What to do to detect and prevent spying

Today, economic spies are often concerned with financial data, intellectual property and customer data. They can steal information for blackmail purposes, but 'the most common intrusion motivation is industrial reconnaissance & r

Today, economic spies are often concerned with financial data, intellectual property and customer data. They can steal information for blackmail purposes, but 'the most common intrusion motivation is industrial scouting'.

Here are some common tricks and preventive measures that can be used to detect and prevent these abusive behaviors.

Tail

One of the most successful ways for outsiders to infiltrate an organization is not technically high: follow a competent employee to enter the front door. To do this, the spy only needs to wear a uniform or a fake badge.

Once inside, the spy has many ways to infiltrate sensitive information. They can disguise the IT staff to photocopy the documents found at the empty tables. Or they can go into an empty meeting room, open a laptop and steal data from the system. Under this scenario, spies often go into pairs to make it easy to persuade, a fake is a counselor and an employee.

How to prevent? Regulations must be strengthened to prohibit security guards, receptionists and other employees from allowing non-employees to enter the company.

Identify employees

Spies often disguise as IT assistants because this makes them seem legitimate when sitting at the computer. The most commonly used strategy is to find empty offices or ask employees to leave the desk to upgrade their antivirus software. They can also disguise as sanitation workers to penetrate after work hours.

How to prevent? Enhance the awareness of employees. ' *Most organizations are less interested in equipping employees with consciousness. People tend to assume that once someone has entered the company, it must be a valid person, and criminals have taken full advantage of this assumption. There should be standards for matching and not matching and reinforcing by suspecting those who do not comply with these limits* , 'Ira Winkler, author of Spies Among Us (Wiley, 2005) and President of Internet Security Advisors Group, the group that creates spy simulations and provides other services, says.

The second line of defense is to use security tools such as screen savers with passwords, encrypting data and requiring hard passwords for employees with access, such as administrators network for example.

Finally, according to Peter Wood of First Base Technologies, an English consulting firm that specializes in hacking services, must categorize information and store them by value. Applying encryption and passwords to network administrators and senior members can also solve 70% of problems.

Pretend to be a guest

Another way to infiltrate a company is to pretend to be guests like electric maintenance workers or phones, monitor burglar alarms or people from the fire department to check the fire alarm.

How to prevent? According to Wood, outsiders who want to enter the company must be fully examined for all types of documents. Staff should ask guests about the employer and should check the information on the Internet, accompanied by a call to the client's company to confirm the legality.

Web applications

Of course, not every spy applies a low-tech approach. More and more names take advantage of the insecurity of web applications, according to the SANS Institute (SysAdmin, Audit, Networking, and Security) about the Top 20 Internet security risks in 2007. The report named the applications. Web applications are not equipped with the full range of security tools that are the top threats, making data easy to steal and computers being controlled. The report also said that attacks on web applications will increase significantly in 2008.

How to prevent? Web scanning tools can help find vulnerable applications, especially when combined with source code viewing tools and application intrusion tests. The SANS Institute also suggested checking the configuration of the web application framework and strengthening it.

Intra thief

An effective way of spying is to spend money on internal employees to steal information. According to Winkler,

this trick doesn't need high technology, employees only need to use access to download more data than normal.

How to prevent? Winkler uses a combination of access control and pre-audit. For example, customer service representatives often access 30 records per day, suddenly accessing 100 times a day, which is alarming. Ken van Wyck, security consultant, added that it was alarming when suddenly an employee started accessing data from his home.

According to a report by the SANS Institute, another way to stop it is to disable USB ports via a password-protected BIOS or use tools to restrict the use of ports and peripheral devices to steal data. material.

Keystroke typing tool

Spies once inside can be dangerous by using keystroke loggers. Some of these devices send e-mail about the user's typing information to a predetermined e-mail address while other devices store this information in memory. These devices are almost impossible to detect. Wood knows a case of spies disguised as sanitation workers using this technique to steal nearly 300 million pounds from a bank.

How to prevent? According to Wood, increasing computer mechanical testing is the only way to detect keyboard information theft tools.

Phishing

Wikipedia defines phishing as a form of application where spies use a variety of techniques to make people disclose information (such as passwords) or reveal confidential data by clicking on the allowed links. others can control the remote computer. Indeed, the SANS Institute considers phishing to be one of the biggest Internet security risks.

For example, a spy can call from a prepaid mobile phone to the office, declare that he or she is working from home and ask to send a username and password as a message to his phone. Others use the way SANS called 'spear phishing' in which they send the most anticipated e-mail messages to employees, including specific information to make messages seem real (requires your username and password to be sent from the HR manager for example).

How to prevent? Wood offered to train staff to be cautious and how to detect these phishing applications. They must refuse to provide information when the caller appears to be in a hurry, not to name, threaten, ask strange questions or ask for prohibited information. There should also be clear policies to report incidents to the responsible person.

The SANS think that it is necessary to continuously raise the awareness of employees, perhaps by practicing with phishing techniques. In addition, companies need to avoid disclosing as much information as employees' logos and e-mail addresses on public websites.