Securing Shared Cloud-Based File Repositories

M. E. Kabay, PhD, CISSP-ISSMP

Here's another block of material I added to a chapter as I'm editing a security textbook.

File-sharing services such as Dropbox and Google Drive have put effort into securing the data stored and shared by individuals and groups. For example, Dropbox answers the question "How secure is Dropbox?" as follows:

> We have a dedicated security team using the best tools and engineering practices available to build and maintain Dropbox, and you can rest assured that we've implemented multiple levels of security to protect and back up your files. You can also take advantage of two-step verification, a login authentication feature which you can enable to add another layer of security to your account.
>
> Other Dropbox users can't see your files in Dropbox unless you deliberately share links to files or share folders. Dropbox employees are prohibited from viewing the content of files you store in your account. Employees may access file metadata (e.g., file names and locations) when they have a legitimate reason, like providing technical support. Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so). But that's the rare exception, not the rule. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances. In addition, we employ a number of physical, technical, and heuristic security measures to protect user information from unauthorized access.[1]

Nonetheless, there are serious security concerns about cloud-based file-sharing tools and Dropbox in particular. At a Black Hat EU conference in 2013, the paper "DropSmack: How cloud synchronization services render your corporate firewall worthless" caught the eye of writer Michael Kassner. The paper summary included the following points:

- ….[C]loud-based synchronization solutions in general, and Dropbox in particular, can be used as a vector for delivering malware to an internal network."
- …Dropbox synchronization service can be used as a Command and Control (C2) channel.
- …[F]unctioning malware is able to use Dropbox to smuggle out data from exploited remote computers.

The paper's author, experienced penetration-tester Jacob Williams, warned that if a bad actor has any access to a secured Dropbox folder, it is possible to synchronize a remote-access Trojan he wrote called DropSmack with all the shared Dropbox folders. The tool would allow the infiltration of the entire corporate network. Williams also warned that access to a Dropbox folder by employees using their personal computers raises legal issues:

> "Many general counsels are more than a little worried about the appearance of authorizing us to pen test what could end up being be home machines. That's becoming a sticky issue with pen-testers these days as people open spear phishing emails delivered to the corporate email addresses on machines that may be privately owned. "Many general counsels are more than a little worried about the appearance of authorizing us to pen test what could end up being be home machines. That's becoming a sticky issue with pen-testers these days as people open spear phishing emails delivered to the corporate email addresses on machines that may be privately owned."[2]

Integrated collaboration tools have another danger, especially for inexperienced users who don't take daily backups: deleting one or more files (or all of them) in a shared Dropbox folder will propagate the deletion to all users of the shared folder. If any one of the users keeps a daily backup, the entire group of users can be protected against disaster; if none of them do, they may be in serious difficulty. In a related issue, any user who moves the files out of the Dropbox folder into a local folder will wipe the data from all the other users' Dropbox folders too.[3]

In a 2012 article, Matthew J. Schwartz urged corporate uses to pay attention to Dropbox use among their employees. His five recommendations (with more details in the original article) are

- Monitor Dropbox use
- Compare cloud service security
- Beware lackluster security cloud practices
- Treat Dropbox as a public repository
- Beware insider data exfiltration.[4]

A free tool, Cloudfogger, automatically encrypts data on the client side when it is uploaded to any external collaboration tool using 256 bit AES encryption. The tool then automatically decrypts the data when it is downloaded by an authorized user.[5]

NOTES

[1] (Dropbox 2013)
[2] (Kassner 2013)
[3] (Kabay 2013)
[4] (Schwartz 2012)
[5] (Cloudfogger 2012)

WORKS CITED

Cloudfogger. "Protect Your Privacy on SkyDrive, Dropbox, Google Drive in the Cloud." cloudfogger. 2012. http://www.cloudfogger.com/en/ (accessed 05 25, 2013).

Dropbox. "How secure is Dropbox?" Dropbox. 2013. https://www.dropbox.com/help/27/en (accessed 05 25, 2013).

Kabay, M. E. "Dropping the Ball on Dropbox." InfoSec Perception. 04 19, 2013. http://resources.infosecskills.com/perception/dropping-the-ball-on-dropbox/ (accessed 05 25, 2013).

Kassner, Michael. "DropSmack: Using Dropbox to steal files and deliver malware." TechRepublic | Security. 04 15, 2013. http://www.techrepublic.com/blog/security/dropsmack-using-dropbox-to-steal-files-and-deliver-malware/9332 (accessed 05 25, 2013).

Schwartz, Matthew J. "5 Dropbox Security Warnings For Businesses." InformationWeek | Security. 08 14, 2012. http://www.informationweek.com/security/management/5-dropbox-security-warnings-for-business/240005413?pgno=1 (accessed 05 25, 2013).

*** * ***

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

*** * ***

