Help in the cloud minefield - A structured approach for an AWS pentesting framework

M. Sc. Tobias Kolb, Senior Penetration Tester, Spike Reply DE
Prof. Dr. Max Moser, HDBW – Hochschule der Bayerischen Wirtschaft

A trend that has long been an integral part of a stable corporate IT landscape in the USA has now also arrived in Germany. According to the "Cloud Monitor 2023" study by KPMG[1],, "practically almost" every German company uses cloud services. However, very few rely on a single cloud technology. According to "Cloud Monitor 2023", 82 percent pursue a multi-cloud strategy.

1. Market Share AWS

Microsoft, Amazon, and Google - three dominant companies in the tech scene. These three also occupy the top spots when it comes to the cloud. Amazon (AWS) remains the market leader with 30%, closely followed by Microsoft (Azure) with 26% and Google (GCP) in third place with 9% (Status Q2 2023).[2]

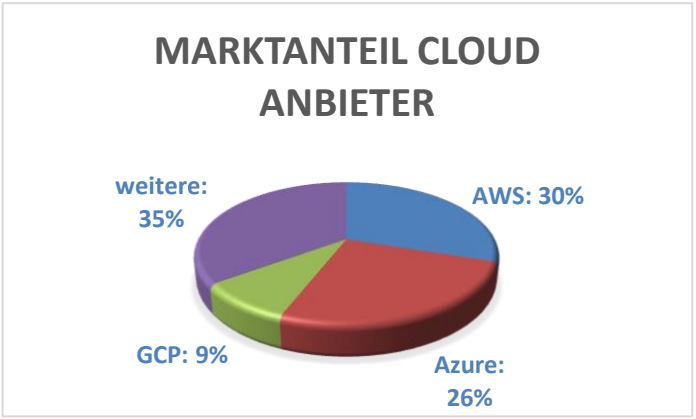

Figure 1 Market share in the cloud segment (own presentation based on ZDNET [3])

[1] https://hub.kpmg.de/de/cloud-monitor-2023
[2] https://www.zdnet.de/88411152/markt-fuer-cloud-dienste-waechst-16-prozent-im-zweiten-quartal/
[3] https://www.zdnet.de/88411152/markt-fuer-cloud-dienste-waechst-16-prozent-im-zweiten-quartal/

2. Schwachstellen in AWS

„No system is safe“ - a quote from a German hacking movie („Who Am I“[4]) - describes an existing problem with IT technologies. Cloud is no exception in this case.

In general, two types of vulnerabilities can be distinguished: Vulnerabilities caused by the cloud provider at the structural level and vulnerabilities at the configuration level of the end customer.

Many technical vulnerabilities have been reported in the AWS cloud service in recent years [5] [6] [7]. As a rule, these vulnerabilities are fixed by Amazon's development teams immediately after the vulnerability is disclosed. A threat from this type of vulnerability at structure level exists in principle for all end customers who use the affected AWS services. However, as the vulnerability is usually fixed quickly, the threat is only temporary. In contrast, configuration vulnerabilities caused by the end customer in connection with the customer infrastructure itself are often more persistent.
The increasing complexity of cloud environments combined with the shortage of specialists in many IT departments provide an enormous breeding ground for errors. These errors can lead to reputational and / or financial damage for companies. In the last two years alone, many well-known companies have fallen victim to data breaches.[8] [9]

Betroffenes Unternehmen	Datum des Data Breaches	Schaden
Capital One	Juni 2022	100 million customers affected
Pegasus Airlines	Mai 2022	Unsecured S3 cloud storage loses 6.5 terabytes of data
FlexBooker	Dezember 2021	Loss of 19 million files from unsecured S3 cloud storage

Chart 1 Previous Data Breaches

But what are these data breaches due to? Amazon's shared responsibility model generally provides a clearly defined answer to this question (see Figure 2). According to this model, Amazon is responsible for the infrastructure ("responsibility of the cloud"), while the end customer is responsible for their own AWS cloud instances ("responsibility in the cloud"). The end customer using AWS is therefore responsible for securing their AWS cloud infrastructure and ensuring that it is adequately protected against attacks and data loss.

[4] https://www.imdb.com/title/tt3042408/
[5] https://portswigger.net/daily-swig/vulnerability-in-aws-appsync-allowed-unauthorized-access-to-cloud-resources
[6] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29527
[7] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23511
[8] https://firewalltimes.com/amazon-web-services-data-breach-timeline/
[9] https://snyk.io/de/learn/aws-security/aws-security-breaches/

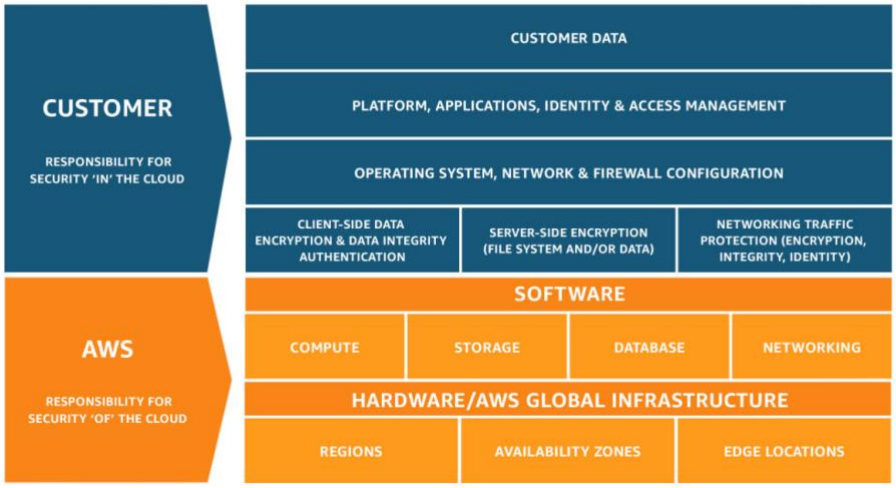

Figure 2 Shared Responsibility Model by AWS[10]

The top 10 list of risks in AWS cloud environments, published in 2023 by the company Snyk[11], also clearly shows that the risks for a successful compromise of AWS cloud environments are predominantly due to misconfiguration by the end customer.

Rang	Risiko
1.	Insecure S3 buckets
2.	IAM permissions
3.	Accidentally public AMIs
4.	Lack of cloud security visibility
5.	Lack of defined roles and liability
6.	Unsecured sensitive data stored in the cloud
7.	Misconfiguration vulnerabilities
8.	Vulnerabilities in source control and function repos
9.	Container vulnerabilities in Amazon Elastic Container Registry (ECR)
10.	Open Source Vulnerabilities

Chart 2 Top 10 Vulnerabilities in AWS-Cloud Infrastructures by Synk

Despite the far-reaching effects of a successful cloud attack, companies are still reluctant to have their cloud infrastructure tested regularly. According to CoreSecurity, only 46% of companies had their cloud infrastructure tested in 2023.[12] By the end of 2021, Gartner was already forecasting *„[..] Cloud Will be the Centerpiece of New Digital Experiences"*.[13]

[10] https://aws.amazon.com/de/compliance/shared-responsibility-model/
[11] https://snyk.io/de/learn/aws-security/aws-security-risks-prevention/
[12] https://www.coresecurity.com/blog/importance-penetration-testing-cloud-infrastructures
[13] https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences

Furthermore, Gartner expects more than 85% of companies to adopt a cloud-first approach to platform adoption by 2025 [14], i.e. will prioritize cloud as a technology within a digitalization strategy.[15]

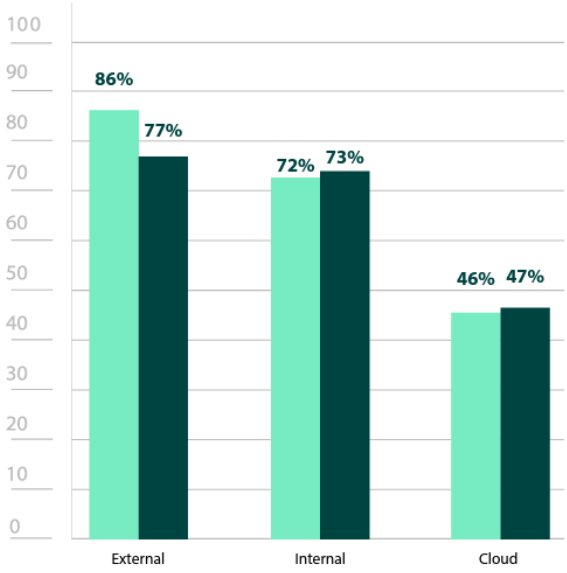

Figure 3 Typically tested Infrastructures[16]

3. Necessary Support

Despite the increasing adoption of cloud technologies in organizations and the rising successful compromises of AWS cloud environments, over 50% of organizations are still reluctant to have their cloud infrastructure tested by trained security personnel.[17] The lack of trained experts for testing AWS cloud setups is often the only reason why in-house testing fails. This is exacerbated by the fact that there is currently no generally recognized framework for AWS pentests. A comparable framework has been developed and published for the direct competitor Microsoft and its Azure Cloud - the so-called "Azure Active Directory and Microsoft 365 Kill Chain".[18] The framework was published in 2020 by Dr. Nestori Syynimaa, one of the leading experts in the field of Azure Cloud Security. Since then, it has served as the basis for penetration tests in Azure environments but cannot be directly transferred to AWS cloud setups.

In general, such a framework or process model offers relief and support. On the one hand for the AWS customer, who can better assess the test scope of their AWS cloud environment based on a comprehensible procedure. On the other hand, a predefined structure enables testers to assess the current security status of an AWS cloud environment reproducibly and comprehensively.

[14] https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences
[15] https://www.makonis.de/blog/cloud-strategie#
[16] https://www.coresecurity.com/blog/importance-penetration-testing-cloud-infrastructures
[17] https://www.coresecurity.com/blog/importance-penetration-testing-cloud-infrastructures
[18] https://aadinternals.com/aadkillchain/

4. A Framework as structured approach for AWS-Cloud-Pentesting

In the master thesis *„Development and evaluation of a cloud security testing framework for penetration testing and red teaming of AWS cloud environments“* by Tobias Kolb such a framework was developed.
The framework can support pentesters and red teamers in testing known AWS services for their security in a structured and comprehensible manner, while at the same time responding to individual customer needs. The framework was designed to be as service-independent as possible so that it can be applied to as many Amazon Web Services as possible.
Three perspectives are considered, which correspond to the roles of using the AWS cloud setups: Outsider, User and Admin (see Figure 4). An individual run-through cycle is described for each perspective. The transitions from one perspective to another are also defined. If the tester was able to achieve a goal in the Outsider perspective, e.g. extension of rights, it is possible to switch to the next higher User perspective. The subdivision into perspectives enables extensive flexibility for different test scenarios. Each cycle within the perspectives offers the testers a structure with which they can analyze as many aspects of the AWS cloud as possible in a comprehensible and repeatable manner.

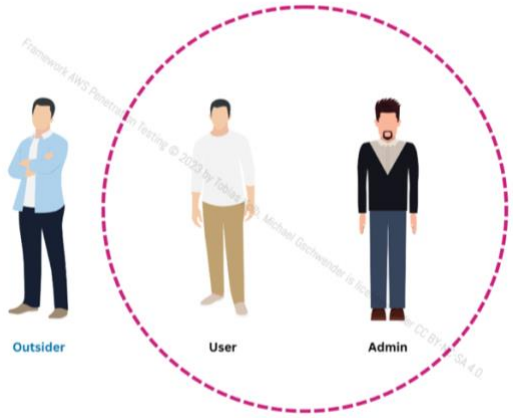

Figure 4 The three perspectives in the AWS-Framework

Outsider: This perspective describes a tester who tests an AWS cloud environment from "outside". In contrast to the other two perspectives, the outsider is by definition not able to authenticate themselves to AWS. The aim of the outsider is to generate so-called "interaction points" that can be exploited. All interaction points are then analyzed further in order to determine the possibility of successful exploitation.
A decisive difference to Microsoft Azure lies in the publicly available interfaces (APIs). Validation on existing users of an Azure AD tenant can be carried out easily as an outsider, whereas an AWS cloud environment does not offer this option.

User: This perspective can authenticate against an AWS cloud environment. However, the user does not have the highest authorizations in any AWS service. The aim of this perspective is to identify both lateral propagation and escalation of privileges (privilege escalation).

Admin: The admin represents a perspective that is able to authenticate itself to at least one AWS service with the highest possible rights.

As part of the thesis, this AWS penetration testing framework was evaluated using established AWS cloud security training labs. Criteria such as the number of existing attack vectors, the meaningful design of the phase change and the verification that the phases were completed were taken into account. As a result of this evaluation, the attack vectors could be found by applying the framework - the arrangement of the phases could be proven to make sense.
There were limitations, particularly in the recon and enumeration phases. In some cases, the training labs examined were documented in too much detail on the Internet in so-called walkthroughs. Walkthroughs represent a step-by-step guide to a specific problem. During a detailed recon and enumeration phase, these walkthroughs would have been easily discovered and would have provided a sample solution to the task of the training lab. However, this would have distorted the result of the evaluation.

5. Conclusion

Companies have understood the potential of cloud solutions for their business models and have already begun to make intensive use of this technology. Fail-safe infrastructures can precisely map scalable business cases and support companies in achieving their business goals.
On the other hand, fatal errors have also been identified in the configuration and operation of cloud scenarios. These errors have caused enormous damage to some companies. Regardless of whether this was financial and/or reputational damage. Targeted and structured penetration tests and red teaming operations offer the opportunity to prevent possible attacks and the resulting damage.
Further information on the framework and its use as well as the request for penetration tests or Red Team Assessments for your AWS environments can be found on my **Blog**.[19]

Please send inquiries to:

- t.kolb@reply.de or via LinkedIn
- max.moser@hdbw-hochschule.de
- sabine.rathmayer@hdbw-hochschule.de

More about HDBW: https://www.hdbw-hochschule.de/

[19] https://t-s3c.de/aws-framework