How dangerous is ransomware attack?

What is a ransomware attack? Why is it a dangerous threat to businesses? On the occasion of World Backup Day 5.3, the following article will help you better understand ransomware and thereby help raise society's vigilance against cybercrime.

What is Ransomware?

On the evening of March 30, the Department of Information Security issued a warning about strengthening network information security for information systems after many domestic organizations and businesses suffered ransomware attacks recently. Ransomware is a type of software used by hackers to infiltrate a computer or data system and encrypt files or lock the victim's entire system. The attacker will then demand a ransom to receive the unlocking tool.

Common ransomware attack methods include sending email attachments or malicious websites, taking advantage of system vulnerabilities to access the victim's computer system. Once successfully infected, it encrypts files, makes them inaccessible, and displays a ransom demand. Typically, these requests will have a fixed deadline. Failure to pay on time can lead to the risk of deleting encrypted data or publicly disclosing victim information.

Ransomware affects financial institutions, government agencies, schools, hospitals, businesses. It can attack local drives and affect all connected devices or even wipes entire network and backup data in one go.

Although it is still possible to restore data, it will be time consuming and costly if the victim is not prepared. To prevent ransomware, organizations should carefully manage email security, network security, regularly update systems and regularly back up important data.

Ransomware is persistent and increasingly dangerous

The first ransomware attack happened in 1989. After more than 30 years, ransomware has become more complex, dangerous, and increasing in density. The number of cyber attacks has increased by 22% in Asia-Pacific and 40% worldwide between 2021 and 2022.

It usually takes businesses a few weeks to a few months to recover after a ransomware attack. However, according to a study by Kaspersky1, up to 71% of businesses cannot even restore data after being attacked. Even if organizations are willing to pay the ransom, it is still uncertain that lost information will be recovered. According to statistics, up to 50% of organizations still lose part of their data and 13% even lose all of it even after paying the ransom.

Today, ransomware has evolved into a profitable business model, leading to increasingly sophisticated attacks with specific targets. Typically, ransomware follows steps from gathering information, to tricking victims into accessing malicious links to exploit vulnerabilities and intrusions. After that, hackers will continuously collect important information and data and encrypt the original data at the source. Finally, there will be the negotiation and blackmail step. If it fails, the organization's important information will be directly disclosed or deleted.

To protect against ransomware, it is necessary to ensure systems and software are always updated, install anti-virus software and whitelist software, train employees not to install software of unknown origin, and be alert to threats. Latest ransomware threats. Additionally, regular backups with immutability are essential, helping to isolate data from attacks. In the event of an attack, it is necessary to ensure that the recovery process takes place quickly to ensure business operations are not interrupted.

Faced with the rise of ransomware, data protection is more important than ever. Every year, ransomware causes millions of dollars in damage, and despite preventative measures, the problem continues. Hackers can try thousands of attacks, while organizations only have one chance to fight back. In such a situation, data protection solutions are extremely important for organizations to deal with ransomware.