

Cyber attack on Google Frequently Asked Questions January 13, 2010

What happened in the recent cyber attack on Google?

As you can see from these story links, Google was recently the target of a cyber attack, and as a result, is considering a move out of the China market.

<http://www.nytimes.com/2010/01/13/world/asia/13beijing.html>

http://online.wsj.com/article/SB126333757451026659.html?mod=WSJ_hpp_LEFTTopStories#articleTabs%3Dcomments

Why was Rackspace mentioned in the story?

A single server at Rackspace was also the target as part of this attack. As soon as it was identified, we disabled the server and worked directly with Google, contributing to the investigation and elimination of this attack.

What did Rackspace tell the media?

This is what Rackspace said in media inquiries yesterday:

“Rackspace hosts tens of thousands of websites for customers and we take every precaution to make them safe and secure. As a hosting and cloud computing company, we run the servers and operating systems for our customer’s websites, but customers run their own applications on those servers. In this case, a server at Rackspace was compromised, disabled, and we actively assisted in the investigation of the cyber attack, fully cooperating with all affected parties. Cyber attacks are a common occurrence in today’s online world, and we work every day to combat them and make our servers safe for our customers.”

Was my data compromised?

No customer data at Rackspace was compromised or altered as a result of this action.

What is Rackspace doing to prevent this from happening again?

Cyber attacks will always be a concern. Rackspace employs intrusion detection systems (IDS) to identify and help prevent cyber attacks. An IDS records incoming and outgoing traffic going through the firewall and provides filtering information based on blacklists and other criteria. Once questionable traffic is identified, it is then blocked. Rackspace is constantly reviewing its policies and procedures to keep up with the latest cyber threats.”

How do I know my data is safe?

Cyber attacks are an ever-present threat in today’s online world. At Rackspace, security is a daily presence and our ultimate goal is to protect our customer. We recommend that all customers consider making use of our firewall, VPN, SSL certificate, and antivirus products, as well as intrusion detection services with our partners, to help control and mitigate their risks. We also recommend that customers engage in security reviews of their network environment and applications, on a routine, periodic basis. Rackspace also has offerings (both directly, and through partners) that may supplement or improve a customer’s security review process. Finally, while Rackspace offers patching services for its major product offerings, customers should supplement this activity with routine updates to their own, in-house custom software deployed on Rackspace servers.