Response to Request for Information

Reference FOI 0815142
Date 27 August 2015

Cyber-security

Request and response in 'blue':

I am writing to you to request information about the cybersecurity practices across your corporate network, and other networks that you may use. This request is applicable under the Freedom of Information Act 2000.

Here is the Request

"If you please, I would initially like you to establish contextualising information about the corporate network(s) that you use.

1a. May you confirm who deployed these networks and their names (i.e. in the instance of Sunderland City Council's corporate network, it has been reported that the network was deployed by BT: http://www.telecompaper.com/news/bt-delivers-corporate-network-for-sunderland-city-council--819112)
Virgin Media

1b. May you provide me with copies of the tender award documents (these may be 1b.1 – the invitation to tender, and 1b.2 – the final contract, and 1b.3 etcetera, wherein they display an evaluation of the tender process) relating to the deployment of your corporate network.
The corporate network contract is currently undergoing a re-procurement when, once completed, these documents will be available.

1c. I would like to be able to contextualise the successful bid by understanding how many bids you received and how they were evaluated. If you may, I would like you to provide this as a table in a spreadsheet format, the rows of which would list those tendering and the columns of which would list the evaluation criteria. If such a document does not exist, please provide me with a facsimile which might only include the financial range of the bids, in a spreadsheet format.
The corporate network contract is currently undergoing a re-procurement when, once completed, these documents will be available.

This information is of obvious value in understanding the deployment of your corporate network which is necessary information to complement the following questions regarding your security practices.

2a. I would like to know what anti-virus and anti-malware solutions you use, this information would be the names of the solutions, the locations at which they are installed, and the names of the companies who have provided them.
Microsoft System Centre Endpoint Protection is installed across the entire corporate network.

2b. May you provide me with copies of the tender award documents for these solutions, as per 1b. Here I would like to understand the procurement process for these solutions and the degrees to which they are expected to provide security. I ask for these as I am aware the solutions may be purchased alone, while also an AV solution is often provided as part of a Microsoft Enterprise Agreement, for instance.
This solution is provided as part of a Microsoft Enterprise Agreement.

2c. May you confirm the date these solutions have been running for.
This solution has been in place for 2 years.

2d. May you confirm the number and type of machines across which these solutions are installed.
Approximately 5.000 devices including Windows Servers and clients.

2e. May you inform of of whether there is an employee responsible for maintaining these solutions, and whether this employee does so exclusively. If you may also explain to me their title and pay range in pounds sterling.
No individual is responsible for maintaining these solutions, it is the responsibility of a number of teams throughout the ICT division.

I am also interested in the threats that you are facing.

3a. May you inform me of the number of malware alerts that your AV solutions detected in the past twelve months.
179 alerts on 88 machines.

3b. Most solutions will provide alerts when it comes to malware detections, may you inform me of the number of alerts your solutions have provided, by solution. These alerts should be held on a database which provides a high degree of granularity in recording the causes of the alerts.
As 3a.

3b.2 May you provide me with a copy of this granular information – preferably in spreadsheet format – for the period covering the last twelve months, or shorter if not applicable.
number of infections
Reports cannot be exported in this format as they cover a number of different machine collections.

3c. I also wish to receive information about the number of infections that have occurred in the last twelve months, and in what areas, and on what machines these occurred.
No infections have occurred – all detected viruses were remediated.

3d. I would like to know at what account level these infections occurred.
N/A – as per 3c.

3e. I would like to know how many instances were there in which these infections were not contained, but spread to another part of the network.
N/A – as per 3c.

3f. I would like to know what the entry-point of these infections was, in each case.
N/A – as per 3c.

3g. I would like a list of the number and type of unauthorised accesses within your networks.
None.

3h. I would like to know how many of these were classified as personal data incidents, and how many were reported to the Information Commissioner's Office.
All detected viruses were remediated and did not result in any loss of personal data that required reporting either internally or to the Information Commissioner's Office.

Finally, I would like to ask about your security maintenance policies.

4a. If one exists, may you explain your password policy and its enforcement.
We enforce a strict, complex, password policy that complies with Central Government recommended standards.

4b. If one exists, may you explain your log-on policy and its enforcement.
We enforce a strict logon policy that complies with Central Government recommended standards.

4c. If one exists, may you explain your email policy and its enforcement.
No specific email policy exists, this is contained within our Acceptable Use Policy. Details of our Information Governance can be found at http://www.wolverhampton.gov.uk/igov

4d. If one exists, may you explain your device policy (i.e. nothing from home) and its enforcement.
A mobile device policy is in place and all devices used are managed using a Mobile Device Management utility. Access is restricted based on user and device.

4e. May you clarify whether you store and or process bank card data?
We do not store any bank card data. On premise processing is done using a 3rd party solution.

4f. May you clarify whether you are PCI compliant?"
We can confirm that we are PCI compliant.