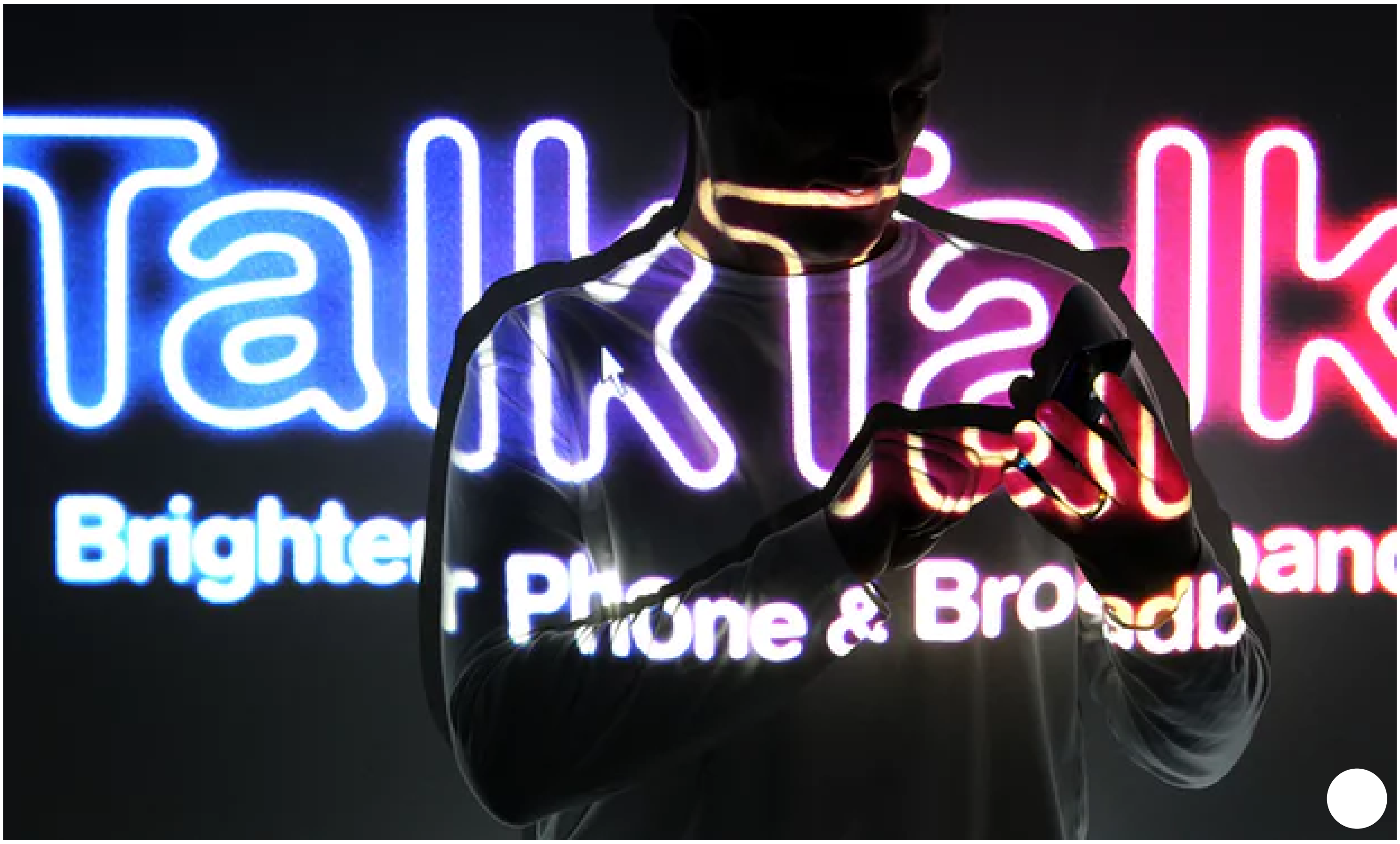
The Guardian



TalkTalk hit with record £400k fine over cyber-attack

Internet service provider handed fine by Information Commissioner's Office after security failings allowed customer data to be accessed 'with ease'

Alex Hern

Wed 5 Oct 2016 14.00 BST

TalkTalk has been hit with a record £400,000 fine for the security failings that led to the company being hacked in October 2015.

The Information Commissioner's Office levied the fine saying that the attack "could have been prevented if TalkTalk had taken basic steps to protect customers' information".

The hack resulted in the attacker accessing the personal information of more than 150,000 customers of the internet service provider, including sensitive financial data for more than 15,000 people.

The 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 technique used by the attacker, called SQL injection, has been well known in security circles for almost 20 years. "SQL injection is well understood, defences exist and TalkTalk ought to have known it posed a risk to its data," the ICO said. "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."

The amount the ICO can fine companies for serious breach of data protection obligations is capped at £500,000, leaving TalkTalk's fine almost as large as it could possibly receive. Repeat offenders can also be issued "enforcement notices" under the same legislation, which entail the ICO requiring a business to take particular steps to prevent a re-occurrence.

The previous highest fine ever issued by the ICO was £350,000, against Prodial, a spam-calling company responsible for over 46 million automated nuisance calls.

In a statement, TalkTalk said: "TalkTalk has co-operated fully with the ICO at all times and, while this is clearly a disappointing decision, we continue to be respectful of the important role the ICO plays in upholding the privacy of consumers.

"During a year in which the government data showed nine in 10 large UK businesses were successfully breached, the TalkTalk attack was notable for our decision to be open and honest with our customers from the outset. This gave them the best chance of protecting themselves and we remain firm that this was the right approach for them and for our business.

"As the case remains the subject of an ongoing criminal prosecution, we cannot comment further at this time."

In September this year, Daniel Kelley, 19, was charged with hacking the company. Kelley appeared at Westminster magistrates court accused of demanding 465 bitcoins, then worth over £200,000, from the company after allegedly carrying out the attack.

Data was taken from an underlying customer database that was part of TalkTalk's acquisition of Tiscali's UK operations in 2009, the ICO said. It added that the data was accessed through an attack on three vulnerable webpages in the "inherited infrastructure".

TalkTalk was said to have failed to properly scan this infrastructure for possible threats and was unaware the vulnerable pages existed or that they enabled access to a database that held customer information.

TalkTalk was not aware that the installed version of the database software was outdated and no longer supported by the provider, according to the ICO. 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 watchdog said, adding: "The bug allowed the attacker to bypass access restrictions. Had it been fixed, this would not have been possible."

When the cyber-attack was revealed, TalkTalk said it did not know how many customers were affected, raising concerns that hundreds of thousands of customers could be at risk. It had been criticised for failing to to take precautions after being hacked twice in the recent past.

In December 2014, the company saw customers hit by India-based scam calls after a data breach. It happened gain in again in February 2015, when TalkTalk customers were subjected to further scams, despite the company describing the information stolen in the breach as limited and non-sensitive. TalkTalk Mobile customers were also affected by an attack on Carphone Warehouse systems in which the personal information of up to 2.4 million customers was stolen.

Topics
- TalkTalk
- ISPs
- Hacking
- Telecoms
- Telecommunications industry
- news