UK Health
Security
Agency

By email
request-811786-0054c1b8@whatdotheyknow.com
request-815541-c7d4a5dc@whatdotheyknow.com

Our ref: 30/11/21/kl/1845
13/12/21/kl/1953

13 January 2022

Dear Gloria Zimba,

Re: Freedom of Information request - Information Technology Request

Thank you for your request received on 29 November and 13 December 2021 addressed to the UK Health Security Agency (UKHSA). In accordance with Section 1(1)(a) of the Freedom of Information Act 2000 (the Act), I can confirm that UKHSA does hold the information you have specified.

Request

1. Do you have a formal IT security strategy? (Please provide a link to the strategy)

A) Yes

B) No

2. Does this strategy specifically address the monitoring of network attached device configurations to identify any malicious or non-malicious change to the device configuration?

A) Yes

B) No

C) Don't know

3. If yes to Question 2, how do you manage this identification process – is it:

A) Totally automated – all configuration changes are identified and flagged without manual intervention.

B) Semi-automated – it's a mixture of manual processes and tools that help

track and identify configuration changes.

C) Mainly manual – most elements of the identification of configuration changes are manual.

4. Have you ever encountered a situation where user services have been disrupted due to an accidental/non malicious change that had been made to a device configuration?

A) Yes

B) No

C) Don't know

5. If a piece of malware was maliciously uploaded to a device on your network, how quickly do you think it would be identified and isolated?

A) Immediately

B) Within days

C) Within weeks

D) Not sure

6. How many devices do you have attached to your network that require monitoring?

A) Physical Servers: record number

B) PC's & Notebooks: record number

7. Have you ever discovered devices attached to the network that you weren't previously aware of?

A) Yes

B) No

If yes, how do you manage this identification process – is it:

A) Totally automated – all device configuration changes are identified and flagged without manual intervention.

B) Semi-automated – it's a mixture of manual processes and tools that help track and identify unplanned device configuration changes.

C) Mainly manual – most elements of the identification of unexpected device configuration changes are manual.

8. How many physical devices (IP's) do you have attached to your network that require monitoring for configuration vulnerabilities?

Record Number:

9. Have you suffered any external security attacks that have used malware on a network attached device to help breach your security measures?

A) Never

B) Not in the last 1-12 months

C) Not in the last 12-36 months

10. Have you ever experienced service disruption to users due to an accidental, non-malicious change being made to device configurations?
A) Never

B) Not in the last 1-12 months

C) Not in the last 12-36 months

11. When a scheduled audit takes place for the likes of PSN or Cyber Essentials, how likely are you to get significant numbers of audit fails relating to the status of the IT infrastructure?

A) Never

B) Occasionally

C) Frequently

D) Always

Response

In accordance with Section 1(1)(a) of the Act, UKHSA can confirm that the UKHSA holds some of the information you have specified. However, the information you have requested is exempt from disclosure in accordance with the *Section 24 – National Security* exemption of the Act.

In accordance with the relevant Information Commissioner's Office (ICO) guidance "national security" means the security of the United Kingdom and its people. The interests of national security include actions by an individual which are targeted at the UK, its system of government or its people and reciprocal co-operation between the UK and other states in combating international terrorism which is capable of promoting the United Kingdom's national security.

The Section 24 exemption applies where withholding the information is "required for the purposes of safeguarding national security". Required is taken to mean that the use of the exemption is reasonably necessary. Section 24 is a qualified exemption, which means that before applying the exemption, the UKHSA must consider the public interest arguments for and against disclosure of the requested information. The public interest inherent in maintaining Section 24 relates to safeguarding the UK's national security. It follows that we are concerned with the public interest of the UK and its citizens.

In order to determine whether the above exemption is sufficiently engaged the UKHSA must assess the public interest considerations. Accordingly, the UKHSA has set out below the factors it has taken into consideration in determining its disclosure position.

Factors which were considered in favour of release include:

- the public interest in transparency and commitment and the wish for PHE to be open and transparent;
- disclosing information to present a full picture to enable wider public scrutiny of decision making.

Factors supporting maintaining the exemption include:

- UKHSA consider that providing this information may pose a threat to the security of UKHSA infrastructure. By specifying any details relating to Network Monitoring; Service Disruption; IT Processes; Malware; Security attacks; Service disruption; or Cyber Audit Failings, it would be possible for a motivated threat actor to assess our organisations vulnerability, with view to targeting our network infrastructure. This could result in an exploitation of our infrastructure.
- disclosure of this information could make the UKHSA's ICT systems more vulnerable to cyber-attacks, which could lead to data breaches or cyber incidents that could place the organisation at risk, or place individuals who work for the organisation or whose personal information is held by the organisation at risk.

Taking into account the above factors, whilst there is a public interest in transparency around the UKHSA's IT processes and network infrastructure, the public interest in the disclosure of this information is outweighed by the national security threat posed by cyber-crime.

Under Section 16, a public authority has a duty to provide advice and assistance. Such information could be considered the Reconnaissance phase from the published 5 or 7 phase Cyber Kill Chain model proposed by Lockheed-Martin, 2011. For more information see: https://www.graylog.org/post/cyber-security-understanding-the-5-phases-of-intrusion

If you have any queries regarding the information that has been supplied to you, please refer your query to the Information Rights Team in writing in the first instance. If you remain dissatisfied and would like to request an internal review, then please contact us at the address above or by emailing InformationRights@UKHSA.gov.uk.

Please note that you have the right to an independent review by the Information Commissioner's Office (ICO) if a complaint cannot be resolved through the UKHSA complaints procedure. The ICO can be contacted by calling the ICO's helpline on 0303 123 1113, visiting the ICO's website at www.ico.org.uk or writing to the ICO at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely
Information Rights Team