Is your data secure in the cloud?

NOVEMBER 11, 2014

4 9 6

Is your data secure in the cloud?

BusinessCloudProtectionYuval Ben-Itzhak

YuvalBen-Itzhak
Chief Technology Officer
More articlesOther authors

It’s a very broad topic so I chose to focus my answers on three particular things.

When you put your data in the cloud, someone else holds it?

There's a security gap between the private and public cloud. You might have invested heavily in your own private cloud or on premise systems, but data on the public cloud are not secured by you. Who controls this data? Who is responsible for it and who is accountable should something go wrong? This needs to be addressed as a priority. Consider that CTOs and CIOs must as part of SOX compliance procedures sign off on their company data being secured and under control. Yet if that data is held in the cloud and you cannot audit the security measures there, then the reality is that it is being managed by someone else – the cloud service provider.

So what we need to focus on is understanding how we can help businesses get back control of securing their data.

Cloud and mobile has changed the assumptions businesses had that they can control all the devices being used within their organizations to access their data.

With cloud services, businesses have limited authority to define what security is being used by their provider to protect their data. Company executives might not like this situation, but they will still have had to confirm that their data is secure and compliant with regulations. This is a no-win scenario for businesses.

That fact that critical data is stored on cloud services means that the business is now effectively in someone else's hands. There is the additional challenge of how the IT department can control a situation where an employee has their own device and wants to use it to connect to this cloud-based data using tools like Salesforce, for example.

If the malware is running on that device, the IT manager is not in control of identifying and fixing that. They are in the position of having to guarantee to the business that company data is secured when in fact that might not be the case.

Hackers realized this pretty quickly. They started to target individuals within organizations when they were off the network and interacting with the cloud via a device in order to retrieve data they needed.

I expect that this risk will soon become untenable. And in the near future, that we will start to see companies pushing back on signing documents that their data stored in the cloud is secure because in reality, that data is no longer part of their business, no longer within their control.

In small to medium sized businesses, there is less likelihood they will even have any sort of systems in place to manage this and so they ultimately have less control and less confidence that their private, business data is safe in the cloud.

The Internet of Things means businesses need long-term perspective for their cloud strategy.

This brings me to this last point. If we fast forward two or even five years, and look at the impact of the Internet of Things, it's clear we need to start thinking already about how to connect and manage these new devices and sensors for business. More importantly, we need to harness the data that is coming out of them. We'll want them to be under control and we will all start to use services.

We also have privacy to consider. This is one of the rising stars in security. It's a big challenge and even law enforcement agencies are becoming more active in this area.

As the panel drew to a close, I emphasized that things will start to change. Cloud service providers should start to work with their client teams on premise to give back to that business a degree of control. This will be the first step towards giving CIOs and CTOs that confidence to sign compliance documents because they will be able to verify that company data is indeed secure.

Yuval Ben-Itzhak
November 11, 2014