SANS AWS InSecurity Summit

Austin, TX
June 11, 2018

Today's Agenda

- The State of AWS Cloud Security / Top 10 Problems
  - Ben Hagen - Hi!
- Morning Presentations
  - Will Bengston ~ Netflix
  - Mark Hillick ~ Riot Games
  - Steve Woodrow ~ Lyft
- Afternoon Training
  - Part 1 ~ AWS Security Fundamentals, Bringing it all together
  - Part 2 ~ Programmatic AWS / Lambda / Events

The State of Cloud Security

But seriously ...

Yet another NSA intel breach discovered on AWS. It's time to worry.

by TRISTAN GREENE — 6 months ago in OPINION

Uber Discloses Year-Old AWS Data Breach, Exposing Millions of Users

By Gladys Rama ▪ 11/21/2017

On Tuesday, ride-sharing app Uber disclosed that its Amazon Web Services (AWS) account was hacked last year, compromising the personal information of 57 million users worldwide, including 600,000 U.S. drivers.

Uber CEO Dara Khosrowshahi, who came into his post just this past August, said **in a statement** that he only learned of the hack "recently," even though it happened in "late 2016" under the watch of his predecessor, Travis Kalanick. Kalanick resigned as Uber's CEO in June.

February 15, 2018

Open AWS S3 bucket exposes private info on thousands of Fedex customers

In what has become an alarmingly routine occurrence, an unsecured Amazon S3 server – this time affiliated with FedEx – has exposed personal information of tens of thousands of users.

Kromtech Security Center researchers came across the exposed information, which included 119,000 scanned documents such as passports, driver's licenses, security IDs and the like, on an open S3 server belonging to Bongo International, a company FedEx purchased in 2014 and which became part of the shipping firm's now-shuttered FedEx CrossBorder service.

A FedEx S3 server was left unsecured, exposing information on thousands.

System Shock: How A Cloud Leak Exposed Accenture's Business

Updated on March 26, 2018 by Dan O'Sullivan

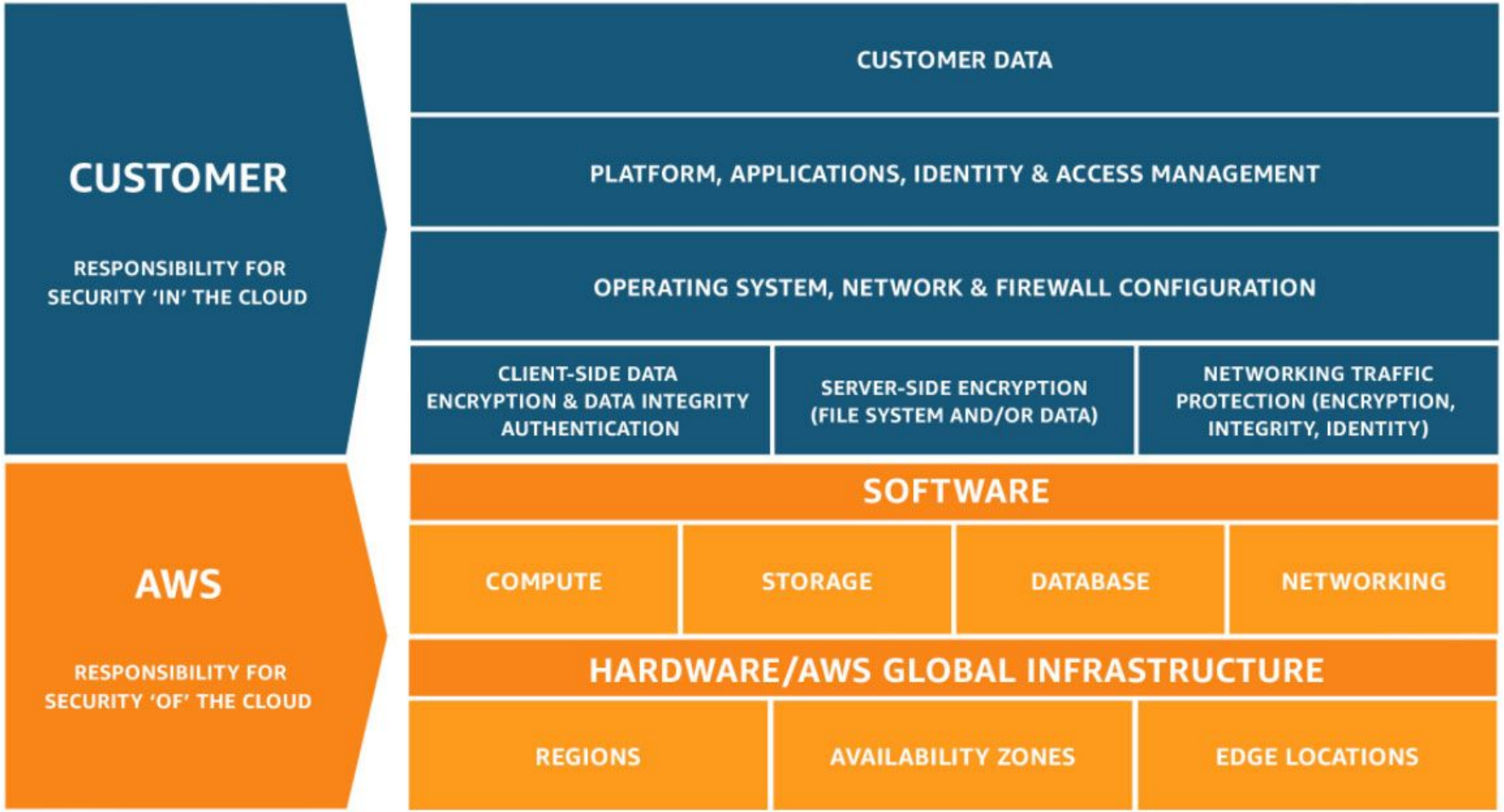
I wanted to make you aware that Splunk Cloud experienced an incident that has subsequently been resolved. It impacted Splunk Cloud availability for a small number of our customers. In the late afternoon of February 9, we discovered the unauthorized use of a former employee's credentials which permitted access to a limited portion of our cloud system. Splunk terminated that access in minutes. Based upon our investigation to date, no customer data was viewed, accessed, or taken. We have contacted law enforcement and are cooperating in the investigation.

A well architected & instrumented AWS environment is more secure than its counterpart in a datacenter.(*)

(*) but only if you know what you’re doing.

Meaning ... the state of cloud security

SHOULD BE BETTER


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Top 10 AWS Security Risks

1. Insecure use of developer credentials

2. Publicly accessible S3 buckets

3. Improper use of default configurations

4. Access controls do not follow principles of least privilege

5. Misconfigured network constructs

6. Lack of appropriate logging and monitoring

7. Lack of inventory management

8. Domain hijacking

9. Lack of a disaster recovery plan

10. Manual account configuration

Bonus!

`http://169.254.169.254/latest/meta-data/iam/security-credentials/`

To sum things up ...

- We’ve covered 10 common mistakes organizations make ... there are more
- But the opportunities and advantages of public cloud environments can be worth it
- As security professionals we must understand the technology and environment we are securing
- In the case of AWS this translates to a fundamental understanding of how AWS works and how you can instrument and manage not only the security features of your account, but the account itself towards your organization’s security goals

Thank you!