Bedrohungsorientierte Bewertung in Public Cloud-Infrastrukturen

Malte Stoffers, Referat V21,
Bundesamt für Sicherheit in der Informationstechnik

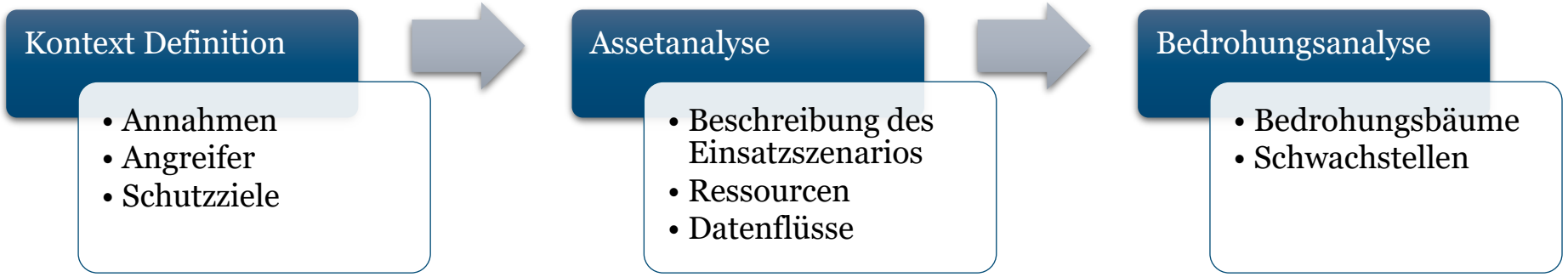
Bedrohungsanalyse

- Ziel: Identifikation von Bedrohungen für behördenspezifische Einsatzszenarien

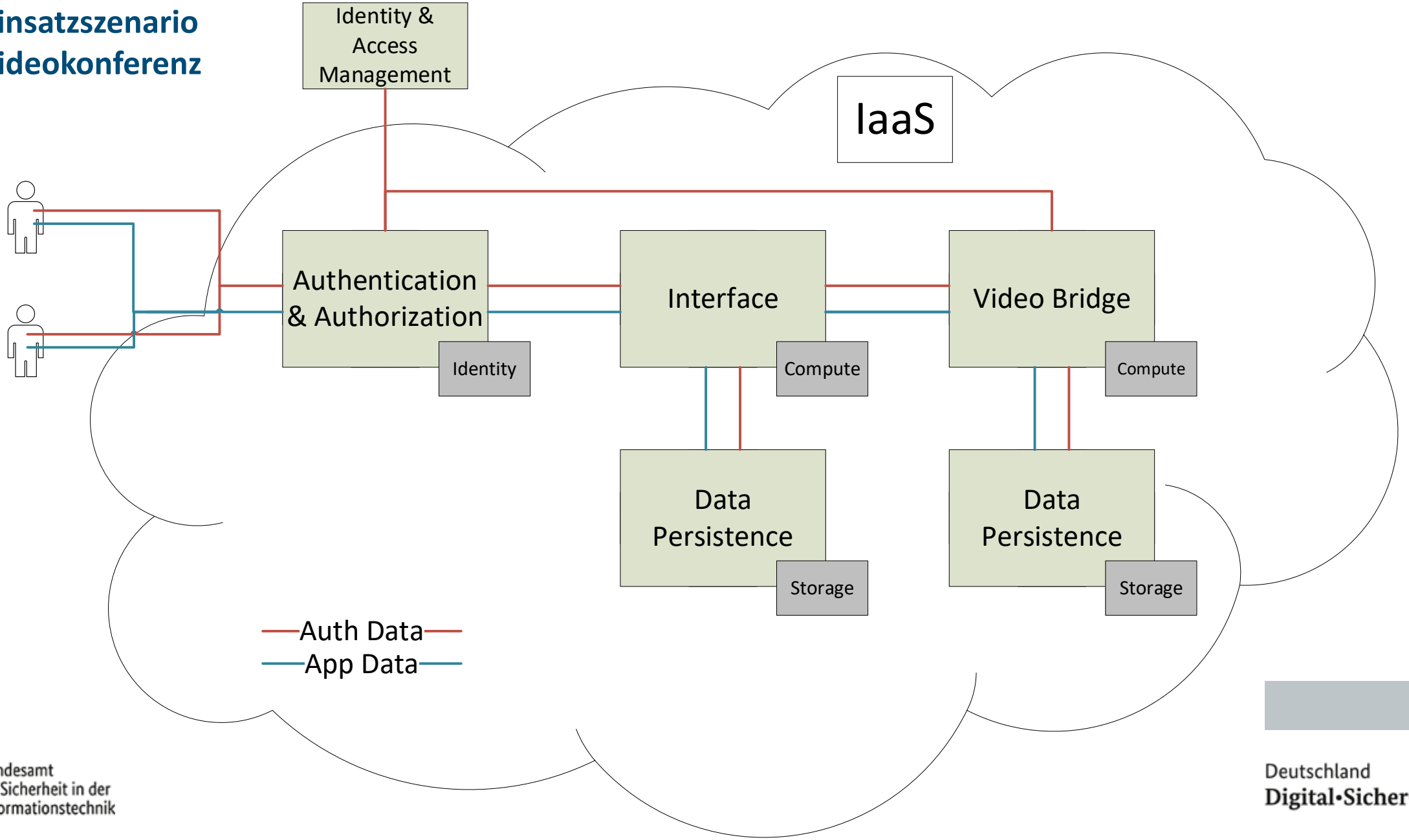
- Fokus auf Komponenten und Services in der Cloud bzgl. der Sicherheitsziele Vertraulichkeit, Authentizität und Integrität von VS-NfD Informationen (Security of the Cloud)
- Struktur:
  - Bedrohung der Vertraulichkeit von VS-Informationen in der Komponente X
  - Bedrohung der Integrität von VS-Informationen in der Komponente X

