Sri Lanka Institute of Information Technology

Top 4 Threats on Cloud Computing

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT19957258	Edirisinghe A. D

Table of Contents

Abstract

The main purpose of this report is to provide an analysis about the top threats on cloud computing security and the future developments on this area of cloud computing security. The objective of this report is to make awareness about the emerging threats on cloud computing.

In adopting to cloud computing, what the users should be more serious about is security of the resources and infrastructure. Confidentiality, integrity and availability is totally dependent on the strength of the security methodologies and practices that is used to secure the highly sensitive and confidential data of users. Threats like Data breaches, misconfigurations, insecure interfaces and APIs and lack of cloud security architecture and strategy were the top security threats towards cloud computing.

At the end of this report, the future developments of cloud security services and who will be more responsible for the security of these services are defined. Outcome of this report has explained that the threats on cloud computing increase rapidly as the increasing growth of adaptation of cloud computing by different companies and how these threats should be mitigated and controlled.

1 Introduction

Computers are widely used in completing human tasks and humans demand an increasing amount of computing power every day. To fulfill this issue, a technology called cloud computing arise. The on-demand supply of computer hardware, IT resources and services through the internet with pay as you use pricing method is known as Cloud Computing. Raw computing power, disk storage, database storages and any type of technology functions or applications can be obtained through cloud computing.

Major companies like Apple, Microsoft, Google started using cloud computing to address the growing demands of their customers and to benefit the organizations through utilizing more computing power while reducing the costs of scalability and maintaining high valued hardware and software, and easy deployment of hardware and software.

Cloud computing is operated and accessed through the internet, due to this reason cloud computing will face many threats to the security of its assets and services provided. Confidentiality, integrity and availability can be easily compromised. Different types of threats can be identified as Data breaches, Account high jacking, Insider threat, Lack of cloud security and architecture and Insecure interfaces and APIs.

In this report, 4 major recent cloud computing threats and future evolution of different new threats will be addressed. The four major recent threats would be Data Breaches, Misconfiguration and inadequate change control, Lack of cloud security architecture and strategy, and Insecure interfaces and APIs.

2 Evolution of the topic

The concept of cloud computing started to spread quickly and the number of organizations and people who started to use cloud computing rapidly increased. The amount of confidential data stored and transmitted from server to client and client to server increased massively. The services like E-mail, social media platforms and other relative services provided by different companies through cloud computing increased. Due to these reasons, the threats like compromising confidentiality by stealing and viewing confidential and sensitive data, compromising integrity by injecting malicious codes using SQL injection techniques to modify or delete data and compromising availability of systems and platforms to its legitimate users by performing attacks like Denial of Service started to evolve.

Security Threat: Data Breaches

An incident where protected, highly sensitive and confidential information is stolen or release to public by an unauthorized individual can be identified as a data breach. Data breaches is not a new concept since data breaches were happening way before cloud computing technology arrived. In the past, attackers had to attack local area networks of companies to barge in to steal sensitive data but cloud computing has made it easier for attackers to breach data easily because the sensitive data is not stored in private local area networks. It is a matter of time until the attackers compromise a user credential of a user to log into the organization’s website to breach data. Data breaches can happen due to a malicious attack, human error or system malfunction.

The negative impacts of a data breach include the following:

1. Incident response and forensics costs incurred
2. Impacts on the brand name that will reduce the market value and reputation
3. Trust and faith of the users and partners will be impacted
4. Damage or loss of physical confidential and sensitive data

Examples of Data Breaches:

- 21 million users of Timehop were affected due to a data breach because of a cloud computing environment compromise. At the same time social media access tokens were also compromised [1]
- Millions of customer call log, short message service logs and credential were exposed in 2019 of Voipo, a telecom company which provides Voice over Internet Protocol (VoIP) services. All the call and message logs dating back to 2015 were exposed and detailed call records like who called, time of the call were contained in most of the exposed files. In total, 7 million call logs and 6 million messages were exposed. [2]
- In late 2016, Amazon Web Services (AWS) account of Uber was hacked and compromised personal information of 57 million users worldwide. [3]

There are many ways to mitigate these attacks of data breaches

- Implementing proper access controls on data and define who has access to what.
- Using proper encryption techniques to encrypt user credentials and other sensitive data.
- Having almost zero errors in misconfigurations of assets that are accessible through the internet.
- Having a well-tested incident response plan.

