ISACA®

Trust in, and value from, information systems

San Francisco Chapter

T2 – IaaS and PCI Compliance

Robert Zigweid, IOActive

Introduction

Robert M. Zigweid

- Principal Compliance Consultant at IOActive, Inc.
- PCI QSA, PCI PA-QSA
- QSA for Amazon Web Services

Creating a PCI Compliant Cloud Environment

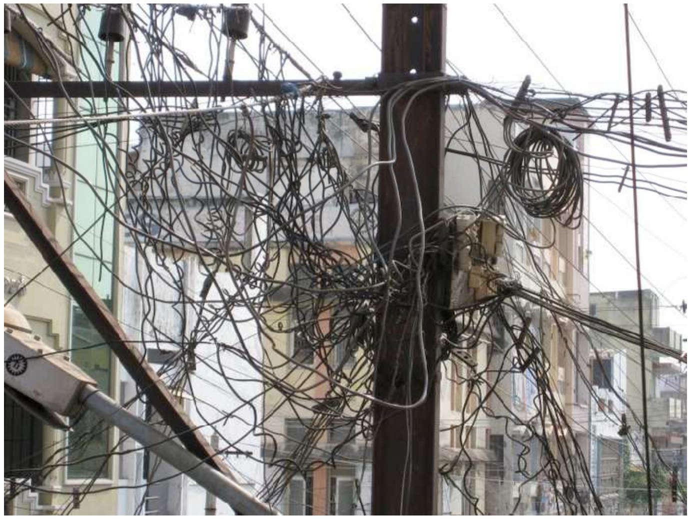
- Understand the Type of Cloud in Use
  - SaaS: Software or Service as a Service
  - PaaS: Platform as a Service
  - IaaS: Infrastructure as a Service

Customer Responsibilities for PCI Compliance

- Ultimately: EVERYTHING!
  - That’s the short answer
- Practically:
  - Outside of an IaaS environment there is no change

Customer Responsibilities for PCI Compliance

- Requirement 1: Firewall and Router Configuration
  - Establishing rules
  - Reviewing rules
  - Don't forget inbound and **outbound**



IaaS Responsibilities for PCI Compliance

- Accurate definition and disclosure of Scope and Requirements

Who is Responsible?

Requirement 1: Firewalls and Routers

- Remember, it depends upon the service
  - **IaaS**
    - Underlying rules for purposes of internal segmentation and function
    - These do not get exposed to customers
  - **Customer**
    - Exposed routing controls
    - This might vary widely

Who is Responsible?

Requirement 2: Vendor Defaults and Hardening

- IaaS
  - Underlying rules for purposes of internal segmentation and function
  - These do not get exposed to customers
  - Includes Hypervisor!
- Customer
  - Customer installed, customer responsibility
  - IaaS provider has no visibility

Who is Responsible?

Requirement 3: Protect Stored Cardholder Data

- Critical Requirement
- **IaaS**
  - Generally, no control or responsibility
- **Customer**
  - Full control, full responsibility
  - Encryption
    - Which service is being used?

Who is Responsible?

Requirement 4: Protect Transmitted Cardholder Data

- Critical Requirement
- **IaaS**
  - No control or responsibility
- **Customer**
  - Full control, full responsibility
  - Elastic Load Balancer (ELB)

Who is Responsible?

Requirement 5: Anti-Virus

– IaaS
  - Internal control and responsibility

– Customer
  - Full control and responsibility

Who is Responsible?

Requirement 6: Secure Applications

- IaaS
  - Internal control and responsibility
- Customer
  - Full control and responsibility
  - 6.6 Web Application Firewall

Who is Responsible?

Requirement 7: Restrict Access to Cardholder Data

- IaaS
  - Internal control and responsibility
  - Depends upon the service
- Customer
  - Full control and responsibility

Who is Responsible?

Requirement 8: Unique IDs

- IaaS
  - Internal control and responsibility
  - Depends upon the service
  - Identity and Access Management (IAM)
- Customer
  - On instances, customer responsibility

Who is Responsible?

Requirement 9: Physical Security

- IaaS
  - IaaS responsibility
- Customer
  - On instances, customer responsibility

Who is Responsible?

Requirement 10: Tracking and Monitoring

(AKA the bane of PCI)

- IaaS
  - Internal control and responsibility
  - Required to make available via Appendix A
- Customer
  - On instances, customer responsibility

Who is Responsible?

Requirement 11: Testing and Scanning

- IaaS
  - Internal control and responsibility
- Customer
  - Policies almost completely customer’s responsibility
  - Incident Response
    - Contact your account representative

Who is Responsible?

Requirement 12: Policies, Risk Assessment and Incident Response

(AKA the other bane of PCI)

- IaaS
  - Internal control and responsibility
  - Not really applicable to customer's policies
- Customer
  - Customer responsibility

QSA and Customer Concerns and Issues

- Disclaimer!
- Reminder, ask questions

QSA and Customer Questions and Issues

- Can I review the provider’s ROC?
  - Is it your common practice to request Service Provider’s ROCs?
  - A ROC is not a public document
  - Guidance states to clearly indicate scope, not to reassess the service provider

QSA and Customer Questions and Issues

- Can I visit the IaaS data center?
  - Which one?
  - Do you visit all your Service Provider’s Data Centers?
  - It’s not your equipment

QSA and Customer Questions and Issues

- How does the virtualization technology separate entities?
- Consider asking for single-tenant systems
  - This is available for some IaaS providers

Lessons Learned in the Real World

- Requirement 1: Firewalls and Network Routing
  - Host-based Firewalls and Routers
    - These can be compliant
    - Difficult to manage

Lessons Learned in the Real World

- Requirement 1: Firewalls and Network Routing
  - AWS Security Groups
    - Centralized and automatically synchronized
    - Managed through the IaaS portal or command line
    - TCP and UDP network access protection; stateful by default
    - Only permits *allow* rules; deny by default
  - Example: EC2 versus VPC
    - EC2 permits only ingress rules
    - VPC allows ingress and egress rules

Lessons Learned in the Real World

- Requirement 1: Firewalls and Network Routing
  - AWS ACLs
    - Centralized and automatically synchronized
    - Managed through the IaaS portal or command line
    - Second layer of defense
    - IP Layer isn’t stateful
    - *Deny* and *Allow* rules for both ingress and egress

Lessons Learned in the Real World

- Requirement 10.4: Time Synchronization
  - Instance time-skew is a fact

Lessons Learned in the Real World

- Requirement 11: Scans and Penetration Tests
  - Refer to the AWS Penetration Test Agreement
    - http://aws.amazon.com/security/penetration-testing/
  - Medium or larger instances are required
    - Even on single-tenant systems

Lessons Learned in the Real World

VPC vs. EC2

- VPC allows more network control
  - Subnets
  - Egress Security Group Rules
- EC2 has more services available
  - Elastic Load Balancer

Lessons Learned in the Real World

VPC vs. EC2

If possible, I recommend VPC

Lessons Learned in the Real World

IDS and IPS

- With no physical routers and firewalls how do you handle IDS?
- Enter Snort!
  - Requires duplication of traffic
  - Will work as IDS as opposed to IPS
  - Not the only solution

Lessons Learned in the Real World

Elastic Block Store (EBS)

- Block device storage mountable on instance
- Helps separate the Hypervisor from the instance

Lessons Learned in the Real World

IAM (Identity and Access Management)

- Critical to avoid shared accounts (8.5.8)
- Is deny-by-default

Questions!

Thank You!

rzigweid@ioactive.com