Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

# Sicher in der Cloud

Über die Bedrohung von Cloud-Sicherheit
aus der Cloud-Nutzer Perspektive

Heiko Großkopf, Referent BSI

Omnisecure – Berlin 2024

# Cloud-Dienste angreifen – Wie gehen wir vor?

- Es ist i.d.R. einfacher Cloud-Nutzer direkt anzugreifen als einen Cloud-Anbieter zu hacken
- Suche nach [öffentlich] erreichbaren Cloud-Diensten und Zugangsdaten
  - Mittels Open Source Intelligence (OSINT)
    - Suchmaschinen wie Google und Shodan; Tools zur Enumeration, z.B. von Subdomains (DNS)
      - Wir finden Web- und Cloud-Services, APIs, Portale, ggf. offenen Cloud-Speicher, Datenbanken etc.
    - Wir sammeln alle Informationen die wir bekommen können
      - Benutzernamen, Credentials, Token, weitere Informationen über Services …
      - In öffentlich verfügbaren Dokumenten, Cloud-Speichern, Code-Repos, auf Social-Media und Hacker-Seiten
      - Es gibt überall Hilfestellungen für Angreifer, z.B. zu Google Dorking oder anderen Tools
  - Wenn das nicht ausreicht, nutzen wir die Informationen für weitere Schritte, z.B.
    - [Spear-]Phishing, generell Social-Engineering
    - Malware, Angriff auf Drittsysteme und Clients, um an Credentials zu gelangen

# Prinzip der geteilten Verantwortlichkeiten

| Verantwortlichkeiten | On-Premises | IaaS | PaaS | CaaS | FaaS | SaaS |
|---|---|---|---|---|---|---|
| Client-Sicherheit | Nutzer | Nutzer | Nutzer | Nutzer | Nutzer | Nutzer |
| Datensicherheit | Nutzer | Nutzer | Nutzer | Nutzer | Nutzer | Nutzer |
| IAM | Nutzer | Nutzer | Nutzer | Nutzer | Nutzer | Nutzer |
| Functions | Nutzer | Nutzer | Nutzer | Nutzer | Nutzer | Anbieter |
| Applikationen | Nutzer | Nutzer | Nutzer | Nutzer | Anbieter | Anbieter |
| Laufzeitumgebung | Nutzer | Nutzer | Nutzer | Anbieter | Anbieter | Anbieter |
| Middleware | Nutzer | Nutzer | Anbieter | Anbieter | Anbieter | Anbieter |
| Betriebssystem | Nutzer | Nutzer | Anbieter | Anbieter | Anbieter | Anbieter |
| Virtualisierung | Nutzer | Anbieter | Anbieter | Anbieter | Anbieter | Anbieter |
| Phyisches Netzwerk | Nutzer | Anbieter | Anbieter | Anbieter | Anbieter | Anbieter |
| Server-Hosts | Nutzer | Anbieter | Anbieter | Anbieter | Anbieter | Anbieter |
| Physische Sicherheit | Nutzer | Anbieter | Anbieter | Anbieter | Anbieter | Anbieter |

# Angriffsfläche Software as a Service (SaaS)

- Zugangsdaten nicht hinreichend geschützt, schwache Passwörter
- Authentifikation nicht sicher konfiguriert, keine Multi-Faktor-Authentifikation
- Kein effektives Rollen-Rechte-Konzept / keine Funktionstrennung, kein Least Privilege
- Anwendung unsicher konfiguriert, z.B.
  - Kann auf vertrauliche Ressourcen/Datenhaltung zugreifen - rwx?
  - Über die Anwendungen kann Code auf Drittsystemen ausgeführt werden (RCE)
- Absicherungsansätze:
  - Aufgezählte Punkte vermeiden
  - Sicherheits-Empfehlungen der Cloud-Anbieter berücksichtigen

# Angriffsfläche Function as a Service (FaaS) – „Serverless“

- Ein Ereignis, löst eine Funktion aus, die Berechtigungen auf weitere Ressourcen hat
- Angriff auf FaaS direkt oder indirekt möglich, z.B. Angriff auf den Auslöser
- Angreifer könnte ggf.
  - die Rechte der Function missbrauchen
  - Secrets aus dem Container der Function auslesen
- FaaS kann missbraucht werden, um Persistenz für Angreifer in Systemen zu erreichen
- Absicherungsansätze:
  - Siehe OWASP Serverless Top 10
  - Loggen und Monitoren von FaaS Diensten

# Angriffsfläche Container und Platform as a Service (CaaS / PaaS)

- Unzureichende Absicherung und Konfiguration der CaaS/PaaS Dienste selbst
  - Angriff/Zugriff auf die Container-Orchestrierung – falsche Konfiguration/Berechtigungen
  - Angriff auf weitere PaaS Komponenten und ihre Lieferkette
- Schwachstellen in Container Images, Software Artefakten und deren Abhängigkeiten
- Nicht vertrauenswürdige bzw. nicht abgesicherte Container-Registries bzw. Code-Repositories

→ Ausnutzung der Anwendungen in den Plattformen z.B. über Web-Schwachstellen

- Absicherungsansätze
  - Sicherheitsempfehlungen des Providers
  - IT-Grundschutzkompendium SYS.1.6 + APP.4.4 zu Container-Sicherheit
  - OWASP Web Security Testing Guide

# Angriffsfläche Infrastructure as a Service (IaaS)

- Bedrohungslage überwiegend wie bei klassischen Servern
  - Ungepatchte Systeme, unzureichende Härtung, Fehlkonfiguration
  - Gesamter Software-Stack auf der virtuellen Maschine
- Angreifer kann nach kompromittierung beliebigen Code ausführen, und weitere Systeme angreifen
- Zugriffe auf Metadata-API höchstwahrscheinlich möglich!
- Angreifer findet Keys und Secrets zum lateral Movement oder Informationen zu höher Privilegierten Konten um Privilegien zu Eskalieren
- Absicherungsansätze
  - Goldene Images
  - Patching
  - Überwachung der Maschinen

# Unsere Empfehlungen

- Nutzen Sie nur so viele unterschiedliche Anbieter wie Sie auch gut beherrschen können.
- Berücksichtigen Sie die Empfehlungen und Best-Practices der Cloud-Anbieter
- Nutzen Sie Cloud-Eigene Sicherheits-, Monitoring- und Logging-Tools
- Nutzen Sie ggf. auch vertrauenswürdige Analyse Tools von Drittanbietern, um [Multi-] Cloud-Umgebungen zu scannen
  - Vermeiden Sie überprivilegierten Konten und Shadow Admins, Nutzen Sie MFA
  - Scannen Sie das System, Images und Software Pakete auf Schwachstellen
- Schützen Sie ihre Secrets, Images und Software-Artefakte – kein hardcoding
- Generelle Informationssicherheit, Web-, Container-, Software-Sicherheit sind weiterhin relevant
- Bevorzugen Sie falls möglich Service-Modelle, die mehr Cloud-Anbieter Zuständigkeiten umfassen
- Machen oder beauftragen Sie Penetrationstests

# Danke für Ihr Interesse

Deutschland
Digital•Sicher•BSI•

**Kontakt**

Heiko Großkopf

cloudsecurity@bsi.bund.de

Quelle: Fotalia