9 misconceptions about security and how to resolve

Almost every recent study of security vulnerabilities has come to the same conclusion: people are more risky factors for a business than technology gaps.

People can make mistakes, but if it involves security and network security, that mistake can cause great damage to businesses.

Almost every recent study of security vulnerabilities has come to the same conclusion: people are more risky factors for a business than technology gaps.

This conclusion, which is also agreed by the majority of experts, is that it is because users are not aware of the increasingly sophisticated security threats or there is also the case that users do not care about the call is network security.

So is the multiplication, and so is security. There is no solution, no application is absolutely safe. However, security issues will be better if your employees at every level in your organization, your business are aware of the common mistakes about security knowledge:

1. Being cheated

This is one of the most common mistakes. Users can be deceptive when clicking on links (links) or attachments in phishing emails, social networks, advertising information on legitimate websites. Scammers often design quite sophisticated so that users do not have any doubts, making you think that this is an old friend, family member or newly established business with attractive products.

How to resolve : Train employees to be skeptical about everything, and just click on the link to know for sure the sender is reliable. Businesses should also periodically perform 'controlled active fraud' activities to check and raise awareness for employees.

David Monahan - Director of security research and risk management at Enterprise Management Associates, warning even emails sent from trusted people can still be spoofed. Always be wary of emails that require you to verify information, as they may contain malicious code. If you need to check the information, call the sender directly.

2. Using cloud services or unauthenticated applications

Dan Lohrmann, CSO's strategy director at Security Mentor, said that the mistake also includes sending personal information, data to the cloud that is not yet authentic.

Meanwhile, Dave Frymier, Unisys security expert, adds other forms of this mistake from installing remote desktop access applications to buying and using virtual cloud servers. business operations. Dave Frymier said that people do this obviously without realizing the danger.

Solution: Use a reliable cloud storage solution with high authentication features / solutions.

3. Simple password, easy to guess

Using simple, easy-to-guess passwords is similar to unlocking doors. In addition, a common mistake is to use the same password for multiple access accounts or password sharing for colleagues. According to David Monahan, since everything requires passwords, users often use simple, duplicate passwords to make them easy to remember. However, this is a serious mistake sometimes causing disastrous consequences. Many important compromised accounts come from users' ' *impermanent* ' accounts.

How to resolve : If you still want to use a password that is easy to remember, use the letter for the first word or sentence, followed by a few numbers or special characters. Security experts recommend using password management and two-factor authentication (*also known as 2-step authentication*) to improve security (*especially with popular services like Google Gmail, Facbook*). Finally, don't share your password with anyone.

4. Remote access

This is a fairly common method when users work from home to transmit data from the workplace or access remote devices. Expert Dave Frymier said remote access also includes enterprise data storage on a third cloud service. According to David Monahan, in addition to the risk of malicious code, corporate or user data is also vulnerable to leakage, on an unmanaged system. Moreover, users will encounter some legal problems when storing business data on personal devices, when business policies do not allow.

How to resolve : The company needs to issue clear policies on remote access, set the right to use files, applications on personal devices and regularly remind employees to comply with regulations. Security experts believe that a good identity management system can effectively control user access and minimize the number of application access passwords. Technology will help solve the problem of remote access through strict encryption methods.

5. Disable security features

This is only possible when the user has administrative rights. Often users will disable security features to turn off warnings and make it easier to install and use applications and services. Obviously, if security is disabled, the system will have no protection, at which point the catastrophic consequences may occur, analyst David Monahan said.

How to resolve : Enterprises should prohibit web access by admin account. If you accidentally download malware, then with normal access, malicious software will not be able to install. Dave Frymier advises IT administrators to take care of this and ' *lock in* ' security and authentication settings to prevent users from disabling them.

6. Social network

Social networks help employees communicate, work collaboratively more conveniently. But besides the positive side, social networks also have many potential risks such as leakage of personal information and business secrets. Hackers prefer attack techniques based on *social engineering* through the exploitation of information from social networks.

How to resolve : Regularly train employees with practical examples.

7. Few mobile security concerns

Personal mobile devices are increasingly popular. It is easy to see millions of personal mobile devices at work, cafes, on public transport, etc. However, too many mobile devices are not given adequate attention to security, even Minimum security mechanisms such as encryption, user PIN setting are also not set.

How to resolve : Issue a mandatory policy of personal mobile devices of employees must set a PIN. Train employees to perceive threats in their surroundings, public areas, where personal mobile devices can be stolen or stolen. And make sure all business data if stored on personal mobile devices must be thoroughly encrypted.

8. Sharing high administrative rights

Eye Firstenberg - LightCyber's vice president of research, said that in the process of working, he found that the IT department and other business divisions often used the same high-admin account. This makes it quick and convenient to handle work, but the risk cannot be monitored and identifies who has used this administrative right.

How to resolve : High administrative rights should only be assigned to individuals, should not be used for the whole department.

9. Do not update the software patch

One of the most common security mistakes is that users do not update software patches for a time-consuming and troublesome reason. The risk is obvious, when new threats always appear while the system is not updated to

prevent risks.

Solution : Update as soon as the software patch.

You finished reading the article "**9 misconceptions about security and how to resolve**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.