Lack of Employee Education Means Insider Threats Won’t Stop in 2016

By Guest
Contributor

As we move towards Data Protection Day this week and continue to navigate the constantly evolving security landscape where new malicious hacks are made each day, we often overlook the ones closest to home: insider threats.

In the last several years, some of the most notable security breaches were caused or believed to have been caused by insiders, including those affecting Target, the NSA, and Sony.

An *insider threat* is an employee action that unintentionally exposes their organization to security risk. This can be something as simple as using a cloud application not approved by IT, or unknowingly sharing proprietary data with an outside source.

Because the workers inside an organization are often seen as a less serious threat – *or not a threat at all* – employees often don’t even think that the cloud service or app they downloaded isn’t approved by IT, or that the Excel grid they shared is unauthorized.

Guest article by Roman Foeckl, CEO & Founder, CoSoSys

According to research conducted by Crowd Research Partners though, 62 percent of security professionals say insider threats have become more frequent in the past year, while only 34 percent expect additional budget to address the problem.

While there has been significant focus on enterprise adoption of security software, enabling companies to more successfully secure and track sensitive data, there is a big missing link to tie these efforts together: *employee education*.

A recent survey by CoSoSys found that 35 percent of enterprise employees believe that data security is *not* their responsibility. Considering that 70 percent of these employees have access to and use confidential company files, most companies find themselves with a serious problem.

Additionally, 60 percent of employees admitted that they don’t even know which files are confidential. Throw in unhappy or recently fired employees whose system access had not yet been removed, and companies are opening themselves up to potentially disastrous — and expensive — data leaks.

There are a number of actions organizations can take to help employees understand the importance of working responsibly, while also taking precautions that mitigate risk of an insider data breach.

Training, Training, Training: Tailor it

Companies have to reevaluate how they convey security regulations internally. Too often, employee education on data security is a one-size-fits-all program that provides little compelling or applicable insights.

Organizations must be sure that their security education program is effective, by simplifying and tailoring it to each employee or business unit, ensuring that they clearly understand what is at stake, and feel confident in their ability to protect themselves and their company. Especially when deploying security software, IT departments need to be sure that workers are properly trained on how to use and understand the technology – otherwise, the investment is worthless.

It is also a good idea to develop ongoing check-ins to ensure that over time, employees still remember security policies and protocols, and make sure that any new technologies implemented are clearly outlined.

Access Divided

Dividing access between groups of employees is a helpful way to mitigate insider threats. By doing this, organizations can more easily control data movement and pinpoint weaknesses in security. By restricting access to confidential files to only those who need it, organizations can dramatically decrease the chances of a non-malicious insider inadvertently exposing sensitive information.

Employee Tools: Monitor and Limit

With the number of devices and applications available, it is necessary to proactively deploy technology like mobile management tools in the workplace, so that organizations can prevent users from taking confidential data outside the company or bringing potentially harmful files into the company.

As the line continues to blur between work and leisure, companies need to be aware of the technology available tc them to protect and manage sensitive information stored on personal devices used in corporate environments, while still allowing a clear delineation between business and private employee data.

Can You Detect a Breach Caused by Insiders?

In this day and age, your company is only as good as the technology that alerts you of security breaches. In addition to accidental insider data breaches, companies should be aware that they can also be victims of malicious insider hacks – whether from a disgruntled current employee or a recently let go employee who still has server access. As a result, organizations must be doubly cautious in handling potential security threats.

There are a number of technologies on the market that check employee activities and monitor confidential data, capable of alerting IT of a breach. Potential revenue lost from a data breach only increases as time goes by, and adds to what it costs a company to clean up after a breach, including fines, and notifying employees, vendors, anc customers of the compromised data.

In any organization's security strategy, *employees* can be the weak point. But with the right education, security technology, and practices in place, the potential risk of insider threats can be greatly mitigated.

For related information on this topic, check out Aberdeen Group's free research report, The Last Mile in IT Security: Changing User Behaviors.

Roman Foeckl is the Founder and CEO of CoSoSys. Roman's vision is to offer an easy-to-use and implement Data Loss Prevention Solution that covers all popular platforms, from Mac OS to Windows and Linux, so large and small businesses can protect their data against accidental loss or intentional data theft.