Media title: PwC beefs up security for rising threat of cybercrime
Author: Robert Trong Tran
Source: Vietnam Investment Review on 21 March 2016
Online link: http://www.vir.com.vn/pwc-beefs-up-security-for-rising-threat-of-cybercrime.html

Tech

10:10 | 21/03/2016

PwC beefs up security for rising threat of cybercrime

According to PricewaterhouseCoopers' 2016 report, around 45 per cent of boards now have a cybersecurity strategy.

Also revealed in PricewaterhouseCoopers' (PwC) study is the fact that the recorded number of corporate cybercrime incidents in 2015 stood at 59 million – most likely a fraction of the true figure. Corporate cybercrime has seen double-digit growth over the last five years. Breaches originating from cloud-connected devices jumped by 152 per cent in 2015 compared to a year earlier. With the continuing rise of the Internet of Things, we can expect the number of breaches to accelerate. And cybercrime losses can be heavy: 7 per cent are greater than $1 million.

However, almost half of all company boards still view cybersecurity as an IT matter, rather than an enterprise-wide risk issue. Boards are concerned about cyber threats but are not actively engaged in solving or preventing them.

Moreover, many Vietnamese business leaders still think that a cyberattack could only happen to "other" people or hold the mindset of "locking the barn door after the horse has bolted" (where cyber protection would be considered only after an attack occurs).

More and more Vietnamese and foreign corporations are victims of ransomware, a malware-based method of attack where companies' computer networks are held hostage by hackers until a ransom is paid. A recent, well-publicised victim is the Hollywood Presbyterian Medical Centre, whose IT system was locked until the centre paid $17,000 to the cybercriminal. In Vietnam, a multinational company was hacked with ransomware and its whole system was inaccessible for two days.

These are just a couple of examples from a long list of businesses who have become victims of cyber crooks and have proved ready to pay the cybercriminals to get their business back on track.

So how does ransomware work, and what impact could it have on your business and reputation?

Organised criminal gangs exploit weaknesses in business security systems and use them to breach their internal network, which then prevents the company accessing its own systems and servers. The gangs do this by encrypting the server hard drive or database. This inevitably disrupts the business.

Vu Thi Thu Nguyet, Marketing & Communications Manager, Tel: +84 4 3946 2246, Ext: 4690, Email: vu.thi.thu.nguyet@vn.pwc.com

Media title: PwC beefs up security for rising threat of cybercrime
Author: Robert Trong Tran
Source: Vietnam Investment Review on 21 March 2016
Online link: http://www.vir.com.vn/pwc-beefs-up-security-for-rising-threat-of-cybercrime.html

The business owners are then forced to pay a ransom through bitcoin payment methods in order to gain access, once again, to their own systems.

This is one of many possible examples of cybercrime. Why does it continue to grow so quickly? The answer is simple: because cybercrime is more lucrative than drugs. It is one of the most profitable industries in the world. A recently-released report revealed that cybercriminals receive an estimated 1,425 per cent return on their investment in the purchase of exploit kits and ransomware schemes, which trick corporations into paying hackers who have installed malicious software on their computers.

This is thanks to Malware-as-a-Service (MaaS), which is the business delivery model that today's online black market heavily relies upon. Using the MaaS model, anyone who is willing to commit a crime online is now able to launch attacks to disrupt corporations anywhere in the world, and they don't even need to own the necessary equipment or possess the skills to carry out such an attack. They can easily pay others to do it, or rent out the necessary tools.

Once the ransom has been paid, are you still vulnerable to another attack? The answer is yes – the attackers not only now understand your system and its weaknesses, but also know you are willing to pay ransom money. This is why business leaders need to learn more about cybersecurity as well as other areas of the business. Cybercrime could happen to anyone, and it could taint a business' reputation that has taken years to build.

Thus it is urgent to assess your current cybersecurity state. Are you ready to protect your customers' data and your reputation? Or are you prepared to see the story of your company's data breach on the front page of the newspaper?

PwC Vietnam has set up a dedicated cybersecurity team. We provide a comprehensive range of services that help you assess, build, and manage your cybersecurity capabilities, and respond to incidents and crises. Our services are designed to search for potential threats and vulnerabilities, secure your environment, and help you build confidence in your digital future.

(*) Senior manager, Cybersecurity Assurance at PwC Vietnam

By Robert Trong Tran*

Vu Thi Thu Nguyet, Marketing & Communications Manager, Tel: +84 4 3946 2246, Ext: 4690, Email: vu.thi.thu.nguyet@vn.pwc.com