NZ Incident Response Bulletin

Standard Edition - November 2019

In this issue:

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

NZ information security award finalists revealed

The iSANZ awards, established five years ago to recognise outstanding achievements in cyber security, has announced this year's finalists. Companies including an electronic payment provider, healthcare agency and large media company have been named along with specialist security businesses and professionals. The finalists are:

Best Startup or New Business: *Darkscope, Cyberprep and Mindshift.*

Best Security Project / Initiative: *Aura Information Security's partnership with Institute of Directors, healthAlliance for its Northern Region Secure USB Project and Gallagher for its Security Health Check.*

Best Security Awareness Campaign: *healthAlliance for its Cyber Heroes campaign, NZME for an internal cyber security campaign targeted at staff across 40 regions and Paymark for its RSP awareness campaign.*

Best Security Company: *Chillisoft, Defend and SafeStack.*

Up and Coming Cybersecurity Star: *Christine Dewes from Quantum Security, Chris Hislop from BNZ Bank and Ian White from ZX Security.*

NZ Incident Response Bulletin

Standard Edition - November 2019

World

DDoS attack sidelines AWS DNS web service for hours

Amazon Web Services was recently hit with a Distributed Denial of Service (DDoS) attack lasting eight hours. A DDoS attack is an attempt by attackers to overwhelm systems with network traffic or interference, rendering services inaccessible.

"*We're investigating reports of intermittent DNS resolution errors with Route 53 & our external DNS providers,"* AWS Support tweeted on 22 October at 1:06 p.m. ET. Later, at 9:30 p.m., AWS Support tweeted that *"The AWS DNS issues that may have affected your experience with Route 53 or our external DNS providers has been resolved."*

Baltimore to purchase $20M in cyber insurance

After suffering a major ransomware attack in May in which many of the cities systems were crippled, the City of Baltimore has purchased $20 million USD in cyber insurance, for a period of 1 year, at an approximate cost of $850,000 USD in premiums.

It is the first cyber insurance ever purchased by the city and is intended to cover any additional disruptions to the city's networks including business interruption costs, data recovery, and attack investigation. It is anticipated that the city will continue to hold cyber insurance into the future.

Norsk Hydro gives details on initial cyber insurance payout

Norsk, the multinational aluminium and renewable energy company, was hit by a cyber-attack in March this year.

"The cyberattack on Hydro on March 19 affected the entire global organization, with extruded solutions having suffered the most significant operational challenges and financial losses", the supplier reported.

It estimates the financial impact of the attack as being approximately $60-70 million USD. They have also recently disclosed that the insurance company pay out received was less than 10% of the overall costs. Approximately $3.6 million USD.

'One million pages stolen': Aussie giant accuses former exec of espionage

A former senior employee of Commonwealth Serum Laboratories (CSL), the Australian blood giant, has been accused of stealing tens of thousands of documents including trade secrets in order to gain a job at a key competitor.

CSL has initiated court action in America alleging a large competitor, Dutch pharmaceuticals group "Pharming", and the former CSL employee misappropriated CSL trade secrets by taking 25 gigabytes of data. This equated to one million pages of information across 21,000 files.

Update - Accused CSL 'corporate spy' sacked from competitor

The doctor accused of corporate espionage and stealing trade secrets from blood giant CSL to further his career and to land a job at rival group Pharming has been sacked from his job.

Dutch pharmaceutical company Pharming announced on Thursday that it had permanently terminated Joseph Chiao's employment. A key claim by CSL is that Dr Chiao downloaded computer files containing "patient and physician information relating to the use of CSL Behring's products". Pharming said it was in the process of conducting a forensic review with CSL.

NZ Incident Response Bulletin

Standard Edition - November 2019

Our Views:

This month's theme is "Communication during an Incident Response".

In addition to the technical response, communication is also an important aspect requiring active management.

Data breach notifications

An investigation into the data breach suffered by the Australian National University in late 2018 found it was a well-planned and sophisticated attack that was likely to have been carried out by a team of 5 to 15 people working 24/7. The attackers used custom-built malware and zero-day exploits to infiltrate the university systems and steal an unknown quantity of data.

Learnings from the incident report include increasing phishing attack awareness, accelerating the use of two-factor authentication and the need for ongoing practice and cyber-attack simulation exercises. The full incident report has also been made public to allow other institutions and businesses to learn from it and protect themselves.

Approaches to communication following discovery of an incident differs depending on circumstances such as the severity, potential impact and the timing of the incident. For example, an organisation may choose not to notify immediately following a breach until they are certain of the impacts and its containment.

It is important to strike the correct balance between being open with affected parties and protecting systems from further attack. Revealing too much information may result in undue escalation or exposure of vulnerabilities yet to be fixed, however withholding vital information may hamper recovery efforts and create a negative impression of your business. Planning for effective communication is therefore an integral part of your overall Cyber Incident Response Plan.

If you are uncertain of your data breach notification responsibilities, refer to the Privacy Commissioners guidelines. Consider engaging a specialised communications professional to assist if the incident may result in media attention.

Determine the communication channels and technology you will use ahead of time and test this regularly. The quality, frequency and content of your communications to stakeholders will have a significant impact on their perception of your organisation and ability to manage an incident.

Enhancing Incident Response Communication

The NIST Cybersecurity Framework offers support for ensuring communication processes are robust within your Incident Response Plan. The framework lists five areas for attention within the "Respond" function including:

1. *Ensuring personnel know their roles and order of operations when a response is needed*
   Create an Incident Response Plan that describes your incident response capability. Regular testing of your response capabilities will also strengthen your skills and identify any potential weaknesses in your planning.

2. *Ensuring incidents are reported consistently with established criteria*
   Formalise the incident response team activation process by defining what constitutes an incident for your organisation and ensure that communication and escalation processes are clear and documented.

3. *Ensuring information is shared consistently with response plans*
   Updates regarding security assessments, monitoring and incident response plans should be shared with all stakeholders.

4. *Ensuring co-ordination with stakeholders occurs consistently with response plans*
   An individual should be responsible for providing a consistent and coordinated view of the incident to stakeholders. Criteria for escalation to outside agencies should be clarified in the plan where possible.

5. *Ensure that information is shared voluntarily with external stakeholders to achieve broader cybersecurity awareness*
   By sharing learnings, the entire security industry can benefit through security education, allowing your team to stay current with recommended security practices, technology, threats and vulnerabilities.

NZ Incident Response Bulletin

Standard Edition - November 2019

Upcoming Events:

Date	Event	Location
11-14 November 2019	Enfuse Digital Investigations	United States
25 November 2019	NZ ICS Cyber Security Summit	Rotorua
25-26 November 2019	Advancing Digital & IT Law	Auckland
20-21 February 2020	OWASP New Zealand Day	Auckland

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

Share our Bulletin: