Wenn es Schwachstellen regnet

Wie prüft man die Sicherheit cloudbasierter Infrastrukturen?

17. März 2022 – Jan-Tilo Kirchhoff, Compass Security Deutschland GmbH

Darf ich mich vorstellen?

Jan-Tilo Kirchhoff

- Geschäftsführer Compass Security Deutschland GmbH
- verheiratet, zwei erwachsene Kinder
- Werdegang: Von der TK-Security zur IT-Security
- Kompetenzen
  - Netzwerk Sicherheitsprüfungen
  - ICT- Security (VoIP, PSTN, GSM …)
  - IT-Forensik

Hobbys

- Meine Familie
- Musik (Trompete und Chor)
- Electronic Jazz, Jazz Funk
- Laufsport
- ICT-Security

CISSP® Certified Information Systems Security Professional

OFFENSIVE security (OSCP)®

Red Team Operator

Awarded to **Jan-Tilo Kirchhoff**

Issued on **28.02.2022** at 9:36 PM

Compass Crew

Was macht Compass?

seit 1999

Penetration Tests

Als Angreifer untersuchen wir Geräte, Netze, Dienste und Anwendungen auf Schwachstellen. Mittels Social Engineering und Red Teaming testen wir das Verhalten der gesamten Organisation.

Digital Forensics

Unsere Forensik-Experten helfen bei der Koordination von Vorfällen und Sofortmassnahmen sowie bei der gerichtsfesten Bearbeitung von Daten. Zudem bieten wir eine unkomplizierte und schnelle Ursachenforschung.

Security Reviews

Erfahrene IT Analysten unterstützen Sie mit Zweitmeinungen zu Security-Konzepten und prüfen nach Wunsch den Aufbau, die Konfiguration und den Quellcode Ihrer Lösung.

Security Trainings

Profitieren auch Sie vom Wissen unserer Analysten zu Penetration Testing, Netzwerkanalyse, sichere Apps und Anwendungen, Digitale Forensik und trainieren Sie in einem eigens dafür erstellten Labor.

Wir sind “nette” Hacker

Bild von Free-Photos auf Pixabay

Klassischer Penetrationstest

https://commons.wikimedia.org/wiki/File:Deal_Castle_Aerial_View.jpg

Penetrationstest

Ablauf

- Scope – Was soll geprüft werden?
- Information Gathering – Welche Informationen stehen dem Angreifer zur Verfügung?
- Service and Vulnerability Discovery – Welche (angreifbaren) Ziele gibt es?
- Manual Hacking & Exploitation
  - Initial Access – Welche Angriffsvektoren führen zum Ziel?
  - Persistance – Wie kann ein späterer Zugriff sichergestellt werden?
  - Privilege Escalation – Ausweitung der Zugriffsrechte
  - Lateral Movement – Ausweitung des Zugriffs auf weitere Systeme
  - Exfiltration – Welche Daten kann der Angreifer finden, wie kann er diese entwenden?
- Reporting – Aufbereitung der Ergebnisse als Grundlage für Verbesserungsmaßnahmen
- Debriefing – Abschlussbesprechung mit dem Kunden (und den Verteidigern)

Was heißt eigentlich Cloud?

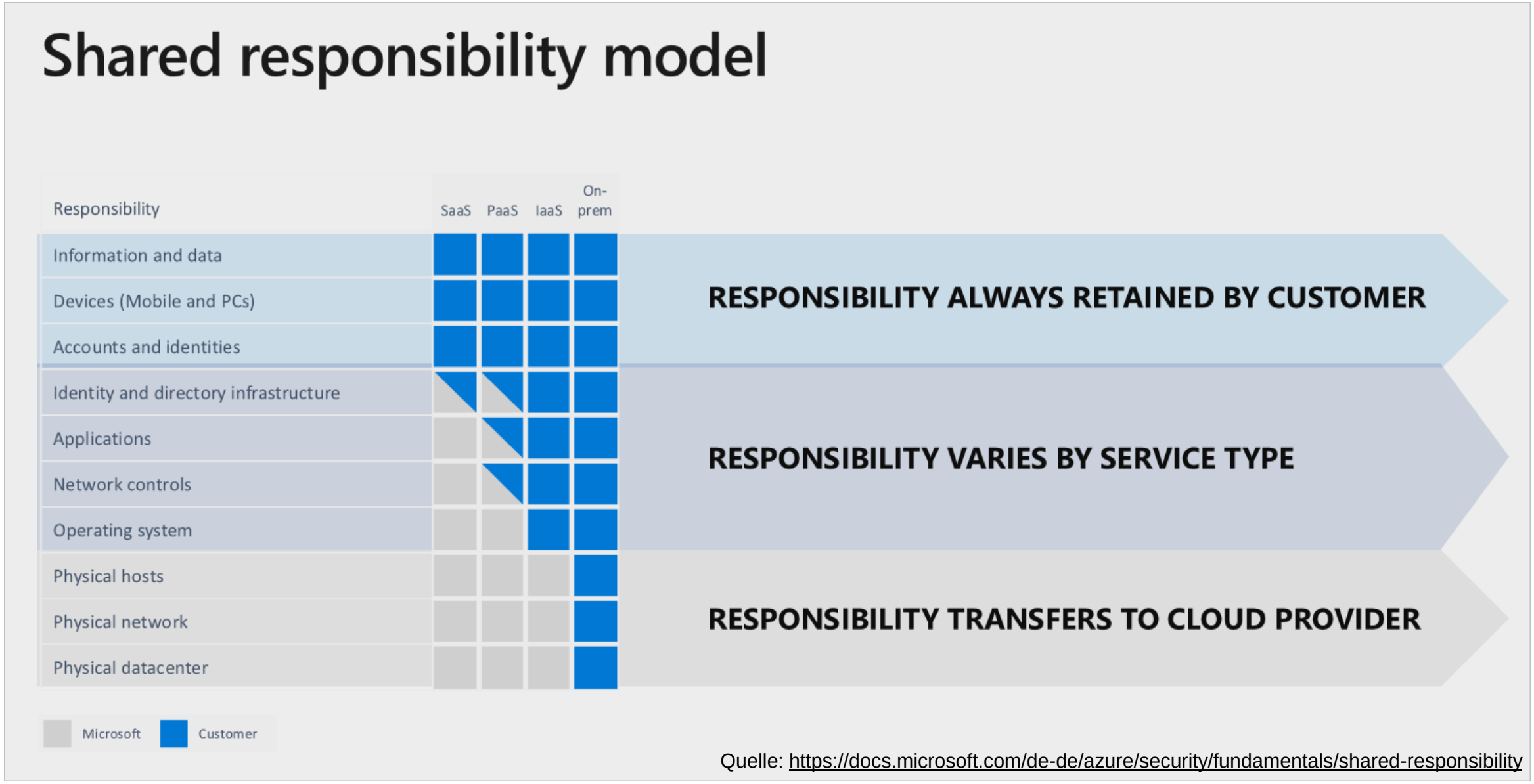
- Public vs. private

- IaaS – Infrastructure as a Services
- PaaS – Platform as a Service
- SaaS- Software as a Service

