Corban Sy
Jamison Stalter
Erik Ziegler
Alac Springer
Epifanio Solano

Security Analysis of Cloud Security

By conducting a thorough and rigorous analysis of the security practices used by leading cloud services, we aim to see if these products will uphold the increasingly important triad of Confidentiality, Integrity, and Availability (CIA). As more and more products move to the cloud and/or use the cloud as the backbone of their services, it becomes crucial to know the current state behind their security offerings and regularly validate that there are no known vulnerabilities and risks.

To achieve this analysis we will conduct several testing methodologies such as light penetration testing, vulnerability scanning, and analysis of security permissions. We will be able to use both manual and automated testing to conduct our research and through these tests assess whether the services pass against common flaws such as a role having access to files or locations it should not.

Specifically, our testing will focus on identifying common security flaws, such as misconfigured access controls and unauthorized data exposure. Through penetration testing, we will simulate real-world attack scenarios to evaluate the resilience of cloud services against potential threats. Additionally, vulnerability scanning will enable us to identify and prioritize security vulnerabilities within cloud infrastructures. Furthermore, analysis of security permissions will allow us to assess the granularity and effectiveness of access controls implemented by cloud providers.

By conducting these comprehensive tests, we aim to provide valuable insights into the security posture of leading cloud services and identify areas for improvement. We hope that our results will lead to more resilience in cloud security infrastructure and help services be more proactive in their defense against bad actors.

To effectively bolster our cloud security initiatives, we will require a range of essential resources. Firstly, access to cloud providers such as AWS, Azure, and Google Cloud will be pivotal for comprehensive evaluation and comparison of their respective security features and capabilities. This will enable us to make informed decisions regarding the selection and configuration of cloud services that align with our security requirements. Additionally, hands-on experience in a simulated cloud environment is essential for practical exploration and identification of potential security risks and vulnerabilities. Furthermore, resources focused on cloud compliance and governance for security will be indispensable for ensuring regulatory compliance and adherence to industry best practices, establishing robust governance structures that uphold security standards and mitigate risks effectively. Collectively, these resources will equip us with the tools and knowledge necessary to fortify our cloud security posture and safeguard our digital assets effectively.

To ensure a systematic approach to enhancing cloud security, we'll divide our efforts into several key activities with designated checkpoints for progress tracking. Initially, we'll set up teams and communication channels, assigning leaders for each task. Over the course of two weeks, we'll conduct cloud penetration testing, with red and blue teams simulating attacks and defenses. Following this, a one-week period will be dedicated to vulnerability scanning, while a separate team analyzes the cloud security architecture over three weeks. Meanwhile, ongoing research will identify common security vulnerabilities and assess tools for threat detection. Subsequent weeks will focus on evaluating the security features of leading cloud services, providing training and awareness sessions, and conducting threat modeling exercises. Finally, in the last week, we'll compile all findings, review them, and document the entire process for future reference. Through this structured approach, we aim to fortify our cloud security posture effectively.

Article surveys

https://www.businesswire.com/news/home/20240227531064/en/Orca-Security-Report-Reveals-81-of-Organizations-Have-Vulnerable-Neglected-Public-Facing-Cloud-Assets-with-Open-Ports

The Orca Security 2024 State of Cloud Security Report reveals critical insights into the current landscape of cloud security. Key findings indicate that a staggering 81% of organizations have neglected public-facing cloud assets with open ports, making them prime targets for cyberattacks. Additionally, misconfigured data storage and severe vulnerabilities in code pose significant risks, with 21% of organizations exposing sensitive data and nearly two-thirds having vulnerabilities with the potential for data breaches. The report also highlights the rising trend of exposed Kubernetes API servers and emphasizes the need for stringent security protocols for managing cloud-based AI models. Despite the growing complexity of cloud environments, basic security practices like Multi-Factor Authentication (MFA) remain lacking in many organizations. The report underscores the urgent need for prioritizing and efficiently remedying the most critical cloud security risks to protect business-critical assets from evolving cyber threats.

Google pays hacker duo $22k in bug bounties for flaws in multiple cloud projects | The Daily Swig (portswigger.net)

In January 2023, a couple of security researchers found a server-side request forgery bug and a subsequent patch bypass in 4 projects from Google Cloud Platform. The flaw was in Vertex AI, one of Google's Cloud Platform projects, where an attacker would create a notebook on Jupyter. By editing the notebook's index.html to have a malicious redirect, giving a victim IAM privileges, and getting a victim to click on the bad link, an attacker could get their Google Cloud Authorization token and have access to all of the victim's GCP projects.

Russian cyberespionage group APT29 targeting cloud vulnerabilities | SC Media (scmagazine.com)

Russia's elite cyberespionage groups are looking into vulnerabilities of the cloud since many corporations and governments are moving their infrastructure on to it. One group is experienced in brute force hacking and targets service accounts that have weaker security features than individual accounts. These service accounts tend to have higher privilege and don't have multiple factor authorization. They also target dormant accounts from members that have long left an organization. NSA recommends daily logging of accounts and their activities and to avoid generic multiple user accounts.

https://www.guidepointsecurity.com/education-center/cloud-penetration-testing/

Cloud penetration testing is quite different from normal pen testing because they have to examine cloud-specific configurations. It is used to determine the strengths and weaknesses of a cloud system to

improve the security posture. Cloud usage is based on a shared responsibility model which means you examine the security in the cloud instead of the security of the cloud. 3 types of cloud pen testing are Black Box, Grey Box, and White Box. Black Box simulates an attack with no prior knowledge about the cloud system. Grey Box simulates the attack with limited knowledge and admin privileges. Lastly, the White Box pen testing is when the attackers are given all access to the cloud system. The testing examines the cloud perimeter, internal cloud environments, and on-premise cloud management, administration, and development infrastructure. There are 3 stages to this type of testing, Evaluation which highlights the potential vulnerabilities, risks, and cloud security needs. Stage two uses this information to perform relevant pen-testing. The last stage is just a follow-up to ensure the steps have been properly followed.
https://www.researchgate.net/publication/327111449_Security_in_Cloud_Computing_A_Systematic_Literature_Review
The paper provides a comprehensive review of security challenges in cloud computing, aiming to shed light on the various aspects of security concerns associated with the adoption of cloud solutions. It begins by defining key terms in cloud environments and delves into the different models of cloud computing, including deployment and service models. This sets the stage for understanding the complexities of security issues in cloud environments, considering factors such as multi-tenancy, virtualization, and infrastructure distribution.

One of the key insights from the review is the importance of establishing consistent standards and service level agreements (SLAs) to address security concerns effectively. Despite the emergence of various standards-setting bodies, such as the IEEE Cloud Computing Standard Study Group and the Cloud Security Alliance, the lack of widely accepted standards remains a challenge. As a result, SLAs play a crucial role in defining the terms and conditions of service provision, although they often focus on minimum levels and may not adequately address all security aspects.

The review identifies several specific security challenges in cloud computing, including issues related to infrastructure, virtualization, availability, confidentiality, integrity, backup and recovery, and identity management. For example, the distribution of infrastructure across multiple locations raises concerns about data privacy and compliance with different regulatory frameworks. Similarly, virtualization introduces new vulnerabilities, such as hypervisor-based attacks, while also enabling more efficient resource allocation.

Furthermore, the review highlights the need for ongoing research to address gaps in existing security measures and to develop innovative solutions to emerging threats. This includes exploring client-focused security solutions, considering legal and governmental factors, and enhancing collaboration between academia and industry. Overall, the paper provides valuable insights into the complex landscape of cloud security and lays the groundwork for future research and development efforts in this critical area.

Other Literature Survey References:

1. https://link.springer.com/article/10.1007/s10660-022-09615-y
2. https://www.researchgate.net/publication/350883353_A_Systematic_Literature_Review_on_Cloud_Computing_Security_Threats_and_Mitigation_Strategies
3. https://www.sciencedirect.com/science/article/pii/S2667096822000775
4. https://www.researchgate.net/publication/332621618_LITERATURE_REVIEW_ON_DATA_SECURITY_IN_CLOUD_COMPUTING

5. https://www.researchgate.net/publication/327111449_Security_in_Cloud_Computing_A_Systematic_Literature_Review