Ten Ways to Protect Your Network From Insider Threats

By Paul Rubens | May 18, 2010 |

Insiders -- people who work within your organization -- pose a huge potential risk to network security. That's because while hackers and other outsiders have to break in to your network and gain access to systems and data, many insiders have valid credentials to log on quite legitimately and access the systems and data they need to carry out their jobs. Unless appropriate steps are taken, it can be quite trivial for employees to copy your confidential data on to a memory stick and walk out the door, install a logic bomb to destroy data in the future, or set themselves up with login credentials to ensure that they have access to your systems even after they have left your employment.

Here are ten things you can do to protect your network from the insider threat:

1. Screen potential new employees before you hire them

According to CERT, over 30 percent of insider attacks are carried out by people who have criminal records at the time that they are hired. Basic checks can help you identify prospective employees with a history of fraud or theft, while in certain industries it may also pay to have a third party carry out more specialist background checks to try to identify industrial spies or agents from foreign governments.

2. Look out for changes in employee behavior

Many attacks carried out by insiders are motivated by a desire for revenge for a perceived slight -- failure to get a promotion or a pay rise, for example. "These people are often unusually emotional at work and display a change in behavior," says Michael Davis, CEO of Chicago-based security consultancy Savid Technologies. Things to look out for include a drop in work performance, arriving late, and yelling or other inappropriate work conduct. Once identified, these employees should be closely monitored for malicious activities including data theft, and also preparatory activities, Davis says. "If someone has read on the Internet how to put a logic bomb on your network to destroy your data after they have left, they will have to put a script or series of programs on your systems, and they will usually have to test it. When they try it out on your network, that is your opportunity to detect it," says Davis.

3. Publicize you security policies

Well meaning employees who take data home to work on a laptop and then lose it, or who write their passwords down on Post-IT notes where colleagues can see them, also pose an insider threat -- albeit without malicious intent. The best defense against these threats is to remind people continually of your security policies and the reasons why these policies exist. It may also be appropriate to remind employees of the consequences to them of failing to adhere to security policies or any other negligent behavior.

4. Carry out exit interviews

68 percent of insider attacks are carried out by former staff within three weeks of leaving, according to CERT. An exit interview is an opportunity for you to remind staff leaving your organization of the consequences of any illegal actions. Some organization present employees with printouts of recent emails or Web sites that they have visited to reinforce the message that their actions have been monitored. "If a staff member gets fired, he may go and have a beer, and start thinking about revenge. If you talk to him about the security precautions you have in place, and mention the consequences of revenge attacks including prosecution, this may go a long way to preventing such action," says Davis.

5. Implement end point data leak protection

59 percent of staff that lose their jobs take confidential corporate information with them on a DVD or USB drive, according to the Ponemon Institute. End point security systems aim to restrict what portable storage devices can be used, and by whom, and to monitor what information is copied. Such systems can be useful in making it harder to copy information maliciously without being detected, but can't prevent a trusted insider with authority to copy data from doing so maliciously.

6. Monitor databases

"Monitoring data sources, not exit points, is the most cost effective solution," says Amichai Shulman, head of the application defense center at California-based data security company Imperva. "You need strong monitoring to let you put your finger on anomalous behavior or behavior that goes against your policies, in real time. The key is to be able to react in a timely manner, not wait until the data has got out." If a user normally accesses order data one record at a time, and then suddenly accesses hundreds of records in one go, or starts accessing different applications or databases to those that they normally use, then this anomalous behavior should be detected and investigated immediately, he says.

7. Use honeytokens

A honeytoken is a piece of made-up data, such as a particular meaningless string, that can be inserted into a database where it should never be accessed under normal circumstances. If your monitoring systems detect that the honeytoken is accessed then this is clearly not normal business behavior and may provide a warning that database records are being accessed (or copied) maliciously. You can also configure intrusion detection systems to alert administrators if packets containing the honeytoken travel over your network.

8. Monitor sensitive records closely

While honeytokens should never be accessed, certain sensitive records (such as the salary of the CEO) may be accessed legitimately, but only rarely, and by a very small group of people (such as those working in the HR department.) When such records are accessed, steps should be taken to verify who accessed them and why -- even if the records appear to have been accessed by someone with the authority to do so. The reality may be quite different: a disgruntled employee accessing the records from an unattended computer in the HR department, for example.

9. Watch your DBAs

38 percent of insider attacks are carried out by IT administrators or superusers, according to Verizon's 2009 Data Breach Investigation Report. Database administrators have enormous powers over your database, so particular care needs to be taken to ensure that you are in a position to detect any malicious behavior on their part. "If you have a good database management system, controlled by a security officer rather than a DBA, then you can check that a DBA is accessing structural changes to your database without actually accessing the data," says Shulman.

10. Use rights management systems

Insiders pose a greater threat than outside hackers because they have access credentials to your data. But you can reduce the threat any insider poses by ensuring they only have access to data they need to carry out their day to day duties. A good rights management system will enable you to compare any employee's data access rights with the data they actually need, and flag any unnecessary rights that can be removed.

<img alt="" border="0" name="DCSIMG" width="1" height="1" src="http://www.qsstats.com/dcs9xqfq400000spui4ozu2wa_4l4w/njs.gif?dcsuri=/nojavascript&WT.js=No&WT.tv=8.0.2" />
This page
is safe
Bitdefender Antivirus Plus 2012