(NCSC, 2020)

NATIONAL CYBER SECURITY CENTRE

CYBER THREAT REPORT 2019/20

The National Cyber Security Centre is hosted within the Government Communications Security Bureau.

5th

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Foreword

The National Cyber Security Centre (NCSC), part of the Government Communications Security Bureau (GCSB), helps protect New Zealand's nationally significant organisations from advanced cyber threats and responds to cyber incidents that may impact New Zealand's national security. This report aims to provide insight into the cyber threats and incidents encountered by these organisations this year.

From 1 July 2019 to 30 June 2020, the NCSC recorded 352 cyber security incidents. Self-reported cyber incidents continue to increase, reflecting the growing cyber awareness and willingness to report incidents among New Zealand organisations. The NCSC's international partners are also increasingly notifying the NCSC about cyber incidents affecting New Zealand organisations, highlighting the value of international partnerships, as well as the transnational nature of activity affecting New Zealand.

The NCSC continues to provide a significant cost avoidance benefit to New Zealand. Over the year, the NCSC provided a cost benefit to New Zealand's nationally significant organisations in the order of $70.5 million. Since June 2016, the NCSC's capabilities reduced harm from malicious cyber activity by around $165.2 million.

The NCSC continues to build and grow New Zealand's cyber defence capabilities, most recently through the successful pilot and initial delivery of Malware Free Networks (MFN). MFN will bring the NCSC's cyber security capabilities to a much larger number of consenting New Zealand organisations.

In response to the global COVID-19 pandemic, the NCSC rapidly changed the way it works to minimise the risk to staff and to maintain continuity of essential services. The NCSC also published cyber security advice and resources to encourage a high level of cyber resilience and awareness throughout the national pandemic response.

During late 2020, a global campaign of denial of service (DoS) events affected a range of New Zealand organisations. These events demonstrated the willingness of cyber actors to carry out persistent malicious activity that has a high national impact. Throughout the activity, the NCSC provided advice to New Zealand's nationally significant organisations.

In addition to responding to cyber threats, the NCSC works proactively with organisations to build their cyber resilience. In the past year, two flagship products about information security governance and incident management were released, and the NCSC contributed to a range of sector-based information sharing forums where sectors enhance collaboration on cyber security challenges.

The NCSC aims to provide unique insight into the nature and extent of serious cyber threats targeting New Zealand's nationally significant organisations. In an increasingly complex and adversarial international cyber environment, the NCSC hopes this report helps to improve the understanding of the cyber threats to New Zealand.

Hamish Beaton
Director, National Cyber Security Centre

Overview

By publishing the Cyber Threat Report 2019/20, the NCSC seeks to increase the understanding our customers and the broader public have about the cyber security threats to New Zealand's nationally significant organisations. This report also aims to promote greater awareness of the work the NCSC does to safeguard New Zealand's nationally significant organisations.

This report covers the NCSC's role as the lead government agency for responding to state-sponsored cyber threats and cyber threats that may affect New Zealand's national security. This includes an overview of some of the NCSC's cyber defence capabilities and services, key areas of work over the 2019/20 fiscal year, and domestic and international relationships.

An overview is also provided about the international cyber threat landscape, with a focus on identifying trends and tradecraft which can inform efforts to defend the New Zealand's nationally significant organisations. This includes malicious cyber activity counter to internationally accepted norms of behaviour in cyberspace, the continued prevalence of data breaches, the exploitation of known vulnerabilities, and the emergence of well-planned ransomware incidents targeting large multinational organisations.

Also provided is a summary of New Zealand's domestic cyber threat landscape, with specific reference to cyber incidents which affected New Zealand's nationally significant organisations. This includes providing insights into some of the ways the NCSC is safeguarding New Zealand's nationally significant organisations from malicious cyber actors of all types.

The report concludes by highlighting what this means for New Zealand's nationally significant organisations, including some straightforward, practical steps organisations – of any size – can take to increase their cyber resilience. Organisations seeking further information about increasing their cyber security and resilience can visit the NCSC website (www.ncsc.govt.nz), where cyber security guidance and resources are regularly shared with the public.

Te Reo Māori terminology

The New Zealand Government, including the GCSB, is committed to increasing the use of Te Reo Māori, one of New Zealand's official languages. Here are a few cyber security terms you can learn and use:

Whakahaumaru	– security
Aumangea ā ipurangi	– cyber resilience
Taihara ā ipurangi	– cyber crime
Hītinihanga	– phishing
Pūmanawa utu uruhi	– ransomware
Whakaraeraetanga	– vulnerability
Whakatūturu pārongo	– credentials
Raraunga wāwāhi	– data breach

By the numbers

P.

30%

had indicators of links to state-sponsored actors

38% IN 2018/19

41% preparation

42% engagement

7% presence

10% effect/ consequence

352

cyber incidents recorded

339 IN 2018/19

83%

incidents detected before significant harm occurred, 17% post-compromise

$70.5 million

worth of harm prevented to New Zealand's nationally significant organisations in 2019/20

$165.2 MILLION SINCE JUNE 2016

82

security advisories or incident reports disseminated in 2019/20

THE NCSC IN A TYPICAL MONTH

Detects 12 cyber intrusions affecting one or more of New Zealand's nationally significant organisations, through the NCSC's CORTEX capabilities

Receives 18 new incident reports or requests for cyber security assistance, unrelated to the NCSC's CORTEX capabilities

INCREASING CYBER RESILIENCE OVER THE YEAR

Recorded 1,770 engagements with customers

Published 24 reports for general customers

Facilitated 20 regional and sector-based security information exchanges

New Zealand landscape

New Zealand's nationally significant organisations continue to be frequently targeted by malicious cyber actors of all types. Throughout 2019/20, state-sponsored and non-state actors targeted public and private sector organisations to steal information, generate revenue, or disrupt networks and services .

Malicious cyber actors have shown their willingness to target New Zealand organisations in all sectors using a range of increasingly advanced tools and techniques. Newly disclosed vulnerabilities in products and services, alongside the adoption of new services and working arrangements, are rapidly exploited by state-sponsored actors and cyber criminals alike. A common theme this year, which emerged prior to the COVID-19 pandemic, was the exploitation of known vulnerabilities in internet-facing applications, including corporate security products, remote desktop services and virtual private network applications.

Organisations with poor security are more likely to become a victim of malicious cyber activity, and are much less likely to detect such activity before harm is caused. It is important organisations continue to adhere to strong cyber hygiene measures, such as regular patching and account audits, to ensure their systems are not susceptible to malicious exploitation.

Cyber security by consent

The NCSC works with organisations with their willing participation. Recognising this, the Intelligence and Security Act 2017 (ISA) does not require warrants for all activities. The NCSC is directly empowered to provide immediate assistance to organisations who have consented to receiving it, without the additional requirement of a warrant. This facilitates more effective and timely responses to potentially significant cyber incidents.

NCSC recorded cyber incidents

The NCSC identifies cyber incidents from a number of sources, including detection through its advanced cyber defence capabilities, self-reporting by victims, or reporting from domestic and international partners. NCSC incidents either involve organisations of national significance, or cyber threats that may affect New Zealand's national security and economic wellbeing.

During the 2019/20 financial year, the NCSC recorded 352 cyber incidents. Due to the NCSC's focus on nationally significant organisations, these incidents represent only a small fraction of the cyber security incidents that affected New Zealanders and New Zealand organisations.

For example, New Zealanders reported 5,653 incidents to CERT NZ over the year. Many compromises are also never detected or reported to New Zealand government agencies.

In a typical month, the NCSC's CORTEX capabilities detect 12 cyber intrusions affecting New Zealand organisations. In addition, the NCSC receives an average of 18 new incident reports per month, unrelated to CORTEX detection. These are typically self-reported by the impacted organisation or reported by the NCSC's partners.