Hilfe im Minenfeld Cloud – Ein strukturierter Ansatz für ein AWS-Pentesting-Framework

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

Ein Trend, der in den USA schon lange fester Bestandteil einer stabilen Unternehmens-IT-Landschaft ist, ist mittlerweile auch in Deutschland angekommen. Laut der Studie „Cloud-Monitor 2023“ von KPMG[1], nutzt „praktisch fast“ jede deutsche Firma Cloud-Dienste. Dabei setzen die wenigsten auf eine einzelne Cloud-Technologie. Laut „Cloud-Monitor 2023“ verfolgen 82 Prozent eine Multi-Cloud Strategie.

1. Marktanteil AWS

Microsoft, Amazon und Google - drei dominierende Unternehmen in der Tech-Szene. Auch beim Thema Cloud belegen die drei die ersten Plätze. Amazon (AWS) bleibt mit 30% weiterhin Marktführer, dicht gefolgt von Microsoft (Azure) mit 26% und Google (GCP) mit 9% auf Platz 3 (Stand Q2 2023).[2]

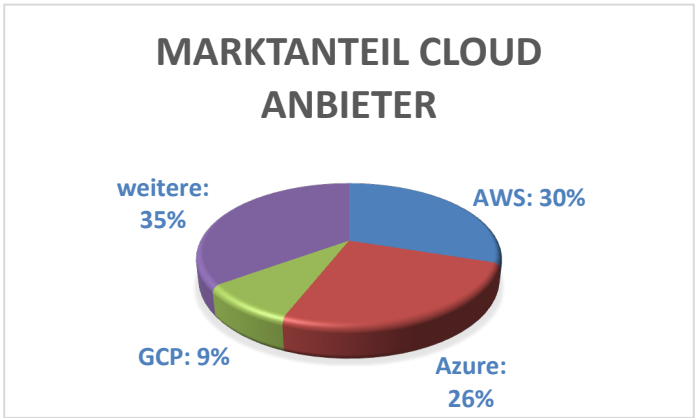

Abbildung 1 Marktanteil im Cloud-Segment (eigene Darstellung basierend auf ZDNET [3])

[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“ - ein Zitat aus einem deutschen Hacking Film („Who Am I“[4]) - beschreibt ein bestehendes Problem bei IT-Technologien. Cloud bildet in diesem Fall keine Ausnahme.

Generell können zwei Arten von Schwachstellen unterschieden werden: Schwachstellen, die durch den Cloudanbieter auf **Strukturebene** entstehen und Schwachstellen auf **Konfigurationsebene** beim Endkunden.
In den letzten Jahren wurden in dem Cloud Service AWS eine Vielzahl an technischen Schwachstellen gemeldet [5] [6] [7]. In der Regel werden diese Schwachstellen unmittelbar nach der Bekanntgabe der Schwachstelle durch die Entwicklerteams von Amazon behoben. Eine Bedrohung durch diese Art von Schwachstellen auf **Strukturebene** besteht prinzipiell für alle Endkunden, die die betroffenen AWS-Services einsetzen. Durch die meist schnelle Behebung der Schwachstelle ist die Bedrohung jedoch nur temporär. Dagegen sind **Konfigurationsschwachstellen**, die durch den Endkunden im Zusammenhang mit der Kundeninfrastruktur selbst verursacht sind, oftmals langlebiger.
Die zunehmende Komplexität von Cloud-Umgebungen kombiniert mit dem Fachkräftemangel in vielen IT-Abteilungen bieten einen enormen Nährboden für Fehler. Diese Fehler können u.a. zu Image- und / oder finanziellem Schaden von Unternehmen führen. Allein in den letzten zwei Jahren wurden viele namhafte Unternehmen Opfer von Data Breaches.[8] [9]

Betroffenes Unternehmen	Datum des Data Breaches	Schaden
Capital One	Juni 2022	100 Millionen betroffene Kunden
Pegasus Airlines	Mai 2022	Nicht gesicherter S3-Cloud-Speicher verliert 6.5 Terrabytes mit Daten
FlexBooker	Dezember 2021	Verlust von 19 Millionen Dateien von nicht gesicherter S3-Cloud Speicher

Tabelle 1 Ausgewählte Data Breaches

Worauf sind aber diese Data Breaches zurückzuführen? Darauf liefert das *Shared Responsibility Model* von Amazon in der Regel eine klar definierte Antwort (siehe Abbildung 2). Laut diesem Modell ist Amazon für die Infrastruktur verantwortlich (*„responsibility of the cloud*“), während der Endkunde die Verantwortung für die eigenen AWS-Cloud-Instanzen trägt (*„responsibility in the cloud“*). Der Endkunde, der AWS einsetzt, ist also selbst in der Verantwortung, seine AWS-Cloud-Infrastruktur abzusichern und sicherzustellen, dass diese vor Angriffen und Datenverlust ausreichend geschützt ist.

[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/

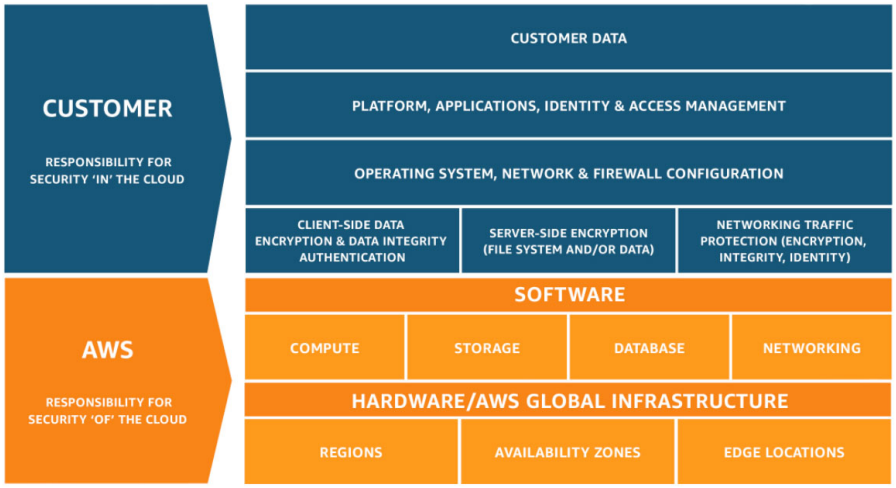

Abbildung 2 Shared Responsibility Model von AWS[10]

Aus der Top-10-Liste von *Risiken in AWS-Cloud-Umgebungen*, veröffentlicht im Jahr 2023 von der Firma Snyk[11], geht ebenfalls deutlich hervor, dass die Risiken für einen erfolgreiche Kompromittierung der AWS-Cloud-Umgebungen überwiegend auf eine Fehlkonfiguration beim Endkunden zurückzuführen sind.

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

Tabelle 2 Top 10 Schwachstellen in AWS-Cloud Umgebungen von Synk

Trotz der weitreichenden Auswirkungen eines erfolgreichen Cloud-Angriffs zögern Unternehmen noch immer, ihre Cloud-Infrastruktur regelmäßig testen zu lassen. So haben laut CoreSecurity lediglich 46% der Unternehmen im Jahr 2023 einen Test ihrer Cloud-Infrastruktur durchführen lassen.[12]
Bereits Ende 2021 prognostizierte Gartner *„[..] 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

Darüber hinaus rechnet Gartner damit, dass bis 2025 mehr als 85 % der Unternehmen bei der Einführung von Plattformen nach dem Prinzip „Cloud-first" vorgehen werden[14], d.h. Cloud als Technologie innerhalb einer Digitalisierungsstrategie priorisieren werden.[15]

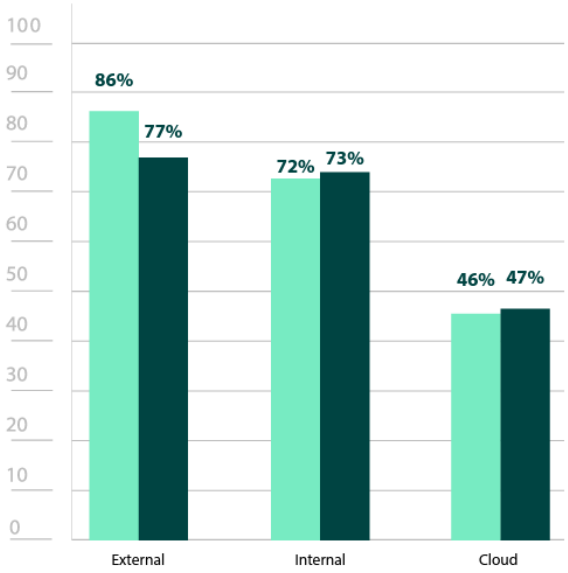

Abbildung 3 Üblicherweise getestete Infrastrukturen[16]

3. Notwendige Unterstützung

Trotz dem zunehmenden Einsatz von Cloud-Technologien in Unternehmen und den ansteigenden erfolgreichen Kompromittierungen von AWS-Cloud Umgebungen zögern über 50% der Unternehmen immer noch ihre Cloud-Infrastruktur durch geschultes Sicherheitspersonal testen zu lassen.[17]

Die Durchführung eigener Tests scheitert häufig allein durch den Mangel an geschulten Experten für das Testing von AWS-Cloud-Setups. Verschärfend kommt hinzu, dass es für ein Vorgehen bei AWS-Pentests bisher kein allgemein anerkanntes Framework gibt. Für den unmittelbaren Konkurrenten Microsoft und seine Azure Cloud wurde ein vergleichbares Framework entwickelt und veröffentlich - die sogenannte *„Azure Active Directory and Microsoft 365 Kill Chain“*.[18] Das bereits 2020 veröffentlichte Framework stammt von Dr. Nestori Syynimaa, einem der führenden Experten im Bereich Azure Cloud Security. Es dient seitdem als Basis von Penetration Tests in Azure-Umgebungen, lässt sich jedoch nicht unmittelbar auf die AWS-Cloud-Setups übertragen.

Generell bietet ein solches Framework bzw. ein Vorgehensmodell Erleichterung und Unterstützung. Zum einen für den AWS-Kunden, der anhand einer nachvollziehbaren Vorgehensweise den Testumfang seiner AWS-Cloud Umgebung besser einschätzen kann. Zum anderen können Tester anhand einer vordefinierten Struktur in die Lage versetzt werden,

[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/

reproduzierbar und flächendeckend den aktuellen Sicherheitsstand einer AWS-Cloud Umgebung einzuschätzen.

4. Ein Framework als strukturierte Unterstützung für das AWS-Cloud-Pentesting

Im Rahmen der Masterthesis *„Development and evaluation of a cloud security testing framework for penetration testing and red teaming of AWS cloud environments“* von Tobias Kolb wurde ein solches Framework entwickelt.
Das Framework kann Pentester und Red-Teamer dabei unterstützen, bekannte AWS-Services strukturiert und nachvollziehbar auf deren Sicherheit zu testen und gleichzeitig auf individuelle Kundenbedürfnisse einzugehen. Das Framework wurde möglichst serviceunabhängig konzipiert, um es auf möglichst viele der Amazon Web Services anwenden zu können.
Betrachtet werden drei Perspektiven, die Rollen der Nutzung der AWS-Cloud-Setups entsprechen: **Outsider**, **User** und **Admin** (siehe Abbildung 4). Für jede Perspektive wird ein individueller Durchlauf-Zyklus beschrieben. Ebenso sind die Übergänge von einer in eine andere Perspektive definiert. Konnte der Tester in der Perspektive Outsider ein Ziel, z.B. Rechteausweitung, erreichen, so ist es möglich in die nächsthöhere Perspektive User zu wechseln. Die Unterteilung in Perspektiven ermöglicht eine weitreichende Flexibilität für unterschiedliche Testszenarien. Jeder Zyklus innerhalb der Perspektiven bietet den Testern eine Struktur, mit der sie möglichst viele Aspekte der AWS-Cloud nachvollziehbar und wiederholbar analysieren können.

