5 things you can do to limit your exposure to insider threats

Tony Bradley

Jan 26, 2015 12:37 PM PT

Insight and analysis to help you understand emerging security concerns, and guidance to minimize risk exposure for your organization.

Target, Home Depot, Michael's, Dairy Queen, Sony…the list of major data breaches that have occurred over the last year or two is extensive. While most—if not all—of those attacks were a function of external hackers penetrating the network, authorized users inside the network still pose a more substantial threat.

The fact is that where the rubber meets the road so to speak, most attacks are "insider attacks". In many of the data breaches cited above, an external hacker was responsible but the attack succeeded because the hacker was able to obtain or compromise valid network credentials. In other words, from the perspective of the company or the network, they were essentially insider attacks.

CoSoSys, a provider of endpoint security solutions, recently surveyed its clients (all with an average of 500 computers) and found that 40 percent of potential customers would not do business with a company that suffered a recent data breach.

A data breach has serious consequences both directly and indirectly. Lost revenue, and a tarnished brand reputation both inflict harm long after the actual incident is resolved and the breach has been cleaned up. Still, many organizations don't take necessary steps to protect themselves from a potentially detrimental breach.

CoSoSys compiled a list of five things companies should do to minimize the risk from insider threats—or external hackers who successfully infiltrate the network by impersonating an authorized insider:

1. Check what documents employees have access to: Six out of 10 employees are not aware which files are confidential and which are not. It's important to limit permissions so employees only have access to the data necessary to get their jobs done. You should also take steps to ensure users with access to sensitive or confidential data are trained to recognize which files require stricter protection.

2. See what tools employees are using to share files: 45 percent of insiders admit copying work files to personal computers or remotely connecting to the company network from home to continue working. It's important for you to know where company data is being stored, and to ensure that the tools and services employees use to access data and network resources are secure.

3. Create a short quiz to find out employee's knowledge regarding data security : 35 percent of employees believe it's not their responsibility to protect data. While the burden ultimately falls on IT management, it's up to every individual to be aware of security risks and do his or her part to protect data from leaks or compromise.

4. Determine if your current security tools can detect a breach caused by insiders in case it happens: Whether it's intentional or inadvertent, would you even know if someone inside your network compromised or leaked sensitive data? Over half of employees indicate they've accidentally sent emails to the wrong person.

5. Do your research to understand the potential impact of data breaches: The average cost of a data breach is $3.5 million.

Does your company have a spare $3.5 million lying around that it wouldn't mind parting with? If so, you might consider spending a small fraction of that to guard against insider threats and prevent data breaches rather than suffering the consequences of failing to do so. If not, you definitely need to invest in appropriate security

measures to make sure your company doesn’t become the next data breach headline.