Media title: Cyber-attacks have become a fact of life
Author: Robert Trong Tran, Director of Cyber Security and Privacy Services, PwC Vietnam
Source: Vietnam Investment Review on 23 May 2017
Online link: http://www.vir.com.vn/cyber-attacks-have-become-a-fact-of-life.html

Cyber-attacks have become a fact of life

Five days after being released, the WannaCry ransomware has infected more than 300,000 devices in over 150 countries worldwide, as reported by the United States Homeland Security Advisor.

"To have cyber peace, prepare for a cyber-attack" - Robert Trong Tran

The magnitude of this cyber attack is unprecedented and the number of victims is still rising in many parts of the world, including Vietnam. This massive attack has pointed to the need for all organisations to take a formal approach to counter similar possible attacks in the future.

A wake-up call

The hackers behind WannaCry exploited a vulnerability in the SMBv1 (Server Message Block version 1) protocol in the Microsoft Windows operating system. Similar to the Conficker worm from 2008, WannaCry can spread automatically via the Internet and local area networks. It does not need any interaction with the user to be able to claim the highest administrative rights in their personal computer or server.

The main difference to Conficker is that WannaCry is a ransomware worm: it encrypts users' files and locks them out of their computers, then demands a payment in the cryptocurrency Bitcoin. It threatens to destroy the data and raise the fee if no payment is made after a few days.

This globetrotting ransomware has attacked all kinds of targets, from small enterprises to multinational companies, from public infrastructure to banks. What is most concerning in this attack is that many crucial service suppliers, such as hospitals, power plants, water plants, and telecommunications companies, can easily become victims. This is due to the fact that many of these suppliers still use obsolete equipment and legacy softwares, which hinders them from installing and applying security patches easily.

A stoppable infection

In fact, many organisations and businesses could have avoided the attack, as over two months ago Microsoft already released security update MS17-010 for the current Windows operating systems in order to protect against the malware. The company offered another patch on May 16 for older operating systems like Windows XP and Windows 2003. We recommend that all Windows users immediately update this patch for their computer system to avoid becoming targets of WannaCry.

Vietnam Computer Emergency Response Team (VNCERT) under the Ministry of Information and Communications has also issued warnings and offered guides to government bodies, businesses, and individuals to protect themselves from the ransomware and its variations.

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

Media title: Cyber-attacks have become a fact of life
Author: Robert Trong Tran, Director of Cyber Security and Privacy Services, PwC Vietnam
Source: Vietnam Investment Review on 23 May 2017
Online link: http://www.vir.com.vn/cyber-attacks-have-become-a-fact-of-life.html

Preparation is key

As I have said in several previous media articles, cyber-attacks are becoming increasingly sophisticated and dangerous, even to modern systems. Vietnamese organisations have to change their mind-set and come to terms with the reality that cyber risks are inevitable. It is impossible to completely prevent attacks and so organisations should always be well-prepared to respond and minimise the losses when an incident occurs.

In order to do that, they need to keep in mind that:

- Cyber-attacks are NOT AN IT RISK, THEY ARE BUSINESS RISKS. According to CGI, cyber-attacks can wipe out 15 per cent of a company value.

- A successful cyber-attack is a matter of "when," not "if." The new National Institute of Standards and Technology's NIST 800-184 "Guide for cyber security event recovery" recommended organisations to prepare response plans and build a "playbook" for recovering after attacks.

- Shift from prevention to detection. Organisations should improve their prevention capabilities with modern technology and tools while augmenting their cyber event detection and response capabilities. The main goal is to detect the attacks as soon as possible before the enemy can steal our most valuable data.

- What can happen will happen: if the attack escalates to high-privileged users with administrative rights, there needs to be a response team ready to handle the worst case scenario. This would include people from the technical team, legal team, PR team, and of course, the executive team.

I strongly advise each organisation to prepare their own playbooks to respond to the event of an incident, such as a Data Breach, DDoS, Website Defacement, Phishing, etc. Each playbook can focus on a unique type of cyber incident and can be organisation-specific, tailored to fit the dependencies of its people, processes, and technologies.

This is of utmost significance for the board of directors to respond quickly and minimise the consequences of such attacks. They should try to automate and test the playbooks regularly, in order to be constantly ready for any type of attack. If businesses had prepared a playbook to respond to network security issues, they could have prevented the spread of WannaCry. With a playbook able to automate and orchestrate actions, businesses can detect and control the ransomware before it diffuses all over their internal network.

Moreover, companies should not consider cyber security a cost centre but rather an added value to their business. Certain investments simply have to be made. However, these are scalable depending on the size of the organisation.

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

PwC in the News

May 2017

Media title: Cyber-attacks have become a fact of life
Author: Robert Trong Tran, Director of Cyber Security and Privacy Services, PwC Vietnam
Source: Vietnam Investment Review on 23 May 2017
Online link: http://www.vir.com.vn/cyber-attacks-have-become-a-fact-of-life.html

For example, many small and medium-sized enterprises (SMEs) in Vietnam have become victims of cyber attacks because they do not have an IT department or employees specialised in cyber security. They often make the mistake of thinking they are too small to be targeted and often choose to pay the criminals when attacked.

For SMEs, I would recommend to focus resources on their core business, outsource their cyber security function to a Managed Security Services Provider (MSSP) and use cloud computing more to protect their data.

Cyber security is a combination of people, processes, and technology. Every element is important, but I think that organisations should first invest in their people, raising their awareness and offering intensive training. Organisations should make their employees the first line of defence for cyber-attacks.

By Robert Trong Tran - Director and Leader of Cyber Security and Privacy Services at PwC Vietnam

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