Bausteine für sichere VS-NfD Public Cloud Architekturen

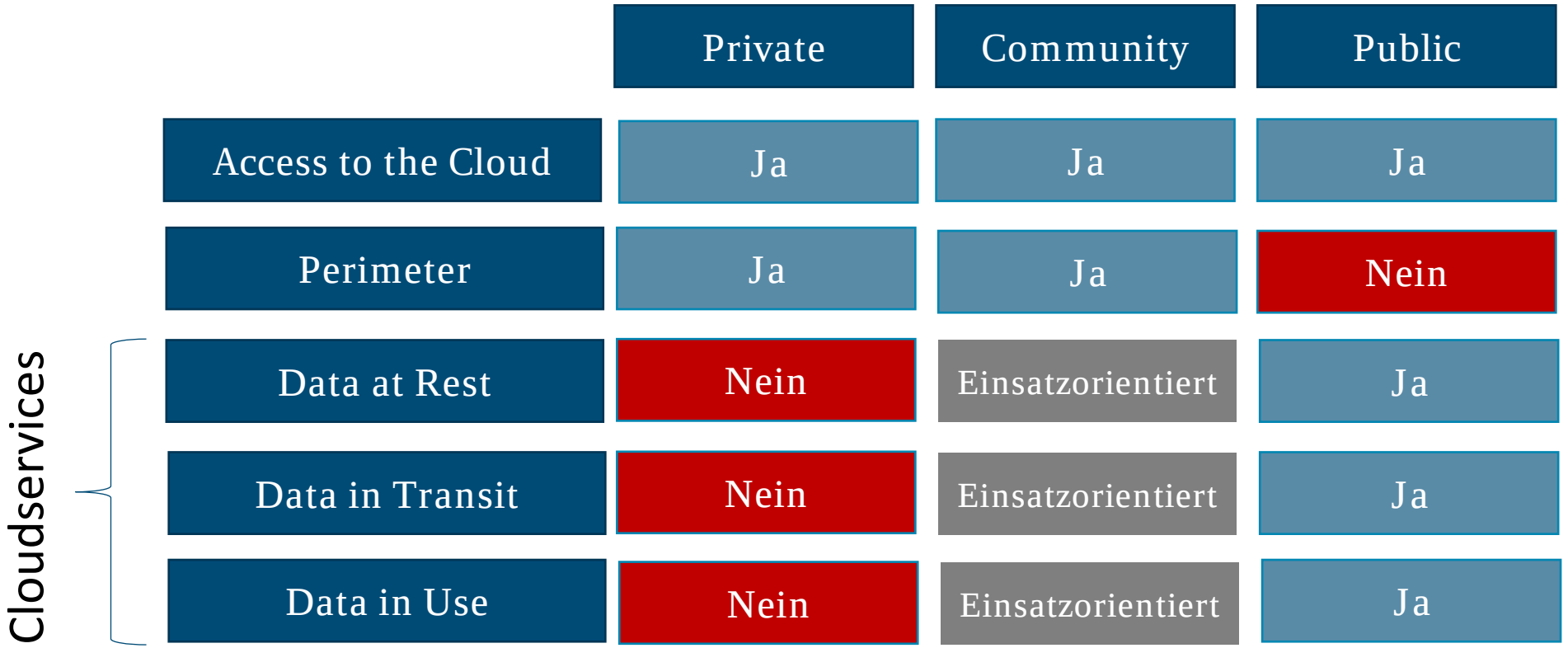
Dominik Esch, Referat V21 – VS-Cloud Architekturen

Bundesamt für Sicherheit in der Informationstechnik

Rahmenbedingungen

- Der Bedarf von VS-Cloud Architekturen muss mit Angeboten unterlegt werden
- Cloud Architekturen sind VS-IT Systeme und unterliegen der Freigabe
- Unabhängig vom Betriebsmodell oder Servicemodell
  - Freigabepflicht nach §50 VSA
  - Freigabe durch Behördenleitung; höher VS-NfD: Freigabevotum durch BSI zusätzlich erforderlich
  - Sicherheitstechnische Evaluierung von relevanten Sicherheitsfunktionen zum Schutz von VS
    - Entsprechende Zulassung nach §51 VSA
    - Freigabeprozess stützt sich auf Zulassungsaussagen ab
- Zulassungsantrag im Kontext eines konkreten Usecases

VS-Zulassungsrelevanz im Kontext VS-Cloud



Grundsätze für die VS-Verarbeitung in Cloud Architekturen

01 - Security by Design
Data at Rest, Data in Transit, Data in Use

02 - Einsatzorientierung
Zielgerichtete Bewertung entlang des Kundenbedarfs

03 - Vertrauenswürdigkeit
Vertrauenswürdigkeit im Sinne des staatlichen Geheimschutzes

04 - Rechtlich-Wirtschaftliche Aufstellung
Bewertung von Risiken aus internationaler Gesetzgebung

01 - Security by Design

Data at Rest, Data in Transit, Data in Use

Sicherheitsfunktion gem. §52 VSA	Services in der Cloud (Beispiele)
1. zur Zugangs- und Zugriffskontrolle	Identity and Access Management
2. zur Identifikation und Authentisierung	Identity and Access Management
3. Zur kryptografischen Unterstützung	Key Management, Hardware Security Module, Services zur Ver- und Entschlüsselung
4. für das Sicherheitsmanagement	Identity and Access Management, Key Management

01 - Security by Design

Data at Rest, Data in Transit, Data in Use

Sicherheitsfunktion gem. §52 VSA	Services in der Cloud (Beispiele)
5. zur Informationsflusskontrolle	Virtual Private Cloud, Software Defined Networking, Hypervisor
6. zum internen Schutz der Benutzerdaten	Identity and Access Management
7. zum Selbstschutz der Sicherheitsfunktionen und ihrer Daten	Jeder sicherheitsrelevante Service
8. zur Netzwerktrennung	Software Defined Networking, Netzwerkverschlüsselungsservices, Hypervisor

01 - Security by Design

Data at Rest, Data in Transit, Data in Use

Sicherheitsfunktion gem. §52 VSA	Services in der Cloud (Beispiele)
9. zum Schutz der Unversehrtheit	Key Management
10. zur Verfügbarkeitsüberwachung	Monitoring Service
11. zur Sicherheitsprotokollierung	Logging-Funktionalität in fast allen Services

Grundsätze für die VS-Verarbeitung in Cloud Architekturen

01 - Security by Design
Data at Rest, Data in Transit, Data in Use

02 - Einsatzorientierung
Zielgerichtete Bewertung entlang des Kundenbedarfs

03 - Vertrauenswürdigkeit
Vertrauenswürdigkeit im Sinne des staatlichen Geheimschutzes

04 - Rechtlich-Wirtschaftliche Aufstellung
Bewertung von Risiken aus internationaler Gesetzgebung

02 - Einsatzorientierung

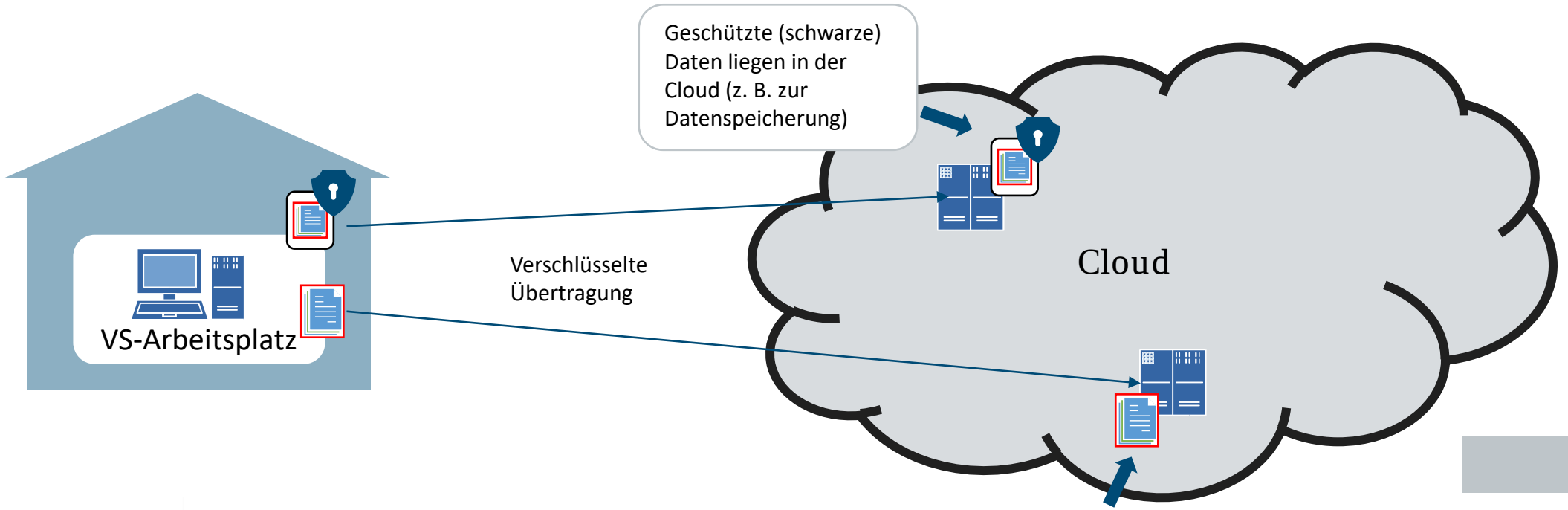
Zielgerichtete Bewertung entlang des Kundenbedarfs

