Title:
You Company Is Growing Fast? It's A Time To Think About Possible Information Leakages

Word Count:
511

Summary:
Do you know all possible ways to take information out of company so that no one would know about this? I'm sure, even there are some certain security rules there are still some possible ways for information leakage. Let's think about how can we control this process.

First, it's necessary to understand that there no any absolute means about security. Even if USB port it blocked, it's still possible to write some data to USB, if there is system that controls outgoing mails, ...

Keywords:
information,leakage

Article Body:
Do you know all possible ways to take information out of company so that no one would know about this? I'm sure, even there are some certain security rules there are still some possible ways for information leakage. Let's think about how can we control this process.

First, it's necessary to understand that there no any absolute means about security. Even if USB port it blocked, it's still possible to write some data to USB, if there is system that controls outgoing mails, then it's still possible to use some trick that intruder might use to send out important data out of the company.

So how to manage information security policies to prevent possible data leakages? Let's list all possible ways to prevent leakage. There are two general categories - active and proactive security. These terms are sometime hard to understand in real word, so let's discuss another approach. There are means that will help to prevent the fact of information leakage, and there are means that will help to find out, if information was leaked. Both methods should be considered when building information security at your company.

How to prevent information leakage. First, it's necessary to apply a security policy which will guaranty the access to the certain data only for trusted persons, in this way you will always know who has access to the data, so it is easier to find possible intruder and to control your employees.

Second, consider all possible ways for information to be stolen, such as sent out by email, copies by some employee, stolen by some spyware software, copies to the external drive, etc. Think about all possible ways and think about risks applied. Try to minimize the risk for the most important data.

Let's list some possible security issues and the ways how we can get rid of them.

Keyloggers and other spyware software. Keylogger is a program that works in background, records all keystrokes and send out information to third-party. The good idea is to start with firewall, which will allow access to the internet only for a certain programs.

Intruder insider your company. Statistics shows that there are some in most companies. The bad news is that these people might produce more damage that all other attackers. Make sure you know about what employee do, what he or she keeps on his hard disk and all you do comply with privacy policy of your company.

Hardware that might be dangerous. There are software that allows to lock USB ports, there are software that allows to block access to any other writeable media, consider installing these tools on computers and user accounts which doesn't need to use this functions during their work.

Finally, the key principle about fighting information leakage is to be proactive. You don't need to wait until some information will be stolen, being a little paranoid will help to save your business. It's easy to install and integrate into the security policy some audit measures, that will regularly check your company for possible security holes, it's simple, but it's work.