für den Einsatz von Cloud-Lösungen im VS-Kontext der Bundesverwaltung
für den Einsatz von Cloud-Lösungen im VS-Kontext der Bundesverwaltung

Grundlagen beim Einsatz von Cloud-Lösungen im VS-Kontext der Bundesverwaltung

Speaker: Dr. Stefan Wüller

Bundesamt
für Sicherheit in der
Informationstechnik

Einleitung

Einsatz von Cloud-Lösungen im VS-Kontext der Bundesverwaltung

- Cloud-Technologien sind wesentlicher Bestandteil der digitalen Transformation öffentlicher Verwaltungen
  → auch im Geheimschutzbereich entsteht ein wachsender Bedarf an skalierbaren, sicheren Cloud-Diensten
- **Leitfaden** soll bei der Umsetzung moderner Cloud-Infrastrukturen im Geheimschutz unter Anwendung regulatorischer Vorgaben unterstützen
- Freigabe und Zulassung
  - Für VS-Verarbeitung: Freigabepflicht nach **§ 50 VSA**
  - Innerhalb der VS-IT nehmen verschiedene VS-Produkte IT-Sicherheitsfunktionen nach **§ 52 VSA** wahr
- Cloud-Architekturen sind VS-IT Systeme und unterliegen der Freigabe
  - Unabhängig vom Betriebsmodell oder Servicemodell
- Sicherheitstechnische Evaluierung von relevanten Sicherheitsfunktionen zum Schutz von VS
  - Entsprechende Zulassung nach **§ 51 VSA**

Grundlagendokumente (I)

Generelle Anforderungen für Informationssicherheit

- **IT-Grundschutz** – methodisches Fundament der Informationssicherheit
  - Methode, Anleitung, Empfehlung für Behörden, Unternehmen und Institutionen
  - Verbindlich z.B. für die Bundesverwaltung
  - Baustein OPS.2.2 "Cloud-Nutzung“ adressiert Cloud-Kunden und stellt fachliche Grundlage für eine sichere Cloud-Nutzung dar
- **Mindeststandard zur Nutzung externer Cloud-Dienste** (MST-NCD)
  - Verbindlich (gesetzlich) für Stellen des Bundes, Unternehmen (die im Eigentum des Bundes stehen)
  - Baut auf OPS.2.2 auf, erweitert und konkretisiert diesen
  - Fordert C5
- **Kriterienkatalog C5** – BSI-Prüfkatalog für sichere Cloud-Angebote
  - Richtet sich an Cloud-Anbieter (deren Prüfer und Kunden)
  - Fokus liegt auf der Sicherheit der Cloud-Dienste (Public Cloud)
  - C5-Prüfung erfolgt durch Wirtschaftsprüfer nach internationalen Prüfstandards (ISAE 3000) und stellt dem CSP bei Erfolg ein C5-Testat aus

→ Für den VS-Schutz nicht hinreichend

Grundlagendokumente (II)

