Is it time to hire a hacker to protect your business?

Cyberattacks are on the rise and businesses seeking to pinpoint weak spots are fighting back by inviting IT experts to break in

November 2017

Asking someone to break into your IT systems might not seem the wisest of ideas. But with cyberattacks a common occurrence, working with hackers is now seen as a smart move.

For some, the word “hacker” conjures up a teenager in a hoodie causing mayhem from a laptop in a bedroom. But not all hackers are the same. The IT industry recognises the importance of “white-hat” hackers – those who probe the security of IT systems by trying to break in. This “penetration testing” helps companies stay ahead of black-hat hackers – the ones acting maliciously.

“The difference between a white-hat and a criminal is permission,” says Andy Gill, author of the blog Adventures in Information Security. “White-hats help businesses to better protect themselves.”

In May, the WannaCry ransomware attack shut down computer systems worldwide, including those of the NHS, forcing many victims to pay a ransom in the form of virtual currency. In the event, it was a British cybersecurity expert who found a way to foil it.

For Gill, WannaCry reminded him of a situation he had faced a few years earlier. He was working as part of a team challenged to deal with a hypothetical ransomware attack on the National Grid. “We had to work out what needed to be done, where the threat was coming from and how to quickly negate it. Looking back, it was quite realistic,” he says.

The simulation was created by Cyber Security Challenge, a not-for-profit organisation that trains and talent-spots for the IT industry. Gill became involved with the group when he was 19, taking part in workshops and competitions before moving on to work in industry. Gill, now 23, says that ransomware and other cyberattacks are becoming more common.

He says businesses are failing to invest properly in virtual security, leaving them vulnerable. “It’s vital to keep systems up to date with the latest patches,” Gill says. “Depending on the technology a business uses, this can be easier said than done because there are charges for updating certain software.”

A common way for ransomware and other malware to arrive is in an email attachment. It becomes dangerous only if clicked on. “Companies must train staff to recognise when something is not quite right,” says Gill. “So if an email says ‘Click on this link’, they know that it might contain malicious software. Being vigilant is key.”

Businesses also need disaster recovery plans for IT breaches, similar to those for fire, flood and theft, he says. “If you’re hit, you put your plan into action to restore systems and isolate the threat.”

With new laws aimed at protecting consumer data on their way, businesses have to be able to show their systems are safe. Penetration testing is just one way of checking. Businesses also need to scan regularly for malware. But absolute guarantees of security are almost impossible. “No anti-virus software is perfect,” Gill says.

https://www.thetimes.co.uk/static/tech-summit/is-it-time-to-hire-a-hacker-to-protect-your-business/?mvt=i&mvn=7cfd65f9b8bd4b5c848f3abbb1e2e598&mvp=NA-TIME-11236249&mvl=Homepage+-+Sponsored+rail