- Container Services
- Serverless

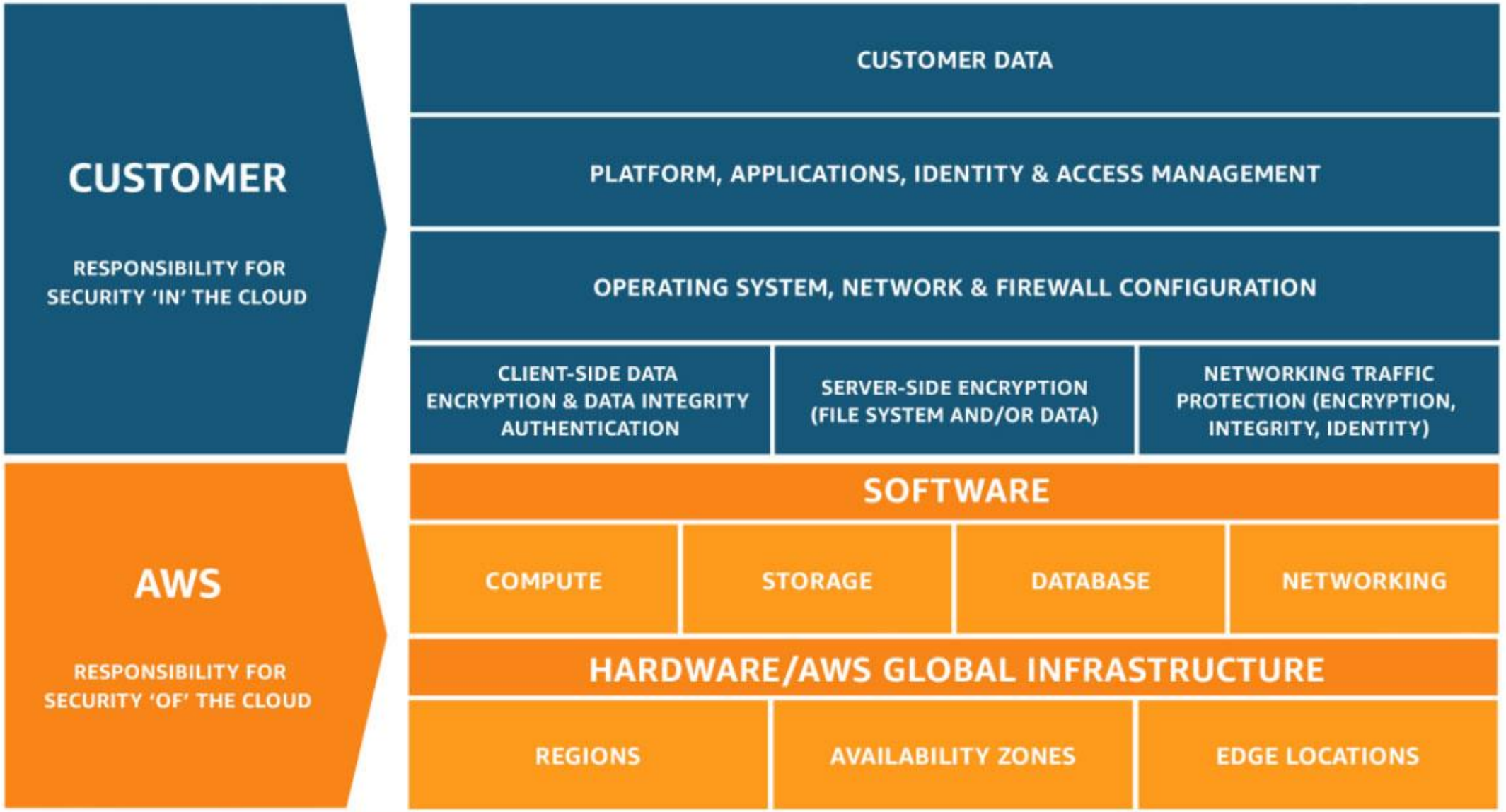
Quelle: https://pizza.de/pizza-wiki/pizza-napoli.html

Microsoft Azure



Quelle: https://docs.microsoft.com/de-de/azure/security/fundamentals/shared-responsibility

AWS



Quelle: https://aws.amazon.com/de/compliance/shared-responsibility-model/

Google

Quelle: https://www.alertlogic.com/solutions/platform/google-cloud-security/

Rechtlicher Rahmen des Penetrationstests

Einwilligung des Cloud Service Providers

- Datenschutz
- Nutzungsbedingungen
- Strafrecht

Relevante Links:
https://aws.amazon.com/de/security/penetration-testing/

https://www.microsoft.com/de-de/msrc/pentest-rules-of-engagement

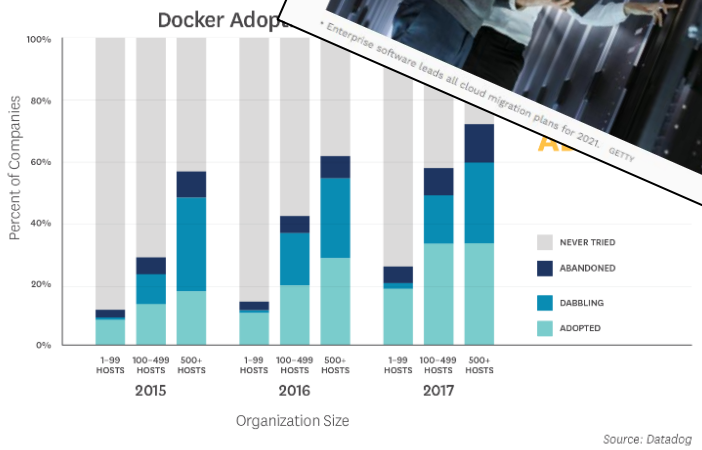
https://cloud.google.com/security/overview?hl=de

Wo sind hier die Grenzen?

