When a Backup Is Not a Backup

RON LaPEDIS, SunGard Availability Services

By RON LaPEDIS, SunGard Availability Services

Unless I quote someone else, these are my opinions and I am not speaking for any organization, including those that I am employed by or a member of.

For Matt Honan [1], his data was not only in the cloud, but also on multiple systems: a MacBook, an iPad, and an iPhone. And he still lost a year's worth of photos, emails, documents, and who knows what else? Here is Matt's story.

A high-tech reporter, Honan had his Apple iCloud account hacked by someone who somehow learned his seven-character alphanumeric password. While Honan didn't use this password anywhere else, he hadn't changed it for a very long time — years in fact. Which of course is a security no-no itself.

After logging in to his iCloud account, the hacker reset Honan's password and tossed the confirmation message into the trash so that he wouldn't see it. Since his backup GMail account was his hacked iCloud account, the hacker requested a GMail password reset, took over that account as well and deleted it. The next target was Honan's Twitter account, followed by Gizmodo's Twitter account [2], which was linked to Matt's account. You can imagine the #@&$ the hacker posted on both accounts.

The hacker then proceeded to remotely wipe Honan's iPhone, iPad and MacBook. Even though he saw it happening, there was nothing Honan could do to stop the process. And since he didn't have any offline backups, his data is gone forever.

Gizmodo [3] has some recommendations, including:

1. Use complex passwords, don't use the same password more than once and change your passwords periodically.
2. Use a password manager if you need to and choose an insanely complex password for it. Personally, I like the cross-platform SplashID [4] with a line

from a poem or song as the password.
3. If it’s available, use two-factor or two-step [5] authentication on websites, especially for password recovery.
4. If you have linked multiple accounts, unlink them unless there is a very good reason for the linkage.
5. If you have accounts that you no longer use (anyone with a MySpace account, raise your hand), try to delete them. If you cannot delete the account, then remove all possible information and lock down the account as tightly as you can.
6. Once again — backup your data offline. A hard drive that you can stuff in a safe, in a closet or under your bed is more secure than anything in the cloud.

While I cover personal security above, the same information also applies to organizations — except that you’re probably going to use tape, virtual tape, or disk-to-disk archives for offline storage rather than cloning hard drives and putting them under your bed. If you have a web presence, blog or use social media, go change your passwords now, and evaluate how those accounts can be locked down before your reputation is tarnished by getting hacked.

What’s your take? Please feel free to comment below! This post was taken, with permission, from LaPedis's blog, http://seacliffpartners.com/wordpress/ [6].

Source URL (retrieved on *04/25/2015 - 4:06pm*):
http://www.chem.info/blogs/2012/09/when-backup-not-backup

Links:
[1] http://www.emptyage.com/post/28679875595/yes-i-was-hacked-hard
[2] http://twitter.com/gizmodo
[3] http://gizmodo.com/5931828/how-gizmodo-got-hacked-and-how-you-should-defend-yourself
[4] http://www.splashdata.com/splashid/
[5] http://support.google.com/accounts/bin/answer.py?hl=en&answer=180744
[6] http://seacliffpartners.com/wordpress/