BBC

Why do companies keep getting hacked?

By Mark Ward Technology correspondent, BBC News 23 October 2015

TalkTalk seems to have been hit by a two-pronged attack that went after customer data

Police are investigating a sustained attack on the TalkTalk website that might have let hackers get at details of the firm's four million customers.

The breach is the third big cyber-attack that TalkTalk has suffered in the last year.

It is not clear who was behind the attack or why they targeted TalkTalk - but it is far from the only company that keeps being hit.

Why does this keep happening?

Almost every large company is being bombarded with cyber-attacks all day, every day.

About one million new malicious programs are created every day, according to security firm Symantec. That is a lot to defend against - and that does not include the many other ways attackers try to get at their targets.

Some attacks are crude and are easy to defend against. Others are more cunning and try to trick people into opening booby-trapped email messages. The most dangerous attacks exploit security holes that most people have not discovered yet in widely-used software.

Surely companies have defences that can stop attacks?

Even the best security can have vulnerabilities

On average companies use 75 separate cyber-defence systems to police their networks. However, these systems can deliver an overwhelming number of alerts and warnings to security staff.

Worse still, it is often hard for companies to correlate the information provided by each separate system, says Darren Thomson, European technology boss at security firm Symantec.

This can mean security teams spend time chasing false positives or problems that look serious but are not the current biggest threat they face.

And technology cannot always help if somebody in an organisation opens a booby-trapped attachment on a phishing email.

Many attackers are increasingly exploiting human frailty because cyber-defences seem to have improved far faster than people.

And even the best security is weakened if a company insider decides to betray their employer.

What happened to TalkTalk?

Details are scant but it looks like there were two elements to the breach.
The first was a distributed denial of service (DDoS) that tried to knock over TalkTalk's servers by hitting them with lots of data.
There are hundreds if not thousands of these kinds of attacks every day, says Roland Dobbins from Arbor Networks, a company that helps firms block the massive data flows.
These attacks simply try to knock sites offline. Often, says Mr Dobbins, they can be used as a smokescreen to distract security staff from other activity. Other groups have used them to steal cash or data.
The DDoS assault on TalkTalk seems to have been accompanied by another attack which sought to get at its customer database. That is why the company has warned that personal information might have been accessed.

But TalkTalk has been hit three times...

PA Image caption The website of chef Jamie Oliver was hit by attackers several times over a period of months
Other high-profile sites have been hit several times by cyber-attacks. The website of celebrity chef Jamie Oliver suffered three successive attacks centred on malicious adverts.
Breaches have, unfortunately, become a fact of life for any company that uses the web for business - which is pretty much all of them.
The website Have I Been Pwned? gathers information on stolen data and now has a database of more than 223 million accounts that were stolen in a variety of hacks over the last few years.
"Five out of six firms that we talked to in a 2014 survey had been attacked," said Mr Thomson. "And given that it can take 230 days to spot a breach that sixth might have been hit but just didn't realise it yet."

Preparing for the worst

Attackers seek to infiltrate a network and then hang around so they can get at saleable data
Many companies now prepare for the day they will be breached rather than expect technology to keep them safe and secure all the time.
Often attackers can get into a corporate network using stolen staff credentials but that just gets them a foothold.
From there they need to explore, expand and gather network privileges that help them get at the data they really want to steal.
The length of time it can take to realise that a breach has taken place gives attackers a long time to bed in, explore and escalate their access. Companies are getting better at spotting that anomalous behaviour but the advantage often still lies with the attackers.
Many companies employ ethical hackers to test their security systems and properly encrypting customer data helps ensure any stolen information is useless to attackers, or expensive to sell.

TalkTalk will have questions to answer if it emerges that hackers were able to steal unencrypted customer information.

Online-Technology.co.uk – 3 Key Points

- Keep IT defences appropriate and up to date, i.e. Information security plan
- Minimise the human risk, i.e. User awareness training
- Protect from third party risk, i.e. Control internal and external access levels