NZ Incident Response Bulletin

Standard Edition – December 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 attacks reach a record high, Cert NZ report shows

Reported cybersecurity incidents have reached a record high, according to Cert NZ's latest quarterly report. From July 1 to September 30, the cybersecurity agency received more than 2,600 incident reports from individuals and businesses; the highest number to date and a 33 per cent increase on the second quarter. The reported, direct financial loss was at $6.4m (the average quarterly loss, based on 14 quarters, was $3.6m.)

Attacks circulated by email were among the most commonly reported incidents. In particular, a variation of malicious software, or malware, called Emotet, which is spread through email links or attachments, was responsible for a 34 per cent increase in malware reports on the previous quarter.

Cyber threats continue to increase in New Zealand, new report finds

A new report has found cyber threats are continuing to grow in New Zealand, as attacks become more sophisticated. The annual National Cyber Security Centre threat report shows:

- 404 incidents impacting nationally significant organisations
- a 15% increase on last year's total
- around a quarter showed links to suspected state-sponsored actors, while about the same amount were criminally and financially motivated
- 26% of incidents had insufficient information to assess anything about the actor responsible or their motivation.

World

UK Spooks Handled Record Number of Cyber-Incidents Last Year

The UK's National Cyber Security Centre (NCSC) has hailed its world-beating cybersecurity expertise after handling hundreds of incidents and disrupting millions of cyber-attack campaigns over the past year. The government agency, part of signals intelligence body GCHQ, said it offered wraparound support for a record 777 incidents over the period, including attacks on COVID-19 vaccine research, distribution and supply chains.

In summary, the report details:

- an increase of over 7% on the previous year
- 20% of cases in total linked to the healthcare and vaccine sectors
- the new Suspicious Email Reporting Service, which accrued 5.9 million reports over the year, leading to the removal of more than 53,000 scams and 96,500 malicious URLs
- the NCSC's Active Cyber Defence program, which took down 2.3 million cyber-enabled "commodity campaigns," 442 phishing campaigns using NHS branding, and 80 malicious NHS apps.

NZ Incident Response Bulletin

Standard Edition – December 2021

FBI Email Server Hacked, Thousands Of Spam Emails Said To Be Sent Out

The Federal Bureau of Investigation (FBI) confirmed that one of its email servers had been hacked, resulting in spam emails being sent to the public that appeared to be from the agency and the Department of Homeland Security. The FBI and the Cybersecurity and Infrastructure Security Agency “encourage the public to be cautious of unknown senders” and to report suspicious activity to them. The hack was uncovered by a cybersecurity watchdog group, the Spamhaus Project, which tweeted that the phony email campaign began at midnight. Spamhaus Project told Bloomberg that it estimated the spam emails were sent to over 100,000 accounts, warning them that they were being attacked by cybersecurity researcher Vinny Troia and cybercriminal group The Dark Overlord.

Cyber Security Baseline Standards published, to build cyber resilience across all Public Service Bodies

The Minister of State at the Department of the Environment, Climate and Communications, Ossian Smyth T.D., has today published Cyber Security Baseline Standards and associated implementation guidelines for use by Public Service Bodies. The publication of Baseline Standards was one of the key measures identified in the National Cyber Security Strategy 2019-2024. The Strategy stated that, under Measure 8, the NCSC (Nationals Cyber Security Centre) would formulate Baseline Standards in conjunction with the OGCIO (Office of the Government Chief Information Officer). The main goal of the Cyber Security Baseline Standards is to improve the resilience and security of information and communications technology infrastructure and systems (ICT) in Public Service Bodies.

FCA to spend $670k on digital currency training and forensics

The United Kingdom’s financial regulator is seeking better oversight over the digital currency industry. The Financial Conduct Authority (FCA) has issued a tender offer for a company that can provide blockchain data forensic services and train its employees on digital currencies. FCA has become ever more involved in the digital currency industry. While it only used to publish warnings against sketchy and unregistered companies in the past, it has taken a more active approach in recent months. In 2020, it became the anti-money laundering regulator for the sector. Two months ago, FCA Chair Charles Randell asked for even more oversight over the industry, saying there was a proliferation of useless pump and dump tokens. Now, the watchdog is looking to spend half a million pounds to beef up its digital currency monitoring capabilities. In a tender offer, the FCA revealed that it was seeking “access to specialist services to support the analysis of cryptoasset blockchain data.”

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

24 November 2021 - CISA Releases Capacity Enhancement Guides to Enhance Mobile Device Cybersecurity for Consumers and Organizations

12 November 2021 – CISA – Palo Alto Networks Release Security Updates for PAN-OS

News Clips

9 November 2021 - AG Merrick Garland Announces Department Of Justice Charging REvil Cybercrime Suspects

NZ Incident Response Bulletin

Standard Edition – December 2021

Our Views: CIS Controls 16-18

This month brings us to the end of our CIS control deep dive by looking at the final three controls: 16, 17 and 18. CIS controls 16 and 18 are more advanced options for business who are medium to large and employ individuals responsible for managing and protecting IT infrastructure. However, CIS 17 is highly recommended for all businesses for basic security hygiene.

CIS Control 16: Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Why is it needed?

Access management applications enable users to easily manage a business's sensitive data and to grant access to system resources. Attackers with access to these applications can therefore also directly use these them to compromise data without needing an elaborate hacking sequence to bypass network security controls. Hence the need to strongly protect user credentials, as outlined in CIS control 6. However, even without access to user credentials, cyber criminals will target applications by looking for application vulnerabilities. Attackers will then exploit these vulnerabilities to take control of network assets.

Application vulnerabilities may exist due to insecure design, coding mistakes, poor authentication practices, infrastructure weaknesses or insufficient testing. Today's applications are more complex and dynamic. Agile "DevOps" cycles are now used that involve frequent code change and most applications are no longer built from scratch but assembled from many contributing parts. All these factors have increased the complexity and challenge of building secure applications. Additionally, the increased use of Software as a Service (SaaS) has decreased the visibility of some application development and security practices and consequently the level of risk they carry. Business should therefore follow the safeguards outlined in this control for all application development and any extension or customisation of SaaS products.

How is it implemented?

No part of this control is recommended as part of basic security hygiene or IG1 (small to medium-sized businesses with limited IT and cybersecurity expertise) however there are 14 safeguards to consider for more mature organisations. To start implementing this control, a secure application development process must be established. Ideally this will introduce security needs early in any software development lifecycle and include addressing secure design and coding standards, developer training, vulnerability management, secure testing processes and third-party code security. The vulnerability process would provide a mechanism for third parties to report vulnerabilities and include procedures for intake, assignment, remediation and testing of vulnerabilities. Additionally, a tracking system should be implemented that can report key metrics on the application vulnerability process, as well as performing root cause analysis on identified vulnerabilities.

Procedures for managing third party components is also required to satisfy this control. An inventory of third-party software components should be created, sometimes called a "bill of materials." This inventory should include any risks that each component could pose. Only up-to-date and trusted third-party software components must be allowed. Further safeguards for this control include:

- Establishing and Maintaining a Severity Rating System and Process for Application Vulnerabilities
- Use Standard Hardening Configuration Templates for Application Infrastructure
- Separate Production and Non-Production Systems
- Train Developers in Application Security Concepts and Secure Coding
- Apply Secure Design Principles in Application Architectures
- Leverage Vetted Modules or Services for Application Security Components

The safeguards outlined above satisfy IG2 requirements. Larger and more mature teams should consider the additional safeguards of:

- Implementing Code-Level Security Checks
- Conducting Application Penetration Testing
- Conducting Threat Modelling

NZ Incident Response Bulletin

Standard Edition – December 2021

Application software security is a large and detailed area and therefore the safeguards in CIS control 16 outline the most critical areas only. The NIST published the Secure Software Development Framework (SSDF) in 2020 to help organisations build their application security requirements and understand whether a products development follows best practice. Using this resource to extend your organisations knowledge is highly recommended. Further recommended industry resources are also freely available as references including: SAFECODE Application Security Addendum, The Software Alliance Framework and OWASP guidelines.

CIS Control 17: Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Why is it needed?

The intent of incident response management is to identify threats to the organisation, respond to them before they can spread, and remediate them before they cause harm. A well-rounded cybersecurity programme follows a recognised framework and includes capability in each area of identification, protection, detection, response, and recovery. Often response and recovery are overlooked in less mature organisations. As protections cannot be relied upon 100%, the ability to respond to a cyber incident and recover from this effectively is therefore vital.

An attacker can dwell within systems for days, weeks, and months, before being detected. This gives them ample time to find and review confidential data and traverse laterally within an organisations network, potentially planting further vulnerabilities and “backdoors” for later compromise. Due to the recent rise in ransomware this behaviour has become more common. A common response to cyber incidents in immature organisations is to just “re-image” assets to the original state and move on. However, without using a thorough incident response process to fully understand the scope of any incident, how it happened, and how it can be prevented in future, the risk of the same or a similar threat will remain.