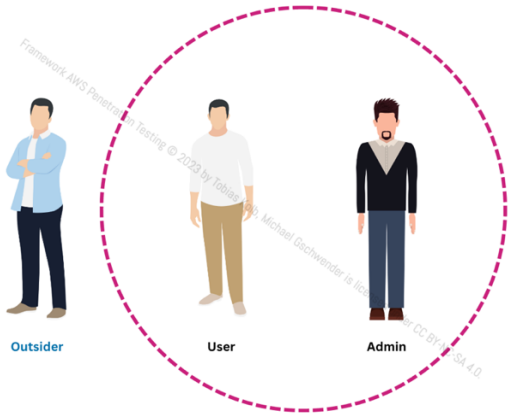

Abbildung 4 Die Drei Perspektiven im AWS-Framework

Outsider: Diese Perspektive beschreibt einen Tester, welcher eine AWS-Cloud-Umgebung von „außen“ testet. Im Gegensatz zu den anderen beiden Perspektiven ist der Outsider per Definition nicht in der Lage sich gegenüber AWS zu authentifizieren. Das Ziel des Outsiders ist es, sogenannte „Interaction Points“ zu generieren, welche für eine mögliche Exploitation ausgenutzt werden können. Im weiteren Verlauf werden alle Interaction Points weiter analysiert, um die Möglichkeit für ein erfolgreiches Ausnutzen feststellen zu können.
Ein ausschlaggebender Unterschied zu Microsoft Azure liegt in den öffentlich verfügbaren Schnittstellen (APIs). Eine Validierung auf bestehende Benutzer eines Azure AD Tenants kann als Outsider problemlos vollzogen werden, wohingegen eine AWS-Cloud-Umgebung diese Möglichkeit nicht bietet.

User: Diese Perspektive ist in der Lage sich gegenüber einer AWS-Cloud-Umgebung zu authentifizieren. Dabei hat der User aber in keinem AWS-Service die höchsten Berechtigungen. Ziel dieser Perspektive ist sowohl eine laterale Ausbreitung als auch eine Eskalation von Privilegen (Privilege Escalation) zu identifizieren.

Admin: Der Admin stellt eine Perspektive dar, die in der Lage ist sich gegenüber mindestens einem AWS-Service mit den höchstmöglichen Rechten zu authentifizieren.

Im Rahmen der Thesis wurde dieses AWS-Penetration-Testing-Framework anhand von etablierten AWS-Cloud-Security-Training-Labs evaluiert. Dabei wurden Kriterien, wie die Menge der vorhandenen Angriffsvektoren, die sinnvolle Gestaltung des Phasenwechsels, sowie die Überprüfung, ob die Phasen vollständig durchlaufen wurden, berücksichtigt. Als Ergebnis dieser Evaluierung konnten die Angriffsvektoren durch die Anwendung des Frameworks gefunden werden - die Anordnung der Phasen konnte als sinnvoll belegt werden. Einschränkungen gab es vor allem in der Recon und Enumeration-Phase. Hier waren die betrachteten Training-Labs stellenweise zu ausführlich im Internet in sog. Walkthroughs dokumentiert. Walkthroughs stellen eine Schritt-für-Schritt Anleitung zu einer bestimmten Problemstellung dar. Während einer ausführlichen Recon und Enumeration-Phase hätte man diese Walkthroughs problemlos entdeckt und hätte dadurch eine Musterlösung zu der Aufgabenstellung des Training-Labs. Dies hätte allerdings das Ergebnis der Evaluierung verfälscht.

5. Conclusion

Unternehmen haben das Potential von Cloud Lösungen für ihre Geschäftsmodelle verstanden und bereits damit begonnen diese Technologie intensiv zu nutzen. Ausfallsichere Infrastrukturen können skalierbare Business Cases passgenau abbilden und Unternehmen bei der Erreichung Ihrer Geschäftsziele unterstützen.
Auf der anderen Seite konnten aber auch fatale Fehler bei der Konfiguration und im Betrieb von Cloud Szenarien festgestellt werden. Einigen Unternehmen haben diese Fehler enormen Schaden zugeführt. Egal ob dies ein finanzieller und/oder Image Schaden war. Gezielte und strukturierte Penetration Tests und Red Teaming Einsätze bieten die Chance, mögliche Angriffe und daraus resultierende Schäden zu verhindern.
Weiterführende Informationen zum Framework und dessen Verwendung sowie der Anfrage nach Penetration Tests oder Red Team Assessments für Ihre AWS-Umgebungen finden sie auf meinem **Blog**.[19]

Anfragen gerne an:

- t.kolb@reply.de oder per LinkedIn
- max.moser@hdbw-hochschule.de
- sabine.rathmayer@hdbw-hochschule.de

Mehr zur HDBW: https://www.hdbw-hochschule.de/

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