KORNERSTONE
a TRAINOCATE company

Training. Makes a differece.

Certified Cloud Security Professional, CCSP®

D2 - Cloud Data Security

Domain 2 – Cloud Data Security

18 APR 2017 NEWS

Widespread AWS Misconfiguration Opens Cloud Environments to Attack

Tara Seals US/North America News Reporter, Infosecurity Magazine
Email Tara

When it comes to securing services in the cloud, misconfigurations are a scourge: Wide-open SSH and infrequent software updates plague cloud-based environments.

In an analysis by Threat Stack, nearly two-thirds were found to have at least one critical security misconfiguration. Configuration lapses that enable an attacker to gain access directly to private services or the Amazon Web Services console, or could be used to mask criminal activity from monitoring technologies are deemed critical by Threat Stack.

Among the most egregious issues found were AWS Security Groups configured to leave SSH wide open to the internet in 73% of the companies analyzed. This simple configuration error allows an attacker to attempt remote server access from anywhere, rendering traditional network controls like VPN and firewalls moot. In fact, Threat Stack observed SSH traffic from the internet using the root account, which could have severe security repercussions.

Additionally, the well-recognized best practice of requiring multi-factor authentication for AWS users was not being followed by 62% of companies analyzed, making brute-force attacks that much simpler. Even AWS-native security services, such as CloudTrail, were not being deployed universally (27%) across all regions.

Data Security

- One of the most important basis for cloud security concerns
- Involves privacy issue

Domain objectives

- Describe the cloud data life cycle based on Cloud Security Alliance (CSA) guidance
- Describe the design and implementation of cloud data storage architectures with regard to storage types, threats, and available technologies
- Identify the necessary data security strategies for securing cloud data
- De ne the implementation processes for data discovery and
- classification technologies
- Identify the relevant jurisdictional data protections as they relate to personable identifiable information
- De ne Digital Rights Management with regard to objectives and tools available
- Identify the required data policies specific to retention, deletion, and archiving
- Describe various data events and how to design and implement processes for auditability, traceability, and accountability

Domain Agenda

- Understand Cloud Data Life Cycle
- Design and Implement Cloud Data Storage Architectures
- Design and Apply Data Security Strategies
- Understand and Implement Data Discovery and Classification Technologies
- Design and Implement Relevant Jurisdictional Data Protection for Personally Identifiable Information (PII)
- Design and Implement Data Rights Management
- Plan and Implement Data Retention, Deletion, and Archival Policies
- Design and Implement Auditability, Traceability, and Accountability of Data Events

The Data Life Cycle Phases

Cloud Data Protection Basis

- **Who are the actors that potentially have access to data I need to protect?**
- **What is/are the potential location(s) for data I have to protect?**
- **What are the controls in each of those locations?**
- **At what phases in each lifecycle can data move between locations?**
- **How does data move between locations** (via what channels)**?**
- **Where are these actors coming from** (what locations, and are they trusted or untrusted)**?**

Key Data Functions

performed with data in cloud-based environments

- Access: View/access the data, including copying, le transfers, and other exchanges of information
- Process: Perform a transaction on the data: update it, use it in a business processing transaction, etc.
- Store: Store the data (in a le, database, etc.)

Key Data Functions

	Create	Store	Use	Share	Archive	Destroy
Access	X	X	X	X	X	X
Process	X		X			
Store		X			X	

Note that each of these functions is performed in a *location* by an *actor* (person).

Some Data Security Technologies

- **Encryption:** For preventing unauthorized data viewing.
- **Data Leakage Prevention (DLP):** Audit and prevent unauthorized data exfiltration
- **File and database access monitor:** Detecting unauthorized access to data stored in les and databases
- **Obfuscation, anonymization, tokenization, and masking:** Different alternatives for the protection of data without encryption

Cloud Model Storage Types

- IAAS
  - Volume storage
  - object storage
- PAAS
  - Database
  - Big Data
- SAAS
  - information storage management
  - Content / File storage
  - app

Other types of cloud storage

- Ephemeral
- Content Delivery Network (CDN)
- Raw storage
- Long-term storage

Match each description with the storage type.

_a. IaaS, b. PaaS c. SaaS

_____ Self-service models for accessing, monitoring, and managing remote data center infrastructures

_____ Many applications can be run directly from a web browser without any downloads or installations required, although some require small plugins

_____ Provides developers with a framework they can build upon to develop or customize applications

_____ Uses volume storage and object storage as storage types

_____ With this technology, enterprise operations, or a third-party provider, can manage OSes, virtualization, servers, storage, and networking

_____ Uses the web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the client's side

Data Dispersion in Cloud Storage

- For high-availability
- Underlying architecture = erasure coding

Threat to Cloud Storage Types

- Unauthorized usage
- Unauthorized access
- Liability due to regulatory non-compliance
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on storage
- Corruption/modification and destruction of data
- Data leakage/breaches
- Theft or accidental loss of media
- Malware attack or introduction
- Improper treatment or sanitization after end-of-use

Cloud Data Protection - DLP

- Data Loss / Leakage Prevention
  - Discovery and classification
  - Monitoring
  - Enforcement
- DLP Architecture
  - Data at rest
  - Data in motion
  - Data in use

Cloud-based DLP considerations

- Data in the cloud tend to move and replicate.
- Administrative access for enterprise data in the cloud could be tricky.
- DLP technology can affect overall performance.
- Need to address:
  - **What kind of data is permitted to be stored in the cloud?**
  - **Where can the data be stored (jurisdictions)?**
  - **How should it be stored? Encryption and storage access consideration.**
  - **What kind of data access is permitted? Which devices and what networks? Which applications? Which tunnel?**
  - **Under what conditions is data allowed to leave the cloud?**

Cloud Data Protection - Encryption

- Data at rest
- Data in motion
- Data in use

- Challenges

- Architecture : data, engine, keys

Cloud Data Encryption

- IAAS
- PAAS
- SAAS

Encryption – Key Management

- Considerations
- back-up and replication of key
- Store Key in cloud

Other Cloud Data Protection Technologies

- Masking
  - static, dynamic
  - Random substi, algo sub, shuffle, masking, deletion
- Obfuscation
- Anonymization
- Tokenization
  - Deployments
  - Cloud considerations

Emerging Data Protection Technologies

- Bit Splitting
- Homomorphic encryption

Data Discovery

- Approaches
  - Big data
  - Real-time analytics
  - Agile analytics and agile biz intell
- Techniques
  - Meta data
  - Labels
  - Content analysis

Data Discovery

- Issues
  - Poor data quality
  - Dashboards
  - Hidden costs

Data Classification

- What data types are available?
- Where is certain data located?
- What access levels are implemented?
- What protection level is implemented, and does it adhere to compliance regulations?

some
Data Classification - Categories

- Data type (format, structure)
- Jurisdiction (of origin, domiciled) and other legal constraints
- Context
- Ownership
- Contractual or business constraints
- Trust levels and source of origin
- Value, sensitivity, and criticality (to the organization or to third party)
- Obligation for retention and preservation
  - Poor data quality
  - Dashboards
  - Hidden costs

Cloud Data Classification - Challenges

- Data creation
- Classification controls
- Metadata
- Classification data transformation
- Reclassification considerations

Data Privacy - Acts

Key questions -

- What information in the cloud is regulated under data protection laws?
- Who is responsible for personal data in the cloud?
- Whose laws apply in a dispute?
- Where is personal data processed?

