UNIVERSITY OF PORTSMOUTH

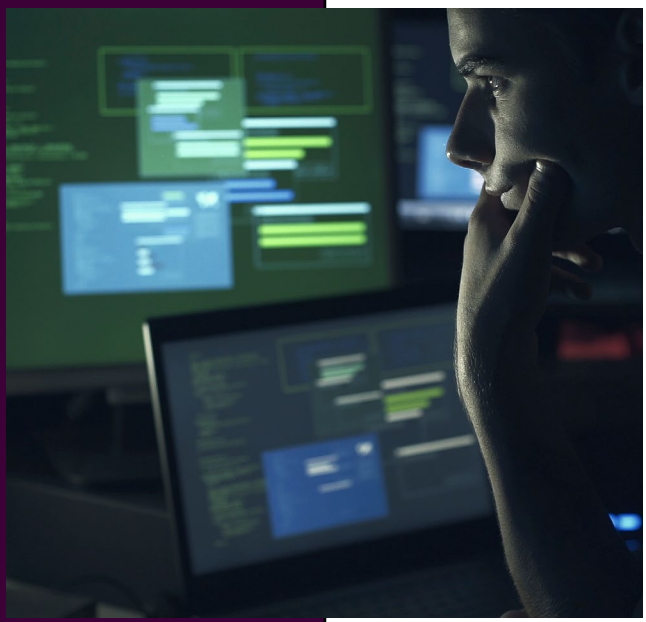
CASE STUDY
THE TALKTALK HACK

On 21 October 2015, the website of TalkTalk – a large telecommunications company and internet service provider – suddenly became unavailable.

TalkTalk had discovered that their website was being attacked, which forced them to bring down the website to prevent further attacks and to investigate the scope of the damage. It turned out that there were ways to gain unauthorised access to the underlying database that was associated with the website. The database contained personal information such as the names, addresses, phone numbers, email addresses, dates of birth and financial information of TalkTalk's customers. The company initially feared that personal information belonging to all four million of their customers had been stolen, but later found that the scale of data lost was much smaller.

TalkTalk issued a statement in November of the same year confirming the following lost data (BBC News, 2015):

- 156,959 customers had personal details accessed.
- From those customers, 15,656 bank account numbers and sort codes were stolen.
- 28,000 stolen credit and debit card numbers were 'obscured' (some digits of the card number were hidden) and 'cannot be used for financial transactions'.



Nevertheless, for these 156,959 customers, it could have been the start of a nightmare. They were vulnerable to identity crimes and scams. In fact, a number of customers claimed that they received scam phone calls a few days before TalkTalk disclosed the attack (Bain, 2015).

For those who were in a long contract with TalkTalk, this was especially frustrating because TalkTalk did not allow customers to terminate the contract early unless they paid an early termination fee or proved they had suffered financial loss as a result of a scam directly related to this data breach. No doubt this policy angered customers and dented their trust in the company further (Millman, 2017).

In TalkTalk's quarterly report release in February 2016, the financial loss resulting from the attack was estimated to be £60 million, which included costs related to responding to the incident, extra loads put on the call centres, and repairing vulnerable systems. In three months, TalkTalk also lost 95,000 customers, who left because of the attack (Burgess, 2016).

TalkTalk not only suffered a big financial loss but also damaged its brand, and left its customers facing the possibility of identity theft crimes and scams for years to come.

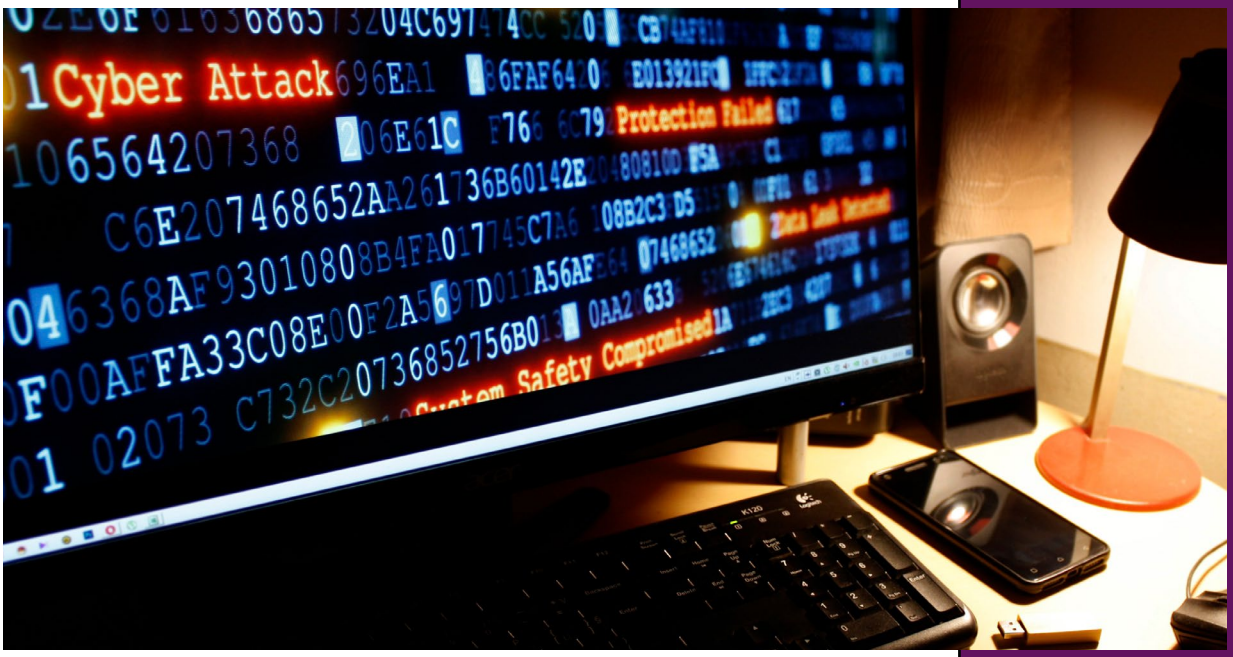
In addition, the Information Commissioner's Office (ICO), which is the UK's independent authority for upholding information rights in the public interest, fined TalkTalk £400,000 for 'security failings that allowed a cyber attacker to access customer data with ease' (ICO, 2016). The ICO's investigation concluded that the attack could have been prevented if TalkTalk had taken basic security measures to protect their systems. The fine was the largest the ICO had ever issued at that time.

THE SCENARIO OF THE ATTACK

The TalkTalk attack was a relatively simple one. It was a type of attack known as a **Structured Query Language injection** (SQLi) – which, at the time of writing, has been well known and understood within the security field for over a decade.

The Structured Query Language (SQL) is a programming language that is used for managing **relational databases** and their data. As the contents of most modern commercial websites are database-driven, many web pages are dynamically created based on templates, user inputs, the data in the database and other information. This method enables web pages to be more easily personalised.

However, if the designer of the template – which is usually a **script** or program that can access the databases – does not consider SQLi prevention, an attacker can append SQL codes to their input fields in the web page to manipulate data in the database, even if they are not authorised to do so.



HOW DOES AN SQLi ATTACK HAPPEN?

Watch **this video** to get an insight into how the SQLi attack works .

Suppose there is a landing web page that asks you to enter your username and password. This web page is controlled by a script, which will create a personalised web page if the user logs in successfully. The script takes the entered username and password from the input fields of the web page and uses them to construct a SQL query statement.

For this example, the query statement is to ask the database to return the user's stored information, including the password, so that it can compare it with the entered password. As 'John' and 'myPass' were entered, the script will create a query statement like the one below:

SELECT * FROM Users WHERE Name = "John" AND Password = "myPass"

The first part:

SELECT * FROM Users asks the database to select all the fields (as the * symbol means all the fields) in the data table named Users.

If the attacker can find a way to make the database bypass the checking of the username and password, it can potentially obtain all the information in the database. One way to achieve this is to construct the SQL statement as follows:

SELECT * FROM Users WHERE TRUE

As the condition statement is now always TRUE regardless of what the entered username and password are, the database will return everything in the Users table.

An attacker cannot change the SQL query statement directly as they have no control of the script. Nevertheless, they may be able to influence what the constructed SQL query statement will be by carefully crafting and appending SQL codes to the 'Username' and 'Password' fields in the landing web page. The Figure below shows an example.

UserName:

whatever" OR "a" = "a

Password:

whatever" OR "a" = "a

These inputs are missing the beginning and ending quotation marks. However, they are specially crafted such that when the script combines the entered username and password to construct the SQL query statement, it will become:

SELECT * FROM Users WHERE Name = "whatever" OR "a" = "a" AND Password = "whatever" OR "a"="a"

The condition statement now contains two OR clauses and one AND clause. The OR operator will output TRUE if either of the conditions on the left and right sides of the OR operator is TRUE. As "a"="a" (two identical letters) will always be evaluated as TRUE, the query statement is in effect equivalent to:

SELECT * FROM Users WHERE TRUE AND TRUE

The AND operator will output TRUE if both of the conditions on the left and right sides of the AND operator are TRUE. This means the query statement is equivalent to:

SELECT * FROM Users WHERE TRUE

This query statement will make the database bypass the checking of the username and password and show all the information in the Users data table.

The TalkTalk attackers used a similar SQLi principle to steal TalkTalk's customer information. SQLi can also be used to add or delete data or even to delete the whole database. The web page designer must therefore ensure that any user inputs obtained through fields in a web page are free of SQL codes.

THE INVESTIGATION

Two days after TalkTalk discovered the attack, its then chief executive, Dido Harding, said during a media interview that the company had suffered a 'significant and sustained' cyber-attack and received a ransom demand from someone purporting to be the hacker.

The cybercrime unit of the Metropolitan Police had started investigating the attack, but very little information about the attack was available. However, a former detective from the cybercrime unit, Adrian Culley, suspected that the attack was the work of Islamist militants, as a group claiming responsibility for the attack had stated that it was done in the name of Allah. The group also posted sample customer data, claimed to be obtained from the attack, on the website Pastebin, which is often used by hackers for publishing stolen information (Khomami, 2015).

However, three days later, a 15-year-old boy was arrested in Northern Ireland on suspicion of being related to this attack. On 29 October 2015, a 16-year-old boy was arrested in Feltham, west London. Two days later, a 20-year-old man was arrested in Staffordshire. A further two male teenagers were arrested in Wales and Norwich within the next few weeks. They were all arrested on suspicion of offences under the *Computer Misuse Act 1990*. It became apparent that the attack had been undertaken by a group of British youngsters.

According to a report from *Channel 4 News* (White, 2015), a hacker who claimed to have been involved with the TalkTalk attack said the event happened days before TalkTalk discovered the attack. The hacker was in a Skype group call with friends when one member shared a security flaw he had discovered in TalkTalk's website via a Google search.

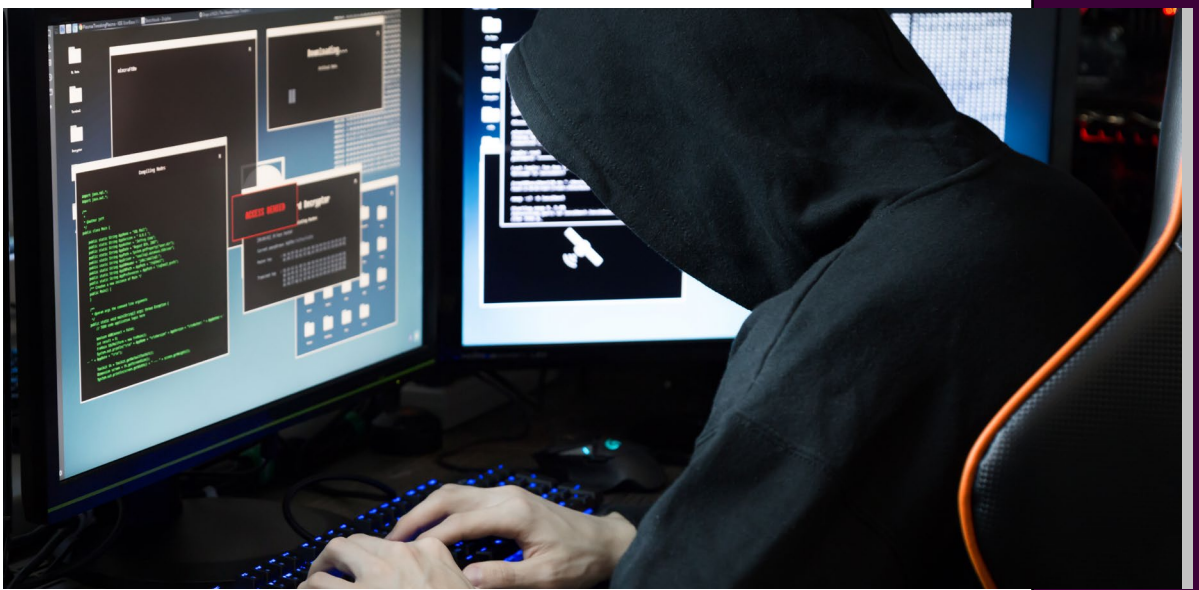
Such a basic flaw discovery technique should not have worked on a big company like TalkTalk, so they were laughing about TalkTalk's unbelievably bad security. The hacker further said that multiple people had used the security flaw to extract data from TalkTalk's customer database: 'it got passed around … at least 25 people had access to it'.

He claimed he only did it for fun and to impress his mates. He further claimed that he warned TalkTalk about the security flaw by posting a tweet an hour before the attack that highlighted the flaw and tagged TalkTalk's Twitter account, but TalkTalk were not interested.

However, not all the attackers did it for fun. The then 20-year-old man arrested in Staffordshire in 2015, Matthew Hanley, and his friend Connor Allsopp, aged 18 at the time and arrested in 2017, were trying to sell the data that Hanley had stolen from TalkTalk's website and the website's security flaw for profit. The pair pleaded guilty to charges relating to the TalkTalk attack.

At the time of writing, six people have been arrested in relation to the TalkTalk attack and five of them have been charged:

- Aaron Sterritt (aged 15 at the time of the attack, so his name was not revealed until 2018) was charged under the *Computer Misuse Act* and admitted to unauthorised access to computer material. He was ordered to complete 50 hours of community service, apologise to TalkTalk in writing and complete at least one cybercrime education session (News Letter 2018).
- A 17 year-old, who could not be named because of his age, was arrested in Norwich in November 2015. He was charged under the *Computer Misuse Act* and admitted to seven offences at Norwich Youth Court in November 2016. The prosecution produced evidence that in addition to performing the initial breach of the TalkTalk site, the teenager had shared information about the site's weaknesses on the internet. He was given a 12-month rehabilitation order.
- Daniel Kelley, aged 19 from Wales, was charged with 18 offences including money laundering and blackmail against the then-CEO of TalkTalk as well as offences under the *Computer Misuse Act*. Kelley pleaded guilty to eleven charges, including that of blackmail.
- Matthew Hanley and Connor Allsopp were jointly charged with eleven offences at a trial at the Old Bailey in London. They were alleged to have attacked not only TalkTalk but also computers belonging to NASA, the National Climatic Data Center, Spotify, Telstra and the RAC. Hanley was charged under the *Computer Misuse Act* with committing fraud against TalkTalk customers. Allsopp was charged with two offences of supplying articles. In April 2017, the two were tried at the Old Bailey in London. Allsopp pleaded guilty to all offences. Hanley admitted to the charge of attacking TalkTalk, but not to the other attacks.



HOW COULD THE ATTACK HAVE BEEN PREVENTED?

Based on an analysis carried out by Colin Tankard, managing director of a data security company, here is a summary of what went wrong and how the attack could have been prevented (Tankard, 2015):

- The three web pages that were vulnerable to SQLi were inherited from Tiscali when TalkTalk took over its UK business in 2009 (ICO, 2016). According to the ICO's investigation, TalkTalk did not undertake proper security testing or secure the problem web pages before allowing them to access their databases. This obviously was a big mistake.
- According to the ICO's investigation, there was a security bug in the database management software in use at that time which allowed attackers to bypass access restrictions. The patch for that bug had been available for over three and a half years before the attack. However, TalkTalk did not apply the patch in time. Tankard (2015) believes that this indicates poor patch management practice.
- TalkTalk may not have proactively monitored network activities, such as server logs, to detect unusual behaviour at the time of the attack. According to the report from Channel 4 News (White, 2015), the attack happened continuously for days before TalkTalk discovered it. The ICO also reported two previous SQLi attacks in the same year. This should have given TalkTalk enough warning to undertake proper proactive action. Tankard (2015) believes it is possible that TalkTalk's technical team were aware of the alerts but chose to ignore them. Therefore, management should have had a mechanism to receive these alerts as well.
- Given that TalkTalk had suffered two previous attacks within a year, they still did not appear to have a good strategy to manage such an event and their response to the attack was slow (Tankard, 2015). They didn't report the incident to the ICO until a full day after they discovered the attack. They also failed to inform their customers straight away so that their customers could be more vigilant to scams. During the first press interview, TalkTalk's CEO, Dido Harding, did not know whether the data was encrypted and was unable to give any details of the attack. This made customers frustrated. According to Tankard (2015), TalkTalk should have prepared a robust disaster recovery plan. They also had not significantly strengthened their defences after the previous attacks, which was another big mistake.
- Although investment in a proactive threat detection system is costly, the damage of a breach can be much more expensive. It is better to prevent an attack from happening than to have to deal with the consequences of it.
- Finally, the TalkTalk attack demonstrates how vulnerable business networks can be. Businesses must start to check their networks and isolate any parts not strictly necessary for providing services to their customers. In case one area is compromised, the isolated parts are still protected. They should also incorporate in their network some 'honeypots', which are fake servers that lure attackers to them in order to monitor and analyse their activities. This would allow the businesses to determine a strategy to stop the attack and to report the suspicious activities to the police.

REFERENCES

- Bain, I. (2015) 'TalkTalk cyber-attack: customer got scam call nearly a day before', *The Guardian*, 23 October. [online] Available at: www.theguardian.com/business/2015/oct/23/talktalkcyber-attack-customers-scam-calls-day-before-announcement [Accessed: 5 October 2020]
- Ball, T. (2017) 'Top 5 critical infrastructure cyber attacks', *Computer Business Review*, 18 July. [online] Available at: www.cbronline.com/cybersecurity/top-5-infrastructure-hacks/ [Accessed: 5 October 2020]
- BBC News (2015) 'TalkTalk hack "affected 157,000 customers"', *BBC News, 6* November. [online] Available at: www.bbc.co.uk/news/business-34743185 [Accessed: 5 October 2020]
- Burgess, M. (2016) 'TalkTalk hack toll: 100k customers and £60m', *WIRED*, 2 February. [online] Available at: www.wired.co.uk/article/talktalk-hack-customers-lost [Accessed: 5 October 2020]
- ICO (2016) 'TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack', *ICO News*, 5 October. [online] Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/ [Accessed: 5 October 2020]
- Khomami, N. (2015) 'TalkTalk hacking crisis deepens as more details emerge', *The Guardian*, 23 October. [online] Available at: https://www.theguardian.com/business/2015/oct/23/talktalkhacking-crisis-deepens-as-more-details-emerge [Accessed 5 October 2020]
- MacAskill, E. (2018) 'Major cyber-attack on UK a matter of "when, not if" – security chief', *The Guardian*, 23 January. [online] Available at: https://:www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin [Accessed: 5 October 2020]
- Millman, R. (2017) 'TalkTalk hack: Two men plead guilty to TalkTalk hack', *IT Pro*, 27 April. [online] Available at: https://www.itpro.co.uk/security/24136/talktalk-hack-two-men-plead-guilty-to-talktalk-hack [Accessed: 5 October 2020]
- News Letter (2018) 'Identity of NI TalkTalk hacker revealed', *News Letter*, 14 March. [online] Available at: https://www.newsletter.co.uk/news/crime/identity-of-ni-talktalk-hacker-revealed-1-8415382 [Accessed: 5 October 2020]
- Tankard, C. (2015) 'What can we learn from the TalkTalk hack?', *ITProPortal*, 3 December. [online] Available at: https://www.itproportal.com/2015/12/03/what-can-we-learn-from-thetalktalk-hack/ [Accessed: 5 October 2020]