Cloud Computing & Microservice Architectures

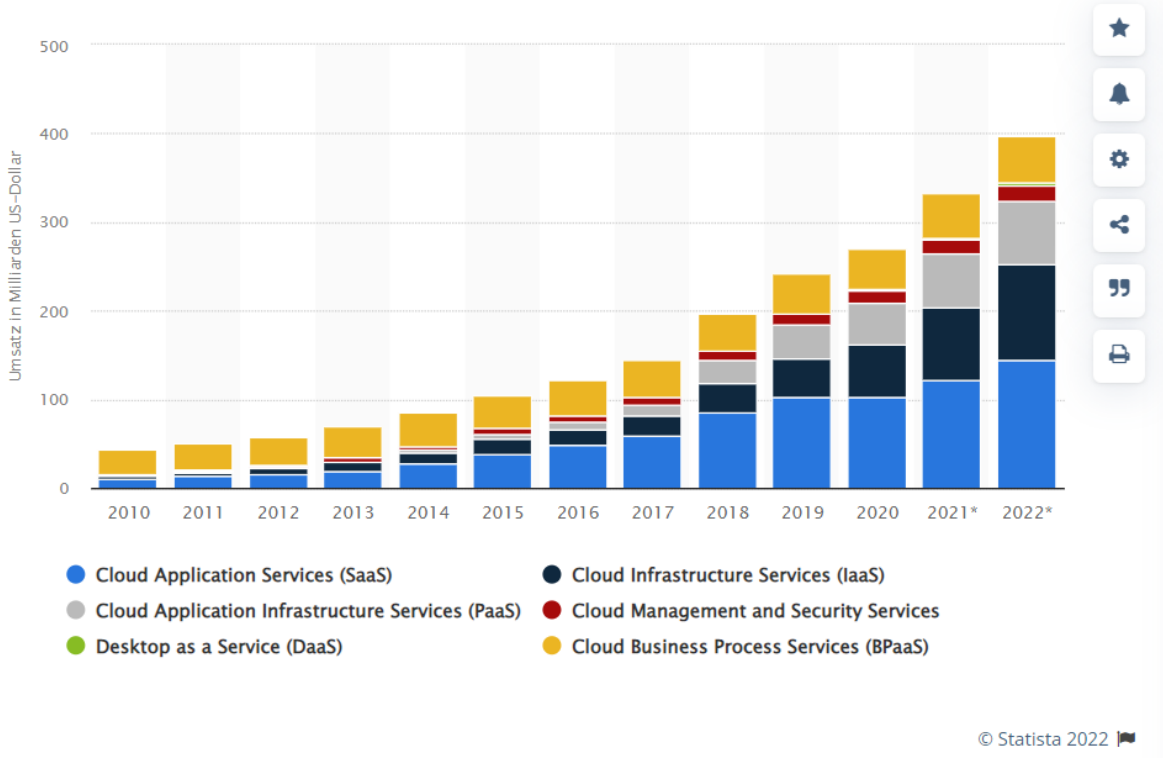
“In 15 months, 80% o budgets will be committed to nd solutions” – Forbe

- Weiteres Wachs
  - Container / M
  - Orchestrati
  - DevOps

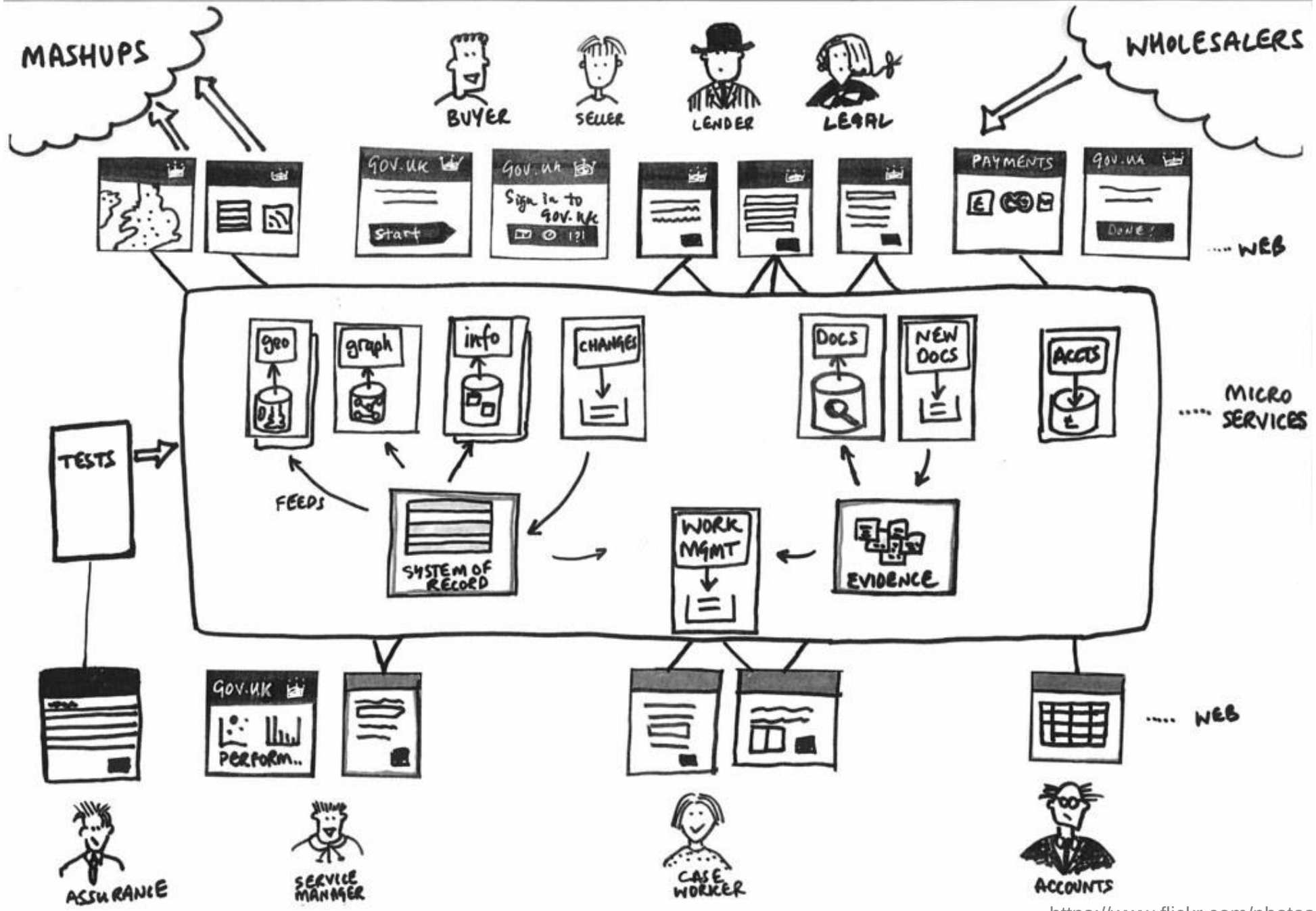


Quelle: https://www.datadoghq.com/docker-adoption/

Umsatz mit Cloud Computing weltweit von 2010 bis 2020 und Prognose bis 2022 nach Segment



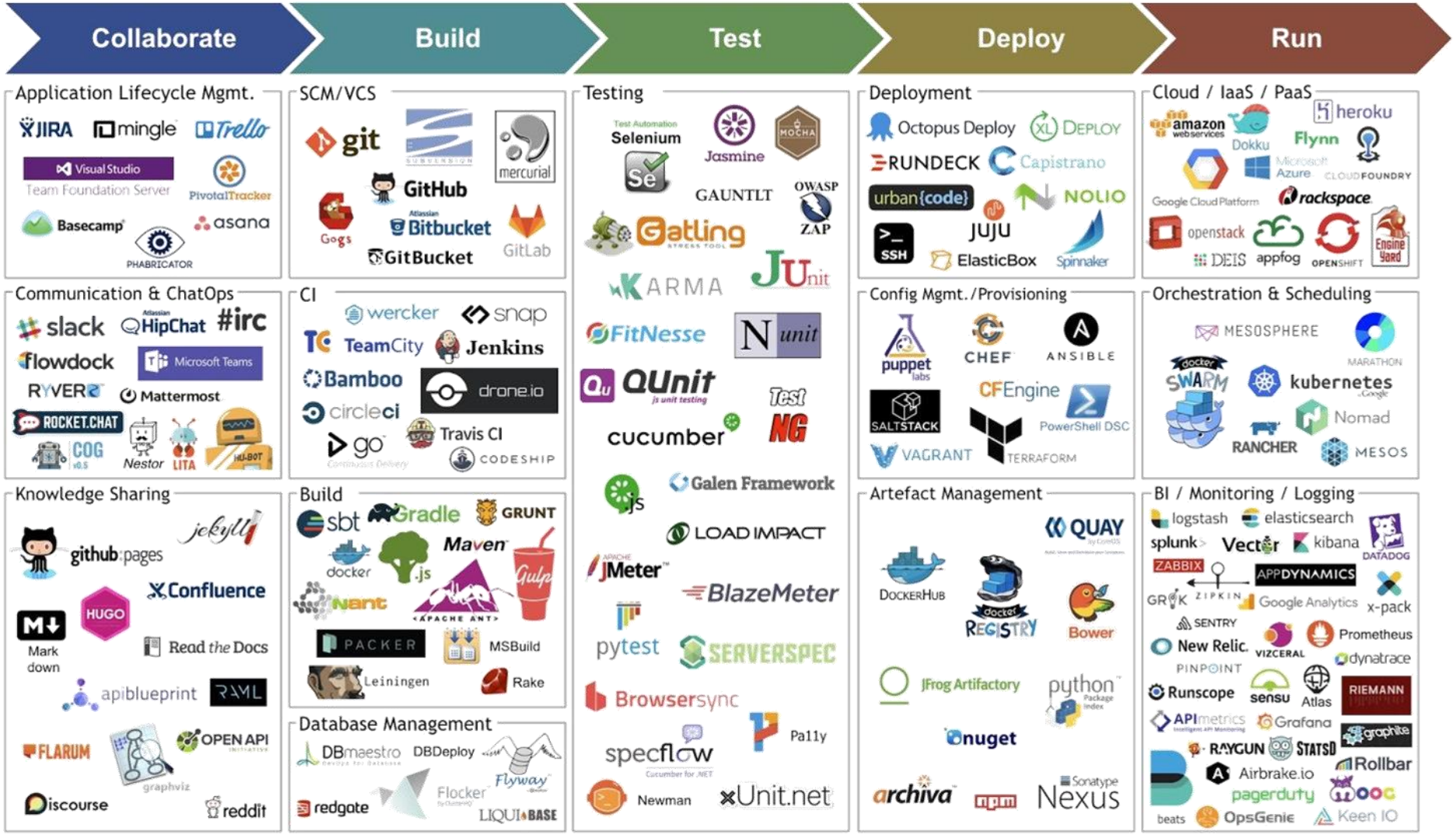
Quelle: https://de.statista.com/statistik/daten/studie/284706/umfrage/prognose-zum-umsatz-mit-cloud-computing-weltweit-nach-segment/



https://www.flickr.com/photos/psd/13109673843

Quis custodes custodiae?

Was ist mit der Entwicklungs und Management Infrastruktur



http://maximelanciauxbi.blogspot.de/2017/04/devops-tools.html

Bekannte Vorfälle aus der Vergangenheit

München 21°

Süddeutsche Zeitung

SZ.de Zeitung Magazin

Shop Jobs Immobilien Anzeigen

Login Abo

Coronavirus Politik Wirtschaft Meinung Panorama Sport München Bayern Kultur Gesellschaft Wissen Reise Auto mehr...

Home > Digital > IT-Sicherheit > Datendiebstahl bei Capital One: Der Kick beim Hacken

5G - Die Zukunft

30. Juli 2019, 17:43 Uhr Datendiebstahl bei Capital One

Die Hackerin, die zu viel prahlte

Eine 33-jährige Hackerin wurde verhaftet, weil sie Bank-Daten von 100 Millionen US-Bürgern gestohlen haben soll. (Foto: AFP)

t:n News Magazin Wissen Themen Pioneers Jobs Firmen Events Shop Anmelden

News > Software & Infrastruktur > Datenleck: Infos von 250 Millionen Microsoft-Support-Kunden waren gefährdet

News

Datenleck: Infos von 250 Millionen Microsoft-Support-Kunden waren gefährdet

Facebook Twitter WhatsApp Pocket E-Mail

Beichte nach Leckreparatur: Bei Microsoft lagen Unmengen Support-Kundendaten offen im Netz. (Foto: VDB Photos / Shutterstock)

23.01.2020, 15:31 Uhr

Julius Beineke

Online-Redakteur und Vollzeit-Nerd. Schreibt über Software, Peripherie, Netzkultur und...

Verwandte Themen

Datenschutz Leak Microsoft Server Adobe

Und von heute

The Daily Swig

Cybersecurity news and views

About

Regions · Hacking News · Data Breaches · Cyber-attacks · Vulnerabilities · Bug Bounties · More

Insecure Amazon S3 bucket exposed personal data on 500,000 Ghanaian graduates

John Leyden 06 January 2022 at 10:58 UTC
Updated: 10 January 2022 at 09:40 UTC

Data Leak · Africa · Cloud Security

Cloud storage misconfiguration left sensitive data openly accessible

UPDATED Authorities in Ghana are investigating an apparent data breach that may have exposed the personal information of hundreds of thousands of citizens of the west African country.

Security Boulevard

Home · Security Bloggers Network · Events · Chat · Library · Related Sites · Media Kit · About Us

ANALYTICS · APPSEC · CISO · CLOUD · DEVOPS · GRC · IDENTITY · INCIDENT RESPONSE · IOT / ICS · THREATS / BREACHES · MORE · HUMOR

Home » Cybersecurity » Data Security » Azure Blob Data Breach Reveals Student Information

Azure Blob Data Breach Reveals Student Information

by Eric Kedrosky on February 8, 2022

An Azure Blob Data Breach

Just a few days ago, the British Council experienced a high-magnitude Microsoft Azure blob data breach compromising hundreds of thousands of student files. These files contained personal student information like names, emails, enrolment details, as well as their login credentials, and were ultimately exposed publicly online. The culprit, an unsecured blob repository.

AzureDemo101

AzureDemo101

Dies ist eine Demoseite für den Workshop "Cloud Security" am 31.03.2022 auf der SecIT in Hannover

GIT Issues

Internetwache.org
Für ein sichereres Internet

Start | Idee | Team | Securitycheck | FAQ | Projekte | Archiv | Kontakt

DI, 28. JULI 2015

Wie ungeschützte .git Repositorys die Sicherheit Ihrer Webseite gefährden - Eine Analyse der Alexa 1M

Sebastian hat vor einigen Monaten an einem CTF (capture the flag) teilgenommen. Eine Aufgabe mit der er dabei konfrontiert wurde, war das Wiederherstellen eines `.git` Repository's auf einem Webserver, welcher Directory-Listing eingeschaltet hatte. Mit der Auflistung der Verzeichnisinhalte ist das Auslesen vergleichsweise einfach, aber geht es auch ohne? Schließlich kann man damit eine Menge Schindluder treiben, etwa fremde `.git` Repository auslesen und somit Zugriff auf den Quellcode einer Webseite und ggf. Passwörter erhalten.

