Cloud Infrastructure Network Security

Hemant Jain, Sapna Patel, Vivek Shakya, Mahesh Vatalu Renukaprasad, Krutarth Vanesa
INFO 7350 – Systems and CyberSecurity Fundamentals (Spring 2021)
Guided By: Prof. Angel L. Hueca

Northeastern University
College of Engineering

Abstract

Cloud computing has become the core internal part of the software development industry. It serves as a platform providing services in various domains right from Virtual Environment resources, databases, messaging services, parallel machine learning, etc.

Due to the leverage of many technologies in one place, it inherits the security issues which persist in those individual platforms involving secure access authentication, authorization, access management, security controls and services.[1]

Through this paper we are exploring the security issues that persists in the cloud infrastructure and the possible solutions and policies to mitigate them or minimize the risk of threats that can be exploited by threat agents

Introduction

The architecture of cloud computing consists of various kinds of distributed systems with wide usage and network connectivity across multiple regions and cross-continents.

The problems which it inherits from its multi-tenancy and agile work model are Misconfigurations, Shared tenancy vulnerabilities, meeting and billing evasions. One of the things which every organization needs to look up while building out or migrating their traditional infrastructure into Cloud.[2]

Due to the heavy transfer of data in real-time with the high-speed mobility in the infrastructure available in the Cloud services providers causes the lack of transparency issues and losing out the full-control.

There are some vulnerabilities which are commonly observed like Misconfiguration which is result from the lack of understanding of shared model for example cloud service policy give access to resources without justifying user role.[3]

Cloud user accounts using MFA are compromised using password reset links to single factor authentication email accounts. There are some other vulnerabilities like shared tenancy vulnerabilities, supply chain vulnerabilities, Data recovery vulnerabilities. Metering and billing data abuse and billing evasion are examples of metering and billing evasion vulnerabilities.[5]

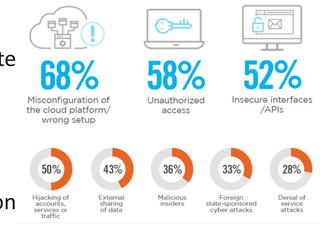
Methods and Materials

Data Integrity and Data Protection is one of biggest concerns which disinclines trust, authenticity on Cloud Infrastructure. It is due to large amounts of data flowing between employees and cloud systems, which can be intercepted by hackers.[4]

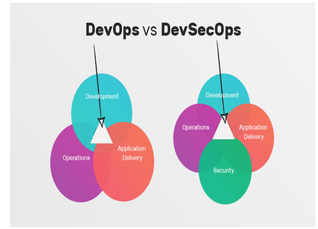
Data loss is another issue which occurs when business processes to cloud, the amount of data you store remotely can quickly grow to an unmanageable size, which makes backups both difficult and costly. Research has found that an average of 51% of organizations have publicly exposed at least one cloud storage service, and 84% of organizations conclude that traditional security solutions don't work[3]

It is very important to develop and implement a security architecture framework that keeps threat models up to date and deploy continuous monitoring capability.

- Secure accounts, by use of two-factor authentication.
- Use strict identity and access controls for users
- Segregate and segment accounts, virtual private clouds
- Take a programmatic, centralized approach to key rotation
- Remove unused credentials and access privileges.



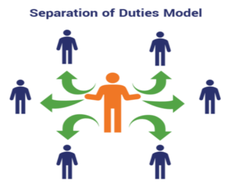
https://www.recordedfuture.com/



https://techmoran.com/

Security Best practices

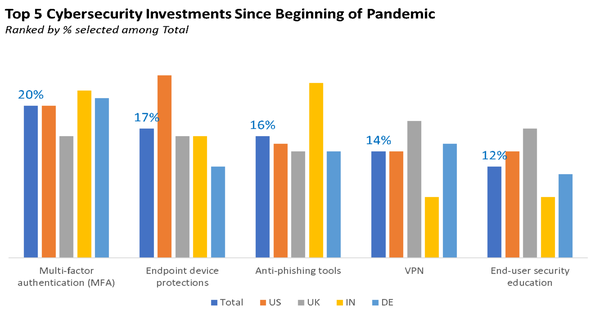
- Prioritize Privileged Access Management (PAM) and Identity & Access Management (IAM) using cloud-native controls to maintain least privilege access to sensitive data starting at the PaaS level
- Start using customer-controlled keys to encrypt all data, migrating off legacy operating systems and controls that rely on trusted and untrusted domains across all IaaS instances.
- Before implementing any cloud infrastructure project, design in Zero Trust Security (ZTS) and micro-segmentation first and have IaaS and PaaS structure follow.[2]



