What You Need to Know About Capital One's Massive Data Breach

July 31, 2019 - Over the past couple of days you may have heard that Capital One has announced a data breach, and it was a big one. The breach included data on 106 million of the company's and applicants. Here is what we know so far.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

The breached data wasn't housed on Capital One's own computers. It was stored in the cloud - which means that the servers and computer network were outsourced to another company. In this case, that company happened to be Amazon Web Services. As you might expect from the name, they are part of Amazon.

According to the initial announcement, the cause of the breach was an incorrectly configured firewall. That configuration was apparently handled by Capital One. But that doesn't tell the entire story. The FBI has already made an arrest in the breach. A software engineer by name of Paige A. Thompson, who just happens to be a former employee of Amazon Web Services. The companies haven't started finger-pointing yet, but our bet is that they will in very short order.

The amount of damage that can be done with the stolen data varies from person to person. Most of the impacted Capital One Customers had their names and contact information included, but that sounds like about it. For any unlucky 140,000 people, the breach included their social security numbers. And 80,000 people had their bank account numbers included in the breach. Capital One has said that they are notifying these victims.

The breach brings up a number of disturbing questions. For instance, why would any company store unencrypted data in the cloud? And more importantly, what are cloud computing companies like Amazon Web Services doing to make sure that their employees don't pose a threat to data owned by the company's customers?

At this point it isn't known if Thompson used knowledge that she gained while working with Amazon to pull off this breach, but if she didn't that would be awfully coincidental.

Capital One has said that their firewall configuration issue has been corrected. The company expects the breach to cost them in excess of $100 million.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS