Gloria Zimba
By email: request-816956-61d01ed5@whatdotheyknow.com

19 January 2022

Dear Gloria Zimba,

G00760: Freedom of Information Request

We refer to your request for information dated 16/12/2021 under the Freedom of Information Act 2000 (the "Act").

Please find below your question, with the University's corresponding response.

Question

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

Please use this email address for all replies to this request:

request-816956-61d01ed5@whatdotheyknow.com

Answer

In accordance with Section 1(1)(a) of the Act, we confirm that the University holds the information of the description specified in your request.

1. Yes, but it is not published publicly.

2. No.

3. N/A.

4. Yes.

5. Immediately, for managed devices.

6. 10,000+

7. This is irrelevant as we allow BYOD.

8. 3500.

9. Yes, we have experienced external security attacks.

10. Yes, we have experienced a service disruption.

11. This is a request for an opinion not a request for information.

If you do not feel that we have dealt with your request in accordance with the requirements of Part I of the Act, you may request a review. Your request for a review **must** specify in what respect you consider that the requirements of Part I of the Act have not been met; mere dissatisfaction with our response is insufficient. Please address your request for a review by completing the form and selecting FoI Review.

In accordance with section 5.3 of the Code of Practice, a request for a review must sent within 40 working days of the date of this letter. The University is not obliged to accept any requests for a review beyond 40 working days. We will acknowledge your request for a review and endeavour to respond within 20 working days of its receipt but please note that a deadline for a review response is not prescribed by the Act.

The Information Commissioner is responsible for enforcing rights of access to information and the operation of the publication scheme. You may apply to the Information Commissioner in writing (FOI/EIR Complaints Resolution, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF) or electronically for a decision whether, in any specified respect, your request for information has been dealt with by the University in accordance with the requirements of Part I of the Act. The Information Commissioner will not normally act unless they are satisfied that the University's review procedure has been exhausted.

Yours sincerely,

foi