
# NZ Incident Response Bulletin

Standard Edition - February 2020

## In this issue:

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

| | | |
|---|---|---|
| New Zealand | Cyber Incident Detection | OWASP New Zealand Day |
| World | Detect Key Considerations | International Conference on Testimony, Forensics and Law Sciences |
| | Practical Actions for Detection | CybersecCon |

*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.*

Transparency and trust present biggest impacts to digital identity in 2020

New Zealanders are increasingly concerned about protecting their digital identity with 79% expressing further concern about the use of personal data by organisations according to new research by Digital Identity New Zealand (DINZ). "Trust is one of the key issues facing digital identity as we move into the 2020s. We are currently operating in an environment of low trust, if not mistrust," says Andrew Weaver, Executive Director of DINZ.

The monetisation of personal information and invasive or murky methods of advertising are no longer being tolerated by New Zealand consumers. A major trend for 2020 predicted by DINZ is the growing emergence of more openness and transparency in how kiwi businesses interact with their customers in this area. Transparency regarding the flow of money and information is required for both verification and to build trust.

The government is currently working on a new trust framework to assist in providing greater certainty in the New Zealand environment in this area. The new framework aims to build confidence and enable companies to invest further and innovate to deliver collaborative solutions that allow consumers to take control of their identity information.

Card skimming tech seized in Auckland

Technology used for the purposes of fraudulently withdrawing money from Automated Teller Machines (ATMs) was seized in Auckland this month with two people being arrested under Section 391 (91) of the Customs and Excise Act 2018. The equipment seized included computers and electronic devices, ATM skimming devices, blank cards and a card writing machine; and tools and equipment for manufacturing further skimming devices.

Skimming involves inserting a device that reads data contained on bank cards magnetic strips. These devices are then placed in ATM readers to obtain credit card details. Vigilance when using ATM machines is the only protection against having credit card details stolen in this manner.

**Subscribe for free to our new service "Cyber Alerts and Tips" on the Web or YouTube**

**We have also improved the user experience of our entire Website**


# NZ Incident Response Bulletin

Standard Edition - February 2020

## World

Citrix and FireEye Mandiant share forensic tool for CVE-2019-19781

Multiple attempts to exploit the Citrix vulnerability (CVE-2019-19781) in its Application Delivery Controller and Citrix gateway products have been observed in the wild. The ultimate aim seems to be to use the vulnerability to deploy ransomware on victims' systems.

As a result, Citrix has announced they have teamed with FireEye Mandiant to deliver a free tool that aids customers in the detection of any compromise related to CVE-2019-19781. The tool is available under the Apache 2.0 open source license and running this locally on a Citrix instance will result in an assessment of potential "Indicators of Compromise". It is highly recommended this tool be run as soon as possible in addition to implementing published mitigation steps until a patch is released for this vulnerability.

Insurers look to curb ransomware exposure as U.S. cyber rates rise

Insurance companies in the US are increasing cyber-insurance rates by as much as 25% and trying to limit their exposure to vulnerable customers after a year of increasingly costly claims. While overall ransomware attack numbers seemed to come down in 2019, the attacks that occurred were more sophisticated, and often resulted in lasting damage. Ransom demands were also higher with some reports indicating the ransom demands grew by a third between Q1 and Q3 2019, at times becoming disproportionate to the targets ability to pay.

In addition to increasing premiums, the increasing costs involved with cyber insurance means that insurance companies are looking at a variety of other methods to manage this. Possible techniques include investigating whether ransomware becomes a separate product from general cyber coverage, introducing co-insurance where policyholders pay 20-30% of the ransom, underwriting firms that have added cybersecurity network features, and lowering amounts paid to companies who are deemed high risk.

Some insurance companies may require their policyholders to have data backup procedures confirmed before offering coverage, and many are looking to drive their clients into a situation where they are better protected from these attacks.

Microsoft issues critical Windows security fix after tipoff from U.S. NSA

Microsoft rolled out an important security fix as part of its regular 'patch Tuesday' in January after the U.S. National Security Agency informed them of a serious flaw in the Windows operating system. This announcement is the first time the NSA has publically claimed credit for prompting a patch and is part of a move to increase transparency within the security research community.

The flaw in question has the potential to allow a hacker to forge the digital certificates used by some Windows systems to authenticate and secure data. As yet there is no evidence that this flaw has been abused, however updating as soon as possible is recommended.

Charges Dropped Against Men Who Broke Into Iowa Courthouses

Charges were dropped against two cybersecurity workers who were arrested after breaking into an Iowa courthouse in September as part of a security test conducted by state court administrators.

The cybersecurity company they worked for were contracted with state court officials to conduct security tests at Iowa courthouses and the state court building. When caught inside the Dallas County Courthouse in Adel, Officers initially responding were about to release the men after confirming they were fulfilling a state contract, but Dallas County Sheriff arrived and insisted they be jailed.


# NZ Incident Response Bulletin

Standard Edition - February 2020

## Our Views:

*This month's theme is "Cyber Incident Detection using NIST and the Cybersecurity Framework".*

### Cyber Incident Detection

Recent news shows that the cost to businesses of cyberattacks such as data breaches are growing. Incident detection time is one area which contributes to the ultimate cost of a breach to the impacted business. The longer a system breach remains undetected, the longer an attacker has to cause damage, and the harder it becomes to investigate the event. According to IBM, the average time taken to identify a breach was a full seven months in 2019.

As cyberattacks continue to grow in complexity, businesses require proactive strategies to combat them and minimise risk. The NIST cybersecurity framework was created to support businesses to protect their critical assets and "Detect" is the third function in this framework.

Cyber detection methods act similarly to physical detection methods such as smoke alarms and $CO_2$ monitors in that they alert you to pending danger. They act as an early warning system highlighting any potential and active cyber threats in your environment. The ultimate goal is to detect any cyber incident in a timely fashion and reduce its impact.

*"The Detect function involves the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event." – NIST*

### Detect Key Considerations

There are three general areas for consideration under Detect in the NIST framework as follows:

1. **Detecting Anomalies and Events -** "Anomalous activity is detected in a timely manner, and the potential impact of events is understood."

   This area includes the ability to recognise and subsequently detect anomalous activity. Establishing thresholds and alerts for system activity is critical here.

2. **Continuous Security Monitoring –** "The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures."

   This area involves monitoring of the network, physical environment, and personal and service provider activity for any anomalous activity including unauthorised access, actions, connections, devices and software.

3. **Detection Processes -** "Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events."

   This area includes defining appropriate roles and responsibilities to ensure accountability, testing detection processes and continuously improving them.

### Practical Actions for Detection

Examples of immediate actions we recommend a business take to increase their detection capabilities include:

- Reviewing any cloud-based systems to ensure that thresholds for activities such as spend, storage or use are configured and that these thresholds trigger an alert when exceeded. Cloud service providers offer products and solutions that allow you to monitor activity and receive alerts. For example Azure Monitor or AWS Cloudwatch

- Reviewing systems such as Microsoft Office 365 to ensure alerts are triggered when actions such as mail forwarding rules are changed, or passwords reset. More information about the kind of activity you can monitor and how to set and manage alerts can be found here. Alert Policies can also be created to simplify this activity across a network.


# NZ Incident Response Bulletin

Standard Edition - February 2020

## Upcoming Events:

| Date | Event | Location |
|---|---|---|
| 20-21 February 2020 | OWASP New Zealand Day | Auckland |
| 27-28 February 2020 | International Conference on Testimony, Forensics and Law Sciences | Sydney |
| 28 February 2020 | CybersecCon | 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: