Wolverhampton
City Council

Response to Request for Information

Reference FOI 0515127
Date 28 May 2015

Cyber Attacks on the Local Authority, School Facilities and Associated Administrative Offices

Request:

I am requesting information about cyber attacks.

By “cyber attack” I mean any unauthorised access to or deliberate disruption of a computer system or device owned or used by the local authority, any school facilities, as well as any associated administrative offices under your responsibility.

1) How many (if any) cyber attacks have there been in the last five years since 1 January 2010?

2) For each separate attack, please provide
   a. The type of attack
   b. The target of attack
   c. Any details you have as to the origin of the attack (country/IP address, etc.)
   d. The type of information accessed (if any)
   e. Whether the attack was reported to police authorities
   f. Whether the attack was reported to the Information Commissioner’s Office
   g. Any internal measures taken as a result.

Response:

1. Over the last 5 years Wolverhampton City Council have not encountered any cyber-attacks however only 2 attacks that have happened during this time in Wolverhampton Schools we are aware of and support. Once in early 2014 and again early in 2015 in 2 different schools.

2a. The type of attack

Both the attacks schools were victim to the same “Ransomware” virus called “Cryptolocker” more information here http://en.wikipedia.org/wiki/CryptoLocker but each school was infected independently and in 2 different ways. In one school it came through an invoice spoof email with a link inside that the administration member of staff without realising the affect clicked the link and agreed to the pop up. The other school it came via a USB memory stick and as an exe file which the user thought was a legitimate download and program they could use within school.

2b. The target of attack

No specific target to the school. In both instances we were able to restore the devices and files immediately.

2c. Any details you have as to the origin of the attack (country/IP address, etc.)

Origin unknown.

2d. The type of information accessed (if any)

This particular virus we understand does not access or transmit information as it only encrypts the files on the system.

2e. Whether the attack was reported to police authorities

As data was not vulnerable or compromised this matter was not reported to the Police as previously agreed with them

2f. Whether the attack was reported to the Information Commissioner's Office

The ICO have produced many documents and guidance on reporting and this depends on the severity of the circumstance. As data was not vulnerable or compromised this matter was not reported see: https://ico.org.uk/media/about-the-ico/events-and-webinars/1043455/dealing-with-data-breaches-andrew-rose-20150225.pdf

2g. Any internal measures taken as a result.

We undertake City wide monitoring of Virus and Malware and have considerable visibility and the ability to detect any type of vulnerabilities efficiently and deal with them. Devices and patches are applied in a timely manner and the position regularly monitored.

Schools are asked to report anything suspicious so we can identify the nature of it and warn other service users if required. This is so it helps them in work but also their own personal devices they own.

All external media must be reported and encrypted by the Technical Support team to be allowed on the device if required by the staff member. External media is encrypted and password protected.