INFOWORLD TECH WATCH
By Serdar Yegulalp, Senior Writer, InfoWorld

Dropbox glitch makes a strong case for encryption by default

It's easy, it's powerful, and it'll give users that much less to worry about. So why isn't it happening?

Though Dropbox's recent outage wasn't a hack -- rather, it was a glitch during planned maintenance -- that didn't make it any less upsetting for users of the service worried about the security of their files, especially because Dropbox, like most every other consumer cloud storage service, doesn't provide a native, transparent way for users to encrypt files before they're transmitted to the cloud.

Over the last couple of years, a slew of third-party outfits have emerged to offer a better layer of security for cloud file-storage services like Dropbox. Most are useful; some are downright transparent. But all of them hint at how the biggest single problem with commodity cloud storage is that the security isn't really in the hands of the user -- and how such security needs to be baked into cloud storage from here on out.

Boxcryptor is one such third-party product. The idea is simple: Files are encrypted on the local system, using an encryption key generated by you -- and to which only you have access -- before being uploaded to Dropbox (Google Drive, SkyDrive, and Sugar Sync are also supported). Cloudfogger functions the same way and likewise works with a broad range of services. Both apps use 256-bit AES encryption, which is likely to remain opaque to prying eyes until quantum computing comes along.

Both apps, though, point out how Dropbox and most of the rest of its ilk -- especially on the consumer side -- all suffer from the same basic drawback. If it's this easy for a third-party company to add per-file encryption to Dropbox, how come Dropbox itself doesn't do it?

Dropbox claims its employees "are prohibited from viewing the content of files you store in your account" and the few people on their end who can access user data are "the exception, not the rule." Unfortunately, a user has no way to verify what's actually going on in Dropbox's data centers, so he or she is stuck in the unenviable position of taking Dropbox's word for it.

It's easy to say that users can add a layer of third-party protection and be done with it. But that requires people knowing about them in the first place and bothering to avail themselves of them to boot. The best long-term solution is to add the option to use such encryption directly into Dropbox or any other

service like it.

Why hasn't this happened? Maybe Dropbox doesn't want to become that much more a target of scrutiny by law enforcement. But with everything else in IT moving to an encrypted-by-default mode, this hardly seems like an outlandish stance to take any more. Plus, it's not wholly unprecedented: The Mozy backup service, for instance, has allowed me to pick my own encryption key for years now. Another possibility is that Dropbox is shying away from supporting such a feature across the full range of clients available for its service, but again, that hardly seems like a complete deal-killer.

If it sounds like I'm picking exclusively on Dropbox here, it's more that I'm holding it as the most prominent example. It's widely used, broadly supported by third parties, and might serve as an impetus to other services if it changed its own ways. But for now, those of us who want encryption for such services -- encryption we control, anyway -- will have to make do with the bolt-on variety.

This story, "Dropbox glitch makes a strong case for encryption by default," was originally published at InfoWorld.com. Get the first word on what the important tech news really means with the InfoWorld Tech Watch blog. For the latest developments in business technology news, follow InfoWorld.com on Twitter.

Related: Encryption Cloud Storage

Serdar Yegulalp is a senior writer at InfoWorld, focused on machine learning, containerization, devops, the Python ecosystem, and periodic reviews.

Follow

Copyright © 2014 IDG Communications, Inc.

- **Stay up to date with InfoWorld's newsletters for software developers, analysts, database programmers, and data scientists.**
- **Get expert insights from our member-only Insider articles.**

InfoWorld FROM IDG

ABOUT US CONTACT PRIVACY POLICY COOKIE POLICY MEMBER PREFERENCES ADVERTISING IDG CAREERS AD CHOICES
CALIFORNIA: DO NOT SELL MY PERSONAL INFO
E-COMMERCE LINKS

IDG COMMUNICATIONS Copyright © 2020 IDG Communications, Inc.

Explore the IDG Network