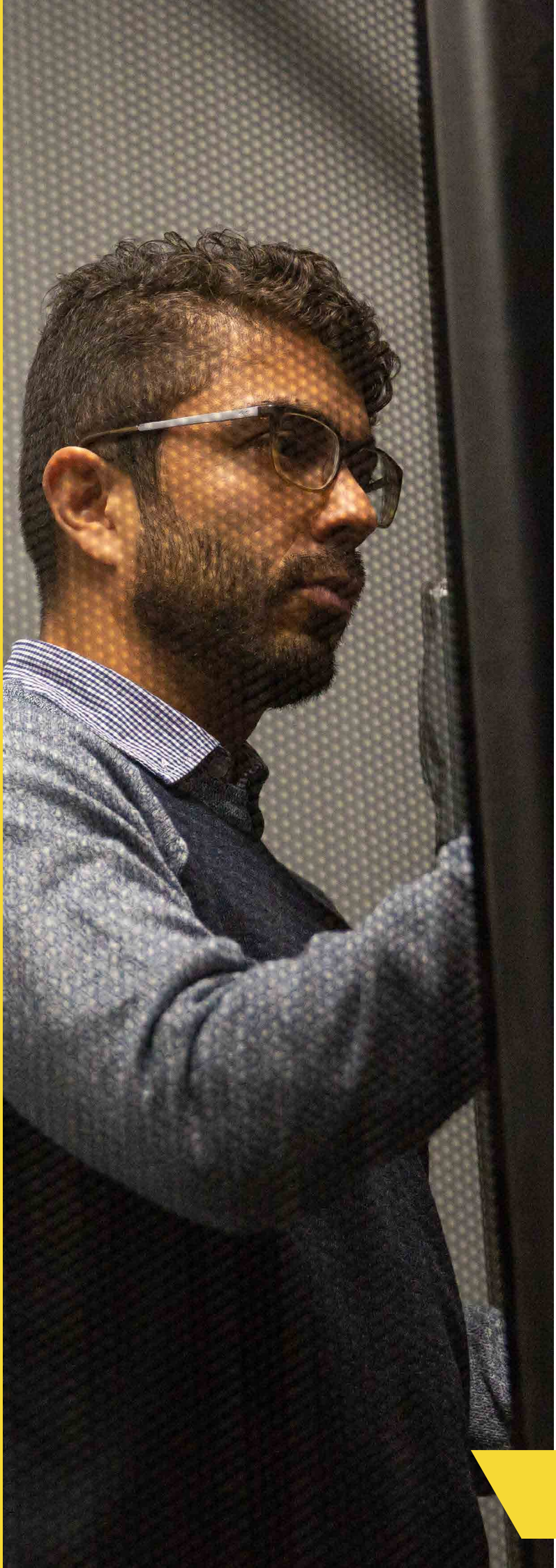
We've seen incidents where attackers used common management tools and protocols to gain control of other machines on a network. There are also tools that are scripted to get credentials. These credentials are then used to access other devices and applications in your network.

You can prevent attackers spreading through your network by using network tools like firewalls, as well as following the other critical controls.

10. Manage cloud authentication

We're aware of incidents where cloud authentication misconfigurations allowed attackers to bypass security controls. They do this by using legacy authentication protocols. Organisations are also moving toward using more cloud-based services. It's easy to end up in a situation where you have multiple authentication systems.

Centralising authentication gives you better control and visibility over who has access to your systems and information. It also provides a unified experience, and lets you configure MFA for applications that may not support it.



Ten critical controls 2019

1. Enforce multi-factor authentication (MFA)
2. Patch your software
3. Disable unused services and protocols
4. Change default credentials
5. Implement and test backups
6. Implement application whitelisting
7. Enforce the principle of least privilege
8. Configure centralised logging and analysis
9. Implement network segmentation
10. Manage cloud authentication

About CERT NZ

We work to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. We provide trusted and authoritative information and advice, while also collating a profile of the threat landscape in New Zealand.

To report an information security incident, visit **www.cert.govt.nz**