Professional SECURITY Magazine Online

wavex
EXPERIENCE EXCELLENCE

INTERVIEWS

Tactics of cyber criminals

19TH MAY 2017

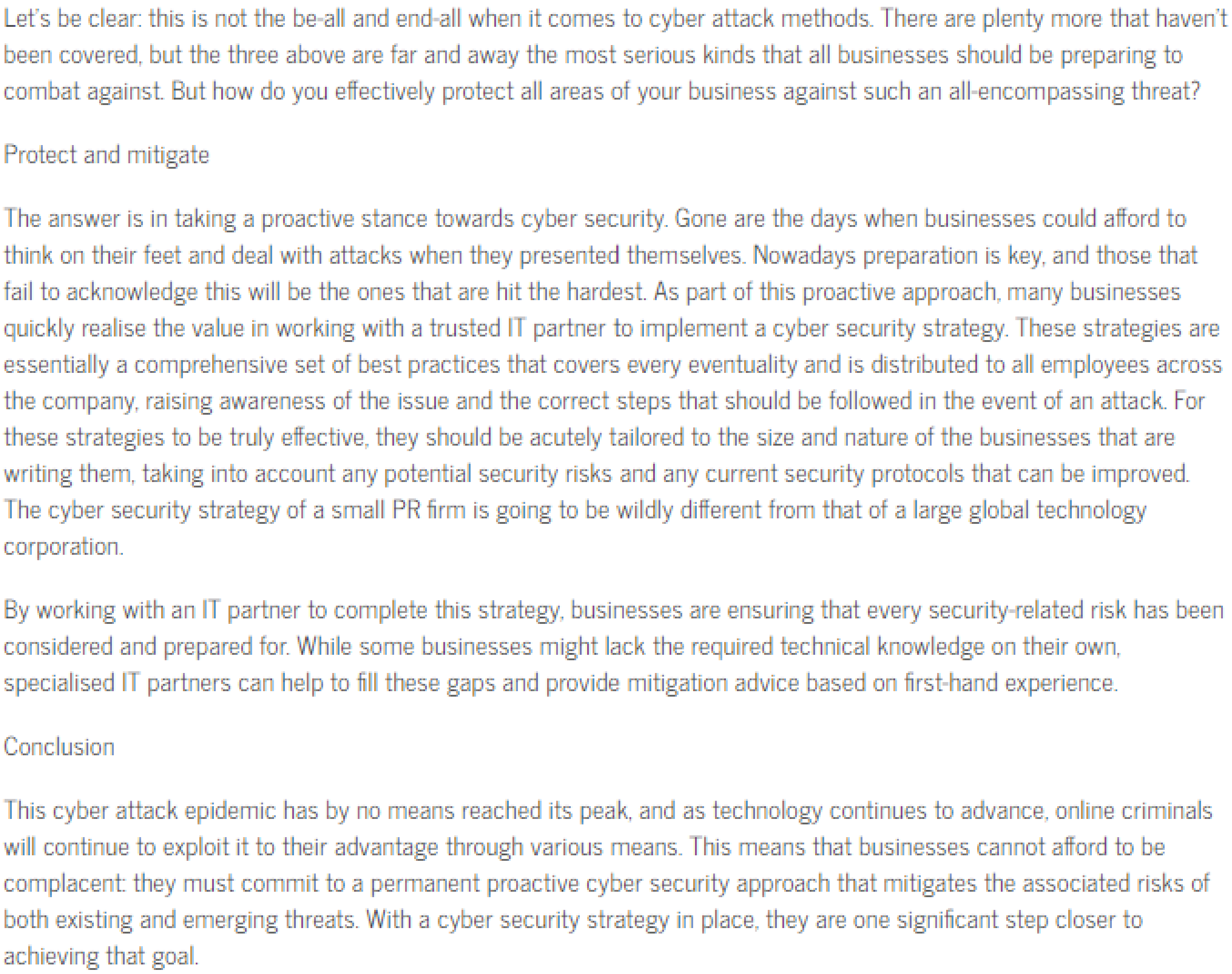
Cyber criminals have become a serious threat for businesses of all sizes, due to both the sophistication and the frequency of the attacks they carry out. Research conducted in April 2017 by the UK government found that almost half (46pc) of all UK businesses have suffered at least one cyber attack in the past 12 months alone, writes Gavin Russell, CEO of IT firm Wavex, pictured.

This figure rises to 66pc and 68pc when considering medium and large-sized firms respectively. Amazingly, those 46pc are the lucky ones. According to the research, a further 37pc said that they experienced online security breaches on a monthly basis, while 13pc said they suffered from attacks every day. As if the frequency of such attacks wasn't bad enough, cyber criminals are often ruthlessly effective in their actions, whether their intention is to seize personal or confidential data and leak it into the public sphere, or to halt the victim's operations entirely. This is thanks to their uncanny ability to constantly stay one step ahead of their victims, and due to the many different methods and approaches at their disposal.

Cyber attack shapes and sizes

The most common method used to bring down businesses is what is known as a 'malware' attack. In a nutshell, this is when a genuine-looking communication — be it an internet pop-up or an email attachment — fools someone into clicking on a link that actually contains a malicious virus or piece of software, which is otherwise known as 'ransomware'. Once the ransomware has been opened, the hacker can easily access the company's IT infrastructure help themselves to whatever they desire.
The latest annual Data Breach Investigation Report from Verizon found that ransomware-related attacks rose by 50pc globally last year, which means that malware is now responsible for 51pc of all the attacks analysed — a significant indicator of this method's wider impact. Another method that is causing headaches for businesses is the 'distributed denial of service' (or 'DDoS') attack. This involves the cybercriminal targeting a server and bombarding it with so much traffic that it collapses under the strain.

While malware attacks are almost exclusively intended to seize or steal data from the victim, DDoS attacks are designed primarily to disrupt regular operations. Once a DDoS attack has taken place, users will not be able to access any affected websites until the issue has been resolved, which presents further problems for businesses in the form of lost revenue and website traffic. DDoS attacks are also often used as a tactic to distract businesses from a more serious data breach that is happening simultaneously. Effective cyber attacks don't always require complex technical knowledge — sometimes all they involve is standard log-in credentials. So-called 'password attacks', where hackers simply gain access to a certain platform or system by copying a user's username and password, are still prevalent on a global scale, and often come about as a result of leaked personal data from a separate cyber attack. The benefit of these attacks from a hacker's perspective is that, once inside the system, they can operate with the freedom that any other user enjoys, which means they can compromise data, plant malicious code or software within the system or change the current log-in details all with relative ease.



Let's be clear: this is not the be-all and end-all when it comes to cyber attack methods. There are plenty more that haven't been covered, but the three above are far and away the most serious kinds that all businesses should be preparing to combat against. But how do you effectively protect all areas of your business against such an all-encompassing threat?

Protect and mitigate

The answer is in taking a proactive stance towards cyber security. Gone are the days when businesses could afford to think on their feet and deal with attacks when they presented themselves. Nowadays preparation is key, and those that fail to acknowledge this will be the ones that are hit the hardest. As part of this proactive approach, many businesses quickly realise the value in working with a trusted IT partner to implement a cyber security strategy. These strategies are essentially a comprehensive set of best practices that covers every eventuality and is distributed to all employees across the company, raising awareness of the issue and the correct steps that should be followed in the event of an attack. For these strategies to be truly effective, they should be acutely tailored to the size and nature of the businesses that are writing them, taking into account any potential security risks and any current security protocols that can be improved. The cyber security strategy of a small PR firm is going to be wildly different from that of a large global technology corporation.

By working with an IT partner to complete this strategy, businesses are ensuring that every security-related risk has been considered and prepared for. While some businesses might lack the required technical knowledge on their own, specialised IT partners can help to fill these gaps and provide mitigation advice based on first-hand experience.

Conclusion

This cyber attack epidemic has by no means reached its peak, and as technology continues to advance, online criminals will continue to exploit it to their advantage through various means. This means that businesses cannot afford to be complacent: they must commit to a permanent proactive cyber security approach that mitigates the associated risks of both existing and emerging threats. With a cyber security strategy in place, they are one significant step closer to achieving that goal.

Link to the original article:
https://www.professionalsecurity.co.uk/news/interviews/tactics-of-cyber-criminals/