Smart business decisions are essential to reduce any further potential impact of the cyber incident particularly when communicating with stakeholders, meeting legal and regulatory obligations, and prioritising remediation activities. If an organisation does not have a cyber incident response plan in place they will struggle with these decisions when a cyber incident occurs. Even with great people, under the pressure and time constraints of a cyber incident it is extremely difficult to know the correct investigative procedure to follow and what reporting, data collection, legal protocols and communication strategies should be undertaken to minimise harm.

How is it implemented?

This control includes safeguards that constitute minimum basic security hygiene for all businesses. Even small organisations with limited resources to conduct incident response activities should have an incident response plan. The plan at a minimum should identify the source of protections and detections (e.g.: where an alert or notification of a potential cyber incident may come from), a list of who to call upon for assistance, and communication plans and mechanisms to inform required parties such as leadership, employees, regulators, partners, and customers.

At a basic level:

- Designate Personnel to Manage Incident Handling
- Establish and Maintain Contact Information for Reporting Security Incidents
- Establish and Maintain an Enterprise Process for Reporting Incidents

After these basic safeguards are implemented, it is recommended a full incident response process be established. Key roles and responsibilities for incident response activities across the business should be defined and reviewed periodically. Primary and secondary communication mechanisms to be used during an incident must also be defined. It is important to remember that some standard communication channels such as email may be either unavailable or no longer secure for use during a cyber incident.

Once these procedures are in place then they must be tested. The incident response team or a third-party should conduct regular scenario walk through’s (sometimes referred to as tabletop simulations or gold-teaming exercises) to fine-tune the

business response. Walk throughs allow the business to fully understand their roles and responsibilities in a cyber incident and these scenarios can effectively identify gaps or dependencies in the current procedures. Finally conducting post incident reviews allows lessons learned to be incorporated into plans and help prevent incident recurrence.

Finally, more mature organisations can also consider including threat intelligence and threat hunting into their incident response process. This enables proactive monitoring for tactics, techniques, and procedures (TTPs) of likely threat actors and can help focus and define the response procedures most suitable for the organisation.

CIS Control 18: Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Why is it needed?

Penetration testing goes a step further than basic security hygiene and therefore it is not included at IG1 level. However, this control includes safeguards at both IG2 and IG3 for consideration.

An organisations cyber defence posture can be strong, but due to the everchanging and complex nature of technology and the evolving nature of cyber-attacks, it is rarely perfect. Penetration testing allows a business to test their defensive controls and identify gaps in these that will impact overall resiliency. Penetration testing can be focused on external network attacks, internal network threats, applications, systems, or devices and may include social engineering techniques to trick users or physical security breaches. It differs from vulnerability testing (described in CIS control 7) as it is an active attempt to exploit weaknesses to see how far an attacker may get, and what data, systems, and business processes may be impacted by success.

Penetration tests can be used as a compelling demonstration of organisations weaknesses, to validate whether the business has the correct defences in place, or as a tool to verify the correct operation of currently deployed defences. They often involve significant human involvement and analysis in conjunction with custom scripts and tools. As penetration testing can be is complex, it may also be expensive and introduce risk, such as the unexpected shutdown of a system or the possibility of data deletion or corruption. Because of this it should only be undertaken by experienced specialists from reputable vendors.

How is it implemented?

The first step to satisfying this control is to establish and maintain a penetration testing program. This includes determining the scope of any penetration testing engagement (For example, will the testing include network, web application, API's, hosted services, physical controls) and key factors such as acceptable hours for testing, excluded attack types, and confidentiality of findings. Defining scope is critical to establish clear rules of engagement and minimise any possible unexpected collateral damage that can occur from invasive testing.

Periodic external penetration tests (based on the requirements outlined in the program established above) should be undertaken at least annually. An external test should include reconnaissance to detect exploitable data. The number of internal people that know about the test should be minimised and ideally a business would focus on testing assets that hold the highest value information or production processing functionality. Consider conducting a penetration test through third-party legal counsel to ensure the report is protected from disclosure. After a test is conducted any test findings must be remediated.

Advanced safeguards in this control include validating security measures after each penetration test and performing periodic internal penetration test. Further detail and support for Penetration testing can also be found in the following resources:

- OWASP Penetration Testing Methodologies
- PCI Security Standards Council

This brings us to the end of our deep dive on the CIS control set. Using this control set gives your organisation a structured and prioritised plan for improving your cyber security posture. We highly recommend starting to define your cyber security program by measuring your organisation against the IG1 group of CIS controls which make up the basic security hygiene measures for any business.

NZ Incident Response Bulletin

Standard Edition – December 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: