The British Museum

Great Russell Street
London WC1B 3DG
britishmuseum.org

Ms Gloria Zimba

By email: request-811843-643f2841@whatdotheyknow.com

29 December 2021

OFFICIAL

Dear Ms Zimba

Thank you for your request for information from the British Museum. Your request has been dealt with in accordance with the terms of the Freedom of Information Act (2000).

Your request, received in the Museum on 29 November 2021, was:

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

The response to your request is:

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

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?

Not applicable

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.

Not applicable

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?

Yes

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

We confirm that we do not hold this information.

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

A) Physical Servers: 107

B) PC's & Notebooks: 966

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

A) Yes

If yes, how do you manage this identification process

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

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

Record Number: 1500

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

10. Have you ever experienced service disruption to users due to an accidental, non-malicious change being made to device configurations?

Yes

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?

We confirm that we do not hold this information.

This concludes the response to your request. We hope this information is helpful. If you are dissatisfied with this response and you wish to make a complaint about how we have handled your request, please contact the Resources Department in the first instance within 40 days of receipt of this response. The internal review of your complaint will be carried out by one of our Deputy Directors who was not involved in the handling of your original request. If this is not possible then the review will be carried out by a member of the Museum staff at Head of Department level. You will normally be informed of the outcome of the internal review within 20 working days following the date of receipt of your complaint, although we may extend this time in certain circumstances. We will let you know should we need to do so.

If you remain dissatisfied with the way your request has been handled following the outcome of our internal review, you have a further right of appeal to the Information Commissioner. To make such an application please contact

FOI/EIR Complaints Resolution
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

You can also contact the ICO Helpline on 0303 123 1113 or visit the Information Commissioner's Office website at https://ico.org.uk/global/contact-us/

Yours sincerely,

Resources
The British Museum