- Ergebnis: 247 Bedrohungen für 6 Einsatzszenarien identifiziert

Bedrohungen identifizieren



Einsatzszenario Videokonferenz



Bedrohungsanalyse
Einsatzszenario Videokonferenz

Beispiele

- Zugriff auf kryptografisches Schlüsselmaterial
- Kompromittierung von Authentifizierungs- und Autorisierungs-Komponenten
- Schwache/Nicht vorhandene Verschlüsselung
- Kompromittierung des Storage/Compute Backups
- Datenleck durch sensitive Informationen in Log-/Debug Dateien
- Kompromittierung der Supply Chain
- Zugriffserweiterung (Lateral Movement)
- Ausnutzung von Schwachstellen
- ...

Bedrohungen adressieren

Bedrohungen müssen durch wirksame Sicherheitsmaßnahmen adressiert und mitigiert werden

VS-Kontext: Evidenzbasierte Evaluierung und Zulassung von Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen müssen richtig konfiguriert werden (SecOPs im VS-Kontext)

Die Verantwortlichkeit für die Erbringung ist abhängig vom Service Modell

Bedrohungen in der Public Cloud im Kontext VS-Verarbeitung adressieren

- Services zum Key Management
  - Sichere Generierung, Speicherung und Verwaltung von kryptografischen Schlüsselmaterial
  - **Schlüsselhoheit muss beim Nutzer liegen**!

Anforderungen für Zufallszahlengeneratoren AIS20 und AIS31

- Services zum Identity and Access Management
  - Durchgängige Authentifizierung und Autorisierung von Nutzerinteraktionen
  - Nutzung von 2-Faktor-Authentifizierung
  - Authentifizierung und Autorisierung von Cloud-Services
  - **Zero Trust Prinzip**

Bedrohungen in der Public Cloud im Kontext VS-Verarbeitung adressieren

Nutzer(daten)-Isolierung in den Phasen Data in Transit, Data in Use und Data at Rest

Data in Transit

- **Kryptografische Netzwerktrennung**
  z.B. durch VPN/TLS-Service
- Informationsflusskontrolle
  z.B. durch Firewall, SDN, Network Security Policies

Data at Rest

- **Kryptografische Speicherseparierung**
  z.B. Anwendungsverschlüsselung oder Festplattenverschlüsselung (vgl. VS-Anforderungsprofil)

Data in Use

- Strikte Trennung von (virtuellen) Ressourcen wie VMs, Container, Arbeitsspeicher, etc.
- z.B. Hypervisor, Container-Orchestrierung, Confidential Computing

Konformität zu
BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

Zusammenfassung / Key Facts

- Bedrohungsanalyse durchgeführt
  - ➢ Zusammenarbeit mit CSPs zur Identifizierung von Sicherheitsmaßnahmen

- Bedrohungen müssen im VS-Kontext mit zugelassenen Sicherheitsmechanismen adressiert werden
  - ➢ Anforderungen
    - ➢ Kryptografische Nutzertrennung in den Phasen Data at Rest und Data in Transit notwendig
    - ➢ Schlüsselhoheit muss beim Nutzer liegen
    - ➢ Zero Trust Prinzip
    - ➢ Weitere werden u.a. in Technischen Richtlinien und VS-Anforderungsprofilen festgelegt

Vielen Dank!

Deutschland
Digital•Sicher•BSI•

Noch Fragen?

Malte Stoffers

Referat V 21 - VS-Cloud Architekturen

Bundesamt für Sicherheit in der Informationstechnik

E-Mail: referat-v21@bsi.bund.de