Incident Response
FORENSIC & CYBER

NZ Incident Response Bulletin

Standard Edition - October 2019

In this issue:

News	Our Views	Upcoming Events	Premium Content
New Zealand spies helped track down cyber-attackers on Australian Parliament	Cyber Security Awareness	Australia Cyber Conference 2019	Threat Alerts
Government contributing $10 million to help Pacific Nations combat cyber security risks	Cyber Security Awareness under the NIST Cyber Security Framework	2019 NZ Cyber Security Summit	Security Frameworks
CrowdStrike CEO says his company is 'nonpartisan' after Trump brought it up to Ukrainian president	Using a Simulation to train on Cyber Incident Response Plans	Kawaiicon 2019	Information Security Surveys
Bill to combat Deepfakes passes House Committee	Actioning Cyber Security Awareness	ISC2 – Monthly Events	Forensic News
Chinese hackers suspected of Airbus cyberattacks - A350 among targets			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

New Zealand spies helped track down cyber-attackers on Australian Parliament

New Zealand's Government Communications Security Bureau (GCSB) provided experts to assist Australia in responding to a major cyber-attack on Australia's Parliament. Andrew Hampton, Director-General of the GCSB, said "We have technical people with great skills who were there to provide support to their Australian partners."

According to the GCSB, New Zealand is invested in preventing these kinds of cyber-attacks so it helped Australia with its investigation. They claim there were 347 cyber-attacks on New Zealand from June 2017 to 2018, of which 39 percent were linked to state-sponsored actors.

Government contributing $10 million to help Pacific nations combat cyber security risks

The Government has announced a $10 million injection over five years to support Pacific countries' response to the region's cyber security risks. The funding will go towards supporting Pacific countries to develop secure infrastructure, national cyber security strategies, enhance online safety and implement cyber-crime laws.

Minister of Broadcasting Kris Faafoi said the Government would create a dedicated advisory role in New Zealand's Computer Emergency Response Team to work with Pacific nations. "Building cyber capability in the Pacific is one of the priority actions of New Zealand's cyber security strategy," Mr Faafoi said.

NZ Incident Response Bulletin

Standard Edition - October 2019

World

CrowdStrike CEO says his company is ‘nonpartisan’ after Trump brought it up to Ukrainian president

Cyber Security and Incident Response company CrowdStrike’s name featured in the summary of a July call between President Donald Trump and Volodymyr Zelensky, president of Ukraine. The conversation between President Trump and Zelensky is now at the centre of an impeachment inquiry.

CrowdStrike’s name was likely invoked by Trump because the company assisted the Democratic National Committee (DNC) in investigating a 2016 hack by Russian operatives. Trump has previously suggested that the DNC should have turned over the email servers to the FBI instead of having CrowdStrike investigate, implying that the lack of cooperation should cast doubt on findings that the Russians helped him win the election.

CrowdStrike responded by saying that it “provided all forensic evidence and analysis to the FBI,” and that “we stand by our findings and conclusions that have been fully supported by the US intelligence community.”

Bill to Combat Deepfakes Passes House Committee

The Identifying Outputs of Generative Adversarial Networks, or IOGAN Act, directs the US National Science Foundation (NSF) and the US National Institute of Standards and Technology (NIST) to study and accelerate the creation of technology that can detect the disruptive content.

Over the course of the last year, major figures of popular culture have increasingly fallen victim to deepfakes, which make them appear to say or do things that, in reality, they never said or did.

The Act requires NSF and NIST to supplement research on digital media forensic tools or comparable technologies to detect and constrain Generative Adversarial Networks and deepfakes, gain input from stakeholders and experts across the public, private and academic sectors, and submit a report on their findings and policy recommendations.

“The underlying bill will help mitigate those problems, but in addition to developing new technologies, we need to teach Americans how to detect manipulated content that seeks to spread disinformation in the first place,” Wexton said during the markup. “This is a critical component to our national security deterrent strategy to combat disinformation campaigns, because the more education and awareness we have, the better we can strengthen and safeguard our democracy.”

Chinese Hackers Suspected of Airbus Cyberattacks - A350 Among Targets

Airbus has been hit by nation-state cyberattacker, according to a media report dated 26 September 2019. Citing security sources, the news agency reported that a notorious Chinese state-sponsored hacking group is being linked to the attacks which targeted key suppliers to access the company’s secure data.

The attacks appear to be part of a persistent campaign - with four hits in the last year - targeting key Airbus suppliers. At risk, the sources say, is personnel data as well as intellectual property associated with the company’s military and passenger aircraft. This is most likely broad scale industrial espionage.

The report named Airbus suppliers Rolls-Royce and Expleo as confirmed targets, as well as “two other French contractors that AFP was unable to identify.”

One of the most worrying elements of this new report is the implication that a virtual private network connecting suppliers to Airbus may have been the entry point for the attack. The whole point of such a system is to keep traffic away from open networks and remove the possibility of compromise.

NZ Incident Response Bulletin

Standard Edition - October 2019

Our Views:

A selection of issues relevant to Forensic and Cyber Security matters during the last month. This month's theme is "Cyber Security Awareness".

Cyber Security Awareness under the NIST Cyber Security Framework

Of the 108 Sub-Categories listed under the NIST Cyber Security Framework, at least five are dedicated to Cyber Security Awareness. These fall under the Function 'Protect (PR)', within the Category 'Awareness and Training (AT)'. By way of definition:

The organisation's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

Specifically, the five sub-categories include:

- PR.AT-1: All users are informed and trained
- PR.AT-2: Privileged users understand their roles and responsibilities
- PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
- PR.AT-4: Senior executives understand their roles and responsibilities
- PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities

Using a Simulation to Train on Cyber Incident Response Plans

For the same reason why fire evacuation procedures are tested, so should your cyber incident response plan. All key staff must understand the plan and practice it, often!

A large portion of a dealing with a Cyber Incident involves non-technical issues such as legal, communications, regulatory issues, etc. Accordingly, it should be more than just your IT team who are preparing for and partaking in a Cyber Incident Simulation.

The key outcome of a Cyber Incident Simulation, or tabletop exercise as it is often referred, is that your organisation will have greater confidence to prepare, respond and recover in a crisis. By conducting a simulation, you will:

- Establish your current state of readiness
- Gain a better understanding of the cyber risks you face
- Practice your decision making in a safe environment
- Identify areas for improvement

Actioning Cyber Security Awareness

We recommend that organisations deliver their cyber security awareness initiatives through training programmes. These can be delivered via numerous forms such as online, gamification, tabletop simulation, or seminars.

You should also set targets for improvement and measure progress over time. The NIST Cyber Security Framework tiers are a good example of this.

For the first of our Cybercrime Q+A sessions, we met with Mindshift, a New Zealand organisation which specialises in Cyber Awareness. Click on the following link to access a video of our conversation.

Incident Response Solutions - Cybercrime Q+A - Mindshift

NZ Incident Response Bulletin

Standard Edition - October 2019

Upcoming Events:

Date	Event	Location
7 – 9 October 2019	Australia Cyber Conference 2019	Melbourne
16 October 2019	2019 NZ Cyber Security Summit	Wellington
17, 18 October 2019	Kawaiicon 2019	Wellington
24th October 2019	ISC2 – Monthly Events	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

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.

Share our Bulletin: