NZ Incident Response Bulletin

Standard Edition – November 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

Cyber Smart Week takes cybersecurity back to basics

Sometimes cybersecurity advice can come across as a rehash of the same tired old rules, and for some, it breeds complacency. However, the seemingly never-ending torrent of advice is necessary to stem the never-ending deluge of cyber threats. There is immense value in repetition - and for a good reason. Cybersecurity awareness is now a critical part of every business, small and large, right alongside accounting and human resources. And it's the critical nature of cybersecurity that drives the ongoing need for awareness and action. Cyber Smart Week, led by CERT NZ to educate and empower New Zealand businesses and individuals to improve their cybersecurity, is a timely reminder that even small changes can make a big difference.

New SCAM Gallery campaign to help educate Kiwis on how to protect themselves online

Online scams have cost New Zealanders tens of millions of dollars in the last few years, but a new education awareness campaign is hoping to help Kiwis protect themselves from becoming victims. The Aotearoa-designed 'Society of Con Artists And Manipulators (SCAM) Gallery' campaign is a partnership between Facebook, Netsafe, New Zealand Police and CERT NZ. The website profiles six common online scams with details about how each scam is carried out and what can be done to avoid it, all provided by curator 'Sam the Scamologist'.

Smaller businesses triple investment in cyber security

Cyber security continues to be priority one for most small and medium-sized businesses (SMBs) as the number of security breaches continue to grow. HP New Zealand's IT Security 2021 survey indicates 41 percent of SMBs saw evidence of a security breach in the workplace over the past 12 months. Businesses with more than 20 employees nearly tripled their IT investment in security since the survey was last conducted in 2018. The survey also found that compared to 2018, three-times more businesses who fell victim to a cyber-attack, saw legal and compliance implications. HP New Zealand enterprise sales leader Mike Jamieson said mid-sized businesses spent an average of $280,000 a year on IT security, while small businesses averaged $41,000. "The average cost of business that experiences an attack is actually around $159,000 per attack," Jamieson said, adding that was twice what it was costing businesses in 2018.

Cyber security tops A/NZ IT budget forecast

Australian and New Zealand security partners are in for a treat next year as 73 per cent of CIOs in the region plan to invest the lion's share of their IT budget on the practice. According to research firm Gartner's annual global survey of CIOs and technology executives, cyber security was the number one priority in A/NZ when it came to planned investments during 2022, based on responses from 114 CIOs in the region across the public, private and non-profit sectors.

NZ Incident Response Bulletin

Standard Edition – November 2021

World

Dutch forensic lab says it has decoded Tesla's driving data

The Dutch government's forensic lab said on Thursday it had decrypted electric carmaker Tesla Inc's closely guarded driving data-storage system, uncovering a wealth of information that could be used to investigate serious accidents. It was already known that Tesla cars store data from accidents, but the Netherlands Forensic Institute (NFI) said it had discovered far more data than investigators had previously been aware of.

US Treasury said it tied $5.2 billion in BTC transactions to ransomware payments

The financial crimes investigation unit of the US Treasury Department, also known as FinCEN, said today it identified approximately $5.2 billion in outgoing Bitcoin transactions potentially tied to ransomware payments. FinCEN officials said the figure was compiled by analysing 2,184 Suspicious Activity Reports (SARs) filed by US financial institutions over the last decade, between January 1, 2011, and June 30, 2021.

A Rare Win in the Cat-and-Mouse Game of Ransomware

A team of private security sleuths, in their first public detailing of their efforts, discuss how they used cybercriminals' mistakes to quietly help victims recover their data. In a year rife with ransomware attacks, when cybercriminals have held the data of police departments, grocery and pharmacy chains, hospitals, pipelines and water treatment plants hostage with computer code, it was a win, rare in the scale of its success. For months, a New Zealand based team of security experts raced to help victims of a high-profile ransomware group quietly recover their data without paying their digital assailants a dime.

Playing dumb no longer an option against ransomware reporting

The Office of the Australian Information Commissioner (OAIC) called out entities who were playing fast and loose when defining which breaches were subject to disclosure. The warning concerned several ransomware incidents where organisations did not report the attack because they had self-assessed it did not rise to a 'notifiable breach'. In making the determination, the OAIC said these organisations had relied on a 'lack of evidence' that exfiltration or access had occurred. In a remarkably blunt statement of guidance, the OAIC summed up its advice for enterprises considering not reporting a ransomware attack in the future: "It is insufficient for an entity to rely on the absence of evidence of access to, or exfiltration of, data to conclusively determine that an eligible data breach has not occurred."

Reporting of ransomware payments to be mandatory (Australia)

A new law is to be introduced requiring the reporting of ransomware incidents as the Australian Government makes clear it does not condone conceding to the demands of cyber criminals. A Ransomware Action Plan, published today, outlines the powers Australia will use to combat ransomware after the nation experienced a 15% rise in attacks reported to the Australian Cyber Security Centre in the past 12 months.

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.

28 October 2021 – 2021 CWE Most Important Hardware Weaknesses

25 October 2021 – NOBELIUM Attacks on Cloud Services and other Technologies

News Clips

26 October 2021 - Putin's army of hackers are targeting the US with new wave of cyberattacks

NZ Incident Response Bulletin

Standard Edition – November 2021

Our Views: CIS Controls 13-15

This month we investigate CIS controls 13, 14 and 15. CIS Control 13 contains advanced safeguards, and it is primarily recommended for organisations that are medium to large and employ individuals responsible for managing and protecting IT infrastructure. However, it may also be considered by organisations with increased operational complexity regardless of size. In contrast, CIS controls 14 and 15 contain vital safeguards for all organisations irrespective of size, resource availability and operational complexity.

