NZ Incident Response Bulletin

Standard Edition – August 2021

The NZ Incident Response Bulletin is a monthly high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month. Each Bulletin also includes a section of our own content, based on a trending theme. We'll give you a brief summary of each article, and a link to more information. Why do we publish this bulletin? Because we want to keep you up to date with the latest Forensic and Cyber Security news, so that you aren't caught by surprise – and you'll know about risks and changes before they become problems.

Refer to our Premium Edition for additional information on Threat Alerts, Security Frameworks, Information Security Surveys, Forensic News and Research.

News:

A high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month.

New Zealand

GCSB boss warns cyber attacks getting more sophisticated

Cyberattackers are getting smarter and the attacks more sophisticated. A North Island kindergarten association is among hundreds of groups hit by a cybercriminal gang believed to be based in Russia. The REvil group is believed to be responsible for the attack targeting users of its remote IT management software Kaseya VSA. Andrew Hampton, who is the director-general of the Government Communications Security Bureau, says the international "threat-scape" is changing.

Government points finger at China over cyber attacks

The government says it has uncovered evidence of Chinese state-sponsored cyber-attacks in New Zealand. The Government Communications Security Bureau (GCSB) Minister Andrew Little said that the foreign intelligence agency has established links between Chinese state-sponsored actors known as Advanced Persistent Threat 40 (APT40) and malicious cyber activity in New Zealand. The GCSB had "worked through a robust technical attribution process" to establish its conclusions, Little said. He reported that the government is joining other countries in strongly condemning what the Chinese Ministry of State Security has been doing both in New Zealand and globally.

Businesses' Attitudes To Cyber Security Shifting, But More Work To Be Done

While businesses' attitudes to cyber security are shifting, three in five small businesses believe they should be doing more to keep secure online, says CERT NZ. According to research from the government cyber security agency CERT NZ, the majority of small businesses with an online presence understand the importance of protecting their website.

Developing cyber resilience for financial advice providers

The new financial advice regime came into force on 15 March 2021. Entities and individuals granted a full Financial Advice Providers (FAP) licence under the Financial Markets Conduct Act 2013 (FMC Act) will be subject to the standard conditions for full FAP licences.

Standard condition 5 sets out requirements around business continuity and technology systems, particularly for maintaining information security of technology systems which, if disrupted, would materially affect the financial advice service.

NZ Incident Response Bulletin

Standard Edition – August 2021

World

Essential Eight Maturity Model Updated

The Australian Cyber Security Centre (ACSC) has refreshed its implementation guide, which now sees all of the strategies become essential. “The Essential Eight Maturity Model now prioritises the implementation of all eight mitigation strategies as a package due to their complementary nature and focus on various cyber threats,” the ACSC said. “Organisations should fully achieve a maturity level across all eight mitigation strategies before moving to achieve a higher maturity level.”

Pegasus: Who are the alleged victims of spyware targeting?

Activists, journalists and politicians are among those believed to have been targeted by spyware developed by a private Israel-based firm, according to a new investigation. They are on a list of 50,000 phone numbers of people believed to be targeted by clients of the company, NSO Group, since 2016, that was leaked to major news outlets. Its Pegasus software infects iPhones and Android devices to enable operators to extract messages, photos and emails, record calls and secretly activate microphones and cameras. NSO denies any wrongdoing. It says the software is intended for use against criminals and terrorists and is made available only to military, law enforcement and intelligence agencies from countries with good human rights records.

Uber found to have interfered with privacy of over 1 million Australians

The Office of the Australian Information Commissioner (OAIC) has determined that in 2016, Uber interfered with the privacy of over 1 million Australians. Australia's Information Commissioner and Privacy Commissioner Angelene Falk said US-based Uber Technologies Inc and Dutch-based Uber B.V. failed to appropriately protect the personal data of an estimated 1.2 million Australian customers and drivers, when it was accessed from a breach. It came to light in late 2017 that hackers had stolen the data and instead of notifying those impacted, Uber concealed the breach for more than a year and paid a hacker to keep it under wraps.

Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says

Up to 1,500 businesses around the world have been affected by a ransomware attack centered on U.S. information technology firm Kaseya, its chief executive said on Monday. Fred Voccola, the Florida-based company's CEO, said in an interview that it was hard to estimate the precise impact of Friday's attack because those hit were mainly customers of Kaseya's customers.

Saudi Aramco data breach sees 1 TB stolen data for sale

Attackers have stolen 1 TB of proprietary data belonging to Saudi Aramco and are offering it for sale on the darknet. The Saudi Arabian Oil Company, better known as Saudi Aramco, is one of the largest public petroleum and natural gas companies in the world. The oil giant employs over 66,000 employees and brings in almost $230 billion in annual revenue. The threat actors are offering Saudi Aramco's data starting at a negotiable price of $5 million. Saudi Aramco has pinned this data incident on third-party contractors and tells BleepingComputer that the incident had no impact on Aramco's operations.

Summary of last month’s Cyber Alerts and News Clips:

Incident Response Solutions posts certain alerts and tips we consider to be in the public interest as it comes to hand. We publish these alerts and tips on our YouTube Channel and this webpage.

Alerts

15 July 2021 – CERT NZ - SonicWall urgent security notice

2 July 2021 – CERT NZ - Critical vulnerabilities in Microsoft Windows Print Spooler service

2 July 2021 – CISA - Kaseya VSA Ransomware Compromise

News Clips

7 July 2021 - Hackers Demand $70 Million To Unlock American Devices

NZ Incident Response Bulletin

Standard Edition – August 2021

Our Views: CIS Controls 4-6

This month we take a deep dive into CIS controls 4, 5 and 6. Controls 4 and 6 have seen the most change in structure from CIS controls version 7 to version 8, with multiple version 7 controls being consolidated to produce these controls in version 8.

CIS Control 4: Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Why is it needed?

Network infrastructure and devices are often purchased pre-configured or with an operating system and applications pre-loaded. Whilst this offers convenience to a business, these default configurations are often designed for ease of use rather than security. This leaves them vulnerable to attackers who search for weaknesses such as open services and ports, default credentials and gaps or inconsistencies in firewall rules to penetrate defences and gain access to your network. This control emphasises the need to develop, review, manage and report on the secure configuration of all endpoint and network infrastructure devices.

How is it implemented?

Meeting this control at a basic level requires establishing and maintaining a secure configuration process, configuring automatic session locking on enterprise assets, and implementing and managing a firewall on servers and end-user devices. It also requires you to manage enterprise assets and software using version-controlled-infrastructure-as-code. Administrative interfaces must be accessed over secure network protocols, and default accounts on all enterprise software and devices managed.

The creation and ongoing management of a secure configuration can be challenging and take some time and effort; however, publicly available resources can be leveraged. There are many security baselines available for each system, starting with publicly developed, vetted, and supported security benchmarks and guides is recommended such as:

- The CIS Benchmarks™ Program
- The National Institute of Standards and Technology (NIST®) National Checklist Program Repository

These baselines are an excellent place to start; however, what constitutes a secure baseline is very contextual and therefore differs for each organisation. A clear understanding of your business security objectives and risk appetite is crucial, and these baselines should be adjusted or added to as required, to fit your security requirements. Any adjustments should be recorded.

Developing a secure baseline image involves multiple steps starting with determining the risk classification of the data stored and used by each asset as high, moderate, or low, which will then drive the security requirements. An example of further steps to build a secure baseline image can be found on the CIS website. Further advanced safeguards should be considered once the basics are implemented.

CIS Control 5: Account Management

Use processes and tools to assign and manage credentials for user, administrator and service accounts for enterprise assets and software.

Why is it needed?

This control is critical and focuses on ensuring good user account hygiene and maintenance. Inactive user accounts are often targeted by attackers for use in impersonation and fraud. As these accounts represented a legitimate user (at some point in time), their unauthorised use can be harder to detect. Additionally, insiders may use these accounts to access systems and data outside of their authorisation level or conduct malicious activities. Administrative or highly privileged accounts are a particular target. These accounts enable an attacker to have greater control and do more damage to the network. Service accounts are also vulnerable as they are often shared amongst teams and require strong management.

NZ Incident Response Bulletin

Standard Edition – August 2021

Additional ways accounts can be vulnerable to attack include leaving service accounts embedded in applications for scripts, employees using the same password as one they use for another online account that has been compromised, social engineering schemes which trick a user into giving out their password, and the presence of malware that captures passwords or tokens in memory or over the network.

How is it implemented?

Account Management can be effectively controlled using properly configured systems or centralised authentication. Meeting this control at a basic level involves:

- Developing appropriate password policies and guidance
- Creating an inventory of credentials and tracking these
- Tracking all accounts and disabling and removing these from the system.
- Conducting periodic audits, paying particular attention to administrative, service, and high privileged accounts.
- Creating separate administrative and basic accounts to reduce risk should a basic account be compromised.
- Using Single Sign On (SSO), Multi-factor Authentication (MFA) and Password Manager applications where appropriate.
- Automatically logging users out of the system after a period of inactivity.
- Training users to lock screens and be cyber aware.

Centralising account management through a directory or identity service is recommended as an advanced step.

CIS Control 6: Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Why is it needed?

Attackers often gain access to less secure systems as a starting point, and then traverse the network to locate sensitive data. Minimising the risk of this involves understanding where sensitive data resides. To prevent attackers misusing privileges, strong access control management is necessary.

How is it implemented?

Whilst CIS control 5 manages account creation and deletion; this control is about effectively determining what access all accounts have and ensuring users only have access to the data or enterprise assets appropriate for their role. Strong authentication must also be enabled for critical or sensitive data or functions.

Meeting this control involves creating a process for granting and revoking access. This process should be based on enterprise roles and need and be implemented through role-based access control (RBAC) techniques. RBAC is based on the principle of least privilege and considers privacy requirements and separation of duties.

MFA should be in place for all privileged or administrator accounts as a minimum. MFA should also be enabled for externally exposed applications and remote network access. In addition, specialised Privileged Access Management (PAM) tools, that require a provided one-time password to be checked out for each use, should be considered.

Finally, maintaining an inventory of authentication and authorisation systems and centralising access control for all enterprise assets through a directory service or SSO provider is encouraged for more mature organisations.

Additional protect and detect actions could involve recording unsuccessful logins to admin accounts and configuring systems to alert when these events occur. Requiring administrative tasks only to be performed on machines air-gapped from the rest of the network is also an advanced security control in this area.

CIS controls 4, 5 and 6 have minimum requirements for all organisations regardless of size or maturity to implement. Therefore, we suggest starting with the primary recommendations in each control before considering more advanced implementations and automated systems for managing them.

NZ Incident Response Bulletin

Standard Edition – August 2021

About the Bulletin:

The NZ Incident Response Bulletin is a monthly high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month. Also included are articles written by Incident Response Solutions, covering topical matters. Each article contains a brief summary and if possible, includes a linked reference on the web for detailed information. The purpose of this resource is to assist Executives in keeping up to date from a high-level perspective with a sample of the latest Forensic and Cyber Security news.

To subscribe or to submit a contribution for an upcoming Bulletin, please either visit https://incidentresponse.co.nz/bulletin or send an email to bulletin@incidentresponse.co.nz with the subject line either "Subscribe", "Unsubscribe", or if you think there is something worth reporting, "Contribution", along with the Webpage or URL in the contents. Access our Privacy Policy.

About Incident Response Solutions Limited:

Our Purpose - We help you with specialist forensic, cyber security and crisis management expertise at all stages throughout the incident response lifecycle.

Our Promise - We will provide you with the confidence you require to prepare, respond and recover from forensic and cyber incidents.

Our specialist Forensic Technology expertise includes Computer Forensics, Cybercrime Incident Response, Social Media Analysis and eDiscovery. We have significant experience in providing expert witness reports and in delivering expert witness testimony at trial. Our background includes experience in Law Enforcement (NZ Police) and Big 4 Professional Services.

Campbell McKenzie
Director
Incident Response Solutions Limited
0800 WITNESS
+64 21 779 310
campbell@incidentresponse.co.nz

This Bulletin is prepared for general guidance and does not constitute formal advice. This information should not be relied on without obtaining specific formal advice. We do not make any representation as to the accuracy or completeness of the information contained within this Bulletin. Incident Response Solutions Limited does not accept any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, when relying on the information contained in this Bulletin or for any decision based on it.

Further Resources:

Alerts	Data Breach Response	Forensic Technology
Cyber Incident Simulations	Social Media Investigations	Guide for NZ Law Firms

Share our Bulletin: