NZ Incident Response Bulletin

Standard Edition - January 2020

In this issue:

News | **Our Views** | **Upcoming Events**

New Zealand	A new Privacy Act in 2020	OWASP New Zealand Day
World	New FMA Cyber Resilience requirements	CybersecCon
		International Conference on Forensic Sciences and Law Enforcement

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 encourages leaders to connect with cybersecurity governance

The Government Communications Security Bureau's (GCSB) National Cyber Security Centre (NCSC) has recently published a resource to assist boards in improving cybersecurity governance. The resource "Charting your Course: Cyber Security Governance" focuses on six areas to improve engagement between governance and security practitioners including:

- Building a culture of cyber resilience
- Establishing roles and responsibilities
- Holistic risk management
- Cybersecurity collaboration
- Creating a cybersecurity programme
- Measuring resilience

The release of this resource follows an NCSC study of New Zealand organisations' cybersecurity resilience which identified a gap between leadership, governance and cybersecurity practice. This resource was the first of a series, with additional releases planned to follow in 2020.

Cyber security incidents reported to CERT NZ at all-time high

The Government's cyber security unit CERT NZ received the highest number of reported incidents for a quarter since launching in 2017, according to its latest report. The report, covering the period from July 1 to September 30, showed 1,354 incidents were reported to CERT NZ.

Of all incidents, 18 per cent reported some type of loss, either financial, data or operational. The report takes an in-depth look at the different types of phishing attacks impacting New Zealanders and provides tips on how to spot them and protect against them.

NZ Incident Response Bulletin

Standard Edition - January 2020

World

Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up

Several prominent ransomware groups (including 'Maze') have signalled that they plan to start publishing data stolen from victims who refuse to pay up. To make matters worse, one ransomware gang has now created a public website identifying recent victim companies that have chosen to rebuild their operations instead of quietly acquiescing to their tormentors.

The information disclosed for each Maze victim includes the initial date of infection, several stolen Microsoft Office, text and PDF files, the total volume of files allegedly exfiltrated from victims (measured in Gigabytes), as well as the IP addresses and machine names of the servers infected by Maze.

The move by Maze Ransomware comes just days after the cybercriminals responsible for managing the "Sodinokibi/rEvil" ransomware empire posted on a popular dark Web forum that they also plan to start using stolen files and data as public leverage to get victims to pay ransoms.

'A cyberattack should be expected': U.S. strike on Iranian leader sparks fears of major digital disruption

Iran's cyber troops long have been among the world's most capable and aggressive — disrupting banking, hacking oil companies, even trying to take control of a dam from afar — while typically stopping short of the most crippling possible actions, say experts on the country's capabilities.

Friday's American airstrike that killed one of Iran's top generals, Quds Force Commander Maj. Gen. Qasem Soleimani, now threatens to unleash a fully unshackled Iranian response, analysts and former U.S. officials warned. They said a variety of potential cyberattacks, possibly in conjunction with more traditional forms of lethal action, would be well within the digital arsenal of a nation that has vowed "severe revenge."

US Coast Guard discloses Ryuk ransomware infection at maritime facility

An infection with the Ryuk ransomware took down a maritime facility for more than 30 hours, the US Coast Guard said in a security bulletin it published before Christmas. The agency did not reveal the name or the location of the port authority; however, it described the incident as recent.

"Forensic analysis is currently ongoing but the virus, identified as 'Ryuk' ransomware," the US Coast Guard (USCG) said in a security bulletin meant to put other port authorities on alert about future attacks. USCG officials said they believe the point of entry was a malicious email sent to one of the maritime facility's employees.

Critical Citrix Bug Puts 80,000 Corporate LANs at Risk

Citrix has announced a critical vulnerability in the Citrix Application Delivery Controller (ADC) and Citrix Gateway. This vulnerability could allow unauthenticated attackers to gain remote access to a company's local network and execute code. "This attack does not require access to any accounts, and therefore can be performed by any external attacker," - Mikhail Klyuchnikov (Security Researcher).

Citrix has released a set of measures to mitigate the vulnerability which can be found here, including software updates that should be applied immediately.

NZ Incident Response Bulletin

Standard Edition - January 2020

Our Views:

A recap of two of the most important changes relevant to Forensic and Cyber Security matters announced during 2019 and how to prepare for them.

A new Privacy Act in 2020

Changes to existing privacy law are due in 2020. Full details can be found here. Key highlights for all businesses to be aware of include:

- **Requirements to report privacy breaches:** If organisations have a privacy breach that poses a risk of serious harm, it must notify the Commissioner and the people affected (unless an exception applies).
- **Compliance notices:** The Commissioner will be able to issue compliance notices to require an organisation to do something, or stop doing something, to comply with the Privacy Act.
- **Decisions on access requests:** The Commissioner will make binding decisions on complaints about access to information, rather than the Human Rights Review Tribunal. The Commissioner's decisions can be appealed to the Tribunal.
- **Strengthening cross-border protections:** New Zealand agencies will have to take reasonable steps to ensure that personal information sent overseas is protected by acceptable privacy standards.
- **New criminal offences:** It will be an offence to mislead an organisation in a way that affects someone else's personal information, and to destroy documents containing personal information if a request has been made for it. The proposed penalty is a fine of up to $10,000. It will be an offence to fail to notify the Commissioner of a serious privacy breach, or to fail to comply with an enforceable compliance notice.
- **Extraterritoriality:** An overseas agency is to be treated as "carrying on business in New Zealand" even if it does not have a physical place of business here - if it charges any monetary payment for goods or services or makes a profit from its business here.

The new bill passed its second reading in 2019, and March 2020 was proposed as a start date for these changes however it may be closer to July 2020 before the bill is passed. You can see the timeline and progress here.

Preparing for these changes

When the new privacy bill passes, there will be a six-month implementation period to prepare. There are steps you can take in advance of these changes to ensure your business is ready.

1. Ensure you are aware of and understand all changes proposed and which may impact your business. The Ministry of Justice website currently has detailed information about all changes proposed.
2. Review your current privacy policies for compatibility with all changes.
3. Develop compliant policies that are ready for use by mid-2020. This should include a mandatory breach reporting policy that can be used from March 2020.
4. Ensure your Incident Response Team are fully aware of new data breach requirements and have processes in place for identifying, protecting, defending, responding and recovering from a breach.
   Points to consider: How will we determine serious harm? Who will manage notification and communication requirements? Do we have protocols in place for containment?
5. Review all data storage and handling policies and service provider agreements for compliance with the new cross-border protections.
   Points to consider: Do we store, process or send any data overseas? Do we have processes in place to adequately protect this data and its end use?
6. Have your privacy officer develop training and communication materials to communicate all changes to all employees. If you don't have a privacy officer, now would be a good time to think about delegating that responsibility to someone in your organisation or consider engaging an external privacy expert to fulfil that function.

NZ Incident Response Bulletin

Standard Edition - January 2020

New FMA Cyber Resilience requirements

The Financial Markets Authority (FMA) released a report in July 2019 reviewing the cyber-resilience of New Zealand financial services which included a series of cyber recommendations. These recommendations included the introduction of a cyber resilience framework for all financial service providers. While this report is targeted at entities regulated by the FMA, it is also useful to other participants in financial markets and businesses generally as it discusses the nature and prevalence of cyber-risk within them.

Changes include the FMA requiring its reporting entities to:

- Include a cybercrime risk assessment within existing AML/CFT Risk Assessment or current Risk Management processes.
- Ensure Cyber Incident Response and Recovery Plans are in place.
- Ensure Cyber Protection and Detection measures are in place.
- Ensure Cyber Risk Analysis and Management is governed and in line with the Institute of Directors Cyber Risk Practice Guide.
- Make use of the cyber resources provided by CERT NZ and New Zealand's National Cyber Security Centre (NCSC).
- Aim to use a "recognised cybersecurity framework to assist with planning, prioritising and managing" cybercrime risks such as The National Institute of Standards and Technology (NIST).

According to the FMA "All licensed firms should take treat the risk of cyber-attacks as real, and plan accordingly".

Tools to Assist

We suggest familiarising yourself with current cyber threats in the New Zealand landscape via the Threat Alerts in this monthly bulletin (including those reported in the premium edition), the NCSC cyber threat reports and the CERT NZ reports.

In its report, the FMA recommended using the NIST Cybersecurity Framework to develop or improve a Cybersecurity programme. The framework allows a business to assess their current level of cyber maturity, determine goals and plan and prioritise an improvement programme.

The NIST website also provides many additional free resources to assist in developing Incident Response and Recovery Plans and procedures.

Upcoming Events:

Date	Event	Location
3-4 February 2020	International Conference on Forensic Sciences and Law Enforcement	Melbourne, Australia
21 February 2020	OWASP New Zealand Day	Auckland
28 February 2020	CybersecCon	Auckland

NZ Incident Response Bulletin

Standard Edition - January 2020

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, cybersecurity 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

Share our Bulletin: