Security Study Notes

Andrew Brown

Shared Responsibility Model

Customers are responsible for Security **in** the Cloud. **AWS** is responsible for Security **of** the Cloud

Key Points

Customer Responsibilities

- **Main Responsibilities**
  - Data (Customer data)
  - Configurations (Operating, Network, and Firewall)
- **Other Responsibilities**
  - Platforms
  - Applications
  - Identity and Access Management (IAM)
  - Client-side data encryption
  - Data integrity authentication
  - Server-side encryption (File system and/or data)
  - Networking Traffic Protection (encryption, integrity, identity)

AWS Responsibilities

- **Main Responsibilities**
  - Hardware
  - Operation of Managed Services
  - Global Infrastructure
- **Other Responsibilities**

- Software
  - Compute
  - Storage
  - Database
  - Networking
- Global Infrastructure/ Hardware
  - Regions
  - Availability Zones
  - Edge Locations

AWS Compliance Programs

Compliance Programs: A set of internal policies and procedures of a company to comply with laws, rules, and regulations or to uphold business reputation.

Key Points

- use if you need to be compliant and want to utilize cloud computing and specifically AWS, but you have one problem.
- compliance programs meet different kinds of standards Eg. HIPPA standards for hospitals
- the infrastructure environment is guaranteed and will have a badge of approval

You can learn more about compliance and the badges AWS provides on the AWS Compliance Programs page.

AWS GuardDuty

GuardDuty is a **threat detection service** that continuously monitors for malicious and suspicious activity and unauthorized behavior.

IDS/IPS

Intrusion Detection System and Intrusion Protection System is a device or software application that monitors a network or systems for malicious activity or policy violations

Key Points:

- GuardDuty uses Machine Learning to analyze the following AWS logs:
  - CloudTrail logs
  - VPC Flow logs
  - DNS logs
- It will alert you of **findings** which you can use to automate an incident response via CloudWatch events or. with 3rd party services

AWS Shield

AWS Shield is a managed DDoS(Distributed Denial of Service) protection service that safeguards applications running on AWS.

What is a DDoS Attack?

A malicious attempt to disrupt normal traffic to a website by flooding the website with a large amount of fake traffic.

Key Points

All AWS customers benefit from the automatic protections of **AWS Shield Standard** at no additional charge.

When you router your traffic through **Route53** or **CloudFront** you are using **AWS Shield Standard**

Protects you against Layer **3, 4, and 7** attacks

- 7 Application
- 4 Tranport
- 3 Network

Shield Standard vs Shield Advance

Shield Advance benefits:

- For additional protection against larger and more sophisticated attacks.
- You get visibility into attacks and 24/7 access to DDoS experts for complex cases
- Available on:
    - Amazon Route53
    - Amazon CloudFront
    - Elastic Load Balancing
    - AWS Global Accelerator

AWS Web Application Firewall (WAF)

AWS WAF protects your web applications from common web exploits.

Key Points

- Write your own **rules** to *allow* or *deny* traffic based on the contents of an HTTP request
- Use a **ruleset** from a trusted AWS Security Partner in the AWS WAF Marketplace
- WAF can be attached to either **CloudFront** or an **Application Load Balancer**
- Helps protect web applications from the attacks covered in the OWASP Top 10 most dangerous attacks

Key Management Service (KMS)

KMS is managed service that makes it easy for you to create and control the encryption keys used to encrypt your data.

Key Points

- KMS is a multi-tenant HSM (hardware security module)
- Many AWS services are integrated to use KMS to encrypt your data with a simple checkbox
- KMS uses Envelope Encryption

Envelope Encryption

When you encrypt your data, your data is protected but you have to protect your encryption key. When you encrypt your data with a master key as an >additional layer.

Amazon Macie

Macie is a fully managed service that continuously monitors **S3 data access** activity for anomalies and generates detailed alerts when it detects a risk of unauthorized access or inadvertent data leaks.

Key Points

- Macie works by using Machine Learning to analyze your CloudTrail logs
- Macie will identify your most at-risk users which could lead to a compromise
- Macie has a **variety of alerts**:
  - Anonymized Access

- Config Compliance
- Credential Loss
- Data Compliance
- File hosting
- Identity Enumeration
- information Loss
- Location Anomaly
- Open Permissions
- Privilege Escalation
- Ransomware
- Service Disruption
- Suspicious Access

Virtual Private Network (VPN)

A VPN lets you establish a secure and private tunnel from your network or device to the AWS global network.

Two types:

1. **AWS Site to Site VPN:** Securely connect on-premises network or branch office site to VPC
2. **AWS Client VPN:** Securely connect users to AWS or on-premises networks

AWS Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

Key Points

- The AWS inspector is a tool that runs **security benchmarks** against your EC2 instances.

- You can run a variety of security benchmarks

- The inspector can perform both **Network** and **Host** assessments

- One popular benchmark you can run is by the Center for Internet Security (CIS) which has *699 checks.*

Penetration Testing

PenTesting is an authorized simulated cyberattack on a computer system performed to evaluate the security of the system.

Key Points

- You are permitted to try PenTesting on AWS.

- There are permitted and prohibited activities when PenTesting on AWS

Permitted Services for PenTesting:

- EC2 instances, NAT Gateways, and ELB
- RDS
- CloudFront
- Aurora
- API Gateways
- AWS Lambda and Lambda@Edge functions
- Lightsail resources
- Elastic Beanstalk environments

Prohibited Activities:

- DNS zone walking via Amazon Route 53 Hosted Zones
- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, and Simulated DDoS
- Port flooding
- Protocol Flooding
- Request Flooding (Login request flooding, API request flooding)

AWS Artifact

AWS Artifact is a no cost, self-service portal for on-demand access to AWS' compliance reports.

Key Points

- Reports available in AWS Artifact:
  - Service Organization Control (SOC) reports
  - Payment Card Industry (PCI) reports
  - certifications from accreditation bodies across geographies and compliance verticals
- Agreements available in AWS Artifact
  - Business Associate Addendum (BAA)
  - the Nondisclosure Agreement (NDA).

Security Groups vs Network Access Control Lists (NACLs)

Security Groups

- Act as a firewall at the instance level
- Implicitly denies traffic
- You create **Allow** rules
  - Eg. Allow an EC2 instance access on port 22 for SSH

Network Access Control Lists (NACLs)

- Acts as a firewall at the subnet level
- You create **Allow** and **Deny** rules
  - Eg. Block a specific IP address known for abuse