NZ Incident Response Bulletin

Standard Edition – January 2021

In this issue:

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

New Zealand	The Privacy Act 2020 and the benefits of forensic expertise	2021 New Zealand Cyber Security Summit
World	Cyber Security Controls	AppSec New Zealand Conference 2021
		Ara Launches New Cyber Security Course in 2021
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

Privacy: Businesses and government could face mass lawsuits, as reported breaches predicted to soar

New Zealanders can now launch mass lawsuits against companies and government agencies that have mishandled their information. The number of breaches of New Zealanders' privacy reported to the privacy watchdog is also expected to jump dramatically in 2021, as the Privacy Act 2020 requires organisations to report all breaches that cause, or could cause, "serious harm".

Prime Minister's Comments on Royal Commission of Inquiry into Christchurch Terror Attack

The Royal Commission of Inquiry into the Terror Attack in Christchurch delivered a comprehensive report to make New Zealand a safer country. New Zealand will sign up to the Budapest Convention on Cybercrime, seeking to address internet and computer crime, by aligning nations' laws, facilitating information-sharing on current threats and sharing best practice.

The Application of International Law to State Activity in Cyberspace

On 1 December 2020, New Zealand issued a position statement on how international law applies to state activity in cyberspace. The application of international law to state activity online is a critical component of the framework of responsible state behaviour online. It is essential for maintaining international peace and stability.

The countries behind cyber attacks trying to hack New Zealand's state secrets as criminal hacker numbers soar

The spy agency is worried about the increasing skill of cyber criminals attempting to steal Government secrets and your private information. The Government Communications Security Bureau (GCSB) was called in to help with hundreds of major cyber incidents this year, which it says are becoming more sophisticated.

New Zealand's new Privacy Act 2020 came into force on 1 December 2020, creating new responsibilities for organisations in New Zealand. The new Act introduces a number of changes concerning how the privacy principles are enforced and regulated including mandatory notifications for privacy breaches where serious harm may result.

For more information, read our special publication here.
https://incidentresponse.co.nz/data-breach-response

NZ Incident Response Bulletin

Standard Edition – January 2021

World

Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit

The Pentagon, intelligence agencies, nuclear labs and Fortune 500 companies use software that was found to have been compromised by Russian hackers. The Cybersecurity and Infrastructure Security Agency issued a rare emergency directive warning federal agencies to "power down" the SolarWinds software.

Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal

Earlier this year, hackers secretly broke into SolarWind's systems and added malicious code into the company's software system. The system, called "Orion," is widely used by companies to manage IT resources. Solarwinds has 33,000 customers that use Orion. Beginning as early as March, SolarWinds unwittingly sent out software updates to its customers that included the hacked code. The code created a backdoor to customer's information technology systems, which hackers then used to install even more malware that helped them spy on companies and organisations.

18,000 customers installed updates that left them vulnerable to hackers. SolarWinds has many high profile clients, including Government and Fortune 500 companies. US agencies such as the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the Treasury were attacked.

Dark Web Pricing Skyrockets for Microsoft RDP Servers, Payment-Card Data

Cybercriminals are vying for Remote Desktop Protocol (RDP) access, stolen payment cards and Distributed Denial of Service (DDoS) for hire services, based on a recent analysis of underground marketplace pricing. During the COVID-19 pandemic, cybercriminals have profited with "increasingly advantageous positions to benefit from the disruption." A successful RDP attack is lucrative for cybercriminals as it would give them remote access to the target computer with the same permissions, and access to data and folders, that a legitimate user would have. While in 2017 researchers rarely saw standard DDoS-for-hire offerings exceed $27, in 2020 a 10-minute DDoS attack (60 Gbps) costs $45, while a four-hour DDoS attack (15 Gbps) averages $55. Meanwhile, a fully-managed DDoS attack costs $165.

Council of Financial Regulators launches framework to test cyber resilience of Australia's financial services industry

The Council of Financial Regulators (CFR) has released a Cyber Operational Resilience Intelligence-led Exercises (CORIE) framework for a series of simulated cyber-attacks designed to test the resilience of the Australian financial services industry in the face of growing information security threats. The release of the new CORIE framework follows the Australian Prudential Regulation Authority (APRA) recently signalling it will step up its review of cyber compliance by regulated financial services institutions as part of its new Cyber Security Strategy.

Microsoft Internal "Solorigate" Investigation Update

Microsoft's investigation into its environment found no evidence of access to production services or customer data. The investigation, which is ongoing, also found no indications that its systems were used to attack others. Microsoft's investigation detected unusual activity with a small number of internal accounts and upon review, discovered one account had been used to view source code in a number of source code repositories. The account did not have permissions to modify any code or engineering systems and Microsoft's investigation further confirmed no changes were made. These accounts were investigated and remediated.

Summary of last month's Cyber Alerts:

Incident Response Solutions post certain alerts and tips we consider to be in the public interest as they come to hand. We publish these alerts and tips on our YouTube Channel and this webpage.

24 December 2020 – CISA Releases Free Detection Tool for Azure/M365 Environment

17 December 2020 – Advanced Persistent Threat Compromise – SolarWinds

14 December 2020 – SolarWinds Orion Cyber Security Alert

NZ Incident Response Bulletin

Standard Edition – January 2021

Our Views:

This month's theme is "The Privacy Act 2020 and the benefits of forensic expertise".

In last month's Bulletin, we explored the concerning rise in Data Leaks associated with Ransomware attacks.

The new Privacy Act 2020 (the Act) came into effect on 1 December 2020, introducing a range of reforms. It is now mandatory for organisations to determine whether they have a reasonable belief that a breach may cause serious harm, and if so, notify both the Office of the Privacy Commissioner and the individuals concerned. Notification is required as soon as it is reasonably practicable to do so, even if the full extent of the privacy breach is unknown.

In assessing notification requirements, an organisation needs to determine whether they have a reasonable belief that a privacy breach has occurred. While this may be obvious if a third party advises you that they received your data in error, it may be more difficult if you receive a ransom demand from a cyber-crime group threatening to publish the material on a Data Leak site.

By adopting a forensic approach, you can work through the incident response process, which involves the key steps of 'Identification', 'Containment' and 'Eradication'. Given the potential of legal proceedings by both individuals and other stakeholders, a forensic approach ensures your evidence will withstand legal scrutiny. A brief overview of this process follows.

Identification

The identification phase includes, amongst other activities, preserving potential evidence, examining the data for Indicators of Compromise (IOC's) and determining the extent of any breach. This phase also assists in determining your security response.

Containment

The containment phase involves limiting and preventing further damage from occurring. This includes determining whether the breach has caused, or is likely to cause, serious harm to individuals. According to section 113 of the Act, when an agency is assessing whether a privacy breach is likely to cause serious harm, and therefore be a notifiable privacy breach, the agency must consider the following:

- any action taken by the agency to reduce the risk of harm following the breach
- whether the personal information is sensitive in nature
- the nature of the harm that may be caused to affected individuals
- the person or body that has obtained or may obtain personal information as a result of the breach (if known)
- whether the personal information is protected by a security measure
- any other relevant matters.

A forensic examination can provide answers to most of the above requirements. For example, forensic tools and procedures can quickly and thoroughly determine the content of personal information, who may have obtained the information and whether the breached information was secured (e.g. encrypted).

Eradication

The eradication phase involves removing the actual risk and starting with the restoration of any affected systems.

A forensic approach can assist in determining the extent of compromise and any ongoing risks, so you can determine whether to rebuild systems, commission additional security measures, and perhaps most importantly, notify any affected individuals of the potential risk of serious harm.

Following a Data Breach Response plan, your next (technical) steps will likely include:

- Configuring and enabling the notification process using a secure and measurable platform
- Conducting Dark Web, Social Media and Credit Monitoring
- Providing Forensic Incident Response reports to regulators and other affected stakeholders

NZ Incident Response Bulletin

Standard Edition – January 2021

Upcoming Events:

Date	Event	Location
10 - 13 February 2021	AppSec New Zealand Conference 2021	University of Auckland
24 February 2021	2021 NZ Cyber Security Summit	Te Papa, Wellington
2021	Ara Launches New Cyber Security Course in 2021	Ara, Christchurch

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: