Is security really the problem?

When talking about security, the scale and importance of it is the difference between big and small and medium enterprises. Subsidiaries often have little internal IT resources; most of them do not have director of economic security

When talking about security, the scale and importance of it is the difference between big and small and medium enterprises. Subsidiaries often have little internal IT resources; most have no director of security due to limited budget and pressure to save costs is always the shadow covering all business activities.

However, all large companies, even small when connected to the Internet, share the same elements of protection: prestige, intellectual property, and even the existence of that business. Without expert hands, no abundant budget, try asking how small businesses can resist the pitfalls and dangers in cyberspace?

The following principles and guidelines will help to approach and solve security issues in the right direction:

The response of the leadership class

The first principle is that the company leader must be aware of the importance of security.

Reason: First, security strategy must be a function of business strategy. Or to put it simply, the purpose of the security function is to ensure the safety of business operations. This means understanding the strategies, approaches, and optimizing business operations is the key need to establish security policies and costs.

The second reason is that business policy needs to be put first. However, most policies do not value security or encourage the development of an IT management team. No analysis of system administrator can replace a leader's statement: "Security is very important to us, and that's why we have to do it." Participation and support from the highest level of management ensures the participation and implementation of all employees in an effort to develop a security policy.

Leaders also need to think about how they manage the actual information they collect. This involves more than just locking down servers or setting passwords. Many organizations use data governance software to set clear rules for how data is handled and stored. These tools help teams follow internal policies and meet legal requirements. This keeps the process from becoming too complex. It creates a foundation where information is both safe and useful for the business.

Appropriate balance

Abundant budgets will help businesses be more proactive in security issues. However, being aware of the importance of security costs is not always possible for all companies, including large companies. Therefore, the larger the enterprise, the more priority must be given to security. In fact, security costs are often commensurate with the size of enterprises. For example, a company worth $ 10 million has a security cost equal to one tenth of a company of $ 100 million.

The core issue is the level of cost that needs to be matched with the protection value. Just like insurance, it is necessary to have a certain percentage of assets to correspond to the cost to reduce the risk of asset loss, or compensate for operating depreciation. That percentage varies depending on the importance of the asset to the business.

Understanding the business strategy, and possible risks, an enterprise can define and apply security policies in the most effective way.

Appointment of security experts

When considering the improvement of network and information security, a commonly asked question is: "How many% of employees will strictly implement security regulations?". The "No" answer is usually not a positive solution, but many companies offer this answer. For small businesses, having a security group is a luxury and almost no one has enough money to do such a thing.

But why isn't there a person who takes on this job, or even an experiment? A person is no better than no one? Who will be responsible for the job, and whose work content should be reported to? Some businesses often assign security to IT departments / departments; But other enterprises are attributed to the financial department. Others have security experts who are responsible for reporting directly to the CEO. However, the answer to this problem is not as important as understanding the real role of security experts in the enterprise, which role and role that the expert plays.

Role of security experts

Security experts must spend at least a significant portion of their time researching security issues. Recognizing the importance of security and related principles will be an important step in strengthening and enhancing enterprise information security.

Secondly, the appointed security experts need to have certain authority over security issues, and this authority needs to be widely recognized within the company.

In terms of responsibility, based on discussions and discussions with managers or through business knowledge, security experts need to identify the top security risks for the company. This expert should draft risk mitigation plans to an acceptable level with adequate funds and time. A problem may take up to 12 months to resolve, but it may take only 3 months on a higher cost. The CEO will be the last person to make decisions on such costly risks after carefully considering the capabilities and resources of the entire business.

Security is the way, not the destination

Security is a matter of degree rather than status. No single product, personnel or policy can provide complete security for security. Any company can improve information security by following the following 3 simple steps:

1. Develop policies and requirements
2. Execute solution
3. Verify results

The above process needs to be repeated, and its results will help improve the security level of the business.

Conclude

Businesses, big or small, share the same risks when connecting to the Internet: intellectual property risks, reputation, and ability to do business. However, small companies often face a problem, which is challenging to deal with security risks while internal IT resources are insufficient or unavailable. This limitation can be overcome by the participation of senior management team in planning security plans, linking security strategies to business strategies, setting aside at least one person to undertake security-related tasks, and cleverly select a provider of the best security solutions.