Dropbox gets hacked ... again

After last year's embarrassing data breaches, Dropbox promised to implement additional safeguards 'to prevent this from happening again.' Whoops, it just happened again.

By Ed Bott for The Ed Bott Report | August 1, 2012 -- 01:47 GMT (18:47 PDT) | Topic: Security

Running a secure online service is hard work. It costs money and it requires nonstop vigilance.

It's the kind of work that gets tested regularly. How a company responds to security challenges defines the difference between earnest startups and companies that deserve to graduate to the big time.

Dropbox just failed that test.

Several weeks ago, Dropbox announced it was investigating some suspicious incidents on its network. The online storage company, which has been a phenomenal success among consumers and small businesses, said it had "brought in a team of outside experts" to investigate the incidents.

And today the other shoe dropped. In a post on the Dropbox blog, VP of Engineering Aditya Agarwal acknowledged that the worst-case scenario had occurred:

> Our investigation found that usernames and passwords recently stolen from other websites were used to sign in to a small number of Dropbox accounts. We've contacted these users and have helped them protect their accounts.
>
> A stolen password was also used to access an employee Dropbox account containing a project document with user email addresses. We believe this improper access is what led to the spam. We're sorry about this, and have put additional controls in place to help make sure it doesn't happen again.
>
> Keeping Dropbox secure is at the heart of what we do, and we're taking steps to improve the safety of your Dropbox even if your password is stolen...

Those are reassuring words. They would inspire more confidence if they didn't echo Dropbox's equally confident reassurances the last time the company suffered a potential security breach.

Let's flash back to July 2011, when Dropbox sheepishly admitted that it had inadvertently published code on its website that allowed anyone to sign in to any Dropbox account without credentials:

> In a blog post, Dropbox CTO Arash Ferdowsi confirmed that the problem occurred and blamed it on "a code update ... that introduced a bug affecting our authentication mechanism."
>
> Dropbox claims the outage lasted nearly four hours. A letter from the CEO to an affected customer confirms that user accounts were accessed during that outage:
>
> Earlier this week, we wrote to tell you about a security lapse at Dropbox. Today I am writing to tell you

> something I never expected to tell a customer. During our forensic analysis, we discovered that an extremely small number of accounts, including yours, were subject to some suspicious activity.
>
> Our investigation revealed that at around 11:25 PM UTC (Coordinated Universal Time) on June 19, 2011 someone logged into your account. It is likely that your account was compromised by a third party. According to our records, neither your account settings nor files were modified, but data was downloaded from your Dropbox account.

Ferdowsi acknowledged, “This should never have happened. We are scrutinizing our controls and we will be implementing additional safeguards to prevent this from happening again.” An update to his blog post adds the detail that “fewer than a hundred” Dropbox users were affected.

At the time, I said, “At the very minimum, Dropbox needs to have a thorough security audit from an independent group to ensure that it has the processes in place to back up those promises.” That obviously never happened.

Dropbox has built up an enormous reservoir of goodwill in its large and loyal user base. It is squandering that goodwill at a record pace.

Maybe it’s time for the company’s investors to turn it over to someone big enough to take security seriously.

RELATED TOPICS: SECURITY TV DATA MANAGEMENT CXO DATA CENTERS

By Ed Bott for The Ed Bott Report | August 1, 2012 -- 01:47 GMT (18:47 PDT) | Topic: Security

SHOW COMMENTS

MORE FROM ED BOTT

Security
Is it OK to use your browser’s built-in password manager?

Windows 10
For business customers, Microsoft's Windows 10 documentation is an unruly mess

Windows 10

The ultimate Windows 10 information hub: Everything you need in one place

Windows 10

After Windows 10 upgrade, do these seven things immediately

NEWSLETTERS

RELATED STORIES

‹ 1 of 3 ›

Google: Mitigating disinformation and foreign influence through social media a joint effort

The local arm of the search giant wants to see cooperation between the likes of industry, the technical community, and government, in addition to education efforts spanning schools ...

Hacker breaches security firm in act of revenge

Hacker claims to have stolen more than 8,200 databases from a security firm's data leak monitoring service.

CONNECT WITH US

Visit other CBS Interactive sites:

Select Site

Topics

Newsletters

Galleries

Site Assistance

Videos

ZDNet Academy

Sponsored Narratives

TechRepublic Forums

CA Privacy/Info We Collect

CA Do Not Sell My Info