NZ Incident Response Bulletin

Standard Edition – July 2022 – Issue #42

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.

Not subscribed to our Premium Bulletin? Click here to join.

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

FMA releases cyber resilience info sheet for financial advice providers

The Financial Markets Authority (FMA) - Te Mana Tātai Hokohoko - has published an information sheet containing principles and resources to help licensed financial advice providers develop their cyber resilience. Financial advice provider licensing was introduced in March 2021 as part of the new regime for regulating financial advice under the Financial Markets Conduct Act 2013 (as amended by the Financial Services Legislation Amendment Act 2019).

The standard conditions for full financial advice providers licences include a requirement to have and maintain a business continuity plan that includes procedures for responding to, and recovering from, events that impact on cybersecurity and continuity (condition 5).

Additionally, the new Code of Professional Conduct for Financial Advice Services requires providers to ensure that client information is protected against loss and unauthorised access, use, modification or disclosure.

How to outwit the scammers' latest ploys: 'Take a breath and pause'

Digital safety specialists are warning people to be savvy of more sophisticated ploys cybercriminals are using to appear official and target victims. Scammers are increasingly imitating or duplicating bank phone numbers (known as spoofing) and websites, as well as replicating call centre dialogue to look authentic and trick New Zealanders into handing over their pin numbers and security codes. Several banks and government agencies said New Zealanders were being tricked out of millions of dollars each year and called for everyone to keep up their awareness about the current tricks being used by cybercriminals, how to spot them, and how to keep safe from them.

Scammers often used urgency and fear, so victims believed they had to react quickly, and made misjudgements or mistakes in not keeping their details safe, said Rob Pope, the director of the government's national cyber security agency: the Computer Emergency Response Team (CERT). One of the best ways to beat them was to: "Take a breath and pause," he said. Most attempts to access people's accounts could be busted simply by turning on two-factor authentication (2FA).

'Tech tipping point': NZ failing to keep up with world on digital performance - report

New Zealand is at a "tech tipping point" and is failing to keep up with the rest of the world on digital performance, according to a new report. The report by the Technology Users Association (TUANZ) shows New Zealand is ranked 42nd in the world for overall access to technology and 56th on cyber security, with Scandinavian countries and Singapore among the leaders.

Christchurch Call making headway

The 'Christchurch Call,' was a call to action to eliminate terrorist and violent extremist content online, following terror attacks on mosques in Christchurch in 2019. Those who have committed to the initiative include 55 governments, 10 major tech companies (with more reportedly coming on board soon) and dozens of participants from civil society working on the problem.

How the government is responding to the challenge presented by violent extremist online activities was under the microscope as representatives of the Department of Prime Minister and Cabinet appeared before the Governance and Administration committee this week.

World

Ex-Amazon Worker Convicted in Capital One Hacking

A former Amazon engineer who was accused of stealing customers' personal information from Capital One in one of the largest breaches in the United States was found guilty of wire fraud and hacking charges. A Seattle jury found that Paige Thompson, 36, had violated an anti-hacking law known as the Computer Fraud and Abuse Act, which forbids access to a computer without authorization. The jury found her not guilty of identity theft and access device fraud. Ms. Thompson had worked as a software engineer and ran an online community for other workers in her industry. In 2019, she downloaded personal information belonging to more than 100 million Capital One customers. Her legal team argued that she had used the same tools and methods as ethical hackers who hunt for software vulnerabilities and report them to companies so they can be fixed.

Interpol seizes $50 million, arrests 2000 social engineers

An international law enforcement operation, codenamed 'First Light 2022,' has seized 50 million dollars and arrested thousands of people involved in social engineering scams worldwide. The operation was led by Interpol with the assistance of police in 76 countries and focused on social engineering crimes involving telephone deception, romance scams, business email compromise (BEC) scams, and related money laundering. Social engineering is a generic term describing the manipulation of victims by threat actors, typically through human interaction, to trick them into performing some act or disclosing sensitive information.

Costa Rica 'at war' with Russian hackers, experts warn other countries

Costa Rica has come under attack - again. Printers at the national health service abruptly churned out copies of a ransomware note. Hospital record-keeping systems went down, and screens flashed up demands for a digital key needed to unlock compromised files and servers. This was just the latest in a string of cyber-attacks that have knocked out basic government services, including the online tax portal and automated system for paying teachers' salaries. Costa Rica is now in an official state of emergency - the first time a country had done this as a response to cyber-attacks. Security experts feared other countries would be next, as criminals spy soft targets in public infrastructure like trains, hospitals, and schools.

FTC Finalizes Action Against CafePress for Covering Up Data Breach, Lax Security

The Federal Trade Commission finalized an order against CafePress over allegations that it failed to secure consumers' sensitive personal data including Social Security numbers and covered up a major data breach. The Commission's order requires the company to bolster its data security and requires its former owner to pay a half million dollars to compensate small businesses. The FTC alleged that the online customized merchandise platform failed to implement reasonable security measures to protect the sensitive information of buyers and sellers stored on its network and failed to adequately respond to several security breaches.

No country immune: Australia among most vulnerable to cyber attack

Australia is among countries most vulnerable to cyberattacks, RIMS (Risk Management Society) says, with an average cost of cybercrime $6.6 million. The US is most vulnerable, with Belgium, Dominican Republic, Hong Kong, Samoa, China, Afghanistan, Tajikistan and South Africa also highly exposed, RIMS says in its Executive Report "Getting Started on Cybersecurity". "As the world has made dynamic strides in digitising many strategies and process, we have in turn created a much larger attack surface for cybercriminals," RIMS said. "It is of paramount importance that every small- and medium-sized business identifies and better understands their threat profile and vulnerabilities."

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

23/06/2022 – Joint Cyber Security Advisory – Keeping PowerShell: Security Measures to Use and Embrace

Our Views:

Over recent months, we have seen a marked change in the most usual form of successful cyber-attacks on New Zealand organisations. After fading away during 2021, Business Email Compromise is now back as the number one threat, surpassing Ransomware for the first time in over a year.

While you may have a number of effective cyber controls in place to protect your cloud-based email accounts, it is well accepted that accounts can still be compromised, e.g., by gaining access to a computer system that is accessing a cloud account.

Poor or non-existent log processes allow attackers to control victim accounts for days or weeks without anyone in the target enterprise knowing.

Assuming a breach is therefore possible, you should consider what auditing is in place to assist in any post incident investigation to mitigate risk. Do not underestimate the importance of appropriate log collection, management and analysis. When logs are can be effectively analysed, then the tactics, techniques and procedures that an attacker has used, can be discovered and responded to in a timely manner.

An effective log management system can provide insights 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. Retention of logs is also critical in case a follow-up investigation is required or if an attack remained undetected for an extended period of time.

The Centre for Internet Security (CIS) defines control number #8 as Audit Log Management:

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

Relevant Safeguards

We consider the following safeguards to be critical in your management of business email compromise risk. Refer to your email vendors guidance for detailed instructions on how to implement these safeguards.

Establish and Maintain an Audit Log Management Process

Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Collect Audit Logs

Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.

Ensure Adequate Audit Log Storage

Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

Collect Detailed Audit Logs

Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

Centralize Audit Log

Centralize, to the extent possible, audit log collection and retention across enterprise assets.

Retain Audit Logs

Retain audit logs across enterprise assets for a minimum of 90 days.

Conduct Audit Log Reviews

Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

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.

Subscribers to the premium edition also obtain access to the following additional information:

- Cyber Governance
- Cyber Incident Landscape
- Cyber Incident Response Resources
- Cyber Framework and Control Updates, Surveys and Research

Click here if you wish to subscribe to our Premium Edition of the Bulletin.

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: