TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack

Share

Date
05 October 2016

Type
News

Telecoms company TalkTalk has been issued with a record £400,000 fine by the ICO for security failings that allowed a cyber attacker to access customer data "with ease".

The ICO's in-depth investigation found that an attack on the company last October could have been prevented if TalkTalk had taken basic steps to protect customers' information.

ICO investigators found that the cyber attack between 15 and 21 October 2015 took advantage of technical weaknesses in TalkTalk's systems. The attacker accessed the personal data of 156,959 customers including their names, addresses, dates of birth, phone numbers and email addresses. In 15,656 cases, the attacker also had access to bank account details and sort codes.

Information Commissioner Elizabeth Denham said:

> "TalkTalk's failure to implement the most basic cyber security measures allowed hackers to penetrate TalkTalk's systems with ease.
>
> "Yes hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. TalkTalk should and could have done more to safeguard its customer information. It did not and we have taken action."

The data was taken from an underlying customer database that was part of TalkTalk's acquisition of Tiscali's UK operations in 2009. The data was accessed through an attack on ulnerable webpages within the inherited infrastructure. TalkTalk failed to properly

TalkTalk was not aware that the installed version of the database software was outdated and no longer supported by the provider. The company said it did not know at the time that the software was affected by a bug – for which a fix was available. The bug allowed the attacker to bypass access restrictions. Had it been fixed, this would not have been possible.

The attacker used a common technique known as SQL injection to access the data. SQL injection is well understood, defences exist and TalkTalk ought to have known it posed a risk to its data, the ICO investigation found.

On top of that the company also had two early warnings that it was unaware of. The first was a successful SQL injection attack on 17 July 2015 that exploited the same vulnerability in the webpages. A second attack was launched between 2 and 3 September 2015.

Ms Denham said:

> “In spite of its expertise and resources, when it came to the basic principles of cyber-security, TalkTalk was found wanting.
>
> “Today’s record fine acts as a warning to others that cyber security is not an IT issue, it is a boardroom issue. Companies must be diligent and vigilant. They must do this not only because they have a duty under law, but because they have a duty to their customers.”

The ICO’s investigation was limited to TalkTalk’s compliance with the Data Protection Act. It concluded that TalkTalk failed to have in place the appropriate security measures to protect the personal data it was responsible for. This is a breach of the seventh principle of the Data Protection Act.

A criminal investigation by the Metropolitan Police has been running separately to the ICO’s investigation.

There's more information about how the ICO’s investigation unfolded in our timeline article.

Notes to Editors

1. The Information Commissioner’s Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

   ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom ıformation Act 2000, Environmental Information Regulations 2004 and Privacy and tronic Communications Regulations 2003.

criminal enforcement and audit. The ICO has the power to impose a monetary penalty on a data controller of up to £500,000.

4. Anyone who processes personal information must comply with eight principles of the Data Protection Act, which make sure that personal information is:
   - fairly and lawfully processed;
   - processed for limited purposes;
   - adequate, relevant and not excessive;
   - accurate and up to date;
   - not kept for longer than is necessary;
   - processed in line with your rights;
   - secure; and
   - not transferred to other countries without adequate protection.
5. Civil Monetary Penalties (CMPs) are subject to a right of appeal to the (First-tier Tribunal) General Regulatory Chamber against the imposition of the monetary penalty and/or the amount of the penalty specified in the monetary penalty notice.
6. Any monetary penalty is paid into the Treasury's Consolidated Fund and is not kept by the Information Commissioner's Office (ICO).
7. The ICO does not have the legal authority to award compensation.
8. To report a concern to the ICO telephone our helpline 0303 123 1113 or go to ico.org.uk/concerns.

Subscribe to our e-newsletter

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

© Copyright
Privacy notice
Cookies
Disclaimer

Cymraeg
Publications
Accessibility
Contact us

0303 123 1113