NZ Incident Response Bulletin

Standard Edition – September 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

Bank could not stop woman sending $30,000 to fake boyfriend

A woman who tried to send $30,000 to a fake boyfriend in the United States refused to believe bank staff who told her she had been scammed. The woman tried to make the transfer via BNZ earlier this year. Staff questioned her about what the money was for and she eventually revealed it was so her boyfriend, whom she had met on the internet, could come to New Zealand.

"She had started an internet relationship with a man who she believed was the head surgeon in a hospital in Kabul," said BNZ head of financial crime Ashley Kai Fong. Cryptocurrencies were also beginning to show up in other scams as the scammers rely on its anonymity and lack of regulation to extract stolen money. "We're now seeing scammers make direct transfers to cryptocurrency exchange services from victims accounts. At that point the money is as good as gone, quickly transferred on market to a traceless cryptocurrency like bitcoin, and then transferred on again to a totally unidentifiable 'wallet' elsewhere in the world, where the scammer can easily and cleanly transfer it back into a currency of their choice," he said. Other common scam types were remote access scams and scams masquerading as government services.

Businesses warned to be vigilant of scams, hacking during lockdown

Businesses and organisations are being urged to protect their customers from cyber hacks as more people work remotely during the lockdown. New research from BNZ shows nearly 80 percent of the public have been targeted by an online scam and a quarter have fallen victim to one. The average amount of money lost to a scam was $1,638, the research shows. Many of these scams pretended to relate to missed online deliveries, invoice scams, and attempts to try and charge people for Covid-19 vaccines.

Ministry of Justice survey: Cybercrime and sex attack victims reluctant to involve police

Victims of computer crime and sex attacks are unlikely to come forward due to shame and fear of reprisal, according to a just-released survey. The latest Ministry of Justice New Zealand Crime and Victim Survey shows that although more people are reporting assaults only a quarter of all illegal activity is ever brought to police attention. While motor vehicle crime had an 89 per cent likelihood of being reported, cybercrime and sexual assault were the least-likely, with up to 93 per cent of violations going unreported.

COVID-19 lockdowns make New Zealand business sitting ducks for a cyberattack

Lockdowns forcing New Zealanders to work from home have cyber security experts predicting a super-spread of cyberattacks across the country. While large companies are generally the target of cyber criminals, Wellington-based cyber security expert Samrat Choudhury warns that now anyone is fair game. "Lockdowns are hunting season for cyber criminals," says Choudhury, "Microsoft has reported eight trillion attacks across its systems every day."

"Although large companies are frequently targeted, what we have noticed in previous lockdowns in New Zealand and Australia is that cyber criminals have begun to heavily target small and medium sized businesses."

NZ Incident Response Bulletin

Standard Edition – September 2021

World

Microsoft: ProxyShell bugs "might be exploited," patch servers now!

Microsoft has published guidance for the actively exploited ProxyShell vulnerabilities impacting multiple on-premises Microsoft Exchange versions. ProxyShell is a collection of three security flaws (patched in April and May) discovered by Devcore security researcher Orange Tsai, who exploited them to compromise a Microsoft Exchange server during the Pwn2Own 2021 hacking contest. Although Microsoft fully patched the ProxyShell bugs by May 2021, they didn't assign CVE IDs for the vulnerabilities until July, preventing some organisations with unpatched servers from discovering that they had vulnerable systems on their networks.

7 Emerging Ransomware Groups Practicing Double Extortion

After a string of high-profile hits in the middle of this year, a number of the largest and most notorious ransomware operations disappeared. Given the massive profit-making potential ransomware still offers, aided by many organisations being under-defended, many security experts believe that the core operators behind Avaddon, DarkSide and REvil will simply set up shop under a different name. Affiliates meanwhile often work with multiple ransomware operations, sometimes simultaneously. Hence, while some groups may appear to come and go, the ransomware business model surges on.

Ransomware gang's script shows exactly the files they're after

A PowerShell script used by the Pysa ransomware operation gives us a sneak peek at the types of data they attempt to steal during a cyberattack. When ransomware gangs compromise a network, they usually start with limited access to a single device. They then use various tools and exploits to steal other credentials used on the Windows domain or gain elevated privileges on different devices. Once they gain access to a Windows domain controller, they search for and steal data on the network before encrypting devices. The threat actors use this stolen data in two ways. The first is to generate a ransom demand, based on company revenue and whether they have insurance policies. The second is to scare the victims into paying the ransom because the gang will leak the data.

Google, Amazon, Microsoft unveil massive cybersecurity initiatives after White House meeting

The heads of Apple, Google, Amazon, Microsoft and IBM are among the business leaders that met with President Joe Biden at the White House to discuss how the government and private sector can work together to improve the nation's cybersecurity, according to a senior administration official. "Most of our critical infrastructure is owned and operated by the private sector, and the federal government can't meet this challenge alone," Biden said during a brief comment at the start of the meeting. "I've invited you all here today because you have the power, the capacity and the responsibility, I believe, to raise the bar on cybersecurity."

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

Incident Response Solutions post 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

21 August 2021 – CISA – Urgent: Protect Against Active Exploitation of ProxyShell Vulnerabilities

18 August 2021 – CISA – Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches

News Clips

3 August 2021 - Companies search for cyber workers after ransomware attacks

NZ Incident Response Bulletin

Standard Edition – September 2021

Our Views: CIS Controls 7-9

This month we look at CIS controls 7, 8 and 9, marking the half way point in our deep dive of all 18 recommended cybersecurity controls .

CIS Control 7: Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimise, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Why is it needed?

Cyber attackers are always looking for vulnerabilities within systems to exploit. To defend against these attacks your business must ingest multiple sources of threat information and act in a timely fashion on software updates, security advisories, patches and more. After a new vulnerability is found and reported on, by either researchers or the IT community, it is essentially a race between the cyber attackers looking to leverage this vulnerability to cause harm and the defenders. As a business, you must wait for vendors to develop and deploy a suitable patch, report indicators of compromise (IOCs) and produce upgrades to combat the vulnerability. Once this is complete you must assess the risk of the vulnerability to your business, regression test against existing systems and finally install the patch or update. Clearly there is a window in this cycle whereby many organisations remain vulnerable and attackers may leverage the gap. The longer it takes for your organisation to assess the risk and patch your systems the more vulnerable you are to exploits.

As vulnerabilities are now being discovered at pace in our environments, not only does vulnerability management need to be a continuous process, but it requires strong prioritisation of the risks and corresponding patches for deployment. Ongoing monitoring of vulnerabilities is needed as devices may only be connected to your network for brief periods of time. Maintaining visibility in this dynamic environment is crucial.

How is it implemented?

Meeting this control at a basic level initially requires establishing and maintaining a vulnerability management and remediation process. This process should encompass the assessment of new threats, a strong prioritisation method, and action steps and accountability for remediation. The process and remediation should be reviewed at least monthly. Automated Operating System and Application patch management is also a baseline requirement to meet this control. These standard automatic updates must occur monthly or more frequently.

At a more advanced level, a business can consider introducing automated vulnerability scanning of all internal and externally-exposed assets. Remediation of any vulnerabilities found from this automated process should occur on a monthly or more frequent basis.

There are many commercial tools available for network vulnerability scanning, at both a manual and automated level and many of these can be managed remotely. The frequency of scanning needed to discover potential vulnerabilities and remain secure is usually determined by the complexity of your business assets. More frequent scans are necessary with a greater number of vendors in order to align with their different patch cycles. Other tools that assist with vulnerability management include free and commercial tools that review your network assets' security settings and secure configuration. Once again more advanced tools can automatically notify you if settings are inadequate or show unauthorised or unintended changes in your network that may introduce risk.

Scanning tools can be linked to ticketing systems in the overall management process to ensure that any vulnerabilities are remediated quickly. When introducing a vulnerability management process, one recommendation is to use standardised schemes and languages such as Common Vulnerabilities and Exposures (CVE), or Open Vulnerability and Assessment Language (OVAL). Additionally, the NIST's Common Vulnerability Scoring System (CVSS) is a good place to start when introducing vulnerability prioritisation in your process. Adding organisational specific information, such as the potential of a specific threat to impact your business and the likelihood of it occurring, to the information in the CVSS will help to produce a contextually relevant vulnerability prioritisation scheme for your organisation.

NZ Incident Response Bulletin

Standard Edition – September 2021

CIS Control 8: Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Why is it needed?

Writing from an incident response and forensic analysis point of view (rather than a general IT or security standpoint) it is hard to stress enough the importance of suitable log collection, management and analysis. In fact, we could probably write a book on this control alone. Poor log collection or analysis processes can allow an attacker to sit inside a network for lengthy periods without anyone being aware they are there. In contrast, if logs are analysed effectively then intrusions can be discovered and dealt with in a timely fashion.

Log data can also provide critical information around suspected cyber incidents and may at times be the only evidence of a cyberattack. If suitable and complete logs are kept, they can provide valuable insight into a suspected attack such as when and how it may have occurred, how long an attacker may have had access to your systems, what data was accessed, and if any data was exfiltrated.

How is it implemented?

The basic level of this control involves establishing and maintaining an audit log management process. This process defines the organisations logging requirements and specifies the collection, review and retention of all log data. Audit logs across all enterprise assets must be collected in alignment with the log management process and adequate storage for log data maintained.

Most assets and software allow logging capability. It is important to differentiate here between system and audit logs as system logs are generally native to the system and easy to turn on, whereas audit logs require more attention. System logs generally show system related events such as process timing and crashes. In contrast, audit logs show vital information around user events such as number of log ins, time of log ins, file and folder accessed etc. Audit logs require more configuration to enable, however they are essential for visibility into your environment.

Once a basic logging management process is embedded in your business the CIS control recommend the following steps for consideration:

- Configuring two standard synchronised time sources across the environment to enable time synchronisation of logs
- Collecting detailed audit logs for any assets that hold sensitive data. *Note: Despite this being an intermediate step in the CIS controls, we believe this should be seriously considered in today's privacy-aware environment.*
- Collecting DNS query, URL request, and command-line audit logs wherever supported. Firewalls, proxies and remote access systems should all have verbose log data enabled where practicable.
- Centralising all logging by sending all enabled logs to a centralised logging server.
- Retaining all logs for a minimum of 90 days. Ideally, encrypted log data should then be saved (but archived) for an additional 365 days.
- Conducting log reviews on a weekly (or more frequent) basis to detect anomalies that may indicate a threat.
- Collecting service provider logs where available such as authorisation events.

Finally, it is wise to regularly perform simulations to test your logging and ensure appropriate logs are generated and able to be accessed for each suspicious event. This is a key part of being forensically prepared to respond to any cyber incident.

NZ Incident Response Bulletin

Standard Edition – September 2021

CIS Control 9: Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement.

Why is it needed?

Email and the web are the primary (digital) ways in which users in your business access the outside world and interact with untrusted users and environments. Unfortunately, this makes them common targets for attackers using malicious code or social engineering techniques to access your network.

Web browsers can be exploited in various ways. The browser itself may be outdated or have a vulnerability that can be exploited. A third-party plug-in to the browser may be outdated, have a vulnerability, or have come from an untrusted source, making it an easy target for malware. Attackers may also create malicious web pages designed specifically to target insecure browsers. Email is generally targeted with spam or malicious messages and attachments (phishing attacks) designed to catch a victim in a moment of inattention.

How is it implemented?

CIS control 9 focuses on implementing safeguards against email and web browser attacks.:

Firstly, ensure only fully supported browsers and clients are used with DNS filtering on all enterprise assets. Browsers and email clients should be from a trusted vendor, with DNS filtering in place to block malicious domains. A more advanced safeguard that follows DNS filtering is the maintenance and enforcement of network-based URL filters. These can be configured in various ways, such as category-based filtering or through block lists allowing businesses to decide what is relevant for them.

Preventing users from installing unsupported plugins, or any unauthorised browser or email extensions is also important to minimise risk. Any unauthorised or unsupported plugins or extensions should be uninstalled or disabled, thereby ensuring all browsers on your network are known and included in the vulnerability management process outlined in control 7.

Implementing Domain-based Message Authentication, Reporting & Conformance (DMARC) will lower the potential for spoofed emails from valid domains. DMARC policy and verification should be implemented starting with Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) standards. Additionally, blocking any unnecessary file typed from accessing your email gateway will reduce the risk.

The final recommended step for robust email protection is to consider deploying email server anti-malware protections that work by scanning attachments to detect potential threats and then sandboxing these for analysis.

NZ Incident Response Bulletin

Standard Edition – September 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

Further Resources:

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

Share our Bulletin: