NZ Incident Response Bulletin

Standard Edition – November 2022 – Issue #46

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.

Not subscribed to our Premium Bulletin? Click here to join.

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

How NZ's top 3 telcos are protecting Kiwis from cyber threats

The computer hacker who stole the personal data of almost 10 million customers of a telecommunications company in one of Australia's worst privacy breaches used techniques to conceal their identity, actions and whereabouts, police said on Friday. But Optus maintains it was the target of a sophisticated cyber attack that penetrated several layers of security.

1News spoke to telecommunications companies, Spark, Vodafone and 2degrees about their security measures and how they help keep their customers' data safe.

- Sam Sinnott, spokesperson from Vodafone, said it's aware of the cyber attack on Optus, "and like all large companies, we take our responsibilities around cyber security extremely seriously".
- A Spark spokeswoman told 1News it operates one of the largest security operation centres in the country with over 180 security subject matter experts.
- The CEO of New Zealand's third largest telecommunications company told 1News "customers can feel secure that cyber security and protecting their data is of the utmost importance to us".

Education Ministry puts record keeping software on hold due to cybersecurity concerns

The threat of hackers has stalled a $40m school IT project for more than a year. The Education Ministry paused the roll out of Te Rito, a system that would help early childhood centres, schools and the ministry share and store information about students, in the middle of last year. The ministry said it reviewed schools' systems for storing student information after major cyber security breaches in New Zealand in June last year.

It found problems with their ability to securely share data so it halted the roll out of Te Rito. "In reviewing the capability of Student Management Systems, we identified issues with the ability to exchange learner and ākonga data securely. We also needed to consider the capacity of the sector in implementing significant change," the ministry said. The ministry said the government was funding school IT improvements, including cyber security, and it had been consulting on a plan for the work through to 2030.

The E-team: Parliament and cyber security

Parliament takes security seriously. Getting into the precinct is similar to going through an airport. But it's not just physical security they focus on, because the biggest threats can come in through the smallest holes. Parliament has its own Cyber Security team headed by Derek Robson.

They manage a wide range of risks ranging from phishy or threatening emails through to preventing electronic spying or other state sanctioned e-naughtiness. For example Derek Robson's team provide travelling MPs with burner phones and laptops if they are heading somewhere problematic. "We'll hook them up with a cellphone that's blank: fresh phone number, no contacts, no data. They can use it while they're travelling. When it comes back we can clean it, wipe it, or potentially shred it." Yes he did actually include "shred it" as one of the options. The world has moved on since the days of Le Carre, as Robson makes clear. "You don't need to get a spy into the embassy if you can get a USB stick into the embassy."

World

Former Uber security chief convicted of covering up 2016 data breach

A former chief security officer for Uber was convicted Wednesday of federal charges stemming from payments he quietly authorized to hackers, who breached the ride-hailing company in 2016. Joe Sullivan was found guilty of obstructing justice for keeping the breach from the Federal Trade Commission, which had been probing Uber's privacy protections at the time, and of actively hiding a felony. The verdict ended a dramatic case that pitted Sullivan, a prominent security expert, who was an early prosecutor of cybercrimes for the San Francisco U.S. attorney's office, against his former government office. In between prosecuting hackers and being prosecuted, Sullivan served as the top security executive at Facebook, Uber and Cloudflare.

Outsourcer Interserve fined £4.4m for failing to stop cyber-attack

Britain's data watchdog has fined the construction group Interserve £4.4m after a cyber-attack that enabled hackers to steal the personal and financial information of up to 113,000 employees. The attack occurred when Interserve ran an outsourcing business and was designated a "strategic supplier to the government with clients including the Ministry of Defence". Bank account details, national insurance numbers, ethnic origin, sexual orientation and religion were among the personal information compromised. The Information Commissioner's Office (ICO) said Interserve Group broke data protection law because the company failed to put appropriate measures in place to prevent the cyber-attack, which happened two years ago.

Germany fires cybersecurity chief 'over Russia ties'

Germany's cybersecurity chief has been fired after allegations of being excessively close to Russia through an association he helped set up. Arne Schönbohm had led the Federal Cyber Security Authority (BSI) - charged with protecting government communications - since 2016. German media have accused him of having had links with people involved with Russian intelligence services.

The interior ministry is investigating allegations made against him. But it confirmed he had been fired with immediate effect. Mr Schönbohm had come under scrutiny after his potential links to a Russian company through a previous role were highlighted by Jan Böhmermann, the host of one of Germany's most popular late-night TV shows.

Cyber responders are outnumbered and under pressure as they defend our modern way of life

As cyber incidents quickly multiply, what's worrisome is that the men and women with the skills to defend against them are still in very short supply worldwide. A recent global study found that it's common for 68% of incident responders to have to defend against two or more attacks simultaneously. Inevitably, many businesses are left without manpower in the face of a cyber crisis. Simply put, incident responders are outnumbered. Even so, they are still showing up, often overwhelmed, pushing through a considerable mental strain according to the data. In fact, disruptive attacks like ransomware have exacerbated the pressure and psychological demands of cyber frontline responders.

British Hacker Charged for Operating "The Real Deal" Dark Web Marketplace

A 34-year-old U.K. national has been arraigned in the U.S. for operating a dark web marketplace called "The Real Deal" that specialized in the sales of hacking tools and stolen login credentials. Daniel Kaye, who went by a litany of pseudonyms Popopret, Bestbuy, UserLoser, and Spdrman, has been charged with five counts of access device fraud and one count of money laundering conspiracy. Kaye was indicted in April 2021, and subsequently consented to his extradition from Cyprus to the U.S. in September 2022.

Spending on cyber security to hit $188bn next year

Cyber security spending will also enjoy double-digit growth in 2024 until cheaper solutions enter the market. Spending on cyber security and keeping businesses safe will grow by 11 per cent to reach $188bn (£167bn) next year, according to Gartner. And cyber security spending will continue that double-digit growth through 2024 until cheaper solutions become available. Gartner includes all information security and risk management products and services in its forecast. Security services including consulting, hardware support, implementation and outsourced services are the largest category of spending, expected to reach $77bn in 2023 compared with almost $72bn this year.

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 this webpage.

11/10/2022 - Fortinet software authentication bypass vulnerability

26/10/2022 - TVNZ - Crime: Need vs Greed

Our Views:

Continuous Vulnerability Management

Continuous Vulnerability Management exemplifies why cyber security governance is most effective when treated as an ongoing business process rather than goal to set and achieve. In the modern business IT landscape, we rely on a wide variety of different devices and tools to get work done.

While these tools enable incredible productive gains, they also pose a risk. Attackers and security researchers are constantly on the search for vulnerabilities in operating systems, applications, and protocols. Many of the vulnerabilities found are critical and enable some level of unauthorised access to your IT environment. Once discovered, attackers rush to develop methodologies to leverage these vulnerabilities and achieve their malicious goals, getting their hands on your money. The end goal of their malicious access is a broad swath of attacks, including ransomware, business email compromise, data theft, and cryptocurrency mining among others.

According to research from Tenable, last year there were around 20,000 Common Vulnerabilities and Exposures (CVE), which is a compilation of publicly disclosed information security issues.

There have been a number of examples of critical vulnerabilities causing global impact. For example, in January 2021, vulnerabilities were found in the common email server software Microsoft Exchange. These vulnerabilities could be leveraged to give attackers administrator privileges on the device hosting the email server and access to connected devices on the network. Estimates suggest around 250,000 Exchange servers world-wide were accessed by attackers. This access was leveraged primarily for ransomware and data exfiltration. Fallout from these included services being disabled, expensive IT infrastructure rebuilds and confidential data being leaked to the dark web.

As it was a "zero-day" attack, many organisations were hit before the vulnerability became public knowledge. For the others, the following days became a test of their Vulnerability Management procedures. Some organisations were monitoring intelligence feeds, identified the issues, sought best practice guidance, and remediated the issues promptly enough to avoid falling victim. Others lagged behind. Over the following two weeks, those who had failed to remediate the issue often became victims.

It's not just zero-day vulnerabilities that have a large impact. Attackers also utilise information provided by security researchers and relevant software vendors to design attacks. While these attacks may not work against patched systems, those slow to implement the patches are juicy targets. Research has shown that over the last 10 years, attackers have become faster and faster at turning known vulnerabilities into full attack procedures. This means the window you have between a patch being released and your unpatched systems becoming compromised is shortening.

Having an effective vulnerability management program enables you to keep ahead of the attackers and keep your IT systems safe. You will need to balance how you keep your systems up to date, between using a cheaper 'manual' method, or subscribing to 'automated' software. Ultimately, either option will improve your security if you are currently managing your vulnerabilities on an ad-hoc manner.

If you operate in the public sector, you will also need to consider the requirements set out in the New Zealand Information Security Manual, published by the Government Communications and Security Bureau. According to the latest release from September 2022, agencies must ensure security patches are applied in a timely fashion to manage software and firmware corrections, vulnerabilities and performance risks, covering both evaluated and non-evaluated software and IT equipment.

The Australian Cyber Security Centre go one step further in recommending time frames for how often to check for patches and when they should be applied, e.g:

- For advanced cyber threats, check internet-facing services daily, commonly targeted applications weekly and other applications fortnightly.
- For internet-facing services: apply patches within two weeks, or within 48 hours if an exploit exists.
- For commonly targeted applications: apply patches within one month.

Something as simple as five minutes spent updating a piece of software could save your organisation weeks of downtime and millions of dollars in response and recovery costs. When a critical security patch was released months ago and widely publicised, failing to patch becomes inexcusable.

We recommend following the CIS Controls Continuous Vulnerability Management safeguards. The first four safeguards should be a starting point for any organisation, large or small, to manage their vulnerabilities:

- Establish and Maintain a Vulnerability Management Process
- Establish and Maintain a Remediation Process
- Perform Automated Operating System Patch Management
- Perform Automated Application Patch Management

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.

Subscribers to the premium edition also obtain access to the following additional information:

- Cyber Governance
- Cyber Incident Landscape
- Cyber Incident Response Resources
- Cyber Framework and Control Updates, Surveys and Research

Click here if you wish to subscribe to our Premium Edition of the Bulletin.

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

Further Resources:

Alerts	Data Breach Response	Forensic Technology
Cyber Incident Simulations	Social Media Investigations	Guide for NZ Law Firms

Share our Bulletin: