MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

29 June 2021

File No. DOIA 2021-2436

Phil Pennington
Phil.Pennington@rnz.co.nz

Dear Phil Pennington

Thank you for your email of 31 May 2021 to the Ministry of Business, Innovation and Employment (the Ministry) requesting, under the Official Information Act 1982 (the Act), the following information:

> *Online material says CERT collates a profile of the cyber security threat landscape in New Zealand, 4 times a year.*
>
> 1. *Pls provide these, going back 3 years*
>
> *CERT also reports on cyber incidents, analyses threats, shares information and advice, coordinates incident responses, promotes good cyber security practices*
>
> 2. *Pls provide any CERT advice/analysis/recommendations in response (in full or in part) to deficiencies identified in the cyber security of DHBs in the last 3 years*
>
> *CERT coordinates government agencies' responses to reported cyber security incidents*
>
> 3. *Pls detail CERT's coordination of agency responses to CS incidents involving DHBs in the last 3 years, at least in enumerating them and locating them, but also providing more details as you can about how CERT helped*

In response to part one of your request, the Ministry's Computer Emergency response Team (CERT NZ) proactively release quarterly reports here: www.cert.govt.nz/about/quarterly-report/. As such this part of your request is refused under section 18(d), as the information requested is publicly available.

The quarterly reports provide an overview of the cyber security incidents which are reported to CERT NZ that impact New Zealanders. The types of advice CERT NZ provides to prevent these incidents can be found here: www.cert.govt.nz/individuals/guides/. Please note all personally identifiable information contained within the quarterly reports has been removed to protect the privacy of reporters.

In response to part two of your request CERT NZ has received 14 reports that relate to the Ministry of Health or New Zealand District Health Boards (NZ DHB) and have been summarised in part three of your request. Please note CERT NZ's primary role when dealing with large organisations such as NZDHB's is to contact the IT Security team at the relevant organisation and ensure they are aware of the incident.

In response to part three of your request please refer to the following table:

Date	Incident	Summary
25/09/2018	14182	Website vulnerability, DHB advised of incident.
03/10/2018	14285	Website vulnerability, DHB advised of incident
03/10/2018	14286	Website Vulnerability, DHB advised of incident.
22/02/2019	16070	Website vulnerability, MoH advised of incident.
15/08/2019	18543	Compromised email account, (Reported by PHO), (no assistance required).

26/08/2019	18718	Phishing email reported by DHB, DHB advised.
12/09/2019	19006	Website compromised, dealt with internally by DHB IT.
09/03/2020	21344	Compromised email account sending phishing. DHB advised of incident.
28/04/2020	22347	Compromised email account sending phishing. DHB already aware and the account had been disabled.
11/06/2020	23076	Website hosting phishing kit. DHB advised of incident.
28/08/2020	24428	Website vulnerability, DHB advised of incident.
03/12/2020	27136	Advised by DHB of an incident relating to compromised email accounts. CERT NZ provided assistance in advising the affected parties.
26/01/2021	28313	Web service vulnerability, DHB advised of incident. DHB acknowledged our correspondence and advised they will look into the matter.
21/05/2021	30150	Compromised email account, (requested further info from reporter).

You have the right to seek an investigation and review by the Ombudsman of our response to your request. Information about how to make a complaint is available at: www.ombudsman.parliament.nz or freephone 0800 802 602.

Yours sincerely

Rob Pope
Director, CERT New Zealand
Ministry of Business, Innovation and Employment