Misconfiguration and inadequate change control

When the computing assets are configured improperly, misconfigurations occur leaving the whole system vulnerable for malicious activity. Due to misconfigurations, confidentiality, integrity and availability of the system will be compromised allowing attackers to perform an attack easily.

Cloud computing environments are difficult to change in respective to traditional Information Technology which makes the common cause for misconfiguration in cloud environments when an effective change control is absent. Expansion of roles, automation and support to rapid change are the factors that the cloud computing is relying on.

One of the mains impacts would be the exposure of data that are stored in cloud repositories. The more the misconfiguration is undetected, the more severe the impact would be. So, the sooner the misconfiguration is found and configured correctly, the safer the system will be.

Examples for misconfigurations occurred recently:

- In 2018, a company named Exactis owned an unsecure Elastisearch database faced a massive data breach containing highly sensitive personal data that belongs to 230 million United States customers. Public level access was given to the database server when configuring. [4]
- In 2018, Highly sensitive proprietary information that belongs to more than 100 manufacturing companies was exposed by Level one Robotics, an engineering company that is specialized in process automation and assembly. The company list includes Ford, Toyota, Chrysler, Tesla, and Volkswagen. Allowing unauthenticated data transfer to any rsync client on the rsync (backup) server was the misconfiguration. [5]

Ways to minimize the misconfigurations would be:

- Implementing more suitable change control mechanisms and management approaches.
- Implementing an automated Real-time misconfiguration scanning system to scan misconfigurations on real-time basis.
- Being mindful while configuring cloud system because cloud systems are highly complex and dynamic.

Lack of cloud security architecture and strategy

One of the biggest challenges faced by the companies that are migrating parts of their IT infrastructure to public clouds are the security architecture implementation which will help to with stand Cyber-attacks. Many companies do not take this issue seriously because they think that shifting their IT stack into the cloud will be safe with the existing traditional security controls and architecture implemented in their traditional systems. Due to this reason, data is exposed to many kinds of cyber threats. To provide a strong security foundation in conducting the business activities on the cloud safely, necessary security architecture and security strategies should be implemented. To increase the visibility in cloud environments, leveraging native tools will reduce the risk and cost.

Financial loss, legal repercussions and fines, and reputational damages are some of severe impacts of successful cyber-attacks. So having a proper security architecture and strategy regardless of the size of the company is crucial for operating and successfully moving forward with cloud environments.

Example of recent issues due to lack of cloud security architecture and strategy:

- The data that belong to the Honda Connect App was exposed online and was discovered by the researches of Kromtech Security Center. The data was exposed because they were stored on two unsecure publicly accessible and unprotected Amazon AWS S3 Buckets. [6]
- In 2017, highly sensitive passwords and decryption keys were exposed because it was stored in four unsecure Amazon AWS S3 buckets and was confirmed by technology and cloud giant Accenture. Anyone who knows the servers web address could download the stored data without any password. [7]

Ways to ensure Cloud Security Architecture and strategy:

- Implementing and developing a security architecture framework
- Threat models should be kept up to date
- Monitoring the overall security posture
- Making sure the goals and objectives are aligning with the security architecture

Insecure interfaces and APIs

Software user interfaces and API are provided to customers by the cloud computing providers to interact with cloud services. Protection against both accidental and malicious attempts should be mainly targeted when designing the interfaces. Misuse and data breaches are some reasons for poorly designed APIs. Security requirements should be understood by organizations in designing and introducing them on the internet. APIs are the only asset that contains a public IP address which is available to the public and the most protectable part since it is the main door to enter the server.

Confidentiality, integrity, availability and accountability are the issues that expose organizations of relying on a weak set of interfaces and APIs. Consumers of these cloud services should understand the security implications that are associated by using a cloud service. Financial and regulatory are some additional impacts due to having insecure interfaces and APIs.