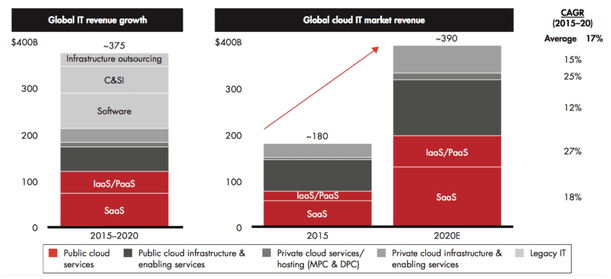
https://martinfowler.com/

https://www.recordedfuture.com/

- Before implementing any PaaS or IaaS infrastructure, define the best possible approach to identifying, isolating and correcting configuration mistakes or errors in infrastructure.
- Standardize on a unified log monitoring system that ideally as AI and machine learning built to identify cloud infrastructure configuration and performance anomalies in real-time.
- Develop and implement a security architecture framework.
- Ensure that the threat model is kept up to date.[6]
- All cloud providers should conduct penetration testing and provide findings to customers.
- All non-approved cloud services should be reviewed and approved by the cloud security.
- Ensure that the threat model is kept up to date.



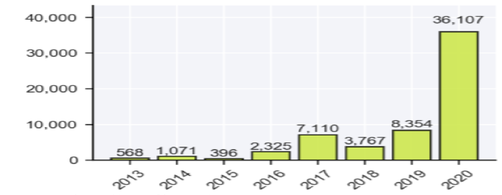
https://www.mcafee.com/



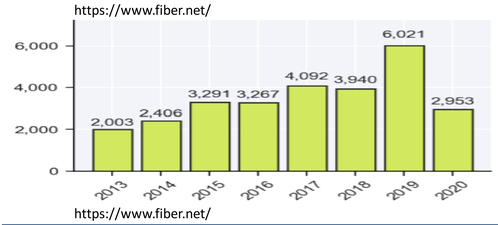
https://www.forbes.com/

How Pandemic changed Cyber Security

- In the first three quarter of 2020, 21% of reported breaches involved the use of ransomware. These ransomware-related events contributed to the unusually high number of unknown (11.2%) and miscellaneous (10.4%) data types exposed.
- Two breaches in Q3 exposed over 1 billion records each and four breaches exposed over 100 million records. Together these six breaches accounted for approximately 8 billion exposed records, or 22.3% of the records exposed through the end of Q3



https://www.fiber.net/



https://www.fiber.net/

Future Directions

Future Ideas to make Cloud Infrastructure more secure[4][5]

- Deploy Multi-Factor Authentication (MFA)
- Manage Your User Access to Improve Cloud Computing Security
- Monitor End User Activities With Automated Solutions to Detect Intruders
- Create a Comprehensive Off-boarding Process to Protect against Departing Employees
- Provide Anti-Phishing Training for Employees on a Regular Basis
- Consider Cloud-to-Cloud Backup Solutions

References

1. Albanese, M., De Benedictis, A., de Macedo, D. D. J., & Messina, F. (2020). Security and trust in cloud application life-cycle management. *Future Generation Computer Systems*, *111*, 934–936. https://doi.org/10.1016/j.future.2020.01.025
2. Advanced Security Architectures for Cloud Computing. (2016). *Cloud Computing Security*, 443–458. https://doi.org/10.1201/9781315372112-48
3. Indu, I., Anand, P. M. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an International Journal*, *21*(4), 574–588. https://doi.org/10.1016/j.jestch.2018.05.010
4. R, P., Tony Santhosh, G., Juben Ratchnayaraj, I. A., & Jemiline, E. (2020). The security in web application of cloud and IoT service. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2020.10.087
5. Steve Mansfield-Devine,Gateway to securing the cloud,Computer Fraud & Security, Volume 2019, Issue 11,2019,Pages 16-19,ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(19)30118-6.
6. K.A. Torkura, Muhammad I.H. Sukmana, Feng Cheng, Christoph Meinel,Continuous auditing and threat detection in multi-cloud infrastructure,Computers & Security,Volume 102,2021,102124,ISSN 0167-4048,https://doi.org/10.1016/j.cose.2020.102124.

Conclusions

We stated how security smells leads to increment in system weakness and what practice can be used by developers to build quality code or IaC scripts. Detailed out threat model built in order to secure the controls of an IaC. The development of IaC threat model should be promoted as it can protect end users from disturbance.[2]

Email security protocol should use encryption, PKI based cryptographic technique, IP address validation and DNS based validation. However, One protocol does not provide all security. It should take user awareness among email users.

Users' data can be saved in multiple locations in various regions across the world to increase the availability/ backups and the security of the data.[4]