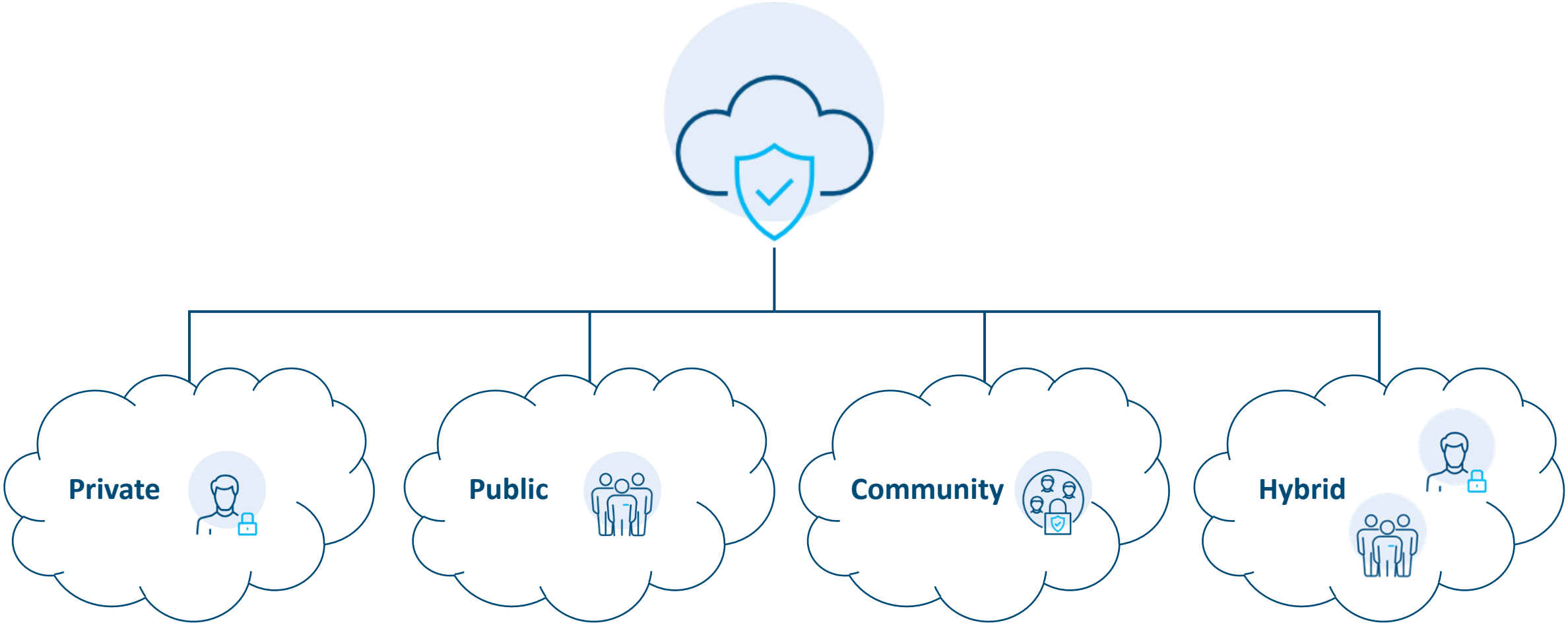
VS-Anforderungen

- **Verschlusssachenanweisung (VSA)** – Geheimschutzvorgaben für die Bundesverwaltung
  - Grundlage für VS-Freigabe (§ 50), Zulassung (§ 51), IT-Sicherheitsfunktionen (§ 52)
  - Richtet sich an u.a. an Bundesbehörden (die VS verarbeiten)
  - Herausgeber: BMI
  - Wird um Technische Leitlinien und Handreichungen des BSI ergänzt
- **Geheimschutzhandbuch (GHB)** – Geheimschutzvorgaben für die Wirtschaft
  - Beinhaltet allgemeine Verwaltungsvorschriften zur Ausführung des SÜG im nicht-öffentlichen Bereich
  - Richtet sich an die geheimschutzbetreute Wirtschaft sowie an auftraggebende Dienststellen
  - Herausgeber: BMWE
  - Teils andere Vorgehensweisen gegenüber VSA, bei überschneidenden Geltungsbereichen VSA als gemeinsame Grundlage

➡ **Zusammen bilden die Grundlagendokumente das normative Fundament für VS-konforme Cloud-Lösungen**

