5 tips to help protect data from being violated

Here are some steps you can take to prevent potential intrusion hazards.

TipsMake.com - **Data infringement cases continue to contribute to news sites. Whether it is a giant technology company or a large retail provider, they can still be attacked: Apple, Google, Sony, Epsilon, Michaels, etc.** This "attack" will probably continue. The increase is due to companies still having difficulty with operating security in a mobile world and the cloud is gradually dominating the market. An attack or leak of confidential data - such as a customer's bank account record or credit card information or a company's plan for a new generation product - can cause great damage to a business in terms of competition, loss of profit and trust.

With all the enterprise IT security applications and strategies in use today, hackers and data leaks are still watching and paying attention to their ability to protect important information. career. This danger continues to be expressed when legitimate users become bad guys or an employee (or partner) carelessly. And if there is an IP breach or leak, important information of a company or customer will always be in danger because files can be copied multiple times and stored anywhere on the Internet. Here are some steps you can take to prevent potential intrusion hazards.

1: Determine where important data is used and how to use it in the company

Implementing an information management strategy and making it a top priority is the first step in categorizing information with the greatest risk to businesses. Sony's incident in April recently gave us a lesson. The company

failed to use a firewall and neglected software updates could help it prevent losses. And even if Sony tried to "correct the formation" from the previous attack, there was a new attack.

2: Protect files in the system

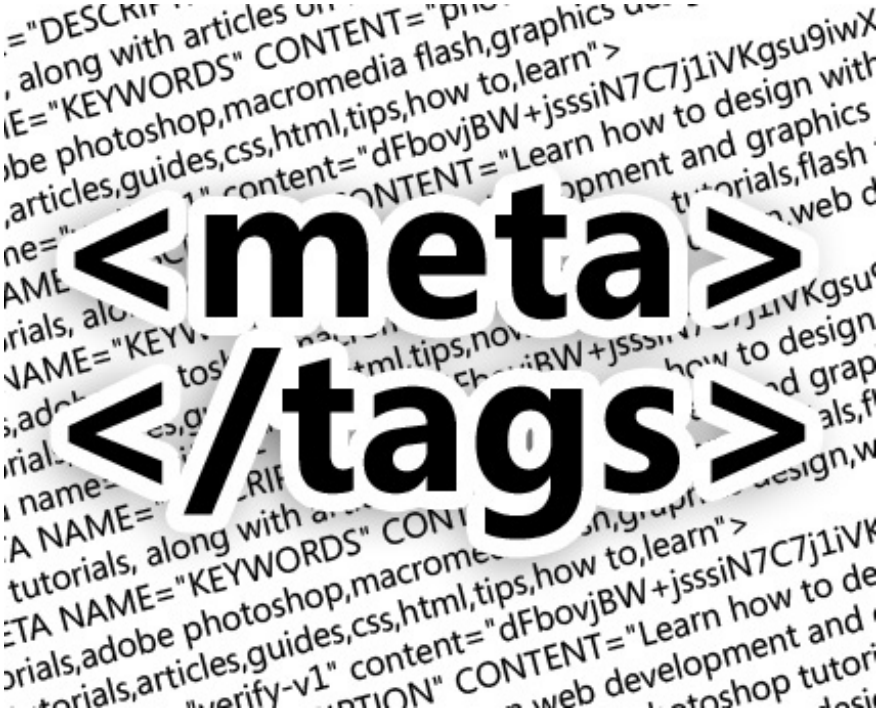
This protection can be done by attaching a security mechanism directly to the file itself without requiring software or changing the way users work. With today's mobile and cloud environments, this security / protection approach needs to be applied to the data or the file itself, as well as being able to remotely destroy the data file when needed.

With advanced file protection methods, organizations can automatically apply policies on the use and protection of important file groups, attach specific policies to determine important files (meet criteria) will be used to limit who can open and forward them.

For example, organizations focus primarily on preventing internal leaks, but they cannot 'mold' internal policies for customers and suppliers who have access to relevant information. important as part of a business relationship. Financial services are an industry that always has security. If bank investment research information is leaked on a trading floor, concerns about insider trading will increase and catch SEC's concern. On the other hand, if an investor does not have secure access to the authorized study, they will lose the information needed to 'turn on the light' for finance. It is possible to enforce mandatory policies that will help investors, analysts and others to share information securely and ensure that important data will not fall into the wrong hands.

3: Tag and monitor company files both active and passive

This includes digital fuzzy marks (displayed or hidden) that are attached to the file. (A hidden mark provides the copyright of the company's Copyright ID and special data identification markings that can be recorded and monitored as part of the testing process).



Tracking files will determine where a file is opened whenever it leaves the corporate network anywhere on the Internet. It must capture the detailed operation of a file in real time, allowing IT staff to know immediately when a file is opened, where the file is opened and whether it is sent or not.

Imagine that a company employee's laptop is the victim of a malware attack, and the employee stores a lot of spreadsheet data that contains important information about customers on the computer. there. If these spreadsheet files have been tagged, the IT department can track and know where they are being read and even 'remotely' them if needed.

4: Collect data about the current use of files

Understanding the current status using data will help set policies for discovery right at the time of application. If a business monitors where information will come when it leaves the corporate network, they will understand the habits and activities of the employees.

If a business collects real-time parameters about where a file is being used, when it is open and who may have opened it, you can expose unauthorized access immediately. For example, customers of companies you live in the US can get a purchase invoice on the company's home page. However, the company was later informed that the bill was also opened in China or Russia - a surprising action. Since then, the company can take the necessary action with this.

5: Continue to train employees and enforce mandatory policies

Companies should continue to follow good habits in implementing traditional 'deep defense' systems (VPNs, identity management, firewalls, device protection, preventing and detecting unauthorized intrusion , .). You should also follow the prepared security policies, stating how employees manage data, with essential consequences and plans to reduce risk.

File protection is the most important

Current security technologies have succeeded in limiting access to files and information important to legitimate users within the enterprise network. However, once the information leaves the corporate network, there is no way to monitor or monitor it, or if a legitimate user has shady actions and shares important data, surely you will be in trouble. Final words: The company's general security strategy now requires a file protection mechanism to emphasize this issue in information security.