CIS Control 13: Network Monitoring and Defence

Operate processes and tooling to establish and maintain comprehensive network monitoring and defence against security threats across the enterprise's network infrastructure and user base.

Why is it needed?

Even with the best intentions, the network defences operated by any organisation can be vulnerable. Attackers often share knowledge of exploits and new techniques to bypass network security defences. Most network security products also require configuration and tuning for each unique environment to provide optimal protection. Human error or a lack of specific tool knowledge can hinder their effectiveness, and therefore, a process of continually monitoring for security issues is vital.

Networks are often compromised months before the compromise is discovered. Accordingly, a network monitoring process that detects, analyses and responds to potential network threats will allow a swifter response, reducing any impact. Good situational awareness plays a key role in enabling a fast response, and this is gained by teams such as security operations identifying the Tactics, Techniques and Procedures of attackers and the Indicators of Compromise.

How is it implemented?

Developing situational awareness requires an organisation to understand its critical business functions, data flows, network architecture, vendor and partner connections and end-user devices and accounts. A good understanding of this environment drives the development of a sound security architecture and the implementation of appropriate security controls and monitoring and response processes. Larger enterprises may choose to set up a security operations centre internally; however, an external service provider or consultancy can equally provide incident detection, analysis, and mitigation.

CIS Control 13 requires security event alerts to be centralised, preferably using a Security Information and Event Management (SIEM) tool that correlates vendor-defined alerts. A log analytics platform is also an option if it correlates relevant security alerts.

Intrusion Detection Solutions can also be deployed to satisfy this control, by capturing logs and enabling alerts. Access control to the network for remote assets should be managed based on whether anti-malware is installed and up to date, whether the device meets the organisation's security configuration standards, and whether the operating system and applications are up to date.

CIS Control 14: Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Why is it needed?

Unlike CIS control 13, the safeguards described in this control are essential for all organisations. Attackers know it is much easier to trick a busy user than to develop a successful network exploit. Therefore, they target human vulnerabilities making people the backbone of a successful or unsuccessful organisational security program. In addition to targeted "social engineering" attacks, people make simple mistakes resulting in unintentional or intentional cyber incidents. These may include sharing sensitive data by sending an email addressed to the wrong recipient, losing a device, or using the same password on multiple sites.

NZ Incident Response Bulletin

Standard Edition – November 2021

How is it implemented?

To satisfy this control, organisations should establish and maintain a security awareness program that educates users (both when they commence employment and then annually and ongoing) about cyber safety in your business.

Making cybersecurity awareness training effective involves designing a program that is topical and relevant to your environment. Cybersafety messages should be dispersed regularly to ensure they remain targeted, relevant and front of mind. For example, a simple reminder of the increase in malicious emails purporting to be from delivery companies as Christmas approaches. Phishing tests should be relevant to the individual roles within your business for greater effectiveness. For example: send a phishing test email that purports to be a vendor asking to change bank account details for invoice payment to the accounts payable team.

Additional essential safeguards are training users on best practice authentication (Multi-factor Authentication and safe password use), secure data handling and the causes of unintentional data exposure, and the risks of connecting to and transferring data over insecure networks.

Finally, training users to recognise and report security incidents allows cybersecurity responsibility to be spread amongst the organisation leading to a greater overall level of organisational protection.

CIS Control 15: Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Why is it needed?

Organisations rely on an array of service providers, vendors and partners to supply infrastructure, applications and data on their behalf. Given they are essential, service providers are also a core cybersecurity governance risk that must be understood and managed as the impact of a third party breach can include business disruption, data loss and reputational damage.

Assessing the cyber security posture of any provider is a fundamental risk management process. Additionally, many data privacy regulations require that protections extend to service providers, making this process essential in many industries.

Service providers may also contract with additional parties to provide services, creating an even greater potential risk footprint. The security of large cloud-based service providers is often scrutinised when they perform business-critical services; however, smaller service providers can be easily overlooked.

How is it implemented?

You cannot manage what you are unaware of, and therefore implementing this control starts with creating and maintaining an inventory of all service providers. All businesses should have this inventory.

Creating a service provider management policy is next. This policy should outline how you will classify, list, assess, monitor and decommission all service providers. Classification of each provider should be undertaken using characteristics such as data sensitivity, data volume, availability needs, applicable regulations, and inherent and mitigated risk.

Service Provider contracts should include minimum security requirements, incident response processes, data breach notification, encryption requirements, data handling and disposal requirements. Regularly reviewing contracts to ensure they still meet your organisation's security requirements should be completed annually.

More advanced safeguards for this control include:

- Assessing Service Providers: The scope of the assessment may consist of reviewing penetration testing, regulatory testing (PCI compliance) reports or targeted questionnaires.
- Monitoring Service Providers: Monitoring may include activities such as reassessment of supplier compliance, review of release notes, dark web monitoring.
- Securely Decommission Service Providers: Consider user and service account deactivation, secure disposal of data.

NZ Incident Response Bulletin

Standard Edition – November 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: