Data Data Everywhere: Are You the Biggest Security Risk of All?

Posted by Roman Foeckl on May 1, 2014 at 10:19am View Blog

Confidential data -- both personal and that of your employer -- is everywhere, and always within reach. It's on your smartphone and laptop, and on the workstation at your job. It's on your company's network, on USB drives, in email, and going back and forth from the cloud. The fact that company data is stored or accessed by you -- on both your work and personal devices -- blurs the lines for where, when and how you and your employer should enforce and extend security, and your own role in protecting data.

How you access and store data comes with risk, of course. Human error plays a big role in creating security vulnerabilities. Let's review some common ways people expose data to risks, and then look at future innovations in security technologies that will better protect you and your data.

Data Dangers

Every day, people use cloud-based solutions and other applications to store, send or access data. Popular programs like Dropbox, Google Drive and Gmail allow anyone to work from anywhere, access and share files, and be more productive -- but they also invite risks.

One of the biggest threats to all file sharing applications is the same -- you. It doesn't matter if you use Dropbox, Google Drive, SkyDrive, etc.; the common threat is the user. Sure, Dropbox may have enforced two-factor authentication. And, you can use a third-party encryption tool when uploading files on Google Drive, but there will always be people using the same password on multiple accounts, which makes using file sharing applications intrinsically vulnerable.

Information can be accessed by or stored on a variety of devices like smartphones, tablets, computers and jump drives, but they aren't always properly secured. For example, smartphones that aren't password-protected, or that are lost and can easily be hacked into. People also put sensitive work and personal data on devices -- like USB flash drives and other portable storage media -- that do not employ encryption technologies, which can also get lost or stolen. If these devices aren't secure, then the information they contain is also unsecure.

Don't forget the name Bradley Manning. He's responsible for one of the largest leaks of restricted documents ever. He easily copied more than 900,000 highly sensitive U.S. intelligence documents onto CDs labeled "Lady Gaga," and sent them to WikiLeaks, which published them. You should be paranoid about safely controlling the personal and work-related data that you or your employees carry around, upload and/or share.

Having said this, the risks of storing and sharing data do not outweigh the advantages of using file sharing services. Continue to use wonderful services like Dropbox, Google Drive and others, but better protect and safely control what you share, and better equip employees to protect your data. IT admins and others involved in security should create clear security and data-sharing policies for users, and implement the right tools to filter out and control confidential information from being shared on the cloud.

One tool you might consider using is Content-Aware DLP solutions. They provide features like allowing the setup of filers based on file type/extension, specific keyword content or regular expressions. This enables documents to be shared on various storage media and web applications, while blocking these same actions on others. For audit purposes, log events are created for each attempted action, and, if needed, a 'file shadow' or copy of the document in question is available.

Can We Kill the Humans ... Please?

Many enterprises and organizations are developing and enforcing such policies, and implementing technologies to protect users and networks. Myriad technologies are on the market -- and more being developed -- to protect data from insecure behavior, criminals, BYOD, BYOC, human error and other risks. Unfortunately, none of them can eliminate -- the human - who can undermine their effectiveness.

Is the Future More Secure?

Don't despair. Education combined with future and evolving innovations in security technologies will make data more secure. Big Data analytics software can identify patterns of policy violations or improper handling of data by individuals, providing a good foundation for intelligent, proactive action and strategies to protect data.

Gamification is another tool security professionals and vendors will continue to develop to use to both educate and protect users and data. Gamification represents a creative and entertaining way to get employees involved in the process of protecting data. It has the ability to educate people to tailor their behavior and handling of data to reduce risks.

Data Classification is another burgeoning area that will improve data loss prevention and help decrease human error. Data needs to be categorized according to its sensitivity, and employees must be better informed about the level of importance of the data they work with and how it must be handled. By doing so, companies will increase the potential for keeping their key data out of places it does not belong or that invites risk.

As data becomes even more available and accessible, and risks grow commensurately, ask yourself, "how can my data be more secure?" It's unlikely you'll be able to completely eliminate all of the risky behaviors in which you engage, or to stop using helpful file sharing programs and apps just because they come with risk, but better awareness, education and emerging security technologies will make you -- and the data you store, share and touch -- safer.

Roman Foeckl is founder and CEO of CoSoSys.