The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

Using The Cloud Safely

GUEST EDITOR

James Tarala is the guest editor for this issue. He is a senior instructor with the SANS Institute and a principal consultant with Enclave Security. He is also the author of numerous SANS training courses, including SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls and SANS Audit 407: Foundations of Auditing Information Systems as well as others.

OVERVIEW

Cloud services are a powerful technology that many individuals and organizations are adopting. Cloud computing is really nothing more than using a service provider to store and manage your data for you. The reason we call this service *the cloud* is that you never know precisely where your data is physically stored; it is being served by the cloud. Examples of cloud computing include creating documents on Google Docs, sharing files via Dropbox, setting up your own server on Amazon Elastic Compute Cloud, or storing your music or pictures on Apple's iCloud. These online services have the potential to make you far more productive. However, with these capabilities come risks. In this newsletter we examine these issues and how you can protect your information.

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, you are handing over the availability and security of your private data to strangers. As such, you must ensure they meet your requirements. Consider the following questions when researching cloud providers.

1. **Support**. If you have a problem, how responsive is the company in providing support? If your data is critical, you may require phone or e-mail support. If the company does not provide such support, does their website have public forums or an FAQ (Frequently Asked Questions) section?
2. **Backups**. Does the company back up your data? If so, exactly what gets backed up, how frequently, and for how long are the backups maintained? If you unintentionally delete files, can you recover them, and if so, how?
3. **Privacy**. Who does your cloud provider allow to access your data? Do only you have access, or do the provider's employees or third-party partners have access?

Using The Cloud Safely

4. **Security**. How will your data get from your computer or device to the cloud? Is the connection secured by encryption? How is your data stored in the cloud, and once again, is it encrypted? Who can decrypt your data?

SECURE ACCESS

Once you have selected a company (or companies) to store your data in the cloud, the next step is to make sure you use their services properly. How you access and share your data can often have a far greater impact its security than anything else. Some key steps you can take to protect your information include:

1. **Authentication**: Use strong, long passphrases to authenticate to your cloud provider. This protects against cyber attackers simply guessing your password. If your provider offers two-factor authentication (sometimes called two-step verification), we recommend that you use it.
2. **Sharing**: The cloud makes it very simple to share data, so take care that you do not accidentally share too much data with others. In a worst case scenario you may unintentionally make your data available to the public. The best way to protect yourself is by default not to share any of your data with anyone. Then only allow specific people (or groups of people) access to specific files or folders on a need-to-know basis.
3. **Settings**: Understand the security settings offered by your cloud provider. If you grant full control to someone else, can they in turn share your data with third parties without your knowledge and consent? Can you purge your data from the cloud provider's systems once you no longer need the service?
4. **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.

Cloud computing has the potential to save you money and make you more productive, but be careful how you store and share your information.

Using The Cloud Safely

5. **Encryption**: How does your provider encrypt your data? Do they control the keys or do you? A more robust security option is to encrypt your private data locally before storing it in the cloud. This extra step protects your data even if your cloud provider is compromised.
6. **Backup**: Even if your cloud provider is backing up your data, consider making regularly scheduled local backups of your own. Not only does this protect your data should your cloud provider go out of business or be shutdown, but it may also be easier to recover large amounts of data from your local backup rather pulling it down from the cloud.
7. **Terms of Service**: Read the Service Level Agreement (SLA) or End User License Agreement (EULA) before you sign up for a service. Consider other providers if there are terms in the contract that you don't understand or that concern you.
8. **Organization Data:** Do not store your organization's data in the cloud without prior permission from a supervisor. Storing your organization's data in the cloud may not only violate your organization policies, but could violate state and federals laws, exposing you and your organization to legal repercussions.

SUMMARY

The cloud is neither good nor evil; it is simply a tool that you can use. The key steps to protecting yourself are choosing a cloud provider that meets your requirements and accessing and sharing your data in a secure manner.

RESOURCES

Some of the links shown below have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

The Cloud Security Alliance (CSA):
https://cloudsecurityalliance.org

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org

SPECIAL PROMOTION

Does your Small or Medium organization need help with securing the most vulnerable part of your organization? Check out a great program to train up to 750 Users for just $3,000. Program runs only from June 01 to July 31, 2012. Learn more at:
www.securingthehuman.org/programs/sme