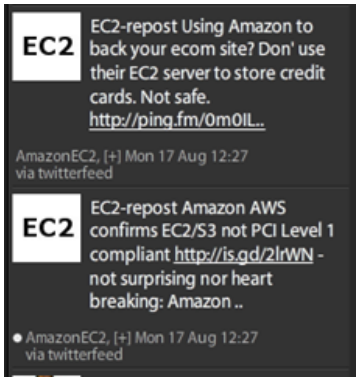
Amazon Compliance Confession About Customers, Not Itself

Lori MacVittie, 2009-18-08

Amazon EC2 and S3 are no more or less safe than they were last week despite hype around PCI compliance admission

The recent admission/announcement that "Amazon EC2 is not PCI compliant" (this is not exactly true, but we'll get to that later) has set off a rush of blogs, articles, and tweets that say, in effect, EC2 is no longer "safe". But a lack of compliance does not make Amazon any more less safe than achieving PCI compliance makes a site more safe.



Ladies and gentlemen of the Internet, I submit as proof the admission of Heartland CEO Robert Carr that even though their "site" and "systems" were designated as PCI compliant, still they were attacked, breached, and the subject of ridicule and scorn for months in the press and security-focused blogosphere.

"*PCI compliance doesn't mean secure. We and others were declared PCI compliant shortly before the intrusions.*" – Heartland CEO Robert Carr in an interview with Bill Brenner, Senior Editor, CSO Online.

PCI compliance doesn't automatically make a site safe. Lack of PCI compliance doesn't make EC2 unsafe, either. It means it isn't compliant with the policies designated by the PCI council for handling credit card transactions and sensitive data. And, if we look past the hand-waving, we'll find that Amazon admits you can't build a PCI Level 1 compliant application using EC2 and S3, but you can build a PCI Level 2 compliant application.

"It is possible for you to build a PCI level 2 compliant app in our AWS cloud using EC2 and S3, but you cannot achieve level 1 compliance."

So how does this statement translate into "OMG! Amazon is unsafe!"? This is clearly about what the customer can and cannot do, not an admission of the security status of Amazon's underlying infrastructure.

Amazon clearly states you cannot be level 1 compliant because it requires on-site auditing that they simply can't (or won't) allow. The inability to meet a requirement because of logistics (level 1 requires an on-site audit which Amazon states is not possible) is hardly the same as failing to meet the requirement for a firewall, or default password use. The inability to meet that one requirement is hardly reason for condemnation of Amazon's overall security posture. Its inability for you to meet PCI compliance does not automatically mean its systems and environment are "unsafe". Amazon points to the "on-site audit" requirement as a reason why you cannot achieve PCI Level 1 compliance. For all we know Amazon meets or exceeds every other requirement for PCI level 1 compliance that is required of a service-provider. Inferring anything about the security posture of Amazon's internal systems from one message in a forum is simply not possible.

Furthermore, Amazon says ***YOU*** cannot build a PCI Level 1 compliant application. In other words, its announcement wasn't an observation about the security of *its* systems, it was an observation regarding what you, the customer, can and cannot achieve using its systems.

In fact, in that same forum message that set off this Chicken Little episode, the Amazon representative clearly states Amazon does, in fact, meet PCI compliance standards elsewhere:

> *Our payment system is PCI compliant and it is an "alternative payment processing service" meaning your users re-direct to our platform to conduct the payment event using their credit cards or bank accounts.* [emphasis added]

Nothing in Amazon's "confession" implies anything about *its* security posture; if anything its note that its payment systems *are* PCI compliant means its underlying systems are as secure as any other meeting PCI compliance. Therefore there is no reason to believe that Amazon is any less safe than it was last week. In fact, the statement that you *can* achieve level 2 compliance means Amazon has, in fact, checked over its systems and that they will meet the requirements required for much of the PCI standard – probably the pieces that are important to assuring the security of systems.

PCI compliance is not a rubber stamp of safety. Achieving PCI compliance does not automatically confer some special safety status upon an organization. Neither does the reverse hold true; organizations that do not fall under PCI and therefore need not worry themselves about compliance with its standards are not necessarily "unsafe".

This entire situation is a raw deal for Amazon. EC2 and S3 are no more – or less – secure than they were before this unsurprising announcement regarding PCI compliance and applications built atop its systems. The misinterpretation of its admission and its viral-like spread is little more than FUD that does more harm than good – both to Amazon and cloud computing in general.

- Heartland CEO on Data Breach: QSAs Let Us Down
- An Open Letter to Robert Carr, CEO of Heartland Payment Systems
- PCI Compliance in the Cloud: Get it in writing!
- Amazon Web Services Developer Community: Does Amazon EC2 meet PCI Compliance
- WILS: InfoSec Needs to Focus on Access not Protection
- Cloud Changes Cost of Attacks
- An Unhackable Server is Still Vulnerable

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113