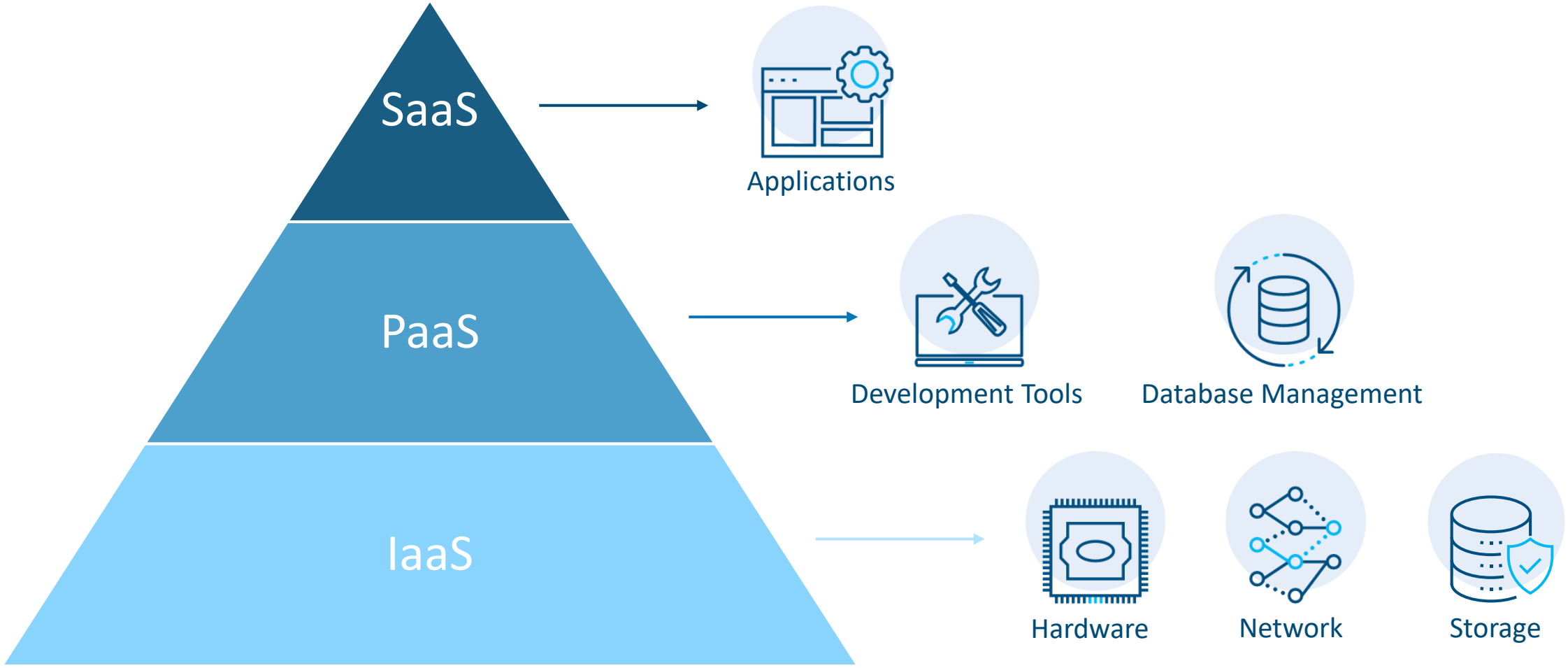
Betriebsmodelle

Verschiedene Ansätze zur Bereitstellung von Cloud-Infrastrukturen



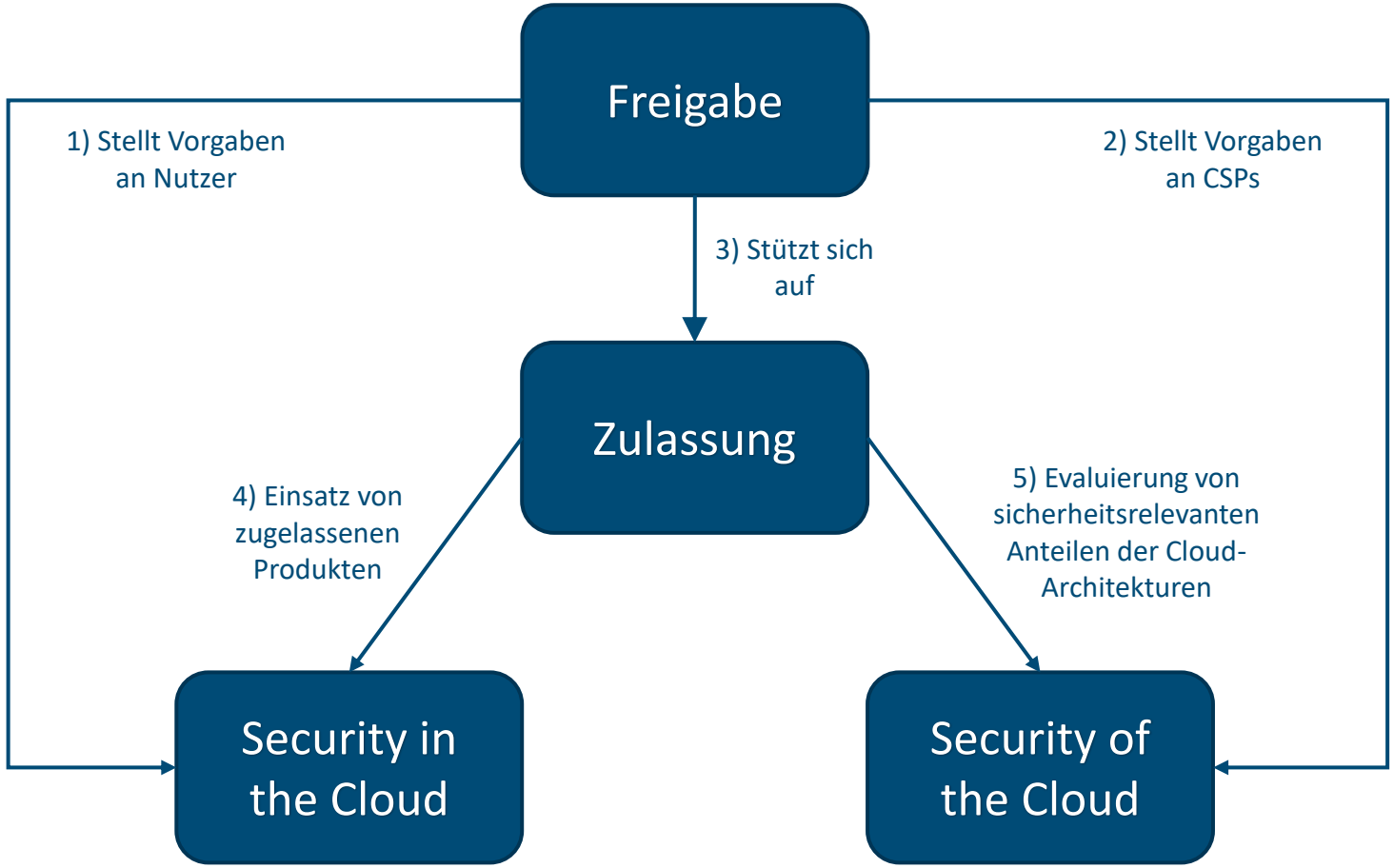
Servicemodelle

und ihr Einfluss auf Verantwortlichkeiten (Shared Responsibility)



Zusammenspiel Freigabe und Zulassung

Security in the Cloud & Security of the Cloud

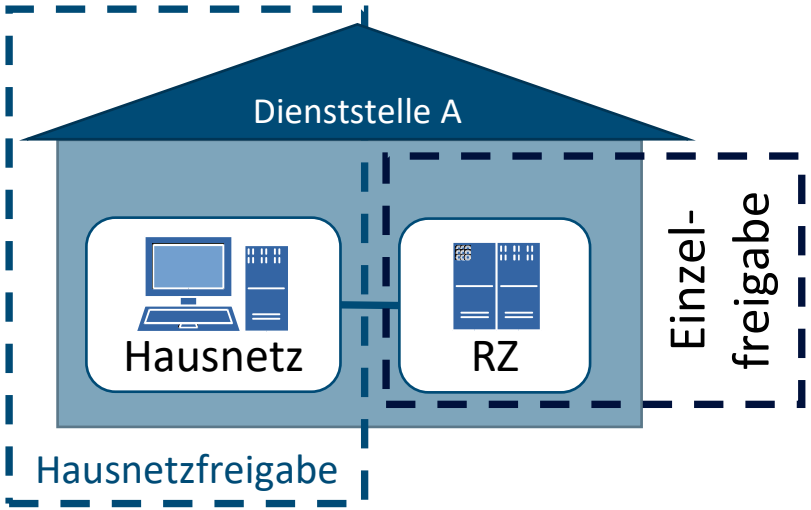


VS-Freigaben und Cloud

Freigabeprozess

Freigabe des Betriebs von VS-IT nach § 50 VSA

- **Ganzheitliche Bewertung** von VS-IT-Systemen (Produkte, Einsatzumgebung sowie personelle und organisatorische Regelungen).
- **Freigabe durch Behördenleitung**
- **Beteiligung BSI:** Freigabevotum durch BSI bei VS-IT zur Verarbeitung von VS-VERTRAULICH oder höher eingestufter VS, Zulassungsaussagen IT-Sicherheitsfunktionen
- **Verantwortung der Freigabe**: Abhängig von der Freigabeart
- **Freigabearten:**
  - Einzelfreigabe: einzelnes System oder Dienst
  - Hausnetzfreigabe: VS-fähige Bürokommunikation
  - Gesamtfreigabe: mehrere beteiligte Dienststellen



Verantwortung der Freigaben: Dienststellenleitung

Merkmale der Cloud zur Einordnung der Freigaben

Standort – An welchem Ort befinden sich die Server der Cloud? Wer hat Zugang?

Cloud-Betreiber – Wer betreibt die Cloud?

Verbindung – Über welche Netze wird VS übertragen?

Rechtsrahmen – Welche Geheimschutzvorschriften sind einschlägig?

Nutzerkreis – Wer nutzt die Cloudplattform?

