itproportal.com
http://www.itproportal.com/2016/01/11/employee-education-why-the-non-malicious-insider-is-quickly-becoming-a-huge-threat/#ixzz3wxZeHEjb

Employee education: Why the non-malicious insider is quickly becoming a huge threat

11/01/2016

In the face of a turbulent security landscape where malicious hackers are waging a cyber war against companies of all sizes, the non-malicious insider has quickly become one of the largest undetected threats to enterprise data security. To define an insider threat, we look at employee actions that unintentionally expose their organisation to security risk – this can include things as simple as using a cloud application not approved by IT or unknowingly sharing proprietary data with an outside source.

Despite the steadily increasing number of enterprises adopting security software, which has proved important in enabling companies to more successfully secure and track sensitive data, there is a big missing link to tie all of these efforts together: employee education.

According to a recent survey we conducted with CoSoSys customers, 35 per cent of enterprise employees think that data security is not their responsibility. This is a serious issue when you consider that 70 per cent of these employees have access to and use confidential company files. Additionally, 60 per cent don't even know which files are confidential or not. When you add disgruntled or recently fired employees whose system access had not yet been revoked to the mix, companies are leaving themselves open to a potentially devastating breach.

Employee education around data security is lagging behind the times and is often overlooked entirely. Of some of the most notable breaches in the last several years, many were caused or believed to have been caused by insiders including Target, the NSA, and Sony. Because insiders are often seen as a less serious threat – or not a threat at all – employees often don't even consider that the cloud service or app they downloaded on their device isn't approved by IT admins, or that they are sharing an unauthorised excel grid with an outsider.

Verizon recently released a data breach study that reported that human error was at fault in 66 per cent of all breaches. This makes a lot of sense when you look at Skyhigh Networks' recent report that found that 89.6 per cent of organisations experience at least one insider threat each month.

There are a number of ways companies can help employees to understand the importance of working responsibly while mitigating risk of an insider data breach:

Develop tailored data security training for employees

Often, employee education on data security is long, boring and of a one-size-fits-all variety. It is imperative that companies re-evaluate how they convey security regulations internally. The content must be rendered effective by simplifying and tailoring it to the employee being taught so that they understand clearly what is at stake, and feel confident they understand what needs to be done to protect themselves and their company. Especially when implementing security software, IT departments need to make sure they are properly training employees on how to use and understand the technology.

Companies can also develop ongoing check-ins to ensure that over time, employees still remember security policies and protocols.

Limit and monitor the tools employees can download

By proactively deploying mobile management tools in the workplace, companies can prevent users from taking confidential data outside the company or bringing potentially harmful files into the company. As the line between work and one's personal life blurs with the increasing number of connected devices in the workplace, technology is available to protect and manage sensitive company information stored on personal devices used in corporate environments, while still allowing a clear delineation between business and private employee data.

Divide data access amongst employees

By creating a clear line between data ownership within a company, organisations can more easily control the flow of data and pinpoint weaknesses in security. Additionally, by restricting access to confidential files to only those who need it, organisations dramatically decrease the chances of a non-malicious insider from accidentally exposing this information.

Determine if your current security tools can detect a breach caused by insiders

You really are only as good as the technology that alerts you to data breaches. In addition to accidental security breaches by insiders, companies can also be victims of malicious insider hacks – whether it be from a disgruntled current employee or a recently fired employee who still has server access. This is why it is doubly imperative that companies be proactive in their approach to handling potential security threats. There are a number of technologies that can monitor employee activities and confidential information and alert the IT department of a breach. Lost potential revenue stemming 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 and customers of the compromised data.

Employees can be the weak point in any company's security strategy, but with the right education, technology and practices in place, this risk can be greatly mitigated.

Roman Foeckl is the Founder and CEO of CoSoSys