NZTech

CONFERENZ

NEW ZEALAND CYBER SECURITY SUMMIT

Securing New Zealand businesses against the next generation of cyber attack

BRIEFING PAPER

CONNECT

PROMOTE

ADVANCE

@NZTechIA

Published: October 2019

NEW ZEALAND CYBER SECURITY SUMMIT

Securing New Zealand businesses against the next generation of cyber attack

OCTOBER 2019

This NZTech briefing paper provides insights from the recent New Zealand Cyber Security Summit in Wellington, including key observations from roundtable discussions involving senior executives and security specialists from a broad cross section of government agencies, large private corporations and the tech sector.

EXECUTIVE SUMMARY

Each year, the cyber threat landscape evolves and we have to continually adapt as criminals seek new ways to disrupt businesses and extract financial gain. However, there is still a relatively low level of awareness in New Zealand businesses about the risk of cybercrime and its impact. This is reflected in part with less than five percent of businesses having any form of cyber insurance. Those who are concerned about security, still tend to rely solely on security software as the solution.

However, as security systems get better at defending organisations there has been a big swing by criminals to targeting the human factor. It is easier to find someone who will click a link than it is to find a way to exploit a browser or operating system. Phishing has grown to be one of the leading causes of cybersecurity issues for Kiwi's according to the Computer Emergency Response Team (CERT NZ), the Government cyber response agency, accounting for 55 percent of all reported incidents by businesses.

The NZTech Security Leaders Forum at the 2019 New Zealand Cyber Security Summit hosted a group of cyber leaders to explore the challenges of securing against the human factor. A combination of approaches will be needed to help New Zealand businesses reduce their cybersecurity risk, including:

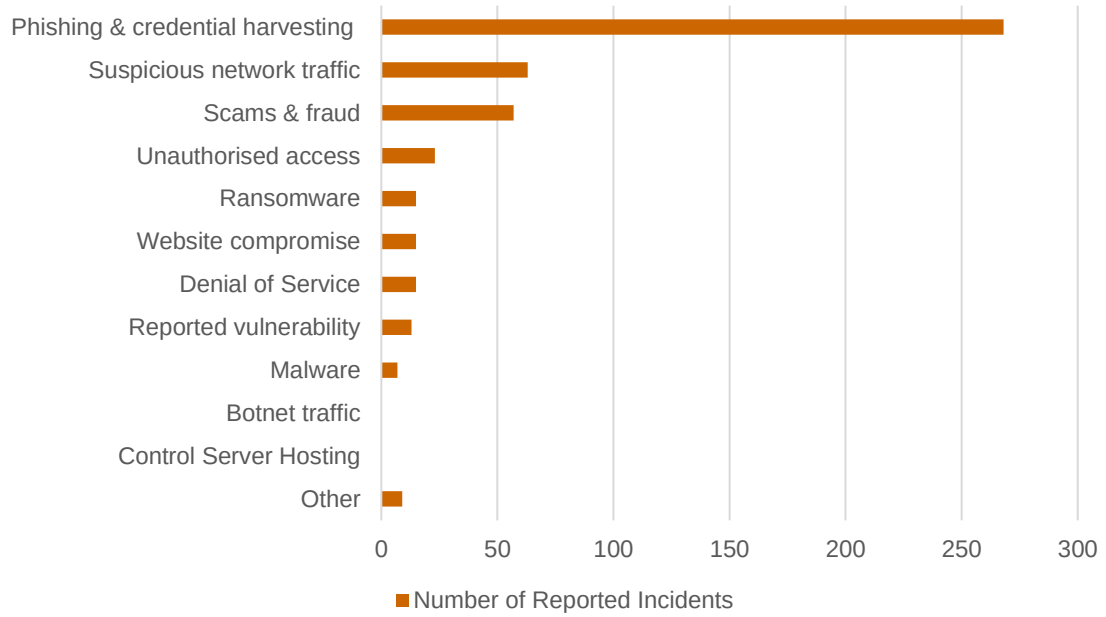
- **We need to raise awareness:** a substantial, planned, national investment should be made in raising awareness of the importance of cybersecurity and the simple steps that can be taken to dramatically reduce individual and business risk.
- **We need to support our teachers:** as the new digital technology curricula is deployed in 2020, we should develop teaching materials to further enable teachers to create course work about cybersecurity.
- **We need to develop simple tools:** to enable businesses to self-assess their risk in ways that make it relevant for them and to help them identify ways to improve their security score.

THE EVOLVING THREAT LANDSCAPE

The 2019 New Zealand Cyber Security Summit examined the evolving cyber landscape and what it means for the New Zealand business ecosystem. As we operate within a global digital environment, all businesses, governments and societies are coming under an increasingly large number of threats from cyber criminals. In fact, as a developed, wealthy country, New Zealand is identified as a notable target.

In 2018 alone, New Zealanders reported a $14 million loss due to cybersecurity attacks. This is considered the proverbial 'tip of the iceberg' as many more attacks likely remain unreported due to business concerns of negative press. Cyber attacks have continued to grow with a dramatic increase of 21 percent in reported incidents between the first and second quarters of 2019 and reported financial losses rising to $6.5 million in the second quarter alone. Of the reported cyber attacks on New Zealand businesses during the second quarter of 2019, 55 percent were attributed to phishing and credentials harvesting, as criminals increasingly target humans, rather than systems and infrastructures. Personal interaction is the last line of defence and is easier and more profitable to exploit.

Figure 1. Reported Attacks on New Zealand Businesses



Source: CERT NZ, Q2 2019 Quarterly Report

Responding to the Changing Landscape

As stated in the 2019 Cyber Security Strategy for New Zealand, there is no simple way to articulate the cybersecurity risk to New Zealand, because the threats are so diverse. However, it is clear that trust and confidence in the internet and our infrastructure is vital for New Zealand and New Zealanders - for our economy, society and national security.

In order to help maintain trust, in 2019 the New Zealand Government launched its third iteration of the New Zealand Cyber Security Strategy. The strategy identifies five priority areas to improve cyber security in New Zealand including cybersecurity aware citizens, a strong and capable security workforce, being internationally active, building a resilient and responsive infrastructure and proactively tackling cyber crime.

The national strategy provides a guiding set of priorities for Government and industry to help address the shifting threat landscape. The New Zealand Cyber Security Summit also helps New Zealand organisations respond to the evolving threat landscape with candid information sharing of the latest challenges, including new ways attackers are exploiting people, building resilience using artificial intelligence, zero trust automation, leveraging threat intelligence and rethinking our approach to cybersecurity.

THE HUMAN FACTOR

The annual Cyber Smart Week campaign, driven by CERT NZ is a response to the need to help raise awareness of the risks of cyber attacks and their implications. As attacks increasingly grow in frequency throughout New Zealand they can affect anyone. It is not just large organisations or businesses who are affected, but small business and everyday New Zealanders are also being impacted. Many of these attacks aren't targeting anyone specifically, but are looking for easy ways to gain money or information. However, most people still don't think a cyber attack will happen to them.

The urgent need to raise awareness

The general lack of understanding continues to create the weakest link in our country's cyber defence. This is clearly illustrated by the growth in phishing and credentials harvesting, as criminals have also identified the human factor as most vulnerable. However, there are some very simple steps that individuals and businesses can take to dramatically reduce the risks that the human factor creates. These steps are so simple to understand and implement that we can assume the reason they are not happening is simply a lack of awareness and a disconnect between the risks and relevance for the individual.

As noted on the CERT NZ website, businesses that regularly install software updates, backup data and use two factor authentication (2FA), significantly reduce their cyber risk. The addition of a plan for when something goes wrong, also ensures a rapid response that further reduces the impact.

Raising awareness of cyber crime, how to avoid it and how to respond to it, should be developed across all parts of our society. There are opportunities to introduce learning at an early age in all schools via the new digital technology curricula. However, a broader campaign that helps educate mature adults, business owners and the general public is needed to reach those most at risk.

Raising awareness should be everyone's responsibility, but it may need to be driven initially by the Government to create impetus and gain momentum. Industry bodies such as the Employers and Manufacturers Association (EMA) or regional Chambers of Commerce could then amplify the message and provide trusted pathways to further raise understanding.

People will still click strange links!

Despite increased awareness, we should assume that people will still unknowingly click on strange or suspicious links. As criminals use more advanced technologies and social engineering techniques, it becomes more difficult to differentiate what is real and what is fake. For this reason, cybersecurity systems and responses to breaches should be designed from the perspective of 'not if, but when'.

An increased used of contextual multi-factor authentication (MFA) is a step towards reducing the human risk, however approaches like these require skilled IT support to set up. Small and medium sized enterprises (SME's) therefore require trusted local partners with the right cyber skills and experience. Locating a skilled partner can be challenging. There may be a need for some form of certification of cyber skills, given the critical nature of good cybersecurity for our economy.

SIMPLE TOOLS ARE NEEDED

Despite regular media coverage of cyber breaches, another challenge is appreciating their relevance as individuals or business owners. This general understanding of risks is lacking across most businesses. However, in most cases, cybersecurity risk can be easily assessed, using simple tools like a risk calculator.

Simplifying security assessments to just a few short questions would help make cyber risk more relevant to more people. Any tools need to be both easy to find and easy to use. Developing a common national tool with multiple front ends could enable industry benchmarking and the ability to provide feedback on where improvements could be made. The addition of gamification and security scores could further enhance engagement.

This may be another way for Government and industry bodies to collaborate on raising awareness in a way that provides direct relevance for individuals and business owners. The creation of a simple online risk calculator also provides a tangible tool to support a national awareness raising campaign.

RECOMMENDATIONS

It is generally agreed that cyber security awareness is improving, however there was consensus that more could be done immediately to increase New Zealand's cyber resilience. The Security Leaders Forum at the 2019 New Zealand Cyber Security Summit and NZTech make the following recommendations:

1. Raise awareness via the education system

Having recently introduced digital technology into the New Zealand curricula, now is the perfect time to raise awareness of the importance of cybersecurity for the next generation. In 2020, the digital technology curricula will be delivered in all schools throughout New Zealand with elements of the curricula focused on digital citizenship, which could include cybersecurity. Teachers will be looking to trusted teaching aids as they design their course work, so now is the right time to collaboratively design these supporting materials.

The Ministry of Education should play a role in helping raise awareness of the importance of cybersecurity as a critical foundation for digital technology learning. With guidance, the tech sector could potentially assist with the development of relevant teaching material.

2. Develop and deploy simple tools

To help individuals and businesses understand potential risks, simple tools such as risk calculators should be developed and deployed. Ensuring they are simple to use, (like a mortgage calculator, for example) will help contextualise the issues for the general population. If a standard approach is used, this tool could be deployed across multiple channels, for example on the CERT NZ website, via industry bodies and through insurance companies.

The Government should consider developing an online tool that allows businesses to calculate their 'Security Score'. This could include benchmarking across industries, gamification and recommended improvements to help stimulate improvement.

3. Further invest in a national awareness campaign

A significant amount of national resilience could be easily achieved through the broad application of simple approaches to better cybersecurity. Excellent recommendations are currently detailed on the CERT NZ website, however very little investment has been made in communicating key information to New Zealanders before they need it.

A concerted national push to raise awareness should include the use of two-factor authentication, the risk of clicking on strange links, the importance of updating devices and how to manage strong passwords.

4. Certification or badging of providers

In the previous iteration of the New Zealand Cyber Security Strategy, 2015 there was a proposal to introduce a 'cyber credentials' scheme to allow businesses to demonstrate that they are cyber secure. In an extension of this concept, it is recommended that IT companies providing cyber security advice and services should be certified or licensed to ensure that consistently high standards of cyber security are available nationally. If electricians have to be certified, why shouldn't security providers?

CONCLUSION

In conclusion, as cyber criminals seek new ways to disrupt businesses and extract financial gain, we must continually evolve to protect ourselves and our businesses. While it is generally agreed that New Zealanders cybersecurity awareness is increasing, there is still an urgent need to dramatically improve our nation's cyber resilience. The Security Leaders Forum at the 2019 New Zealand Cyber Security Summit recommends several approaches. These include a concerted effort to further raise awareness, the deployment of simple assessment tools, certification of security service providers and the development of supporting teaching materials for use in the education system.

NZTech
L1 Building C, 14-22 Triton Drive, Auckland 0632, New Zealand
Ph +64 9 475 0204
www.nztech.org.nz