How to Cite:
Soms, N., Oswalt, M. S., & Santhosh, K. P. (2022). A case study on cloud security controls. *International Journal of Health Sciences*, *6*(S1), 11374–11380.
https://doi.org/10.53730/ijhs.v6nS1.7778

A case study on cloud security controls

Nisha Soms
Department of CSE, Sri Ramakrishna Institute of Technology
Email: nishasoms@gmail.com

Oswalt Manoj S
Department of CSE, Sri Krishna College of Engineering and Technology, Coimbatore, India
Email: oswaltmanoj1986@gmail.com

Santhosh Kumar P
Department of CSE, Sri Ramakrishna Institute of Technology
Email: santhosh23mj@gmail.com

***Abstract*---**Cloud computing is a highly discussed topic in today's technical and economic world. Many big players of the software industry are concentrating more on cloud services. Companies are racing to incorporate cloud infrastructures into their businesses or provide their own. While speaking of development, we cannot let down an important aspect called security. A misconfiguration or a minor vulnerability in a way the services are handled may result in a huge loss of data, which in turn would result in great loss of revenue. Money can be generated in one way or the other, but reputation once lost cannot be brought back again. In this paper, we discuss about the security controls and misconfigurations that frequently happen in AWS environments and discuss ways to avoid it using Capital One Data Breach as an example.

***Keywords*---**Cloud computing, security controls, case study, Capital one data breach, cyber attacks, AFS, SSO, IAM.

Introduction

Cloud Computing can be defined as an on-demand delivery of IT resources over the internet with pay-as-you-use pricing. Instead of buying, owning and maintaining physical servers and data centers you can access services and technologies from the cloud providers[1]. For example, Amazon offers a Simple Storage Service (S3) that offers scalability, availability, security and performance.[2] This means customers of all sizes and industries are able to employ it to store and protect any amount of data for a mixture of use cases, such

as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. The S3 buckets work in four steps.[3]

- First, we create access points to the new or existing S3 buckets.
- Next, we configure these access points in terms of security like allowing and restricting certain access.
- We can also limit access to those access points only from the VPC alone.
- Now scalability comes in handy since the Access points and S3 buckets can be expanded or shrinked.

Security of data is assessed by the CIA triad which ensures that a given data is secured from the malicious actors. AWS provides all these security controls in their Cloud platform, yet, a small disorder has led to a huge incident.

Capital One is the fifth largest consumer bank in the US. It is a highly regulated industry and also spends a lot to maintain their cyber security posture. Recently, it faced a huge data breach exposing 100 million US people's data and 6 million Canadian data which people provide during their credit card application. The interesting thing is that there is no group behind it. All this havoc was performed by a single programmer. [4]

This article is organized as follows. In section 2, the security challenges in cloud are presented. In section 3, the case study on Capital One Data Breach and its reveal on some poor security controls is discussed. In section 4, the security controls available in AWS are described. In section 5, conclusion is prepared.

Security Challenges in Cloud

Security is a major concern while designing networked systems. "No system is 100% secure" fits right in for cloud too. Since cloud computing is an emerging technology, it would have security challenges specific to its own. We will discuss some of the key security challenges in cloud here and in the next section we shall discuss a case study which depicts about the happenings where some security controls do not fall in place.

Cloud outside IT Visibility

With the flourished advent of cloud, organizations have accelerated in IT delivery and business agility. Meanwhile it also opens up security holes, leaving a company exposed to cyber attack. For example, the development team in an organisation may be working on the Cloud, creating new accounts and doing much more as their needs without bearing security in mind and its visibility to the IT department. This poses a security risk because the IT team cannot extend their security services to things which they are unaware of that it is happening.

Incomplete control over data

There is lack of access controls over sensitive data. That is, there is a lack of definition on who has access to the sensitive data that is stored in the cloud.

There should be strict policies that restricts upon who can access the data and how.

Theft of Data

Data that is hosted in the public or even in the private cloud is subject to theft by malicious actors. Malicious actors go behind the sensitive data wherever it is; either on-premise or on the cloud. They are a constant threat to data.

Lack of Skilled Staff

Cloud computing is an emerging technology and it continues to evolve. So there is a lack of skilled professionals. Hence it is essential for the service providers to inculcate continuous learning among professionals to gain expertise in securing the cloud infrastructure from all kinds of malicious activities and to adapt to the its rapid changing nature.

Insider Theft

Insiders are the greatest threat to an organisation. Nearly $3/4^{th}$ of the data breaches are caused by the insiders. The huge problem is that it is not easy to identify the malicious insiders at an early stage, especially those who leaves organisations and revengefully pose risks.

Lack of Security controls

Some organizations operate both on cloud as well as on-prem. The security risk here is that when more operational services or data accessing cum processing in the cloud increases, the operations on on-prem drops resulting in infrastructure exposed to attacks.

Advanced Attacks

Since cloud is an emerging technology, organisations do not have all the time to fully study it. On the other hand, the adversaries invest a lot of time for which they reap by coming up with new and advanced TTPs and attacking the organisations by the time the staff adapt to the cloud environment.

Inability to Monitor

Cloud is a great technology to apply continuous deployment. Also the cloud technology in itself is new; hence there is some inability in monitoring the cloud infrastructure and its running applications for vulnerabilities. Ethical hackers are of great help in this context.

Spread of Attack

A whole IT infrastructure can be migrated to the cloud, either private or public. So when a new virus, worm or any new form of advanced attack hits the cloud, it can easily spread laterally and affect the whole infrastructure. This effect becomes even worse when the IT services are deployed in public cloud.[5][6].

Capital One Data Breach Case Study

Capital One is a company that highly values technology and is a leading bank in the US to adopt cloud computing technologies. Capital One believes in the motto - "We're Building a Technology Company that does Banking." It was successful in moving its on-premise data centers to the cloud such that even Amazon lists this cloud migration as a renowned case study. This migration of services was planned for reducing or eliminating the costs adhered to run the servers on premise.

On July 17 2019, an outsider emailed Capital One that she saw all the sensitive data posted up on a Github page. Immediately complaint was filed and the hacker was arrested by the FBI later. Later Investigations revealed the steps taken by the hacker to perform this breach. Paige A. Thompson, a programmer at Amazon, wrote a script to identify all the AWS Instances possessing misconfigured firewall. This allowed her to execute commands on those instances. The script does run exactly three commands, first it fetched the security credentials, second it listed the available buckets and finally, it copied the data from the buckets to the local machine of the attacker. The overview about Capital One Data Breach is depicted in Fig.1.

What got stolen?	100M US SSNs, 1M Canadian SINs
What was the impact?	• $250K fine, 5 yrs. in jail for hacker • Estimated breach costs of over $300M
How did it happen? Root cause?	• Cap One Firewall Misconfiguration provided access to their AWS buckets. Server-Side Request Forgery (SSRF).
How could it have been prevented?	• Firewall Review • Automated hybrid cloud security scanning.

Fig.1. A quick look about Capital One Data Breach

The steps involved in the cyber attack are summarized as follows:

1. The analysis showed the packets from the TOR and VPN services were used to hide the source IP address.
2. The Firewall (Apache's ModSecurity) that was provided with the AWS instance was misconfigured, causing relay to commands to the private server.
3. The attacker took advantage of the misconfiguration and ran an SSRF attack to fetch the access credentials (AccessKeyID and SecurityAccessKey).
4. Using the credentials, the attacker gained access and listed all the available AWS S3 buckets of Capital One.
5. Then by running the sync command, the attacker copied all the data from the buckets to the local machine, which is nearly 700 buckets according to the report.[4]

Presently, Capital One has strong governance practices regarding cyber security and is stringently following strict policies in the applied normative frameworks.

Security Controls in the Cloud (AWS)

When we get Cloud as a service from a provider, security becomes a shared responsibility for both the client and the provider. Amazon exactly does that, it operates under a shared security responsibility model, where the client is responsible for security of the applications being deployed and AWS is responsible for the underlying cloud infrastructure.[6].

Securing Infrastructure

The infrastructure is secured using the following services provided along with the AWS.

- Firewalls: AWS provides firewalls to protect our infrastructure from malicious actors. It provides WAF, to which we could configure rules to allow benign traffic and block malicious ones. If it is a large organization hosting multiple applications, they can deploy multiple WAFs and manage all of them at once using the Firewall Manager [7]. If it is difficult to configure rules, they may use some preconfigured templates or buy them from the AWS marketplace. Simple misconfigurations in this firewall lead to that breach in Capital One.
- DDoS Mitigation: All AWS instances are by default protected against common DDoS attacks by what is called AWS Shield. In addition, there is a provision to subscribe the AWS Shield Advanced to get additional help and features for protection against DDoS attacks. There are still other methods like Amazon CloudFront and Route53 to ensure availability of the systems under attack. AWS provides firewalls to protect the infrastructure from malicious actors. It provides WAF, to which rules can be configured to allow benign traffic [8].
- Traffic Encryption: All traffic on the AWS global as well as local networks connecting AWS are automatically encrypted thereby providing secured facilities.

Inventory and Configuration Management

AWS recommend a range of tools to permit ones to move fast, while still enabling them to ensure that their cloud resources comply with organizational standards and best practices.

- Deployment Tools: AWS Deployment tools manage the creation and decommissioning of AWS resources according to organization standards.
- Inventory and configuration management: An Inventory and configuration management tool identifies AWS resources and then track and manage changes to those resources over time.
- Template definition and management tools: Template definition and management tools are used to create standard, preconfigured, hardened virtual machines for EC2 instances.

Data Encryption

AWS suggest the ability to add a layer of security to our data at rest in the cloud, providing scalable and efficient encryption features.

- Data at rest encryption capabilities: Amazon provides encryption in most of its services. For instance, S3 Buckets and Amazon EBS use the Server Side Encryption (AES-256) and Amazon RDS supports Transparent Data Encryption(TDE).
- Flexible key management options: AWS Key Management Service (KMS) functions to create and manage cryptographic keys. The organization can either have full control over the keys or have the AWS manage it for them. Those keys are stored in HSM (Hardware Security Modules) by AWS in order to meet the compliance requirements for business. AWS uses Server Side Encryption (SSE) for transmission of sensitive data.

In addition, AWS offer APIs to incorporate encryption and data protection with any of the services developed or deployed in an AWS environment.

Identity and Access Controls

AWS offers various capabilities to define, enforce, and manage user access policies across AWS services.

- AWS IAM: Identity Access Management (IAM) lets one define individual user accounts with permissions across AWS resources such as AWS Multi-Factor Authentication for privileged accounts, which includes options for software and hardware-based authenticators. IAM can be used to grant employees and applications federated access to the AWS Management Console and AWS service APIs, using their existing identity systems, such as Microsoft Active Directory.
- AWS Directory Services: AWS Directory service for Microsoft Active Directory, also known as the AWS Managed Microsoft Active Directory, allows an organization to integrate their Active Directory environment to the cloud, which extends features and security.
- AWS SSO: AWS Single Sign-On (SSO) makes it easy to centrally manage access to multiple AWS accounts and business applications and provide users with single sign-on access to all their assigned accounts and applications from one place. With AWS SSO, one can easily manage access and user permissions to all of their accounts in AWS Organizations centrally.

Monitorig and Logging

AWS provides tools and features that enable the subscribed client to see what is happening in its AWS environment.

- AWS CloudTrail: AWS CloudTrail is a logging service in Cloud. In this facility, one can log in and monitor the account activity occurring in the cloud infrastructure. It logs actions done through a management console, SDKs, Command-line tools and other AWS services. This ensures security analysis easier.
- Amazon CloudWatch: CloudWatch functions as an Intrusion Prevention System (IPS) which collects monitoring and operational data as logs, metrics and events. This is used to detect anomalous behavior, set alarms, visualize logs and even take automated actions and also troubleshoot to keep the application functioning smoothly.
- Amazon GaurdDuty: It is a threat detection service that continuously monitors for malicious activities. It uses Machine Learning, anomaly detection and threat intelligence so it could prioritize risks by itself. By

integrating this service with CloudWatch, it is actionable and we could easily push this to existing SIEM.

In addition to all these promising features, Amazon provides security guidance and expertise through online tools, resources, support and professional services provided by AWS [9][10].

Conclusion

This paper describes the challenges in the cloud platform and explored a data breach involving a security misconfiguration in the cloud firewall. Also a detailed study about the security controls that are already provided by the Amazon is highlighted. The main objective of these security controls is to maintain security in the cloud infrastructure of an organization. Though these are well documented by the Cloud Service Provider, we end up with some security issues which indicate our lack of skill. Some may migrate to cloud knowing its advantages and some may avoid it fearing for the underlying security and privacy issues depending on their point of view. It would be better if there is a third party certification authority like the ISO to maintain the security and standards in the cloud environment.

References

[1] C.N. Höfer, G. Karagiannis, “Cloud computing services: taxonomy and comparison”, published on the Journal of Internet Services and Applications (Volume 2), pp. 81-94, January 2010.
[2] https://aws.amazon.com/s3/features/
[3] https://aws.amazon.com/s3/c=23&pt=1
[4] Nelson Novaes Neto, Stuart Madnick, Anchises Moraes G. de Paula, Natasha Malara Borges, “A Case Study of the Capital One Data Breach” published on the SSRN Electronic Journal, January 2020.
[5] https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/security-issues-in-cloud-computing.html
[6] https://aws.amazon.com/security/?nc1=f_cc
[7] https://aws.amazon.com/firewall-manager/?c=22&pt=11
[8] Amazon WhitePaper, “AWS Best Practices for DDOS Resiliency”, https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/aws-best-practices-ddos-resiliency.pdf#welcome, December 2019.
[9] L.Ertaul, S.Singhal, G.Saldamli, “Security Challenges in Cloud Computing” published on the proceedings of the International Conference on Security and Management, January 2010.
[10] Amazon WhitePaper, “Intro to AWS Security”, https://d1.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf?did=wp_card&trk=wp_card , January 2020