Protect businesses from anger from former employees

Employees who have been discharged may cause destructive behavior. Follow the introductory steps in the lesson to protect your company.

Network administration - *An important employee in the company has just left, along with him are photos of his family, his office supplies or tools at the office - followed by The passwords of hundreds of employees* .

One of the most experienced salespeople in your company heard that she will definitely be fired. And since then, probably before leaving, she will download in her Gmail account a long list of different A + classified accounts and then a series of custody bills paid and must return.

If you think that will never happen to your company, think again. Scenarios like the one above appear a lot today, according to some experts, even the most trusted experts may be involved in data theft and the types of computer crimes that precede Economic downturns and the shadows of people being fired.
Recent statistics have shown that. At the end of 2008, a statistic was made by IT security company Cyber-Ark Software Inc. said about 56% of financial services staff in New York, London and Amsterdam admitted that they were very worried about those who were fired. To prepare for the worst, more than half of them said that these people have downloaded competitive company data they plan to use for their next jobs.

In the US, this percentage is even higher, about 58% of people working on Wall Street say they are the same. 71% of employees said they would bring data with their data if they were threatened by dismissal tomorrow.

When people are desperate to pay for existing money like rent, money to get daily food on the table, they can do anything that they wouldn't normally do, that's Why is crime increasing with economic difficulties. So is there any way to minimize unnecessary risks from the former employees or stay away from it. Following the steps introduced in this article you can protect your company.

Security tips

Regardless of the economic conditions, follow some advice from some experts to make sure the systems are secure and the data is protected when the company's employees leave the office. company.

- Clearly and completely record employee access to networks, applications, servers and company buildings.
- Disconnect remote connections, such as pcAnywhere and VPN systems
- Disable username and password.
- If employees work in IT, change the original access and network access.
- Disconnect external access to the phone system.
- Record handsets, smartphones and cell phones with PCs and laptops.
- Record ID card.
- Use test software to monitor network traffic.

Supply and demand

Clearly, data theft will increase when demand is low and supply is high. At this point, there is a large amount of supply coming from employees and if someone can make him more attractive to new employees later, it will be a great coax.

In the meantime, the staff members quit their jobs to keep increasing. In the past few months, Citigroup, SAP, Sun Microsystems, IBM, Sprint and Microsoft have announced dismissal, adding tens of thousands of unemployed people, many of whom are very knowledgeable and have Access to main computer systems, corporate sensitive data.

What is surprising - and the potential for corporate security - is how many old employees remember such access through so-called 'orphaned' accounts after they were fired. According to research by a security company called Symark International Inc, 4 out of 10 companies have no clue as to whether user accounts are still in a positive state when they are fired.

In addition, 30% of executives reported that they did not have an appropriate process to find and disable these 'orphaned' accounts. Another sad statistic: 38% of them have no way of distinguishing whether an existing or former employee is using or using an 'orphaned' account to access good information. is not.

The most common threat is an employee who can take intellectual property, such as strategic plans or customer data, before or after the person says goodbye.

Many things can be more dangerous in case of firing an IT employee. These are usually employees who have the key to go to every corner of your company.

A *former* UBS IT staff member Paine Webber was convicted and sentenced to eight years in prison on the installation of a "logic bomb", used to sabotage corporate data on a large scale. (A logic bomb is a piece of code used to trigger malicious functions that are in certain conditions; for example, functions can be set to delete all client accounts at a time. that in a specific day).

System administrators and users with privileged account access - such as those who know root passwords - can cause greater dangers because with high privileges they can change data. system data, user access and configuration. Besides, they also easily undermine the IT activities of any organization.

While there are these vulnerabilities, there are still measures that companies need to take to limit potential threats, especially for 'former' employees:

Liberation strategies and security measures need to change depending on the role of each employee . Managers who avoid responsibility for firing certain individuals should not admit that disabling computer access is simply a matter of disconnecting the plug.

Before you fire someone, consider their role. If they are salespeople, human resource or financial managers or important employees, it takes more time (disable access) because they have more access to the systems. compared to other employees.

Expected IT on the issue of dismissal at the beginning when possible . IT needs to be closely aligned with the process of human resource management, but IT staff need to understand how their roles are sensitive and there is no forgiveness for spreading rumors. If an IT employee notifies the person they will be fired, the IT staff member must also list the need to be fired.

Security programs and appropriate policies are required before dismissal . Among the many things that need to be done, you need to make sure that you are using content security systems, preventing data loss as well as threats. Such systems include firewalls, spam filtering tools and antivirus software .

You also need to have an identity and access management infrastructure, known as an Identity and Access Management (IAM) abbreviation, which controls who, what, where and why. for user actions throughout the business. Being able to check and evaluate access rights is an important issue for delegating management and recognizing system abuse.

Division of system access according to employees' roles . This is a principle of designing a secure system that companies need to implement right from the start of any software deployment process. Here access control means tightening business logic layers.

However, many companies skip this step because it is quite time consuming and intellectual in software design. When this initial security design is lacking, the next best measure is software implementation that can record user access to the system and the actions they take while using business applications. other businesses.

Most enterprise applications have some level of security on passwords and user IDs. However with a test system, when a user accesses the database, everything he does here will be recorded and reported.

Plan what bad things can happen . If an action to dismiss your employees goes smoothly, without this employee's disapproving attitude, the company still needs to find witnesses for themselves to prevent some future investigations. .

That is to keep in mind when companies feel there is any breach of security, such as certain data loss related to employees who have quit their jobs, potentially demonstrating that they have used Use all possible precautions and measures to protect that data.

In particular, companies need to use the legal images of staffing laptops, and they will exist if research is done. (A legal image is a copy of your computer's hard drive).

Usually, when something bad happens. In fact, it can take about 6, 12 or even 24 months before being exposed to light. While there are costs for using disk images, you will be compensated for litigation costs if any.