Examples of recent issues of having insecure interfaces and APIs:

- More than 50 million accounts of Facebook have faced a data breach in 28th September 2018. Although a vulnerability of the code was introduced to Facebook on theft of credential in July of 2017. What information was stolen, and the number of other compromised accounts were unknown, the company admitted. [8]

Ways to ensure secure interfaces and APIs:

- Avoiding reuse and implementing proper protection of API keys.
- Using standardized and open API frameworks like Cloud Infrastructure Management Interface (CIMI).
- Good practices like API hygiene should be used.

3 Future developments in the area

Although there are many security implications are in place, always there will be new different ways of threats on cloud computing due its vast and fast growth of it. More companies are starting to adopt to cloud computing in a fast-growing pace. Due to these fast adaptations, to minimize the risks and new challenges on cloud security, cyber security professionals are forced to learn about how to response and mitigate attacks and develop new cyber security strategies.

The most responsibility of cloud security is passed on to cloud providers

Most companies switch to serverless architecture over container-based architecture because it requires less management and can abstract increasing number of system components. Due to this, application owner’s sole responsibility is to make necessary steps to entrust application layer security. Physical security, network security, operating system security configurations and patches, and virtual machine or container security are the security responsibilities of the cloud provider.

The number of components that the cloud providers are responsible are increasing and application owners are dealing less with operating systems, networks and infrastructure security. The traditional corporate IT security teams will be less involved as a result of the internal shift of IT security in an organization. On the other hand, DevSecOps will be adopted in order to develop more secure systems.

Cloud native security will be adopted by the traditional security vendors

To adopt to modern cloud native environments, traditional security vendors are starting to make modernized strategic efforts in their security offerings. Cloud computing is adopted by many government offices, financial sector, healthcare sector and other large corporations. So, vendors have realized that cloud computing is not just a domain of startup companies and need to be secure enough to operate successfully.

Due to these reasons, organizations have realized that public cloud infrastructure has a high level of security integrated and are not less secure than on-premises infrastructure. Data breaches, misconfigurations, lack of cloud security architecture and strategy are less likely to happen due it being backed up by highly professional security teams to ensure the security of their systems.

4 Conclusion

1. Companies that are adopting to cloud based systems should be aware of different threats on cloud-based systems.
2. Security concept on cloud systems are wider than on premises servers.
3. Configurations on systems should be performed in a proper systematic way.
4. Interfaces and APIs should be built and developed in a highly secure manner due to it being the front door of a sever where people get into the system. Poorly secured interfaces and APIs will lead to data breaches and integrity related problems.
5. Due to the fast growth of cloud computing, clients and vendors should be prepared for any future new threats.
6. Security of cloud computing should be considered seriously because on little vulnerability will be enough to take down a whole system and breach highly sensitive confidential data of users.

5 References

1. Timehop Security Incident, July 4, 2018: https://www.timehop.com/security/

2. VOIPO database exposed millions of call and SMS logs, system data: https://www.zdnet.com/article/voipo-database-exposed-millions-of-call-and-sms-logs-system-data/

3. Amazon hit with major data breach days before Black Friday: https://www.theguardian.com/technology/2018/nov/21/amazon-hit-with-major-data-breach-days-before-black-Friday

4. Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records: https://www.wired.com/story/exactis-database-leak-340-million-records/

5. Short Circuit: How a Robotics Vendor Exposed Confidential Data for Major Manufacturing Companies: https://www.upguard.com/breaches/short-circuit-how-a-robotics-vendor-exposed-confidential-data-for-major-manufacturing-companies

6. Personal data of over 50,000 Honda Connect App leaked: https://www.hackread.com/personal-data-of-over-50000-honda-connect-app-leaked/

7. Accenture left a huge trove of highly sensitive data on exposed servers: https://www.zdnet.com/article/accenture-left-a-huge-trove-of-client-passwords-on-exposed-servers/

8. Facebook says at least 50 million users affected by security breach: https://techcrunch.com/2018/09/28/facebook-says-50-million-accounts-affected-by-account-takeover-bug/