5 common errors in managing security vulnerabilities

In the eyes of some people the issue of managing vulnerabilities is considered one of the intensive security management activities. There are others who think this is just a necessary process that Microsoft has to make

In the eyes of some people the issue of managing vulnerabilities is considered one of the intensive security management activities. There are others who think this is just a necessary process that Microsoft has to do to produce monthly updates. And there are many people who see this as just a 'common marketing phrase' of businessmen.

Through the following article we want to review some common errors that organizations should pay attention to in order to achieve perfection in managing security vulnerabilities in both technology and process aspects.

1. Scan but don't take any action

The first common error is scanning and finding security flaws, but there is not any reaction to the results from the process. Security scanning and detection experts have become 'clamps' in many organizations. Scanning and detection technologies have actually grown and matured in recent years with the evidence that the accuracy, speed and safety of tools have improved significantly.

However, modern commercial or open source scanning tools still suffer from a disease similar to early warning detection systems (IDS). First, these types of tools are too noisy for various reasons that produce too many

warnings. In addition, they don't tell you what you have to do to handle these security vulnerabilities alerts, as well as IDSs that don't tell you if you have to pay attention to a specific intrusion warning. .

Because of this, security vulnerability management is not a scan and detection, but the important thing here is to do the job after scanning and searching. This includes resource inventory, prioritization and research of corrective actions as well as actual actions such as patching or reconfiguration or protection.

2. See patching security holes is similar to managing security holes

In fact, the work of fixing security vulnerabilities is a way to fix known security holes. Even some industry experts say that managing security holes is very simple, including patching and fixing all problems.

But there are many security flaws that cannot be fixed or patched simply by updating the latest version of the application, but also require changing or reconfiguring many system parameters. Therefore, security vulnerability management is required to prioritize and smartly fix security vulnerabilities detected by patching or any other method.

So if you're busy every minute of the third day but don't do anything to eliminate any security holes in the business during the remaining 29 days of the month, you really haven't done the hole management. security vulnerability.

3. Assume that security vulnerability management is only a technical issue

If you think managing security vulnerabilities is simply a technical issue then that is really a surprising thing. In order to achieve efficiency in this work it needs to have a keen interest in improving policies and procedures. In fact, focusing on processes and 'soft' faces in security vulnerability quizzes is often more beneficial than a high-tech hole patching system. It can be said that there are still many weaknesses in policies and information technology infrastructure. Here we also do not mention the weaknesses in policy - this is sometimes considered a security hole. For example, if you are not determined to implement a policy that requires a password of the specified length, then it is the weakness or flaw in your policy and the scanning and scanning experts may not. discovered and consequently there will not be any solution to this problem.

Therefore, weak passwords, lack of awareness of data security as well as the lack of client configuration standards can bring more damage to your security picture as well as increase the risk. you have to face.

According to Gartner analysts, 'The process of managing security vulnerabilities must include tasks such as policy definition, environmental identification, priority, protection, mitigation as well as work supervision and maintenance. '

Thus, according to the above understanding, the process of managing security vulnerabilities will begin with a policy definition document on issues such as organizational resources - applications or systems - with users. Such a document along with other security processes must determine the scale of security vulnerability management as well as identify the 'well-considered' stages of information technology resources.

4. Evaluate a security hole without looking at the panorama

Those who try to follow a reasonable security hole management process sometimes get this common mistake. As they face serious challenges in prioritizing fixing security holes, they often overlook the dangerous angles of that priority. Take, for example, their approach to understanding the importance of security vulnerabilities based on

those security vulnerabilities alone, without looking at the overall picture of the security threat and the roles Business of the system is affected.

The only way to avoid this fourth common mistake is to use Risk = Threat formula x Vulnerability x Value (Risk = Threat x Security vulnerability x Value) and use the results of this calculation formula to decide which holes to prioritize first.

But in order to be able to intelligently set security patches and security holes, you need to consider other factors in your own IT environment as well as outside the world. These factors include:

- The danger of security holes
- Information related to security threats
- Business value and information about target systems

Recently, a new standard in the classification of vulnerabilities of security vulnerabilities has been introduced to help organizations prioritize the order of vulnerabilities that need to be fixed. Common Vulnerability Scoring System (CVSS) considers a variety of security vulnerability characteristics such as priority, exploitation and impact. CVSS is promised to provide a unified way of calculating security vulnerability scoring points and will soon be applied by many security information providers. However, CVSS data still needs to be upgraded to add information about business value as well as threats.

Business information is vital in calculating the order of priorities for security vulnerabilities because they are capable of incorporating technical threats and data vulnerabilities into a business function. Organizations differ in every aspect of their characteristics and as such they have different management and application assets. Attacks that affect a number of organizations can make them bankrupt, but for some other organizations it can only be a temporary scrutiny. However, the fact that life is not so simple and the security holes of non-important security holes are sometimes a stepping stone to exploiting a security vulnerability. other more important.

5. Do not prepare carefully for the unknown - zero-day security error

The fifth common error is the zero-day exploit. This security error is the fear of many security managers. While I still see a lot of confusion wondering what makes 'zero-day exploits'? Simply exploiting a previously unknown security vulnerability. So even if you have patched up all known security holes, you still need to be prepared for attacks by attackers using unknown security holes.

What you need to do?Besides a sensitive security vulnerability management program that includes a lot of workloads, you can protect yourself from 'zero-day exploits' and carefully monitor server network security.You also need to make sure that all response plans are available in case of attack.Such situations need to be addressed by using the 'depth security' principle in security infrastructure designs.