OUCH! | November 2016

The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

Using The Cloud Securely

Overview

"The Cloud" can mean different things to different people, but usually means using a service provider on the Internet to store and manage your computing systems and/or data for you. An advantage of the Cloud is that you can easily access and synchronize your data from multiple devices anywhere in the world, and you can also share your information with anyone you want. We call these services "The Cloud" because you often do not know where your data is physically stored. Examples of Cloud computing include creating documents on Google Docs, sharing files via Dropbox, setting up your own server on Amazon Cloud, storing customer data in Salesforce, or archiving your music or pictures on Apple's iCloud. These online services can make you far more productive, but they also come with unique risks. In this newsletter, we cover how you can securely make the most of the Cloud.

Guest Editor

Dave Shackleford (**@daveshackleford**) is a professional consultant who owns Voodoo Security and is the author of numerous SANS training courses, including Security 579: Virtualization and Private Cloud Security and Security 524: Cloud Security Fundamentals.

Selecting a Cloud Provider

The Cloud is neither good nor evil; it is a tool for getting things done, both at work and at home. However, when you use these services you are handing over your private data to others, and you expect them to keep it both secure and available. As such, you want to be sure you are choosing your Cloud provider wisely. For your work computers or work-related information, check with your supervisor to see if your company allows you to use Cloud services. If you are allowed to use the Cloud, confirm which Cloud services you can use and what the policies are on how to use them. If you are considering a Cloud service for your personal use, consider the following.

1. Support: How easy is it to get help or have a question answered? Is there an email address you can contact, public forums you can post questions to, or Frequently Asked Questions on their website?

Using The Cloud Securely

2. Simplicity: How easy is it to use the service? The more complex the service is, the more likely you will make mistakes and accidentally expose or lose your information. Select a Cloud provider you find easy to understand, configure, and use.
3. Security: What data is collected about you, if any? How will your data get from your computer to the Cloud, and how is it stored in the Cloud? Is it encrypted, and if so, who can decrypt your data?
4. Terms of Service: Take a moment to review the Terms of Service. (They are often surprisingly easy to read.) Confirm who can access your data and what your legal rights are, as well as any security responsibilities assumed by the provider or required by you.

The Cloud can make your information more accessible and make you more productive, but be careful how you access and share your information.

Securing Your Data

Once you have selected a Cloud provider, the next step is to make sure you use your Cloud services properly. How you access and share your data can often have a far greater impact on the security of your files than anything else. Some key steps you can take include:

1. Authentication: Use a strong, unique passphrase to authenticate to your Cloud account. If your Cloud provider offers two-step verification, we highly recommend that you enable it. This is one of the most important steps you can take to protect your account.
2. Sharing Files/Folders: The Cloud makes it very simple to share, sometimes too simple. In a worst-case scenario, you may think you are sharing your files with just a specific individual, but you may accidently make your files or even entire folders publicly available to the entire Internet. The best way to protect yourself is to not share any of your files with anyone by default. Then only allow specific people (or groups of people) access to specific files or folders on a need-to-know basis. When someone no longer needs access to your files, remove them. Your Cloud provider should provide an easy way to track who has access to your files and folders.
3. Sharing Files/Folders Using Links: One common feature of some Cloud services is the ability to create a web link that points to your files or folders. This feature allows you to share these files with anyone you want by simply providing

Using The Cloud Securely

a web link. However, this approach has very little security. Anyone that knows this link may have access to your personal files or folders. If you send the link to just one person, that person could share that link with others, or it could show up on search engines. If you share data by using a link, be sure you disable the link once it is no longer needed by setting an expiration date or, if possible, protect the link with a password.

4. Settings: Understand the security settings offered by your Cloud provider. For example, if you share a folder with someone else, can they in turn share your data with others without your knowledge? Also, see if there are ways to see who has viewed your shared content and when they viewed it. Can you restrict sharing to "read only" versus giving read+write, which means people can also modify the files?
5. Antivirus: Make sure the latest version of antivirus software is installed on your computer and on any other computer used to share your data. If a file you are sharing gets infected, other computers accessing that same file could also get infected.

Meet All Your NERC CIP Training Needs

NERC CIP is hard, so the SANS Institute developed a variety of training offerings to make it easier. Whether your goal is to meet CIP-004-6 training requirements or to implement a NERC CIP compliance program, we have the training you need. https://securingthehuman.sans.org/u/mGk

Resources

Two-Step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
What is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524: Cloud Security Fundamentals:	https://sans.org/sec524

License