The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- What To Back Up and When
- How To Perform a Backup
- Recovery
- Key Points

Backup and Recovery

GUEST EDITOR

Dr. Eric Cole is the guest editor for this issue of OUCH! Eric focuses on consulting services that help organizations deploy solutions that protect themselves. He also is an author and teacher for the SANS Institute.

OVERVIEW

Backups are one of the most important steps you can take to protect your information. They are your last line of defense when something goes wrong, such as hard drive failures, accidental file deletions, or malware infections. In this issue, we focus on ways that you can back up your data and develop a strategy that's right for you.

WHAT TO BACK UP AND WHEN

There are two basic approaches when deciding what to back up: (1) any data that you have created or that is important to you, such as documents, pictures, or videos or (2) everything, including your operating system and any programs you have installed in addition to your unique data. The first approach streamlines your backup process; however, the second approach makes it easier to recover in the event of a complete system failure. If you are not sure what to back up, then back up everything.

Your next decision will be deciding how often to back up your data. Common options include hourly, daily, weekly, etc. For home users, personal backup programs, such as Apple's Time Machine or Microsoft's Windows Backup and Restore, will allow you to create an automatic "set it and forget it" backup schedule. Other solutions offer continuous protection, in which new or altered files are immediately backed up as soon as they're closed. If you're part of an organization with multiple computers, you may wish to define your own schedule. A good approach is to consider how much information you can afford to lose in a worst-case scenario. For example, by backing up daily, you might lose one day's work if your computer crashes late in the day. Many organizations schedule daily backups during off-peak hours to minimize the impact on normal operations.

Backup and Recovery

HOW TO PERFORM A BACKUP

In general there are two destinations to which you can back up your information: physical media or cloud-based storage. Examples of physical media include DVDs, USB drives, magnetic tape, or additional hard drives. Avoid backing up to the same device that holds the original files. When using physical media, be sure to label it both internally (in the file name) and externally (on the medium) so that you can easily identify a backup from a particular date and time. You can store a local backup copy in a lockable, fireproof and waterproof container designed for your chosen media. A more robust option is to store copies of your backups off site. For personal backups this can be as simple as storing them at a family member's house or in a safe deposit box. Organizations may want to hire a professional service to securely transport and store backups. Depending on the sensitive nature of your backups and where they are being stored, you may also want to encrypt them.

Many of these issues are addressed for you with cloud backups. Performing cloud backups is often as simple as installing and configuring an application on your computer. After you configure your backup options, new and altered files are backed up automatically over the Internet to servers in the provider's data center.

Reliable backups are your last line of defense in protecting your data.

Finally, you need to decide how far back in time your backups need to go. Home users most likely do not need to go back more than thirty days. Some organizations may have policy or legal requirements for longer retention periods and may also mandate the destruction of old backups. If you are backing up organizational data, check with your information technology, legal, or records management group to be sure. Cloud backup services may charge based on the amount of data that is backed up, so take care not to run up a big bill.

Backup and Recovery

RECOVERY

Backing up your data is only half the battle; you have to be certain that you can easily recover it. Practice your recovery process regularly, just as you would a fire drill, to help ensure that everything will work properly should you need to use it. Check at least once a month that your backup program is working. If nothing else, try recovering a file. For more robust testing, especially in organizations, consider making a full system recovery, and verify that it is restorable. If you don't have spare hardware to use for testing a full system recovery, restore key files and folders to a different location and then verify that you have and can open everything.

KEY POINTS

- Automate your backup process as much as possible, but verify that it runs correctly.

- When rebuilding an entire system or recovering key operating system files, be sure you reapply security patches and updates before putting it back into service.

- Outdated or obsolete backups may become a liability and should be destroyed in order to prevent them from being accessed by unauthorized users.

- If you are using a cloud solution, research the policies and reputation of the organization. For example, do they encrypt your data when it is stored? Who has access to your backups? Do they support strong authentication?

- For robust backup practices, consider the 3-2-1 rule:

    - Three: If something is worth keeping, keep the original plus two backup copies.

    - Two: Use different types of media for your two backup copies. If you must use the same medium for both, use different vendors to mitigate manufacturing defects.

    - One: Store one copy off-site, away from the original and the second copy.

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.

Apple Time Machine:
http://preview.tinyurl.com/3wkytqs

Windows 7 Backup and Restore:
http://preview.tinyurl.com/ylghqgp

Cloud Backup:
http://preview.tinyurl.com/3reftgv

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