Also beschäftigten wir uns etwas mehr mit der Materie, schrieben einige kleine Tools und haben ein paar Beobachtungen angestellt, die wir gern weitergeben möchten. Das Ergebnis war zwar nicht so dramatisch, wie befürchtet, aber dennoch überraschend.

TL; DR

Einige Webseiten hosten ihre Versionierungs Repositorys (wie zum Beispiel `.git/`) öffentlich. Das ermöglicht Angreifern das Herunterladen und Wiederherstellen der Repositorys, um Zugriff auf den Quellcode einer Applikation zu erhalten. Bitte prüfen Sie die Konfiguration Ihres Webservers, um sicherzustellen, dass der Zugriff von außen auf diese Dateien nicht möglich ist.

Was ist ein Versionierungstool?

Vor einigen Jahrzehnten standen Entwickler vor dem Problem gemeinsam aus der Ferne Programme zu entwickeln. Um diesem Problem Abhilfe zu schaffen, wurden Versionierungstools entwickelt. Die primäre Aufgabe dieser Tools ist es verteilte Arbeit an einem zentralen Quellcode zu ermöglichen. Das wird unteranderem darüber erreicht indem sämtliche Codeänderungen (meist "Commit" genannt) protokolliert werden. Ein sehr bekanntes Tool zur Versionierung heißt `git` und wurde damals von Linus Torvalds ins Leben gerufen. Auch im Web ist git mittlerweile stark vertreten, Webseiten wie github.com bieten das kostenlose Hostin dieser Repositorys an.

Wir haben uns während der Arbeit an diesem Artikel primär auf `git` fokusiert:

- Git

Es gibt allerdings noch eine Vielzahl anderer Versionierungstools, die ebenfalls das hier beschriebene Verhalten aufweisen können:

Letzte Beiträge

- Jahresrückblick 2018
- Analyse der .DS_Store-Datei in den Alexa Top 1 Millionen
- Jahresrückblick auf 2017 / Ausblick 2018
- Certificate Transparency als Quelle für Subdomains
- Update zu 2017 - Und wir leben noch!
- Jahresrückblick auf 2016 / Ausblick 2017
- Analyse zum Vorgehen einer Kryptomining-Malware
- Wie wir Wasserwerke im Internet entdeckten
- Zu Besuch auf Troopers 2016
- Internetwache CTF 2016 im Rückblick

Kategorien

- Bug bounty (9)
- Code disclosure (1)
- Csrf (6)
- Events (7)
- Full path disclosure (8)
- Hall of fame (11)
- Internet (17)
- Local file inclusion (1)
- Loginbypass (1)
- Path traversal (1)
- Rce (1)
- Sqli (10)
- Vermittlung (2)
- Xss (34)

https://www.internetwache.org/wie-ungeschutzte-git-repositorys-die-sicherheit-ihrer-webseite-gefahrden-eine-analyse-der-alexa-1m-28-07-2015/

flaws.cloud

flAWS - Level 3

Lesson learned

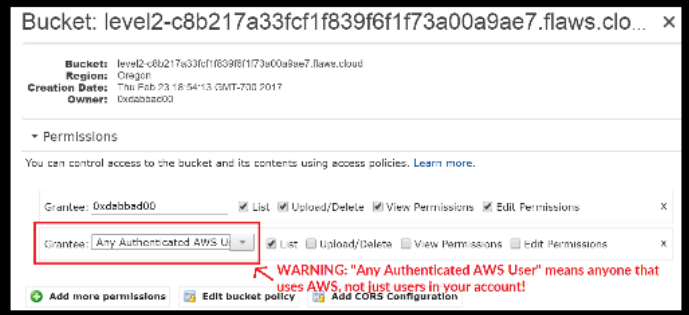
Similar to opening permissions to "Everyone", people accidentally open permissions to "Any Authenticated AWS User". They might mistakenly think this will only be users of their account, when in fact it means anyone that has an AWS account.

Examples of this problem

- Open permissions for authenticated AWS user on Shopify (link)

Avoiding the mistake

Only open permissions to specific AWS users.

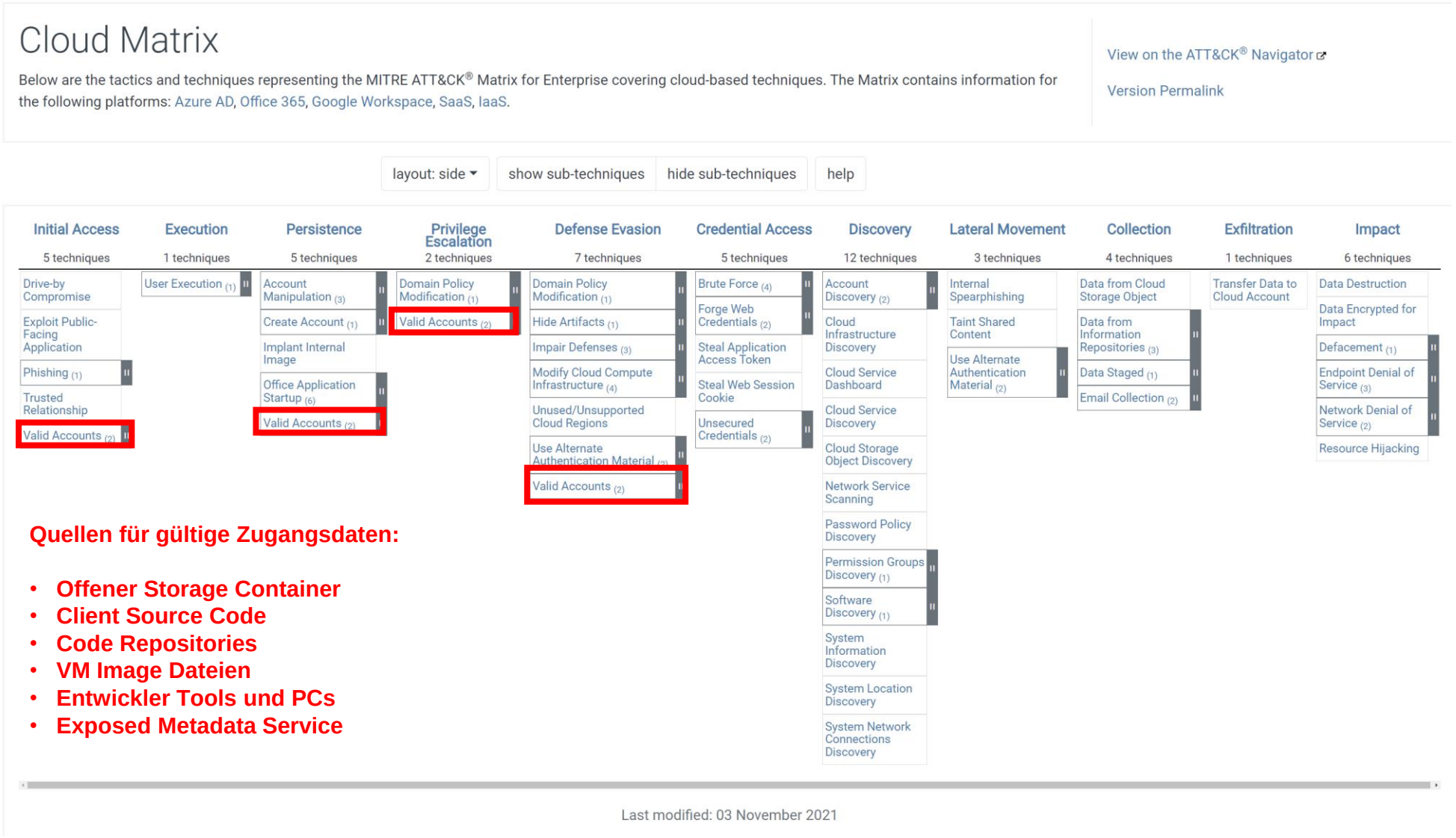


Level 3

The next level is fairly similar, with a slight twist. Time to find your first AWS key! I bet you'll find something that will let you list what other buckets are.

For hints, see Hint 1

MITRE ATT&CK



Quellen für gültige Zugangsdaten:

- **Offener Storage Container**
- **Client Source Code**
- **Code Repositories**
- **VM Image Dateien**
- **Entwickler Tools und PCs**
- **Exposed Metadata Service**

Quelle: https://attack.mitre.org/matrices/enterprise/cloud/

Metadata Service

```
$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/ExampleRole
{
  "Code" : "Success",
  "LastUpdated" : "2018-01-25T23:15:40Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "AKJBD787KHV7JHV7JGC9",
  "SecretAccessKey" : "oqfqoufbqow/qwobOUBuIViyciycIY7ivy7gcUCj",
  "Token" : "FQoDYXdzEID//[CUT BY COMPASS]yUEn5aZeT4o88mp0wU=",
  "Expiration" : "2018-01-26T05:40:31Z"
}
```

→ SSRF

AzureDemo102

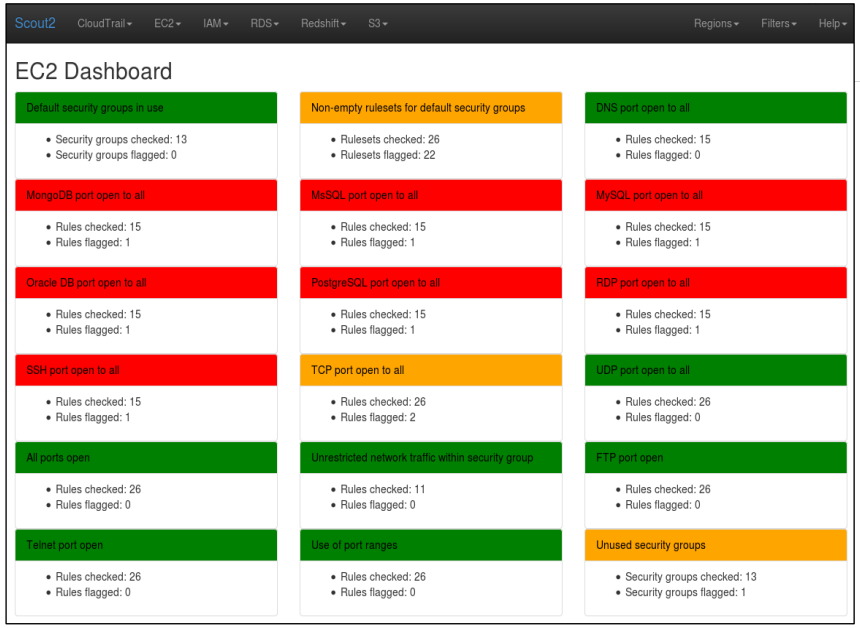
AzureDemo 102

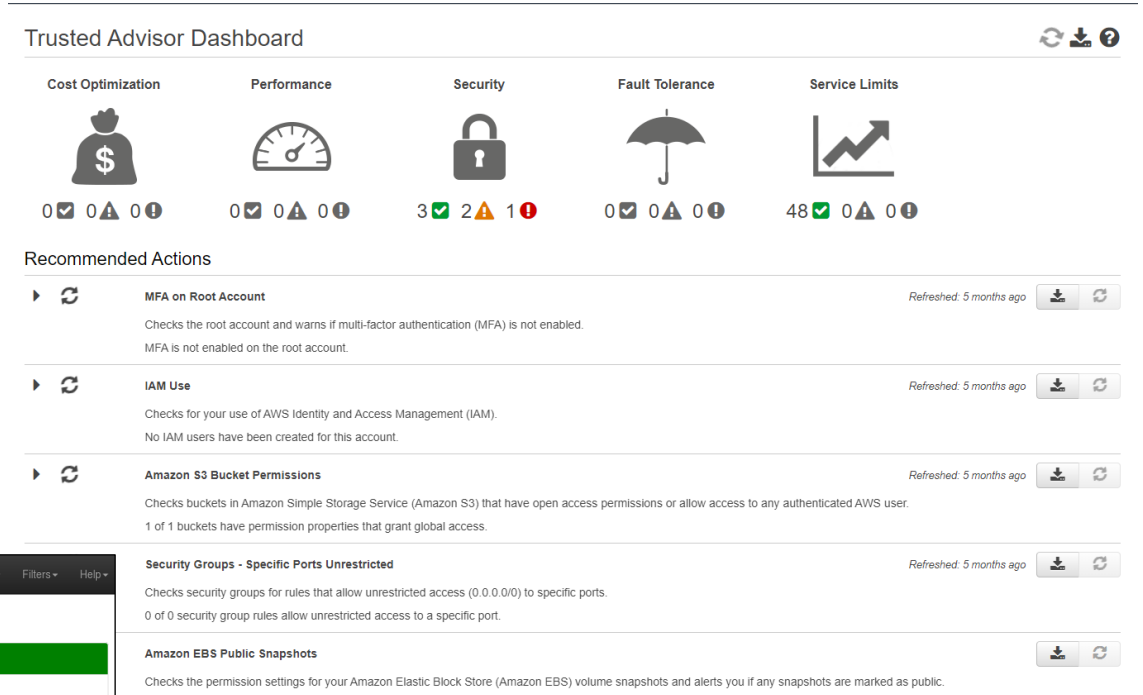
The real content for this challenge is located on a webserver which is not directly accessible from the internet.
Please continue here.

Dies ist eine Demoseite für den Workshop "Cloud Security" am 31.03.2022 auf der SecIT in Hannover

Security Checks

- Management Console (Web)
  - Trusted Advisor (AWS)
  - Azure Advisor
- CLI
  - aws cli
  - az cli
- Audit Tools
  - ScoutSuite
  - Prowler
  - …

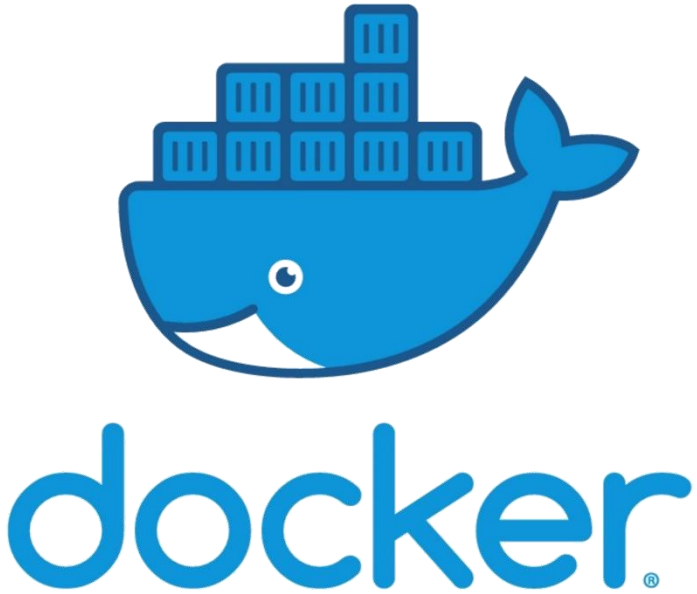




What is Docker? What is a Container?

- Docker
  - is a container manager
  - allows software to be executed in Containers
  - is lighter and faster than VMs
  - allows resource isolation from the kernel

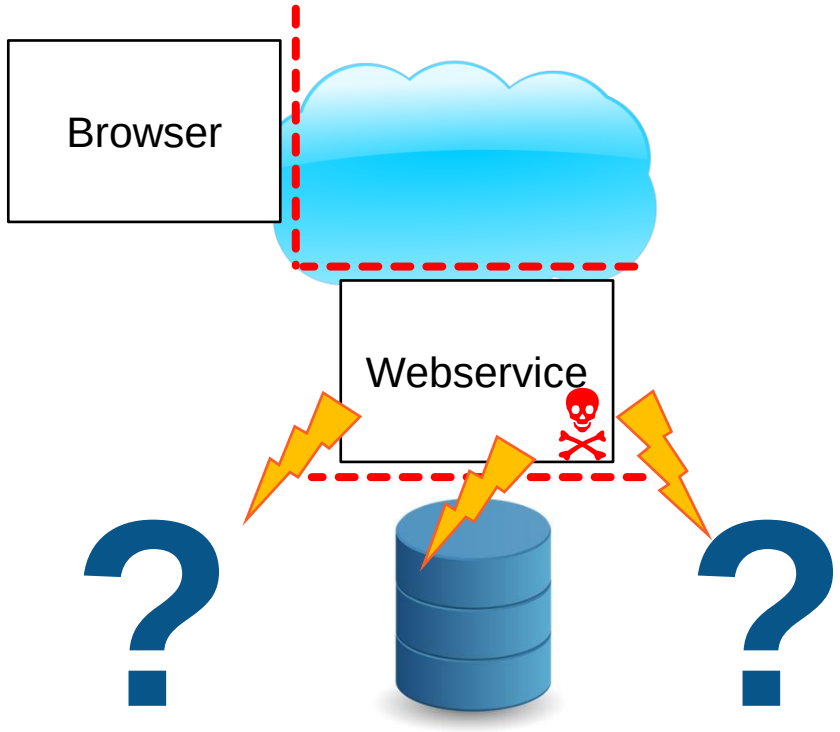
- Containers
  - separate running processes from the host
  - use the host's kernel
  - have their own environment
  - can be used to deploy applications
  - contains all dependencies that the target application needs



Wo geht‘s weiter?

Lateral Movement

Vertrauensstellung ausnutzen



Rechte Eskalation

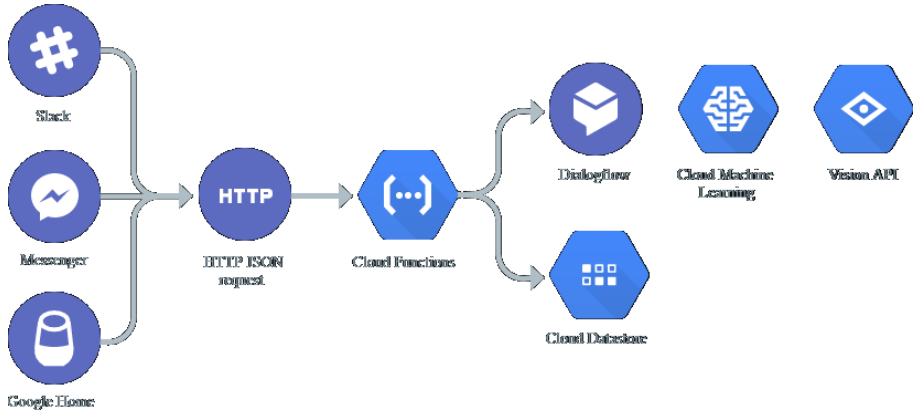
Dirty COW (CVE-2016-5195)

https://upload.wikimedia.org/wikipedia/commons/thumb/1/1b/DirtyCow.svg/895px-DirtyCow.svg.png

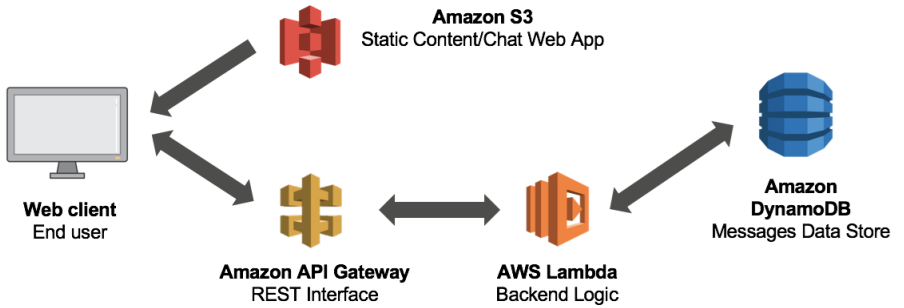
Dirty Pipe (CVE-2022-0847)

Serverless

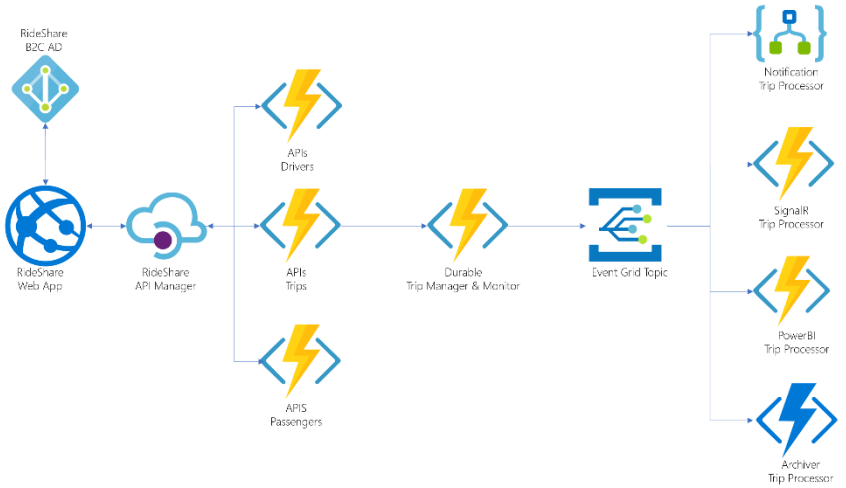
https://cloud.google.com/functions?hl=ca



https://aws.amazon.com/de/lambda/



https://docs.microsoft.com/en-us/samples/azure-samples/serverless-microservices-reference-architecture/serverless-microservices-reference-architecture/



One more thing …

Tatsächlich sind es zwei Punkte

- Subdomain Takeover
  - Verwaiste DNS Einträge zeigen auf IP Adressen in der Cloud
    - z.B. SuperSommerSchlussverkaufsLotterie.IhreFirma.de
    - Angreifer hosten ihren eigenen Dienst in der Cloud unter einem gültigen DNS Eintrag
  - Prüfen Sie regelmäßig ihren DNS Server, am besten über automatisierte Prozesse

- Auto Scaling
  - Gut für die Verfügbarkeit, u.U. schlecht für das Konto
    - DoS Angriffe führen nicht zum Ausfall des Service, sondern zu Bereitstellung von Resourcen
  - Richten Sie Monitoring und Budgets ein

Der Pentest ist vorbei, was nun?

Risikobewertung, Priorisierung, Behebung, Retest

- Führen Sie eine Risikobewertung der Ergebnisse durch
  - In der Regel hat der Pentester keine Kenntnisse über die wirtschaftliche Relevanz der gefundenen Schwachstellen
  - Im besten Falle kann ein technisches Risiko ermittelt werden
- Priorisieren Sie die Punkte anhand der Risikobewertung
- Beheben Sie die wesentlichen Schwachstellen (oder verhindern sie deren Ausnutzung)
- Überprüfen Sie die Gegenmaßnahmen
  - Integration in automatisierte Tests?
  - Ggf. erneute Prüfung durch den Pentester

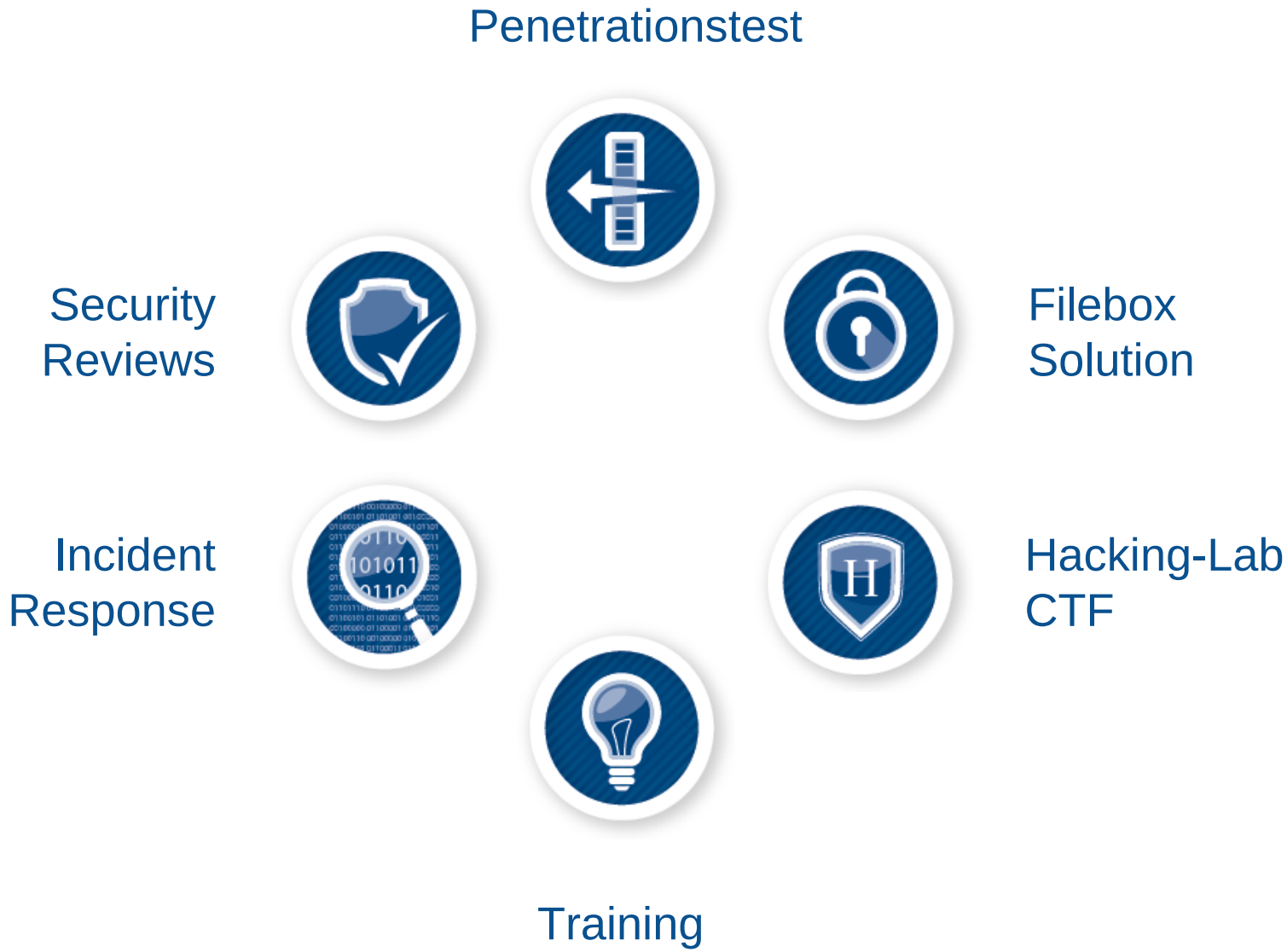
Zusammenfassung

Was ist für die Planung eines Cloud Penetrationstests wichtig

- Penetrationstest ≠ Penetrationstest
- Gute Vorbereitung ist notwendig
  - Wo sind meine Kronjuwelen?
  - Was gehört alles zu meiner Infrastrukur?
  - Wie schätze ich die Bedrohungslage ein?
  - Wen muss ich informieren?
    - Von wem benötige ich eine Einwilligung und wie lange dauert es diese zu bekommen?
  - Habe ich alle mir bekannten Sicherheitsmaßnahmen getroffen?
    - Welche davon kann ich selbst mit Bordmitteln und frei verfügbaren Werkzeugen prüfen?
- Wann führe ich Penetrationstests durch?
- Automatisierung ist hilfreich, birgt aber auch neue Risiken
- Ergebnisse müssen genutzt werden
  - Wie integriere ich die Ergebnisse mit meinen Entwicklungs- und Betriebsprozessen?

Zeit für Ihre Fragen

Compass Security Portfolio



Compass Security Deutschland GmbH
Tauentzienstraße 18
10789 Berlin

team.csde@compass-security.com