Analysis and Learnings from Cyber-attacks on nine well known companies

Senthil Mehalingam
Vice-Chair, Computer Society - IEEE Pikes Peak Section

Agenda

- Introduction
  - Cloud Computing
  - Information Security
- Breaches of nine well known companies
- Controls to mitigate risk
- Learnings from the breaches

Cloud Computing and service models

Cloud computing - Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and de-provisioned with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models and four deployment models.

Key features:

- On-demand self-service
- Broad network access
- Resource pooling
- Elasticity - Rapidly provisioned and de-provisioned
- Measured service

Cloud Computing service models

Infrastructure as a Service (IaaS)
e.g. AWS Elastic Compute Cloud(EC2), Azure virtual machines

Platform as a Service (PaaS)
e.g. OpenShift

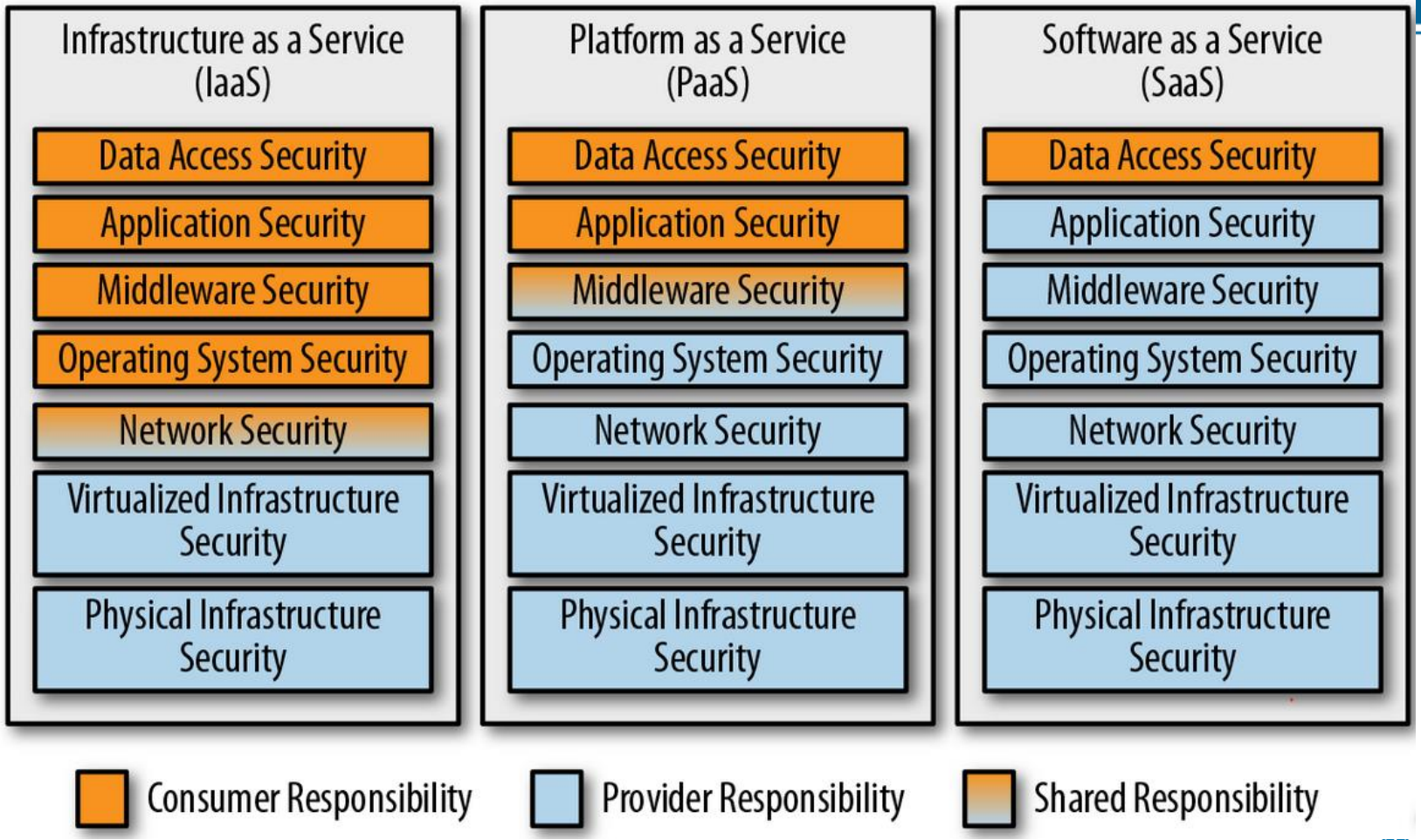
Software as a Service (SaaS)
e.g. Office 365

Function as a Service(FaaS)
e.g. Amazon Web Services(AWS) Lambda, Azure Functions

Cloud Computing deployment models

Deployment Models:

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud


Infrastructure as a Service (IaaS)
Data Access Security
Application Security
Middleware Security
Operating System Security
Network Security
Virtualized Infrastructure Security
Physical Infrastructure Security
Platform as a Service (PaaS)
Data Access Security
Application Security
Middleware Security
Operating System Security
Network Security
Virtualized Infrastructure Security
Physical Infrastructure Security
Software as a Service (SaaS)
Data Access Security
Application Security
Middleware Security
Operating System Security
Network Security
Virtualized Infrastructure Security
Physical Infrastructure Security
Consumer Responsibility
Provider Responsibility
Shared Responsibility

Information Security principles - CIA Triad

Confidentiality
Integrity
Availability

Information Security practices

Least Privilege

Defense in Depth

Threat Modeling

Risk Management

Threat actors

- Script kiddies
- Hacktivists
- Organized crime
- State sponsored actors

Risk Management

- Avoidance
- Mitigation
- Transfer
- Accept

Asset-oriented approach

Asset

- Computing
- Data

Decide what needs to be protected based on classification

- Non-public
- Confidential
- Confidential and Highly Sensitive

Cloud security breaches of 9 companies

Capital One

Incident: Loss of sensitive information(Personally Identifiable Information, SSN, bank account numbers, credit scores, limits, balances) of over 105 million customer accounts

Cause: Misconfigured Web Application Firewall(WAF) which was exploited with Server Side Request Forgery(SSRF)

Impact: 190M+ settlement, stock price drop, staff loss

Preventive controls: Sufficient Identity and Access Management

Learning:

Ensure cloud service's applications are not exposed with misconfigurations and over-permissive.

Cloud security breaches of 9 companies

Disney+

Incident: Loss of credentials

Cause: Credential stuffing

Impact: Legitimate users locked out of their accounts, discouraged new subscribers

Preventive controls: Multi Factor Authentication(MFA)

Learning:

Multi Factor Authentication(MFA), proper risk assessment and incident response strategy.

Cloud security breaches of 9 companies

Dow Jones

Incident: Sensitive data(information about Politically Exposed Persons (PEP), their associates and companies to which they are linked, national and international government sanction lists) was exposed

Cause: AWS-hosted Elasticsearch database left open on the Internet without a password

Preventive controls: Choosing a cloud vendor carefully and validating their work

Learning:

Data should never be stored in the cloud without password protection.

Cloud security breaches of 9 companies

GitHub

Incident: Loss of availability for some time

Cause: Distributed Denial of Service(DDoS) attack

Preventive controls: Business Continuity Management & Operational Resilience

Learning:

Expect attacks and be prepared for it

Cloud security breaches of 9 companies

Imperva

Incident: Exposure of a database snapshot containing emails and hashed and salted passwords

Cause: Compromise of an Imperva cloud server led to unauthorized use of an administrative API key in one of the production AWS accounts

Preventive controls: Double check configured controls

Learning:

Ensure proper cloud security architecture and testing of controls.

Cloud security breaches of 9 companies

Tesco

Incident: Loss of personal data of customers

Cause: Lack of authentication mechanism to access data stored on public cloud used by the web application

Preventive controls: Sufficient Identity and Access Management

Learning:

Ensure vendor checks and Identity and Access Management .

Cloud security breaches of 9 companies

Tesla

Incident: Account Hijacking of AWS access credentials leading to access to unsecured Kubernetes administrative interface

Cause: Misconfiguration of secure authentication mechanisms within the Kubernetes console provided access to confidential data including credentials.

Preventive controls: Sufficient Identity and Access Management

Learning:

Proper credential management

Cloud security breaches of 9 companies

Zoom

Incident: Information shared in Zoom meetings

Cause: Credential stuffing

Preventive controls: Implementing single use meeting IDs and random meeting pins

Learning:

Proper threat modeling.

Cloud security breaches of 9 companies

Equifax

Incident: Loss of sensitive information(Personally Identifiable Information, SSN, bank account numbers, credit scores, limits, balances) of over 105 million customer accounts

Cause: Not patching Apache Struts, an open source development framework CVE 2017-5638

Impact: Large financial settlement, staff loss

Preventive controls: Patch management

Learning:

Patch regularly and often.

Summary

Cloud Security – Evolving landscape

Perform sufficient threat modeling
Identity and Access Management(IAM)
Vulnerability Management and regular patching