Current Threats, Vulnerabilities, Exploits, and Recommended Controls to Secure Information in the Cloud

Michael Bossner

I. INTRODUCTION

Cloud computing is a model designed for providing scalable computing services over the internet. Generally cloud computing services fall into three types of service models:

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a service (IaaS)

And four deployment Models:

1. Private cloud
2. Community cloud
3. Public cloud
4. Hybrid cloud

And lastly comprises of five essential characteristics:

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

All of which are defined by the National Institute of Standards and Technology NIST [1].

The past few years in Australia has seen a large increase in the number of businesses beginning to use paid cloud computing services with 42% reporting use in 2017-2018 compared to only 31% in 2015-2016 a growth of 11% [2]. According to a survey done by [3] the percentage of people using more than 51% of their workload in the cloud is currently at 18% today and is anticipated to increase to 46% over the next 2 years, a remarkable growth of 28%.

With the very large increases of people moving to cloud computing services security remains as important as ever, it is interesting to note then that in a survey done by [4] an overwhelming majority of 93% of organizations are moderately to extremely concerned about cloud security. While 28% of organizations had reported security incidents in the last 12 months compared with Australia which only saw 11% of businesses reporting internet security incidents according to [2]. It is clear that a larger focus on security should be implemented by both organizations, and the providers of the service.

In this paper I will be discussing some of the most common threats, vulnerabilities and exploits experienced at the time of writing and some recommended controls that should be implemented to help mitigate the risks involved. The structure of this paper will be as follows. Section II will be discussing some of the most common threats in cloud computing. Section III will go on to talk about the vulnerabilities and exploits associated with the threats noted in section II. Section IV will discuss some recommended controls to reduce risk.

II. COMMON THREATS IN CLOUD COMPUTING

As cloud computing is inherently connected to the internet it leaves the systems open to many different types of threats associated with being exposed to the world. This section will be covering some of the most common types of threats.

1. Data Loss

According to a survey done by [4] 64% of participants were concerned about Data loss

and leakage in cloud computing putting it at the top spot as the greatest cloud security threat faced in 2019.

Data loss may occur for any number of reasons and in any environment. Examples of data loss include natural reasons like fires and earthquakes to malicious users deleting the data either intentionally or unintentionally. Loss of data may effect individuals differently depending on the type of data lost and can range from easily replaceable to costing a company millions of dollars [5], [6].

2. Data privacy being compromised

In the survey done by [4] 62% of participants found that data privacy and confidentiality was of concern to them, putting it in the second greatest concern to cloud security in 2019. In the last 12 months of the 28% of organizations that reported a security incident 27% of them were exposure of data.

The threat of exposed data is particularly important to organizations where such exposure can cost a lot such as in corporate espionage. Breaches in privacy can come from many areas such as employees intentionally or unintentionally leaking the information to a competitor or an individual gaining access to an authorized account through malicious means. Losses in privacy can occur on all levels of cloud services, IaaS, PaaS and SaaS [5].

3. Hijacking of accounts, services or traffic

Another common threat faced by cloud computing users is their services being hijacked. This threat can come from a few places such as the traffic being intercepted and manipulated on route between the user and the service to someone physically stealing the account credentials that had been written down somewhere in an office. The consequences of having your accounts hijacked can vary but all of them are undesirable. From being redirected to malicious websites to data changes and stolen information [5].

In the survey done by [4] 39% of participants saw hijacking of accounts, services and traffic as one of the biggest security threats in public clouds and 19% of all security incidents reported were of accounts being compromised.

III. COMMON VULNERABILITIES AND EXPLOITS IN THE CLOUD

Vulnerabilities in a system are the means by which threats are realised while exploits are the way a vulnerability is used to achieve that goal. This section will cover common attacks that are used to realise the threats listed in the previous section.

1. Authentication attacks

Authentication attacks attempt to exploit vulnerabilities in the authentication process of cloud systems. There are a few ways a malicious attacker might gain access. From brute forcing weak passwords that legitimate users employ to weak password recovery systems. These vulnerabilities in the systems allow unauthorized users to gain access to accounts that are not their own. While social engineering methods exploit vulnerabilities in the humans themselves and are employed to try and find information about likely passwords that may have been used on the accounts, either in person or via phishing attacks [5], [7], [8].

The results of a successful authentication attack can lead to the hijacking of accounts and services, breaches in data privacy and data loss by the malicious user now having access to all the permissions that the compromised account held. These types of attacks target SaaS cloud service models.

2. Man in the Middle Attacks

Man in the middle attacks attempt to exploit vulnerabilities in the transmission of packets across a network by inserting themselves between the client and the server and tricking each endpoint into thinking they are talking with each other when in fact they are talking with the malicious user instead. A successful

attack of this type can see all of the threats discussed in section I realised as they hijack the traffic being sent and received. If the traffic is in plain text then simply reading the information being transmitted is a loss of data privacy while actually altering the information being transmitted can result in compromised accounts, services and data loss. These types of attacks can target all three of the cloud service models [5], [9].

3. Side Channel Attacks

Side channel attacks attempt to exploit vulnerabilities in servers that run multiple virtual machines on the same system. These attacks are specifically targeting services using the IaaS cloud service model. A malicious attacker will try to gain information of a system being used by monitoring and analysing information collected from the host server such as power consumption, heat or even the cache [5].

A successful attack of this type can see the virtual machine being targeted hijacked by the attacker [5].

IV. Recommended Controls in Cloud Security

Reducing the risk of a threat being realised in the cloud environment today is as important as ever with the large numbers of organizations currently using the cloud and the even larger number expected to be in the future [2], [3]. In this section I will be talking about some of the best controls that can be put into place to reduce the risk of a threat being realised and to reduce the risk of loss if it does.

1. Data Encryption

According to a survey done by [3] 30% of global participants and 29% of those in Australia consider data encryption as one of the top security controls in the cloud bringing it to the top of the list.

Data encryption can prevent breaches in data privacy by changing the information from clear text to cipher text. This can also help reduce the risk of all the threats discussed in section I by hindering malicious users from gaining access to accounts, services and preventing attackers from reading the contents of packets being sent from client to the server. It is important to note however that data encryption can actually increase the risk of data loss in certain situations as a loss of the encryption keys will make the data useless [5], [6].

2. User Identity and Access Management

In the survey done by [3] 25% of global participants and 22% of Australian participants selected user identity and access management as one of the top security considerations in the cloud today.

Knowing who is an authorized user and who is not is very important when it comes to keeping control of your data and accounts. Using stronger passwords and security certificates to verify a user's identity are just some of the ways of reducing the risk of someone gaining access to an account that is not their own [5], [6].

References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud," Institute of Standards and Technology, 2018. [Online]. Available: https://www.nist.gov/. [Accessed 23 Aug 2019].

[2] Australian Bureau of Statistics, "8167.0 - Characteristics of Australian Business , 2017-18," 02 August 2019. [Online]. Available: https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8167.0Main+Features12017-18?OpenDocument. [Accessed 23 Aug 2019].

[3] Telstra, "Telstra Security Report 2019," 2019. [Online]. Available:

https://www.telstra.com.au/content/dam/shared-component-assets/tecom/campaigns/security-report/Telstra%20Security%20Report%202019%20(1).pdf. [Accessed 23 Aug 2019].

[4] Cybersecurity Insiders, "Cloud Security Report," 2019. [Online]. Available: https://www.isc2.org/-/media/ISC2/Landing-Pages/2019-Cloud-Security-Report-ISC2.ashx?la=en&hash=06133FF277FCCFF720FC8B96DF505CA66A7CE565. [Accessed 23 Aug 2019].

[5] L. Alhenaki, A. Alwatban, B. Alamri and N. Alarifi, "A Survey on the Security of Cloud Computing," *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS),* 2019.

[6] A. Hendre and K. P. Joshi, "A Semantic Approach to Cloud Security and," *2015 IEEE 8th International Conference on Cloud Computing,* 2015.

[7] K. D. Mitnick and W. L. Simon, The Art of Deception, John Wiley & Sons, 2002.

[8] C. Hadnagy, Social Engineering: The Art of Human Hacking, John Wiley & Sons, 2010.

[9] A. Narang and D. Gupta, "A Review on Different Security Issues and Challenges in Cloud Computing," *2018 International Conference on Computing, Power and Communication Technologies (GUCON),* 2018.