When Employee Data is Hidden in Cloud Applications

Authors: Chelsea Caldwell Karen Rose Brian Rowland Allison Harris Tammy Adkins

Published Date: 08-03-2014

University of Central Arkansas

School of Exercise and Sport Science

Many organizations are not following security best practices when using file sharing applications. This includes using approved programs and Secure Browsing, SFTP, SSE, VPS, SDK, working with Bluetooth, and owning mobile IP addresses.

Most people think Dropbox, Google Docs, and other cloud based services are secure. Often times, an organization allows employees to access data using external apps, which also becomes an increased concern. When employees are sharing data from internal websites or the organizationâ€™s servers or networks, an organization also needs to protect the data by using plain vanilla public networks.

A few years ago, some companies were using a software called Text Mining that allows the data to be retrieved with a simple Google search. In this case, all the information was generated on the systems or files and was stored centrally. There was no immediate need to access the data, but anyone with a basic computer could readily copy the data by clicking a link. Another example is taking photos that are automatically taken and stored on a file sharing service. There was no user action to make these copies of the photos.

Many times, your entire company may have accessed confidential data through the Google Docs or Dropbox app that is being used. In some cases, these applications may not be adequately protected. An organization may give its employees a free ride to access confidential data in the cloud, as long as they log out. Also, you can take advantage of the current wave of applications such as the â€œSharefileâ€ apps that make it possible to access any file directly from any Windows PC or OS. It is also easy to add printers to a sharefile account, which makes it possible to access the document from different devices. The problem is that these apps do not seem to adhere to security best practices that most organizations use. Just downloading the file and connecting to it without the user action to create a specific folder or file means access is provided.

There are also some cases where employees may be using Dropbox to â€œimportâ€ a document from a remote source into the Dropbox environment. This is much like office workers using Windows explorer from a remote location and accessing the document at any time. This is viewed as an unnecessary risk of office staff from somewhere far away having access to proprietary information from inside the office. Users can have cached versions of all the documents in the Dropbox account in the Dropbox folder, accessible from different devices.

Itâ€™s a good idea to make sure that you are using the appropriate security software to protect your information on email and on cloud based services. Here are some tips that could help you in managing access to your sensitive data:

Â· Make sure that the IP address of the shared computer is used for accessing the information.

Â· Use a firewall so that unauthorized access to the contents of the drive is blocked.

Â· Use a cryptography program to encrypt data.

Â· Enable Secure Downloading to shut off your employeesâ€™ ability to download data.

Â· Donâ€™t allow your employees to have simple email addresses or even smartphones that are easy to find.

This isnâ€™t a magic bullet to defeat the spyware or hackers, but it can help you protect your data.

Dr. Gayathri Chadalapaka, a Past President of Cyber Law Council, is a litigation consultant, a â€œvirtualâ€ courtroom judge, and has been involved in litigation work in Sri Lanka, USA, UK, India, Australia, Russia, China, Saudi Arabia, Australia, Norway, Germany, Australia, and Asia. She was former Legal Director of the online furniture retailer Stop Shop and Warehouse Limited, (StopShop.com)

From Dr. Gayathri:

A Black And White Photo Of A Fire Hydrant