certnz

CERT NZ's critical controls 2020.

This is the third year of CERT NZ's ten critical controls for organisations. These controls would prevent, detect, or contain most of the attacks we've seen in the past year.

It can be challenging to prioritise the right security controls to improve your organisation's security. CERT NZ's ten critical controls for 2020 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.

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.

www.cert.govt.nz

New Zealand Government

Ten critical controls 2020.

01 Patch your software and systems

Keeping software, like operating systems and applications, up-to-date continues to be one of the most cited controls in our list. Most of our advisories in 2019 related to vulnerabilities that could be mitigated if the systems were timely patched.

Patching oftens fits well in an organisation's asset management lifecycle. It is a key step in making sure that assets are maintained and kept secure over their lifetime. We listed patching as a separate control from asset management due to its complexity.

02 Disable unused services and protocols

Legacy systems frequently contain business critical data, or support important processes, which is why they're often left alone. However, business critical systems warrant the highest levels of security and maintenance.

Replace or upgrade any systems in your network that are not being maintained or receiving security updates. Several attacks this year have exploited legacy software such as Windows XP.

03 Implement and test backups

Backing up your data is a critical corrective control if you are hit with a security incident. Hopefully your organisation will not face security incidents regularly, however it's best to be prepared. Testing your backups regularly will ensure that your backups will work when you really need them.

Ransomware attacks are often highlighted in our quarterly reports because they happen often and have massive impacts to an organisation. Backups can reduce those impacts and allow your organisation to roll back to before the ransomware started.

04 Implement application whitelisting

Application whitelisting is a control that can prevent unauthorised files from executing on your computer. Application whitelisting works by creating a list of applications that are authorised to run and all others are blocked.

Malware is often delivered by email or through web browsing. A user might be tricked into downloading a file and opening it, which can cause the malware to execute. Application whitelisting can prevent these malicious files from executing.

05 Enforce the principle of least privilege

The principle of least privilege means granting users the minimum level of access they need to perform their job. This prevents users from accidentally or intentionally making changes that cause security incidents. It also prevents an attacker from getting very far if they manage to steal a user's account credentials.

It can also mean creating separate accounts for users if they use normal and administrative privileges in a system. That way you can set more logging and authentication requirements for the administrative accounts since those are more valuable to an attacker.

06 Configure centralised logging and analysis

Logging is an important control for understanding what's happening in your network. It can help you detect when a security incident has occurred and prevent them from happening again. Your logs should be configured and stored in a central place so it makes analysis easier.

Turning notifications on for unusual events, such as unusual user geolocation or disabling MFA, can help alert you to an attacker in your network. Checking these alerts could help you identify an incident that's underway and stop it from continuing.

07 Implement network segmentation

Network segmentation means breaking down your network into smaller networks and setting access controls to manage connections across them. It allows your organisation to set more granular security controls on the smaller networks that have critical data or systems.

Without effective network segmentation, attackers can move around your network and gain access to additional systems. Implementing network controls limits an attacker's access once they enter your network.

08 Manage authentication

This control is aimed at protecting authentication to your organisation's systems. It recommends changing default credentials and making sure each account has a strong, unique password. Password reuse is still a large factor in incidents, and an easy way for an attacker to get in.

Configuring multi-factor authentication and your central identity provider helps to protect your organisation's accounts so others can't pretend to be you.

09 Follow an asset management lifecycle

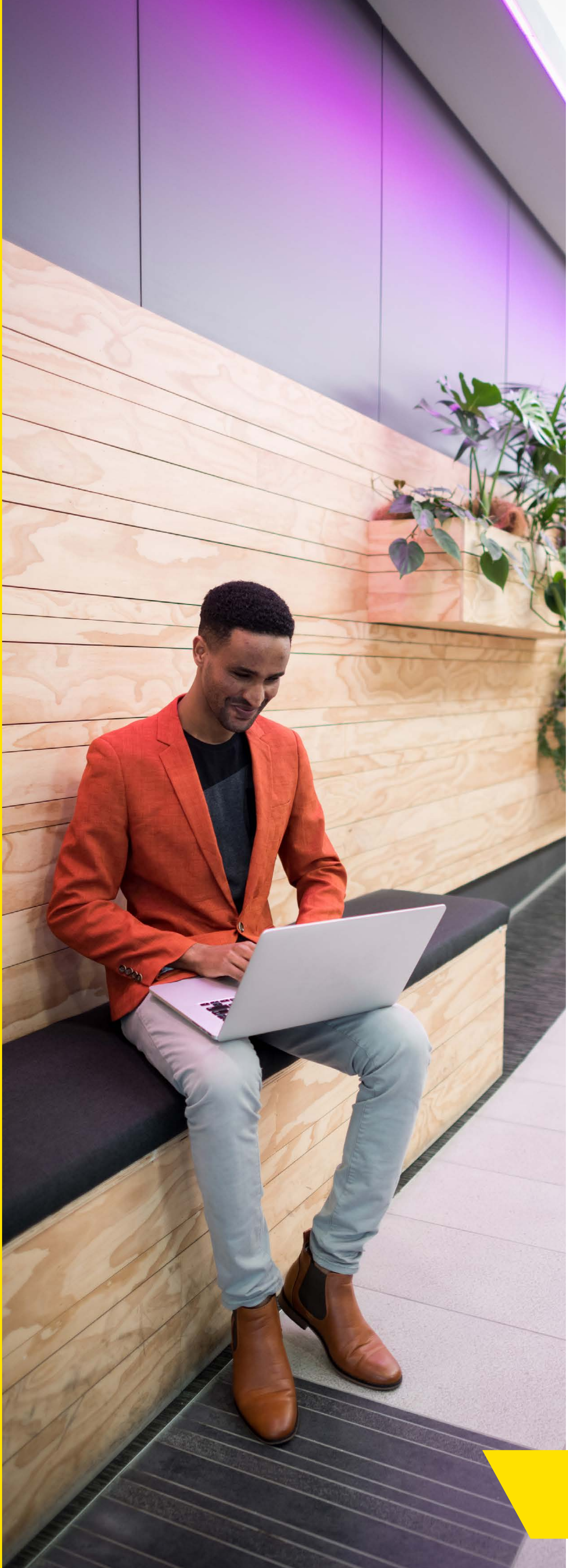
It is important to know what assets are connected and running in your network. An asset management framework allows your organisation to track assets throughout their life, including purchase, development, maintenance, and disposal.

As your organisation grows, so does your number of assets and systems. Without an asset management framework, you could forget to harden, patch, or decommission systems.

10 Set secure defaults for macros

Macros are small programs that can be run in office productivity software, like Microsoft Office. Attackers often use macros for hiding malicious programs. CERT NZ has noticed popular malware families, like Emotet, have been using macros to infect targets and spread.

Using secure defaults and configurations for macros in your organisation can prevent these incidents. If your organisation does not use macros, disabling macros entirely can protect your users from making a mistake. If your organisation does use macros, forcing them to run in sandboxed environments will reduce their impact and reach within your network.



Ten critical controls 2020.

1. Patch your software and systems
2. Disable unused services and protocols
3. Implement and test backups
4. Implement application whitelisting
5. Enforce the principle of least privilege
6. Configure centralised logging and analysis
7. Implement network segmentation
8. Manage authentication
9. Follow an asset management lifecycle
10. Set secure defaults for macros

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**