- Verständnis des Einsatzszenarios für eine zielgerichtete, sicherheitstechnische Bewertung essenziell
  - Wie soll die Cloud genutzt werden?
- Identifikation von sicherheitsrelevanten Services/Komponenten

  sog. **Security Enforcing Services (SES)**
- SES sind wesentlich zum Schutz der VS-Informationen
- Shared Responsibility Model
  - Security in the Cloud
  - Security of the Cloud

02 - Einsatzorientierung

Zielgerichtete Bewertung entlang des Kundenbedarfs



Welche Cloud Services tragen zur Sicherheit der VS-Daten bei?

→

Ungeschützte (rote) Daten liegen in der Cloud (z. B. für Office Anwendungen)

Grundsätze für die VS-Verarbeitung in Cloud Architekturen

01 - Security by Design
Data at Rest, Data in Transit, Data in Use

02 - Einsatzorientierung
Zielgerichtete Bewertung entlang des Kundenbedarfs

03 - Vertrauenswürdigkeit
Vertrauenswürdigkeit im Sinne des staatlichen Geheimschutzes

04 - Rechtlich-Wirtschaftliche Aufstellung
Bewertung von Risiken aus internationaler Gesetzgebung

03 – Vertrauenswürdigkeit

Vertrauenswürdigkeit im Sinne des staatlichen Geheimschutzes

- Vertrauenswürdigkeitsnachweis durch Zulassung von SES und Freigabe des Einsatzszenarios
- Kompetenzbereich zur Identifizierung und Bewertung von Bedrohungen wurde in Abteilung V aufgebaut
- Evidenzbasierte, sicherheitstechnische Evaluierung sicherheitsrelevanter Services
- Kriterien für Prozesse in der Cloud
  (z. B. Sicherer Software Development Life Cycle)
  formulieren und prüfen

Grundsätze für die VS-Verarbeitung in Cloud Architekturen

01 - Security by Design
Data at Rest, Data in Transit, Data in Use

02 - Einsatzorientierung
Zielgerichtete Bewertung entlang des Kundenbedarfs

03 - Vertrauenswürdigkeit
Vertrauenswürdigkeit im Sinne des staatlichen Geheimschutzes

04 - Rechtlich-Wirtschaftliche Aufstellung
Bewertung von Risiken aus internationaler Gesetzgebung

04 - Rechtlich-Wirtschaftliche Aufstellung

Bewertung von Risiken aus internationaler Gesetzgebung

z. B.

- Eigenbetrieb der Bundesverwaltung
- …
- Internationales Unternehmen außerhalb D (unterliegt Recht Dritter)
  - z. B. Cloud Act (USA)

- Diese Risiken der Cloudnutzung müssen unter Berücksichtigung eigener Souveränitätsansprüche bewertet werden

Zusammenfassung

- Die Verarbeitung von VS wird durch die VSA technologieunabhängig geregelt
- Zulassungsrelevanz von SES ist einsatzabhängig
- Evaluierung der Wirksamkeit und Korrektheit von Sicherheitsfunktionen, um nachvollziehbares Vertrauen zu schaffen
- Public Cloud Service Provider sind nicht nur Anbieter, sondern auch Betreiber
- Eigene Souveränitätsansprüche sind zu berücksichtigen

Vielen Dank!

Deutschland
Digital•Sicher•BSI•

Noch Fragen?

Dominik Esch

Referat V 21 - VS-Cloud Architekturen

Bundesamt für Sicherheit in der Informationstechnik

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