29/12/2021

CITB
Head Office
Sand Martin House
Bittern Way
Peterborough
PE2 8TY

Email: information.governance@citb.co.uk
www.citb.co.uk

[redacted]

Dear [redacted]

Freedom of Information Request: 352021

Thank you for contacting CITB requesting information under the Freedom of Information Act (FOIA). Your email, dated 29th November 2021, asked for the following information:

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

My response is as follows:

1. A (see attached strategy document)

2. A

3. B

4. A

5. A

6. As per below:
    a. Not Available
    b. Approximately 750

7. B

8. A response to this question will be provided as soon as possible in the New Year.

9. C

10. B

11. A

If you are unhappy with this response, or you wish to complain about any aspect of the handling of your request, then you should contact me in the first instance. If informal resolution is not possible and you are still dissatisfied, then you may apply for an independent internal review by contacting Adrian Beckingham, Corporate Performance Director, CITB, Sand Martin House, Bittern Way, Peterborough, PB2 8TY or email adrian.beckingham@citb.co.uk.

If you remain unhappy following an internal review, you may take your complaint to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Further details of the role and powers of the Information Commissioner can be found on the Commissioners website: https://ico.org.uk/

Yours sincerely

Jonathan Francis
Information Risk & Data Governance Manager