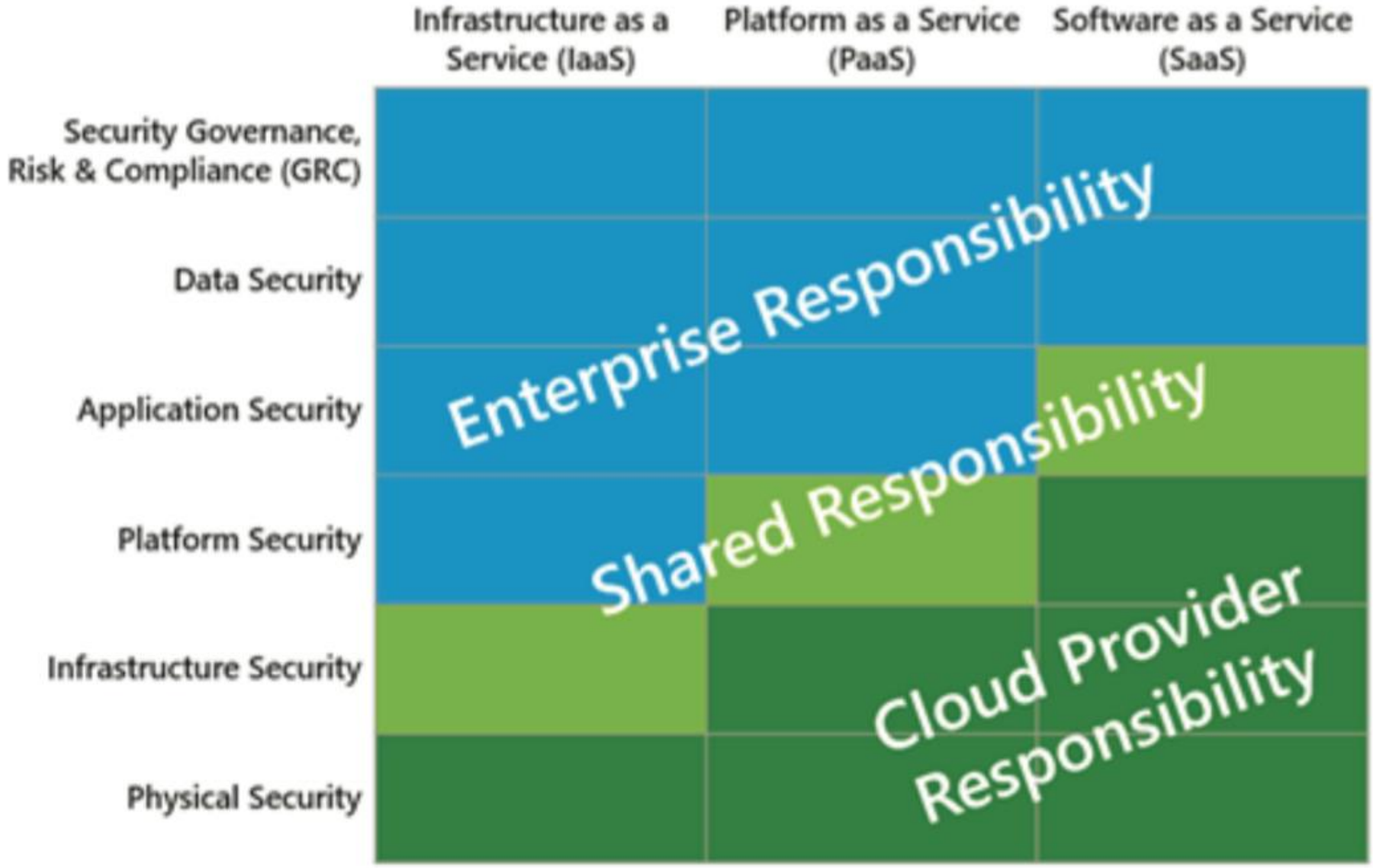
•Geographical : US, EU, APEC

Data Privacy - Laws

Differences Between Jurisdiction and Applicable Law:

- Applicable law: This determines the legal regime applicable to a certain matter
- Jurisdiction: This usually determines the ability of a national court to decide a case or enforce a judgment or order

Responsibility Depending on the Type of Cloud Services



Classification of Discovered Sensitive Data

- **Scope and purpose of the processing**
- **Categories of the personal data to be processed**
  - Collection
  - Recording
  - Organization
  - Selection
  - Retrieval
  - Comparison
  - Communication
  - Dissemination
  - Erasure
- **Categories of users allowed**
- **Data retention constraints**
- **Security measures to be ensured**
- **Data breach constraints**
- **Status**

Application of Defined Controls for Personally Identifiable Information (PII)

- CSA CCM (Cloud Controls Matrix)

(Cloud Security Alliance)

Data Rights Management

- Consumer & Enterprise versions
- Objectives:
  - Adds an extra layer of access controls on top of the data object or document.
  - Is agnostic to the location of the data
  - Is useful for protecting sensitive organization content such as financial documents
  - Is useful for setting up a baseline for the default Information Protection Policy

Cloud Data Rights Management

- Challenges
- Characteristics of Tools

Match each capability with the associated description.

a. Support for existing authentication security infrastructure
b. Persistent protection
c. Dynamic policy control
d. Continuous audit trail
e. Automatic expiration

1. _____ Reduces administrator involvement and speeds deployment
2. _____ Allows content owners to de ne and change user permissions
3. _____ Ensures documents, messages, and attachments are protected at rest, in transit, and after they're distributed to recipients
4. _____ Provides the ability to automatically revoke access to documents, e-mails, and attachments at any point
5. _____ Provides confirmation that content was delivered and viewed

Cloud Data Deletion & Disposal Policy

- Basis
  - Regulation or legislation:
    - Certain laws and regulations require specific degrees of safe disposal for certain records.
  - Business and technical requirements:
    - Business policy may require safe disposal of data. Also, processes such as encryption might require safe disposal of the clear text data after creating the encrypted copy.

- Options / Techniques
  - Physical destruction
  - Degaussing
  - Overwriting
  - Encryption

Crypto-shredding

Cloud Data Accountability & Traceability

- SAAS – event & data sources
  - Web server logs
  - Application server logs
  - Database logs
  - Guest operating system logs
  - Host access logs
  - Network infrastructure devices logs
  - Application level logs
  - Virtualization platform logs and SaaS portal logs
  - Network captures
  - Billing records
  - User access records
  - Management application logs

Cloud Data Accountability & Traceability

- PAAS – (per OWASP recommendation)
  - Input validation failures
  - Output validation failures
  - Authentication successes and failures
  - Authorization (access control) failures
  - Session management failures
  - Application errors and system events
  - Application and related systems start-ups and shut-downs, and logging initialization (starting, stopping, or pausing)
  - Use of higher-risk functionality
  - Legal and other opt-ins

Cloud Data Security – remaining topics

- Identify event attribute requirements
- Storage and analysis of data events
- Security Information & Event management (SIEM)
- Continuous operations
- Chain of custody & non-repudiation