Vietnamnet network crashes: What is anticipated

Vietnamnet's online newspaper, which was hacked by hackers yesterday (November 22), is considered a big warning for all Vietnamese websites today. However, this incident has been predicted by network security experts many years ago.

Vietnamnet's online newspaper, which was hacked by hackers yesterday (November 22), is considered a big warning for all Vietnamese websites today. However, this incident has been predicted by network security experts many years ago.

Vietnamese website is taken advantage of

According to Vu Quoc Thanh, vice president and general secretary of the Vnisa Information Security Association, the case of the Vietnamese e-news website being knocked down is an **expensive lesson about the vigilance and neglect of system security Vietnamese websites are currently available** . These websites do not yet have the best protection even though, many years ago, security experts warned of the risk of being vulnerable.

Meanwhile, according to the latest survey data of Vnisa, 26% of enterprises and organizations do not know if their network has been attacked. Although this number has decreased significantly compared to 2009 (36%), but the rate of 26% is still very high and equivalent to the rate of businesses and organizations in the US are not aware of this problem in 2000. 16% of businesses and organizations said they were attacked but it was unclear how many times they were attacked. Thus, the ability to recognize attacks of businesses is low and do not know the engine is attacked nor quantified what damage.

Only 11% admitted that they were attacked but followed. This number has decreased compared to 2009 (16%). Besides, the percentage of businesses claiming not to encounter any attack also increased sharply from 11% to 27%.

Mr. Thanh also warned that the Vietnamese website is being exploited. Targeted, organized and even international attacks are emerging with increasing frequency and more sophisticated methods.

This is even more evident as the number of Vietnamese emails used to make online fraud appears more and more strongly. 2010 is considered a ' *hot* ' year of information security in Vietnam. ' *Not every year Vietnam has been mentioned as much as this year,* ' Thanh said. Vietnam has continuously been included in many international lists on safety related issues.

Typically, the .vn domain name is listed by McAfee security company as the most vulnerable domain names. According to Mr. Thanh, the reason that the .vn domain name was attacked the most was because cyber criminals took advantage of many vulnerabilities and weaknesses on this website. Each of these vulnerabilities could be used by cyber criminals as a springboard for other attacks. They use Vietnamese websites as an intermediary to attack for another purpose.

The trend has many potential risks

According to Mr. Derrick Ng - Business Manager of Checkpoint, 10 years ago, businesses only needed to use anti-virus software and firewalls. However, at present, the Internet is developing very fast and becomes much more complicated. This becomes even more urgent when switching to the cloud platform. Meanwhile, businesses provide primary users with services, including data storage.

Besides, the growing network environment also creates many opportunities as well as provides users with tools to exchange information more easily, especially social networks. However, it is this permissiveness that brings many risks to users and their businesses.

According to Tran Van Hoa, deputy head of the Department of Crime Prevention of High-Tech Use, cybercriminals now no longer want to break into a website to show off their feats but mainly to financial institutions. with more specific goals, use more automated, destructive methods. Therefore, the risk of losing ATTT often causes great losses mainly to the banking and telecommunications industry.

Cybercriminals primarily take advantage of vulnerabilities on websites, software to illegally access, install back doors, trojans, steal domain names, sensitive information, denial of service attacks, or even bring destructive properties, falsifying information.

DDOS denial of service attacks - BOTNET will block the connection, making it impossible to access the website. This is done by installing a code that controls ' *ghost* ' computers in the network. Meanwhile, most of Vietnamese websites today do not really invest from programming, technical basis to system administration. Small businesses often do not have enough money to invest in website construction, so they sometimes buy back existing websites. Therefore, it is easier and more frequent to be hacked.

On the other hand, most do not have a response process when there is a problem as well as data backup. Therefore, it will take a long time to be defeated when it is knocked down and Vietnamnet is a typical lesson for Vietnamese websites today.

Therefore, businesses and organizations with websites need to have decentralized policies, strict access management, human resource management training as well as having a policy to record and save log files to

detect and investigate tons of resources public. In addition, they need to build a mechanism to coordinate with high-tech crime prevention police, computer emergency rescue centers and network security centers to promptly handle incidents.