certnz

CERT NZ's critical controls 2021.

Each year, we review our critical controls against the incidents we have seen over the past 12 months. When correctly implemented, these controls would prevent, detect, or contain the majority of the attacks we've seen in the past year.

CERT NZ's ten critical controls for 2021 are designed to help you decide where best to spend your time and money. They summarise the controls that would mitigate the majority of information security incidents that CERT NZ has analysed.

These have been developed based on the data and insights we received from reports and international threat feeds. We update the list every year based on the data we receive.

We provide 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 2021.

01 Patch your software and systems

Keeping all software, from operating systems and applications to firewalls and routers, up-to-date continues to be one of the most cited controls in our list.

The majority of the advisories we released in 2020 were related to vulnerabilities that could be mitigated if the systems were patched in a timely manner.

02 Implement multi-factor authentication and verification

This control is focused around enforcing the use of multi-factor authentication (MFA), especially for accounts accessible from anywhere on the internet or accounts with administrative access.

We see a large number of reports relating to unauthorised access, which are often caused by weak credentials. Enforcing MFA is the most effective control for preventing unauthorised access.

We also see incidents where business processes lack a verification step. In this control we emphasis the importance of strong business processes.

03 Provide and use a password manager

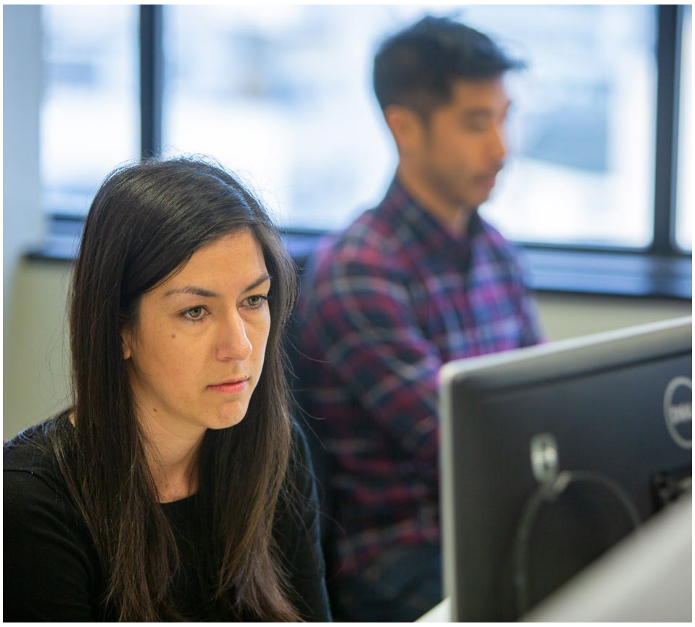
Even with MFA in place, a strong unique password is still important. Giving your people the tools to make this easy increases the likelihood of them using strong passwords that are different for each system. It also makes it easier to manage shared passwords such as your business' social media accounts.

The important point of this control is that your organisation should be providing your staff with a password manager tool that works for them. Without the right tools, your staff won't be able to make strong passwords.

04 Configure logging and alerting

Logging and alerting are key to incident detection and investigation efforts. Having a central logging system, which contains feeds from all your endpoints, is the first step in having visibility of all activity in your environment.

The second step is identifying key events that alert you to incidents, and setting up actionable alerts to let you know when something unexpected happens.



05 Secure internet-exposed services

Keeping unused and unnecessary services running on a system can leave it vulnerable, especially if the host is exposed to the internet. Disabling these services, or segmenting them so they are not exposed unnecessarily, can reduce the risk and your attack surface.

For services that need to be exposed to the internet, you need to ensure you keep them secured. This includes requiring MFA for any authentication that is exposed, and making sure the service itself is up-to-date.

06 Implement and test backups

Most organisations these days are reliant on their systems, and the data they hold. Significant disruption to the availability of this data can be devastating, whether it was caused by a cyber security incident, or simply an accident. In these situations, being able to restore from backup quickly makes all the difference.

Ransomware attacks are often highlighted in our quarterly reports because they happen regularly and have significant impacts to an organisation. Backups can reduce those impacts and allow your organisation to restore the lost data in the most cost effective way.

07 Implement application allowlisting

Malware campaigns continue to cause significant disruption. Application allowlisting (otherwise known as whitelisting) is a control that can prevent unauthorised files, such as malware, from executing on your computer.

Modern endpoint protection software can fulfil the intent of this control and give you visibility into potentially malicious activity in your environment. However you choose to implement this control, it gives your organisation greater protection against malware attacks such as ransomware.

08 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 either accidentally or intentionally making changes that can cause security incidents.

It also strongly reduces the risk an attacker can get very far into the system or network if they manage to steal a user's account credentials.

09 Implement network segmentation

Network segmentation means breaking down your network into smaller segments 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.

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. We 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 2021.

1. Patch your software and systems
2. Implement multi-factor authentication and verification
3. Provide and use a password manager
4. Configure logging and alerting
5. Secure internet-exposed services
6. Implement and test backups
7. Implement application allowlisting
8. Enforce the principle of least privilege
9. Implement network segmentation
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**