# Awareness and experience - the most important factor in every network security process

Need to improve information security capacity in 3 basic elements: people, processes, and technology solutions

We have published a lot of news on quantrimang.com regarding dangerous cyberattack campaigns, security incidents that cause great damage both internationally and in Vietnam. In Vietnam alone in the first 6 months of 2019, there were 6219 network security incidents recorded by VNCERT experts, including 240 cases involving dangerous malware, 824 the destruction of digital infrastructure and 2155 online fraud attacks. This is a huge number for any country, at the same time, it partly portrays the overall picture of the global cyber security situation, with the number of attacks increasing and constantly evolving. more complex, despite the fact that processes, solutions and security technology are also increasingly enhanced.

So what is the cause of this worrying fact? It all comes from the core element of being human.

1. Alarming statistics on the situation of network security in our country in the first half of 2019

## Awareness and experience in network security

1. Some popular forms of cyber attacks are targeted at organizations and businesses
    1. Attack with malware (Malware attack)
    2. Attack ransom
    3. Denial of Service (DDoS) attacks

    4. Database attack (SQL injection)
2. Improve knowledge and awareness in network security security
3. Some basic security solutions that every individual or organization needs to understand
    1. For organizations and businesses:
    2. For each individual:

# Some popular forms of cyber attacks are targeted at organizations and businesses

## Attack with malware (Malware attack)

These are stories related to spam emails that can spread malware, infiltrate the intranet and leak / steal a significant amount of personal information from data centers. in many different cases.

After grasping the details of the target, hackers often try to convince users to open attachments, click on links or exploit personal information through emails that look very much like email from trusted organizations. reliable, like a bank, government agency or online retailer. Just download the malicious file attached to the computer or click the link in the email, the malicious code will spread on your system, and automatically establish a connection with a command server and control (Command & Control - C2) external - server is controlled by attackers.

It is difficult to implement radical countermeasures against this type of malicious infection. You certainly can't completely manage what kind of situation people should open email and vice versa. That's not to mention the case that some malicious spam emails are so disguised as sophisticated that even 'inexperienced' experts will become victims.

1. Secure desktop application - weaknesses are often overlooked


*Malware attack is the most popular form of cyber attack today*

In addition, firewalls and IDS / IPS - popular network defense measures - can easily block any suspicious connections outside your network, but in fact, basic information sent from the outside as a response to contacts starting from within the network.

Another problem to mention is that it is very difficult to prevent individual email recipients from clicking on the malware download link attached to that email. Even if security experts are still working day and night about 'Be careful, don't click on a strange link that can download malware to your computer', at the individual level, sometimes warn this. again ignored. After all, the most serious error still comes from people - something that can be limited, but inevitable, because everyone can make mistakes - by subjectivity or lack of knowledge. Therefore, it is necessary to implement some measures to improve defenses towards the system, but the problem is that no method can give 100% efficiency, at least until now.

In fact, this type of cyber-attack is not a technique for spreading malicious software "bluff." It is becoming a complete, well-prepared attack method. after the information gathering stages and before reaching the target.

1. What is malware analysis? How are the steps taken?

## Attack ransom

A ransom attack is a form of publication by malware. The function of ransomware is to restrict access to the computer system it has infected, and require a sum of money for the person who created the malware in order to remove the restriction of access it created earlier. Most ransomware now go in the direction of encrypting files, data on the hard drive and asking the victim to pay data ransom.

1. Even DSLR cameras can be easily attacked by ransomware

*Ransomware victims will be required to pay ransom in exchange for data decryption keys*

In the case of ransom encryption software, an attacker does not need to be so elaborate as to deliberately attack and this type of software can be deployed in conjunction with hole mining campaigns. Security vulnerabilities exist in the operating system as well as software, so the scope and extent of impact will also increase significantly. In the case of ransomware, it can be said that the level of damage will vary depending on the

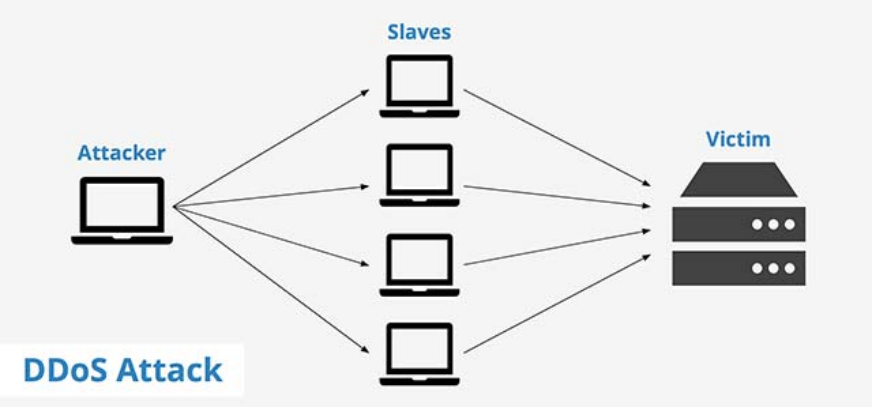
precautions taken earlier. In the case of intentional attacks, the goal is basically those who hold information of value such as a public company or organization, and that data is usually placed in a data center.

In most cases, crooks will target data warehouses and systems of companies that hold specific customer information. The problem gets worse when nothing can guarantee that the data will be retrieved even if the victim has paid the ransom, such cases are not uncommon.

1. Ransomware (ransomware) is showing signs of explosion worldwide, paying is no longer the most effective option.

## Denial of Service (DDoS) attacks

This is a form of attack that hackers' temporarily knock down a system, server, or local network through a huge amount of traffic / requests at the same time, causing the system to be overloaded and people User cannot access the server.




*The diagram simulates a DDoS denial of service attack*

For denial of service attacks, damage caused will depend largely on the bandwidth rate of the attacker and the defender. If you have many broadband connection terminals in hand, and you attack while amplifying packages, small and medium data center operators will be hard to keep up with. On the other hand, if the bandwidth is large enough, some attacks can be overcome but the system does not suffer much damage. This really depends on the balance. DDoS attacks are difficult to block because there are too many terminals involved in the attack, but the ability to effectively defend can still meet to some extent. The defense here is nothing but an active approach, possibly on the data center side. For example, a load balancer along with advanced security features can help identify early and block DDoS attacks by packet.

1. The most dangerous hackers on the planet: Anonymous, Equation Group, Department 121 . What do you know about them?

## Database attack (SQL injection)

This is also a form of attack aimed at organizations and businesses taking place with dense frequency.

Hackers will send a malicious code to the server using structured query language (SQL) to make that server return confidential, important information. Most SQL injection attacks stem from website vulnerabilities, sometimes hackers just insert a malicious code into the 'Search' toolbar that can attack a website. A tool for deploying SQL injection attacks is any web browser, such as Internet Explorer, Netscape, Lynx .

1. Overview of building enterprise security detection and response system


*SQL injection targets organizations and businesses with increasing frequency*

In fact, there are many other forms of cyber attacks such as: Supply chain attack, Email attack, internal attack, . Each attack method has its own advantages and disadvantages, But the common point is that increasingly complex and sophisticated changes, which require each individual and organization to constantly update their knowledge, raise their vigilance, as well as add new security technologies.

# Improve knowledge and awareness in network security security

After all, in addition to weaknesses in telecommunications infrastructure and information technology - leading to the inability to meet essential security requirements, increasing the risk of cyber-attacks - the factor People, awareness and skills of prevention of cyber-attacks are the factors that experts focus on and play the most important role.

Through practical surveys, one of the reasons for the success of cyber-attack campaigns is generally that many businesses and organizations are organizations operating in the financial sector, such as banks, Credit funds, e-commerce enterprises have not given adequate attention to the work of raising awareness as well as the necessary security knowledge for staff, along with the "negligence" when provide access to confidential information for individuals who do not have both expertise and responsibility.

1. What is email encryption? Why does it play an important role in email security?

*Human factors, awareness and skills to prevent network attack activities play a particularly important role*

Many statistics have shown that, in addition to the sophistication in the attack method, the limitations of knowledge and skills to ensure network security, especially the skills to handle invasive situations of the operation team The system is the perfect 'catalyst' for network security disasters. On the other hand, most of the members participating in the network also have a subjective mentality, not strictly implementing the regulations on ensuring safety and information security. All security solutions, no matter how advanced, will still be ineffective when each individual does not know how and is conscious of protecting himself.

In summary, in order to protect themselves in the digital age with many threats of permanent network security, businesses and organizations need to improve information security capacity in three basic elements: children people, processes, and technology solutions. The reason people are the first mentioned factor because this is a prerequisite factor, plays the most important role in every security process. All organizations need to promote investment in training people, improve knowledge and awareness of information security in addition to building a process to ensure information security and handling when incidents occur. declare security solutions in a comprehensive way.

1. What is data exfiltration? How to prevent this dangerous behavior?

# Some basic security solutions that every individual or organization needs to understand

## For organizations and businesses:

1. Promote training and update the latest security knowledge for each employee. Combining instruction and cultivating how to use and take advantage of modern security systems.
2. Build a transparent security policy with clear and transparent terms.
3. Actively update new, modern security systems, and be consistent with their system characteristics. At the same time, the selection of security software for deployment must also be carefully considered. Prioritize the use of products by parties with a commitment to security and regular security updates.
4. Say no to any type of crack software. Prohibit the use of internal crack software.

5. Enhance the use of enterprise cloud services for storage purposes.

## For each individual:

1. Conscious of raising awareness and self-awareness about information security. Improving the experience of security incident response as well as operating new security processes.
2. Regularly update personal computer software, operating system to the latest version. Do not use crack software.
3. Highly alert when browsing email, check the sender's name carefully to prevent fraud. Absolutely do not download attachments or click on links of unknown origin.
4. Limit the connection of peripherals (USB, hard drives) to personal computers in the company.
5. Note to set up complicated and non-repeating passwords (use additional password management tools if necessary). Take advantage of additional security features if available, such as 2-factor authentication, biometric security .

The above is basic information about some common forms of cyberattack targeting organizations, businesses, the importance of knowledge and individual awareness in every security process, as well as a few Basic security solutions that every individual or organization needs to understand. Wish you build yourself an optimal security process.

1. The cybersecurity tools that every business should know