Die Antworten auf die Fragestellungen haben unmittelbaren Einfluss auf die Ausgestaltung der Freigabe

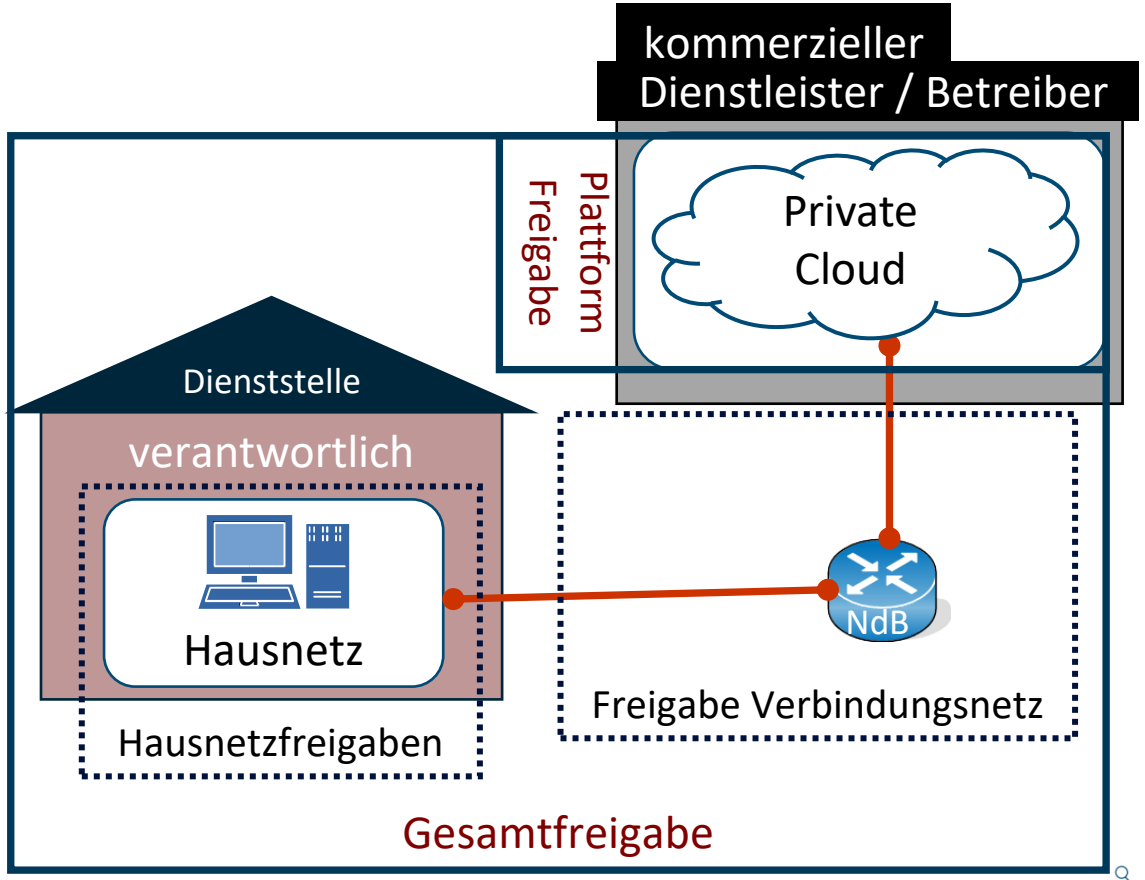
Szenario: Private Cloud (externes „Cloud housing“)

Prämissen

- **RZ eines privaten Dienstleisters in Deutschland**
- **kommerzieller privater Dienstleister**
- über NdB (VS-freigegebenes Netz)
- VSA Bund, **Verträge mit Dienstleister**
- Dienststelle (Single-Tenant)

Freigaben

- **Plattformfreigabe und Gesamtfreigabe**
  durch verantwortliche Dienststelle



Weitere benötigte Freigaben: Verbindungsnetz, Hausnetzfreigabe

Public Cloud mit Service Broker

Prämissen

RZ(n) eines privaten Dienstleisters,
Standort vertragsabhängig

kommerzieller privater Dienstleister

über das Internet

Verträge mit Dienstleister, internationale Vorschriften

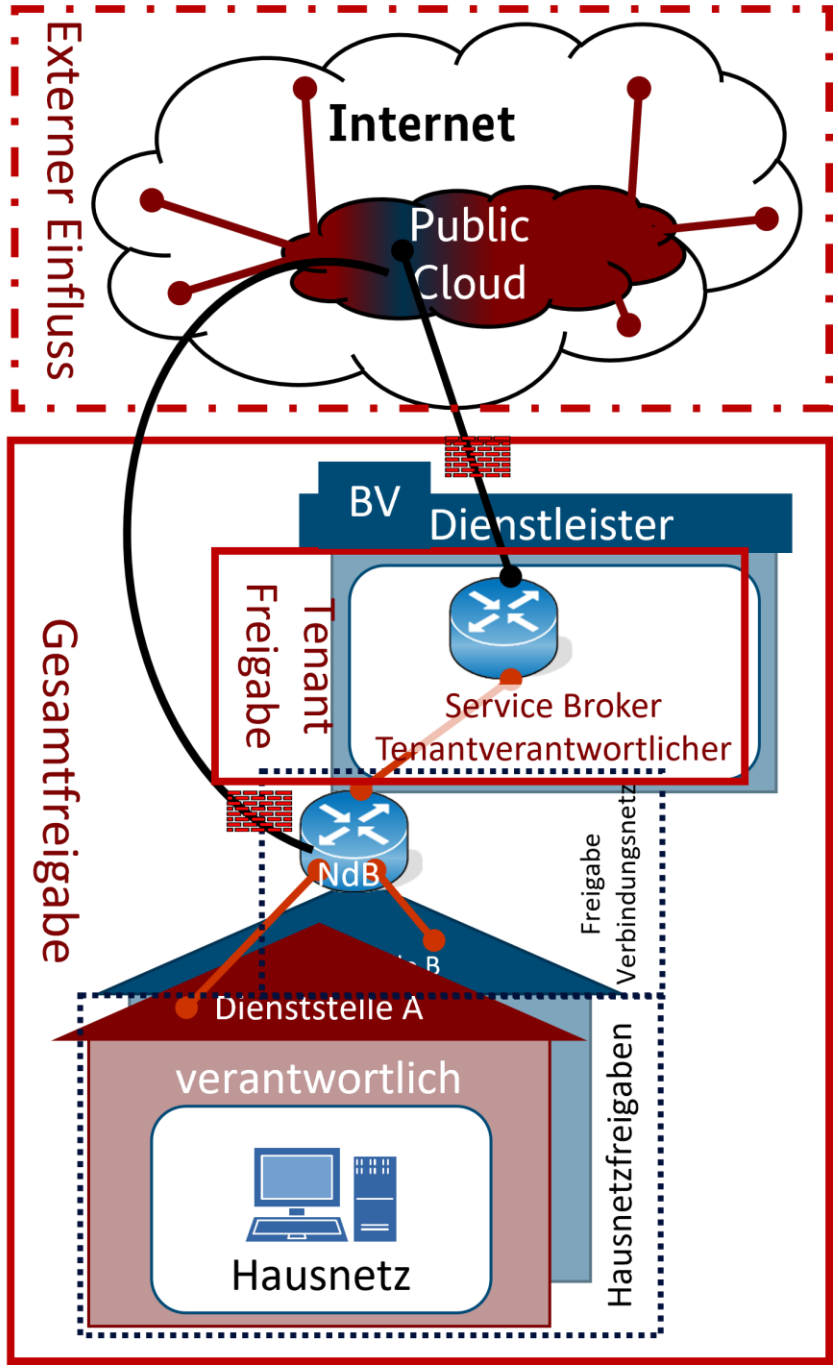
Unbekannt (Multi-Tenant)

Freigaben

Plattform – indirekt über Verträge und die vom Betreiber bereitgestellten Security Enforcing Services

Tenant – öffentlicher Dienstleister

Gesamt – verantwortliche Dienststelle



Zusammenfassung & Ausblick

Kernthemen des *Leitfadens für den Einsatz von Cloud-Lösungen im VS-Kontext der Bundesverwaltung*

Leitfaden verfügbar unter www.bsi.bund.de → Themen → Staat und Verwaltung → Geheimschutz

Im Fokus des Leitfadens stehen die zwei eng miteinander verzahnte Aspekte:

- die Freigabe von Cloud-Architekturen als VS-IT
- die Zulassung sicherheitsrelevanter IT-Produkte innerhalb dieser Architekturen

Diese werden adressiert durch:

- Grundlagen (Grundlagendokumente, Freigabe/Zulassung, Cloud-Architekturen)
- Freigabe und Zulassung in der Praxis
- Unterschiedliche Freigabe-Szenarien in Abhängigkeit von Architekturmerkmalen
- Identifikation von sicherheitsrelevanten Dienste in der Cloud
- Sicherheitsniveaus in Abhängigkeit von Betreibervertrauen und Nutzerkreis

Vielen Dank für Ihre Aufmerksamkeit!

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: