Media title: Vietnamese organisations increasingly vulnerable to hackers
Author: Hong Anh
Source: Vietnam Investment Review on 04 August 2016
Online link: http://www.vir.com.vn/vietnamese-organisations-increasingly-vulnerable-to-hackers.html

Highlight

20:17 | 04/08/2016

Vietnamese organisations increasingly vulnerable to hackers

Vietnam is a rising hot spot for cyber-criminals, as business and financial transactions are becoming increasingly reliant on the Internet.

The Vietnam Airlines cyber incident last week was another warning shot, reminding us that we can never neglect cybersecurity. **Robert Trong Tran**, director of Cybersecurity Services at PwC Vietnam, talked to VIR's Hong Anh about the rising threat of cybercrimes for Vietnamese organisations in the near future.

As a cybersecurity expert with over 16 years of international experience, what are your thoughts concerning last week's incident at Vietnam Airlines?

This incident once again confirmed the famous saying of John Chambers, one of the top brains in the world of technology: "There are two types of companies: those who have been hacked, and those who don't yet know that they have been hacked." I reckon that there will be similar or even worse incidents in the future, given the lack of maturity of cybersecurity in Vietnam.

It is known that cybercriminals can compromise any system, no matter how much was invested in cybersecurity. In 2013, hackers stole 40 million credit card numbers from discount retailer Target in the United States, just six months after the chain invested $1.6 million in a new malware detection tool. The company's brand was severely damaged, resulting in a 46 per cent drop in net profit in the same quarter. Recently, hackers even managed to leak classified emails from the Democratic National Committee and caused presidential candidate Hillary Clinton a lot of trouble. Obviously, cybersecurity has become vital for companies, as it heavily impacts modern organisations' reputation worldwide.

The hackers who failed to hack a Vietnamese bank last year managed to steal $80 million from the Central Bank of Bangladesh soon thereafter. Does this mean that Vietnamese banks, in particular, are better protected than other organisations?

Media title: Vietnamese organisations increasingly vulnerable to hackers
Author: Hong Anh
Source: Vietnam Investment Review on 04 August 2016
Online link: http://www.vir.com.vn/vietnamese-organisations-increasingly-vulnerable-to-hackers.html

Based on my understanding, local banks often have a maximum limit for transfers that can be automatically processed via SWIFT. Maybe this prevented the hackers from stealing the money. But frankly speaking, the maturity of cybersecurity at Vietnamese banks is still in its early stage.

Generally, local bank leaders do not properly recognise the importance of cybersecurity. Many banks still believe that it is as simple as buying technology for a few hundred thousand dollars, and that is it. Local banks are not aware that professional hackers compromise their system by targeting the employees, not by challenging cybersecurity technology. Cybercriminals can easily use employees' computers to access important data stored on the internal server, after tricking them into opening malicious files or clicking on links.

Another issue is budgeting. Some local bank leaders tend to consider a cybersecurity budget as a burden, not as an investment for their future. This is a terrible mistake. Did you know that the Bank of America has an unlimited budget for cybersecurity for the current financial year? Besides the reasons for strict regulations regarding information privacy in the U.S. and ever-rising threats, the Bank of America also recognises cybersecurity as a value-adding factor to its brand.

It is widely accepted that there is no invulnerable cybersecurity system. Why is this so? What other threats will Vietnamese organisations, particularly financial institutions, have to face in the near future?

We do not have a system that can completely prevent hackers from stealing our data, because professional cybercriminals never stop developing more sophisticated and cunning methods. It is only a matter of time, but they will eventually discover and exploit our weaknesses. Based on my observations, Vietnamese organisations and banks will soon fall victim to cyberattacks relying on two major methods.

The first one is phishing, which means stealing data and controlling the computer remotely after tricking the user into opening malicious files or links.

The second method is the watering hole, which is not new but has seen recent use again by hackers. The watering hole is a cyberattack strategy in which the victim is a particular group, such as employees of an important function. Here, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some members of the targeted group get infected.

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

Media title: Vietnamese organisations increasingly vulnerable to hackers
Author: Hong Anh
Source: Vietnam Investment Review on 04 August 2016
Online link: http://www.vir.com.vn/vietnamese-organisations-increasingly-vulnerable-to-hackers.html

The human factor is clearly the weakest link in any cybersecurity system. No matter how technologically advanced banks are, they will be hacked if their employees do not receive adequate cybersecurity training.

PwC's Global State of Information Security Survey 2016 revealed that the number of recorded corporate cybercrime incidents in 2015 stood at 59 million. In Vietnam, VNCERT reported that there were 31.500 cyber-attack attempts last year. The numbers of phishing attacks quadrupled and the number of malware attacks nearly doubled compared to the year before. Although International Telecommunication Union ranked Vietnam at number 10 in their APAC's Cybersecurity Index, the country only tops Laos and Cambodia in the ASEAN.

In another remarkable incident at the end of last year, a commercial bank in Vietnam was targeted by international hackers in a failed theft of $1 million.

It is safe to say that financial institutes will always be the most valuable targets for cybercriminals. What can local banks do to build an effective cyber-defence strategy and prepare for the worst case scenario of successful cyberattacks?

A cybersecurity strategy cannot reach its full potential unless the leader properly recognises how vital it is for the business. Leaders must first change their mind-set about cybercrime and ask themselves when or how the bank's cyber-defence will be compromised. They must be aware that cybersecurity is their own responsibility, not that of the IT department alone. Only after this can a leader give aggressive orders to his subordinates regarding the issue.

Next, an independent third party should be brought in to help examine the current state of cybersecurity and develop a cyber-defence strategy. The strategy must be detailed and clear, with prebuilt worst case scenarios for when the hacker breaches the system, on what prevention or control methods we need to execute. We have to understand hackers' behaviour, how they can dive deeper into our system and what they are looking for. Another suggestion is setting up decoys, like honeypots, dummy servers with fake data to lure hackers in and keep them preoccupied there as long as possible.

Banks should also form their own response team dedicated to cybersecurity issues. Most local banks do not have such a team yet, and even if they have one, its readiness is still highly questionable. Like firefighting, you have to constantly train yourself, or you will stumble when an incident happens.

Last but not least is the human factor. Local banks must continuously educate and train their employees to be aware, to avoid cyber-risks, and to demand cybersecurity assurance whenever possible. This is quite easy and will not cost banks a fortune. For instance, we can update our employees frequently via emails on current cyber-threats, o randomly test their awareness with fake files or links. If employees know how to stay away from potential threats, banks may have already reduced their chances of being digitally compromised by 70-80 per cent. I am a firm believer that cybersecurity is not only for the rich. We can all secure ourselves from cybercriminals and be cost-effective at the same time.

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