SSS Review of CERT NZ Critical Controls 2018

The New Zealand Computer Emergency Response Team (CERT NZ) has released a list of ten critical controls for 2018 which you can see here: https://www.cert.govt.nz/it-specialists/guides/10-critical-controls/

According to CERT NZ, these 'would mitigate, or better contain, the majority of attacks we've seen', and are based on the incidents they have analysed to date. CERT NZ are continuing to publish more information on the critical controls – here: https://www.cert.govt.nz/it-specialists/critical-controls/

CERT NZ is not the only organisation to publish a list of prioritised critical security controls. Two other organisations that do this, and which are often referenced by New Zealand organisations, are the Australian Signals Directory (ASD), and the American Center for Internet Security (CIS). Below we have provided a rough mapping of controls from ASD and CIS against the ten controls published by CERT NZ (the number next to each control indicates the priority placed on that control by the respective organisations):

CERT NZ	ASD	CIS
1. Patch software - Includes OS, firmware, software and applications	2. Patch applications 6. Patch operating systems	4. Continuous Vulnerability Assessment and Remediation
2. Upgrade or replace legacy systems		
3. Disable unused services and protocols	18. Server application hardening 19. Operating system hardening	3. Secure configurations for hardware and software
4. Application whitelisting	1. Application whitelisting	2. Inventory of authorised and unauthorised software
5. Change default credentials		
6. Multi-factor authentication	7. Multi-factor authentication	
7. Privilege management	5. Restrict administration privileges	5. Controlled use of administration privileges
8. Implement and test backups	8. Daily backups	10. Data recovery capability
9. Centralised logging	17. Continuous incident response 37. Capture network traffic	6. Maintenance, Monitoring, and Analysis of Audit Logs
10. Manage mobile devices		

The "Gaps"

Below we comment on the CERT NZ 10 areas that don't have a clear or direct mapping to the AD and CIS controls.

2. Upgrade or replace legacy systems

It is feasible to apply virtually all the controls to this from both the ASD and CIS. The key point is that legacy systems often run unsupported operating systems, firmware, applications or hardware, and thus cannot have adequate security controls applied across them. In replacing or upgrading these systems you increase your capability to apply effective security controls across your environment.

SSS – IT SECURITY SPECIALISTS
A division of Scientific Software & Systems Ltd.

Level 8, IBM Tower, 25 Victoria Street
Petone, Lower Hutt 5012
PO Box 38490, Wellington Mail Centre
Lower Hutt 5045, New Zealand

P +64 4 917 6670
E sales@sss.co.nz
W www.sss.co.nz

5. Change default credentials

It is possible that this recommendation is taken for granted by ASD and CIS in that this is effectively a 'security 101'. ISO27002:2013 mentions it as part of implementation guidance for A.9.2.4 'Management of secret authentication information of users' - *g) default vendor secret authentication information should be altered following installation of systems or software*. It is certainly worthy of inclusion as this is one of the most fundamental procedures that should be done for all new systems. One of the first things an attacker will do is to Google manufactures UID and password for *'insert name of hardware/ application'* and see if it works! This issue is also starting to be addressed by manufacturers themselves where some new systems will enforce a change of UID and password before the system can be put into production.

9. Centralised logging

We have been quite generous in mapping "17. Continuous incident response" and "37. Capture network traffic" from the ASD to the NZ Cert number "9. Centralised logging". The principle here is you cannot have the ASD controls in absence of logging capabilities.

10. Manage mobile devices

You should manage mobile devices in the same way you manage all other systems connected to your organisation's network. In a modern society, business mobile devices (smart phones, tables, surfaces) are all capable of accessing, storing and processing confidential information in much the same way a traditional endpoint (laptop, desktop) can. As such, you should in general apply the same level of control on these devices as you would with a traditional endpoint. There are several ways you can do this depending on how you manage access to information through your policy (access control, acceptable use, BOYD, mobile device management etc.) and how you enforce these policies with the available technical controls on the device itself.

Summary

The first point to make is that this is good advice from CERT NZ, and we recommend that all organisations take heed and put in place the controls as best they can, as soon as they can.

Not surprisingly there is a significant overlap across these three control frameworks, no doubt because the threats CERT NZ sees here in New Zealand do not differ greatly from what is being seen overseas.

All three of these control frameworks are directed at technical controls and are IT centric in their focus. In reviewing and implementing these, it is critical to remember that all good security practices are underpinned by an effective governance model and a solid foundation of policies and procedures endorsed by your leadership team and followed in practice. The absence of these can make security hard to implement effectively and difficult to enforce for any lasting improvements. Information Security should become part of how you do business and be an intrinsic part of your organisation's culture and business practices rather than a set of technical implementations.

SSS has the expertise and experience to help you put in place effective and lasting information security improvements across your organisation. If you'd like to discuss how we could help your organisation, please contact your SSS Account Manager, or call us on 04 917 6670 or email us at sales@sss.co.nz.

Level 8, IBM Tower, 25 Victoria Street
Petone, Lower Hutt 5012
PO Box 38490, Wellington Mail Centre
Lower Hutt 5045, New Zealand
P +64 4 917 6670
E sales@sss.co.nz
W www.sss.co.nz