CLOUD SECURITY & COMPLIANCE

Adam Lloyd – R00117318 – Web Development

TABLE OF CONTENTS

Table of Contents 1

Introduction 2

Physical Security 3

Unauthorised access 3

Power loss and Fire 3

Hypervisor Security 4

Host OS Compromise 4

Guest OS Compromise 4

Access Management 5

Identity Access Management 5

Policy Decision/Enforcement Points 5

Multi-tenancy 6

Data Encryption 6

Types of Attack 7

Man in the Middle Attacks 7

IP Spoofing 7

Port Scanning 7

Packet sniffing 8

Distributed Denial Of Service (DDoS) Attacks. 8

Incident Response 9

Compliance 10

Important Regulations 10

EU Data protection Act 10

HIPAA 10

USA Patriot Act 10

PCI DSS 10

AWS Compliance 11

Shared responsibility model 12

Appendix 13

References 14

INTRODUCTION

With the inherent value that cloud services provide and the high level of adoption by organisations large and small, moving your data infrastructure to the cloud presents significant security and compliance challenges both to the customer and to the cloud provider themselves.

From mitigating external intrusion attempts to ensuring data on multi tenancy systems is compliant with all relevant regulations, there are many concerns which must be addressed to ensure that a cloud architecture and critical data contained within is secure and compliant.

This report will explore the concerns related to the above and how they are mitigated with a look at how Amazon achieve this using their shared responsibility model.

PHYSICAL SECURITY

Before the hypervisor, before the virtualisation and the web services, the base layer of the cloud architecture is the physical metal implementation of the system in a data centre, the physical machines that host all the services and store all the critical data for cloud provider's customers. It is at this level that the system needs to be protected and secured and, as the systems are physical, so are the risks involved.

UNAUTHORISED ACCESS

To provide reliable and accessible cloud services to customers around the world, cloud providers need to have data centres in multiple locations. These locations need to be secured with conventional security measures such as security staff, alarms, and secure areas as, were someone to gain access to these data centres directly, they would be able to interfere with the cloud services at the base level which would be a severe breach of security.

To minimise this risk, Amazon datacentres are houses in inconspicuous facilities which are protected by military grade security and having physical access to the facility controlled and monitors by professional security and modern intrusion detection systems [1].

POWER LOSS AND FIRE

Outside of threats from unauthored individuals, there are further physical threats which may arise from negligence or factors outside of the control of the data center managers. These would be in the form of power outages and fires.

Power outages can be a somewhat common occurrence depending on the part of the world but even when they are a rare occurrence they present a significant risk to the service of a data center and the supported cloud services. To minimize the risks relating to this, cloud providers such as Amazon implement a fully redundant power system to make them independent from the national electricity grid along with uninterruptible power supplies (UPS) to ensure that, should these systems fail, there will be power supplied for a certain amount of time to resolve the issue and return to normal operations.

Fire, sometimes resulting from accidental, negligent or uncontrollable factors would be catastrophic to data center services and with the heat generated by them, it is a real concern. To manage this risk, automatic fire detection and suppression systems are installed.

HYPERVISOR SECURITY

The Hypervisor is what enables the abstraction of multiple virtual machines on an underlying host machine thus enabling the virtualisation which is a major component of cloud architectures. This software allows multiple virtual machines to share the hosts resources such as CPU and memory and scale the provided resources up and down to each virtual machine on demand in some cases.

Its role in cloud architecture makes it the most integral part of a cloud security solution and, as Matthew Garret stated in 2014 [2], "*Once someone gets to the hypervisor then it's game over*".

This is a very accurate statement in that, gaining access to the application which controls all other applications would give the attacker supreme control over the system, over all systems within the host system.

There are two main ways in which the Hypervisor can be compromised, either via the host operating system (OS) or the guest operating system.

HOST OS COMPROMISE

The host OS refers to the system that the hypervisor is installed on, the system which houses all the virtualised systems. A compromise of the host OS would be extremely severe as the attacker would gain access to all the hosted guest systems. Security for the host OS is the responsibility of the cloud provider and relies on the security of the provider's infrastructure.

GUEST OS COMPROMISE

The guest OS is a virtualised system running on top of the hypervisor which provides an environment for the cloud customer to use. Due to the security measures employed by the host OS a compromise in this area would not be as severe as the breach would likely only affect the cloud customer's systems as the hypervisor would prevent the attacker from breaking out of the customer's virtual system.

ACCESS MANAGEMENT

The ease of access to a cloud based infrastructure is one of the benefits, allowing users on demand access to their critical data wherever they are in the world by logging into their cloud via a web based service. Once authenticated the user will likely require access to an active directory based service or virtual desktop or server and a system must be in place to ensure that only the authorised users have access to sensitive data within the cloud.

IDENTITY ACCESS MANAGEMENT

Identity Access Management (IAM) is a framework for business processes that manages user access privileges to ensure that access to sensitive and private data is restricted to authorised users only and implements open standards such as SAML to create user access roles [3].

AWS offers multiple services which ensure users have the correct access rights and minimizes the security risks inherent in the unauthorized access of private data [4]. AWS Identity and Access Management (IAM) allows customers to set individual user permissions across all their AWS based cloud infrastructure, AWS Multi-Factor Authentication allows for extra security measures using hardware authentication devices such as USB dongles or mobile devices to reinforce the security of the IAM and AWS Directory Service which integrates with corporate directory services to allow access to private data once authenticate. [5]

AWS provides native identity and access management integration across many of its services plus API integration with any of your own applications or services as part of an Authorization, authentication and auditing (AAA) service.

POLICY DECISION/ENFORCEMENT POINTS

In systems which implement the above there are two main areas where the system will determine if access is to be given to the requesting user account. The policy enforcement point (PEP) which is usually a network device on which policy decisions are carried out when required [7] and a policy decision points (PDP) which are areas in the system where the PEP will be requested to provide a decision.

An example of this within an AWS based cloud architecture would be an already logged in user trying to access a secured network area such as a college staff section. The PDP is the event triggered from the user trying to access the area and the PEP is the IAM service determining if said user has access to secured area.

MULTI-TENANCY

Multi-tenancy is a common attribute of both public and private clouds [8] and refers to software architecture be it IaaS, PaaS or SaaS, shared between multiple users (Tenants) who share access to a single physical device. These tenants can be from multiple companies or business units in the same company and even with the hypervisor controlling access there is a risk that attackers who gain access to one users systems could gain access to the sensitive data stored within other tenant's virtual machines.

These risks can be managed by encrypting the user's data using a tenant-owned key which would be required to read the data. Using this method, even if the data was compromised the data would be useless without said key.

Aws offers data encryption capabilities for their storage services (EBS, S3, etc.) and flexible key management with the AWS Key Management Service which allows users to directly control their own security keys [5].

DATA ENCRYPTION

There are three options for encrypting user data on multi tenancy systems, Client, Network, and Proxy.

Client encryption where data is encrypted before being sent to the user so the data can be freely transported around the network with minimal risk as it is encrypted from the start.

Network encryption where standard network security methods such as SSL and SSH are employed to secure the data on route to the user.

Proxy based encryption involves the data being sent to an intermediary application or server which encrypts the data before forwarding it on to the user and vice versa. This is often a good option for integrating cloud systems with existing legacy architectures.

TYPES OF ATTACK

There are two main types of attacks which cloud based systems are vulnerable to, the first is the conventional “hack” whereby an individual gains unauthorized access to a system by gaining the users login credentials or their data.

MAN IN THE MIDDLE ATTACKS

A man in the middle attack involves the attacker intercepting network traffic between the client and server and, before forwarding it to its intended destination, modifying it to their own ends. To combat this, AWS endpoints are protected with SSL certificates which provide secure authentication for client server communications [5].

IP SPOOFING

IP Spoofing, like the above, involves the attacker pretending to be a part of the system that they are not. A system may be secured in a way that restricts access to only allow connections from a specific IP address or range of addresses. An attacker could interfere with their own network traffic to make it seem to the target system that the request originated from an authorized IP.

This is handled in AWS by the configuration of the host OS within their infrastructure which disables EC2 instances from sending spoofed network traffic by ensuring that all traffic coming from the instance matches the IP/Mac address of the virtual machine.

PORT SCANNING

Port scanning is the process by which an application is used to query the ports of a target system, usually in numerical order, to see if there is any response [9]. If a system responds on a port, then there is likely a service running on that port on the target system. For example, if a system has port 80 open then it may well have a web server running on it. This is all useful information which an attacker can use to exploit vulnerabilities in a system.

Amazon handles this by immediately blocking any port scans detected and running port scans from any of their EC2 instances on anything but their own network is prohibited by their acceptable use policy [10]. Customers, being responsible for their own network security should ensure that all non-essential ports are closed on the instances to further prevent such attacks.

PACKET SNIFFING

Packet sniffing is a method by which an application is used to analyse network traffic and display it to the user in a way that can be understood. The information in these network packets could be usernames, passwords, IP addresses and other content which would be easily visible to an attacker if it were not encrypted by SLL or other means.

With multiple systems being on the same host OS it may be possible that users of another system will be able to “sniff” packets form your network [1]. Amazon, for example, provides ample protection for this though by preventing this at the host OS level but does encourage users to encrypt all sensitive data communications.

DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS.

The above types of attack would give the attacker access to some or all the compromised users data and is the most severe but this is not the only way in which a system can be compromised.

If an attacker cannot get into a system, or doesn’t event wish to, they can use a DDOS attack to prevent the system from functioning correctly. This is commonly used as an attack against web services or web sites and involves the attacker making multiple (sometimes millions) requests to the server in a short period. This results in the server or service becoming extremely slow as it tries to process the requests and in many cases crashing the service altogether.

As many, if not all, cloud services are web based they are particularly vulnerable to this especially given the relative ease of executing one of these attacks. To combat this, large cloud provider endpoints, like Amazon’s are hosted on their world-class infrastructure and often a team of site reliability engineers work daily to ensure that the system is robust and resistant to such attacks [11]. Furthermore, systems are spread out over multiple internet service providers and geographic locations and have redundant backups should one system go down.

INCIDENT RESPONSE

With all the above systems and contingencies for handling security breaches, it is inevitable that some will still occur. It because of these cases that an incident response plan is required and that incident response time is low to ensure minimal loss of service.

R. Bejtlich defines an indecent as any violation of policy, law, or unacceptable act that involves information assets [12].

Given that an incident has occurred, some or all the established security measures have likely been circumvented so, aside from logging the malicious activity they are redundant. It is at this point that automated systems and decisions cannot be trusted and human intervention is required.

The first action, as with conventional computer systems, a virus scan and network security suite could be run to ensure no malware has entered the system. Changing any relevant user credentials may also be a prudent line of action but, as it may not be clear how far the intrusion has gone, and with critical systems being vulnerable it may be the safest option to roll back the system to a previous, secure snapshot [12]. This, in many cases, would be a last resort as the most recent snapshot will likely have been generated outside of peak hours and could be upwards of 24 hours old. This means that, should a rollback occur, user data will be lost potentially costing them and the cloud provider substantial amounts of money.

COMPLIANCE

Cloud is a highly-regulated industry [13] due to the variety of sensitive data being stored on cloud platforms. Governmental or financial system, for example, may be hosted entirely in the cloud resulting in extremely sensitive data being stored on systems in data centres in many parts of the world. This presents a problem in that regulations relating to that data may vary from country to country and regulations that apply to one type of system may not apply to another on the same host OS.

IMPORTANT REGULATIONS

There are many regulations governing data, there are some that cloud providers must adhere to due to the sensitive nature of the data they store and the locations in which they store this data.

EU DATA PROTECTION ACT

The EU data protection act is an important regulation for operations in the cloud. Even if the cloud provider is based in the US or elsewhere, to provide services to EU customers or store any relevant data in EU governed states they need to be compliant.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a regulation which applied to health information [14]. This act applies stringent rules to the storage and transfer of health information and with many health and insurance companies migrating their services to the cloud it is very important.

USA PATRIOT ACT

This act states that the US government can access data stored outside of the US by US based cloud service providers or subsidiaries. This also has implications for private data as, under the guise of national security the US can bring this act to bear to gain access to private data.

PCI DSS

The payment card industry data security standard (PCI DSS) consists of 12 requirements for the storage and transmission of card payment data. These standards apply to any system that handles card payment data and with many ecommerce sites being entirely cloud based, cloud providers must be fully compliant with these standards to manage this data.

AWS COMPLIANCE

With an array of acts and regulations potentially applying to all their customer’s data stored in the cloud, Amazon must be compliant with all applicable regulations but they cannot be accountable for everything much like the customer cannot be responsible for the larger scale compliance issues. It is using a shared responsibility model that AWS, like many other cloud providers, separates the responsibility for security and compliance [15].

SHARED RESPONSIBILITY MODEL

With all the inherent risks in cloud computing and the measures needed to counteract them, the effort needed to secure all data on a system is substantial and, with the cloud customers having near full control over their cloud infrastructure there is no effective way that providers can enforce the standards required to ensure there are no security breaches.

An example of how to handle this is by operating on a shared responsibility model like the one Amazon uses. This model details the areas for which the cloud provider in responsible for security and compliance and the areas which the cloud customer is [16].

The cloud provider is responsible for the security of the cloud itself, for the security of the data centers, the physical machines and the infrastructure. Should a breach occur in one of these areas then cloud provider would be liable for damages caused as, per their service level agreement it is their responsibility to ensure these areas are secured.

However, the cloud customer is responsible for the security of systems running within the cloud, for configuring user privileges and enforcing password standards for example. Should a breach occur due to lack password complexity or an employee's credentials being phished then the cloud customer would be liable for any damage caused.

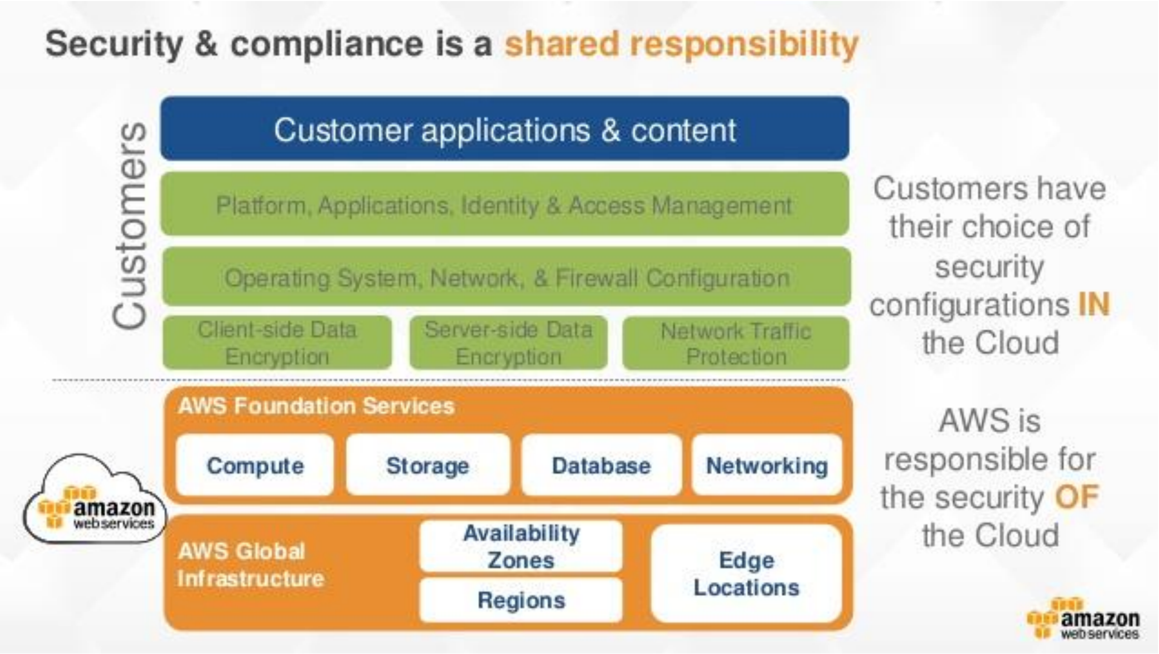
Security & compliance is a shared responsibility
Customers
Customer applications & content
Platform, Applications, Identity & Access Management
Operating System, Network, & Firewall Configuration
Client-side Data Encryption
Server-side Data Encryption
Network Traffic Protection
Customers have their choice of security configurations IN the Cloud
AWS Foundation Services
Compute
Storage
Database
Networking
AWS Global Infrastructure
Availability Zones
Regions
Edge Locations
AWS is responsible for the security OF the Cloud
amazon web services

Figure 1. AWS Shared responsibility model

APPENDIX

AWS – Amazon Web Services

IaaS – Infrastructure as a Service includes virtual servers and network services.

PaaS – Platform as a service is a platform allowing customers to develop applications on top of managed cloud infrastructure.

SaaS – Software as a service is a model for providing on demand software hosted in the cloud.

Hypervisor – The software running on a host operating system which provides virtualisation functionality.

Virtualisation - The act of creating a virtual version of something, including virtual computer hardware platforms, operating systems, storage devices, and computer network resources.

Compromise – An event resulting in the unauthorised access or service disruption of a service.

AAA - A framework which a term for a larger framework for managing user rights, access to resources and monitoring usage of the system [6].

API – Application Programming Interface

IP Address – A numerical label assigned to each device

EC2 - Amazon Elastic Compute Cloud (Amazon *EC2*) is a web service that provides resizable compute capacity in the cloud.

SSL – Secure Sockets Layer is the standard security technology for establishing an encrypted link between a web server and a browser.

Active Directory - A centralized and consistent system that automates network administration of user data, security, and circulated resources.

OS – Operating system

REFERENCES

[1] AWS, “Amazon Web Services:,” 2008.

[2] S. J. Vaughan-Nichols, “Hypervisors: The cloud's potential security Achilles heel,” ZdNet, 29 03 2014. [Online]. Available: http://www.zdnet.com/article/hypervisors-the-clouds-potential-security-achilles-heel/. [Accessed 05 12 2016].

[3] C. Epps, “3 Key Steps for Implementing Identity Access Management (IAM) in the Cloud,” Onelogin Blog, 06 01 2015. [Online]. Available: https://www.onelogin.com/blog/3-key-steps-for-implementing-identity-access-management-iam-in-the-cloud. [Accessed 04 12 2016].

[4] AWS, “AWS Identity and Access Management,” AWS, 04 12 2016. [Online]. Available: https://aws.amazon.com/documentation/iam/. [Accessed 04 12 2016].

[5] AWS, “AWS Cloud Security,” AWS, 04 12 2016. [Online]. Available: https://aws.amazon.com/security/. [Accessed 04 12 2016].

[6] TechTarget, “authentication, authorization, and accounting (AAA),” TechTarget, 10 11 2014. [Online]. Available: http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting. [Accessed 05 12 2016].

[7] CCSkguide, “Policy Decision points,” CCSKguide, 05 12 2016. [Online]. Available: https://ccskguide.org/policy-decision-points-policy-enforcement-points/. [Accessed 05 12 2016].

[8] S. Kajeepeta, “Multi-tenancy in the cloud: Why it matters,” Computer World, 12 03 2016. [Online]. Available: http://www.computerworld.com/article/2517005/data-center/multi-tenancy-in-the-cloud--why-it-matters.html. [Accessed 04 12 2016].

[9] R. Christopher, “Port Scanning Techniques and the Defense Against,” 2015.

[10] AWS, “AWS Acceptable Use Policy,” AWS, 05 12 2016. [Online]. Available: https://aws.amazon.com/aup. [Accessed 05 12 2016].

[11] Linkedin, “LinkedIn,” LInkedin, 04 12 2016. [Online]. Available: https://www.linkedin.com/jobs/amazon-site-reliability-engineer-jobs. [Accessed 04 12 2016].

[12] A. Kliarsky, “Incident Response in Amazon EC2: First Responders,” SANS Institute, 2016.

[13] B. Coat, “Cloud Privacy and Compliance,” Blue Coat, 05 12 2016. [Online]. Available: https://www.bluecoat.com/resources/cloud-governance-compliance. [Accessed 05 12 2016].

[14] “HIPAA,” HHS, 05 12 2016. [Online]. Available: http://www.hhs.gov/hipaa/index.html. [Accessed 05 12 2016].

[15] AWS, “Amazon Web Services: Risk and,” 2016.

[16] AWS, “Shared Responsibility Model,” AWS, 05 12 2016. [Online]. Available: https://aws.amazon.com/compliance/shared-responsibility-model. [Accessed 05 12 2016].