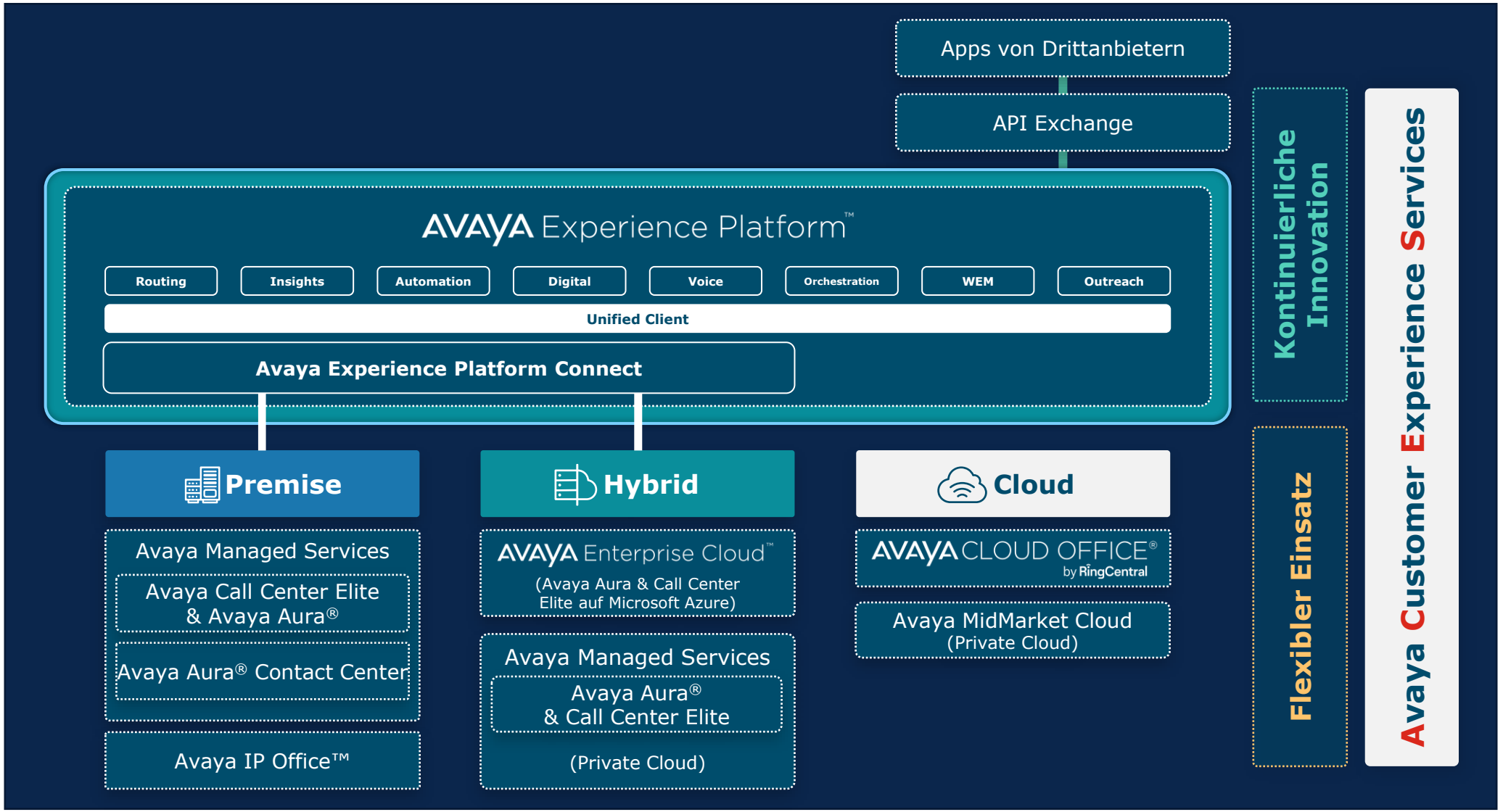
DOK FORUM
ICT TRENDS 2023
27. SEPTEMBER 2023

IT-SICHERHEIT IN DER TELEKOMMUNIKATION

ARMIN SCHMIDT
CUSTOMER SOLUTION CONSULTANT

- Ein **Branchenführer** in Customer Experience und Employee Experience (CX und UX)
- **90.000 Kunden** in über 190 Ländern weltweit vertrauen auf Avaya
- **90 % der Fortune-100-Unternehmen** in den USA zählen auf Avaya
- Führend bei Innovationen **4.300 Patente** und Patent-Anmeldungen
- **OnPremise-**, **Hybrid-** und **Cloud-Lösungen** je nach Wunsch und Bedarf des Kunden

Innovation Without Dispruption



IT-Sicherheit in der Telekommunikation

- **Was** bedeutet IT-Sicherheit in der Telekommunikation?
- **Warum** sollten Sie sich mit diesem Thema befassen?
- **Wie** können Sie Ihre Telekommunikation sicherer machen?

- Erfahrungen aus einem KRITIS-Audit bei einem realen Kunden

Was bedeutet IT-Sicherheit in der Telekommunikation?

IT-Sicherheit in der Telekommunikation

Bedrohungen für TK-Anlagen

- Manipulationen
- Unberechtigtem Zugriff
- Unerlaubtem Mithören
- Missbrauch
- Störungen und Ausfällen

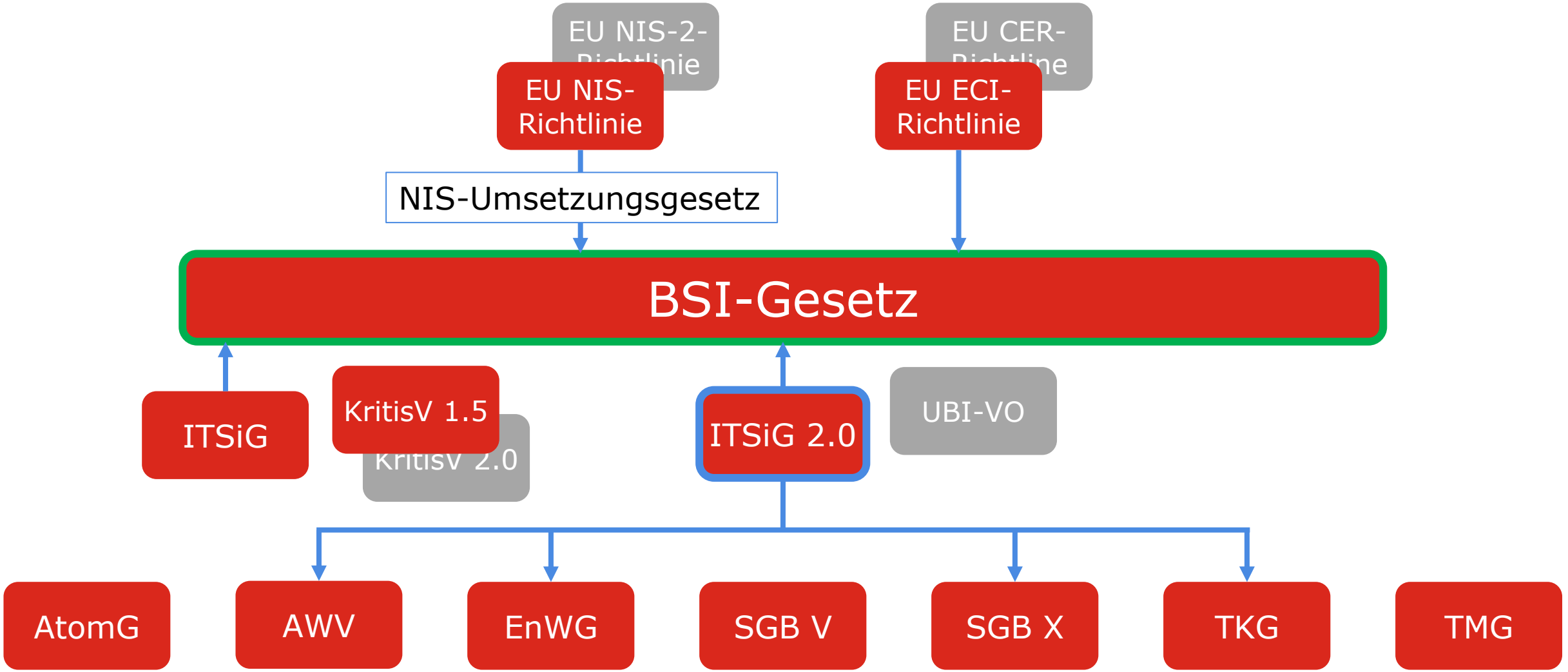
Empfohlene Schutzmaßnahmen

⇨ Härtung des Systems
⇨ Umfassende Zugriffskontrollen
⇨ Starke Verschlüsselung
⇨ Überwachung und Alarmierung
⇨ Hochverfügbare Architektur

Warum sollten Sie sich mit diesem Thema befassen?

AVAYA

IT-Sicherheit – Kritische Infrastrukturen



AVAYA

KRITIS

10 Sektoren

32 Branchen

- Öffentl. Wasserversorgung
- Öffentl. Abwasserbeseitigung

- Elektrizität
- Fernwärme
- Gas
- Mineralöl

- Ernährungswirtschaft
- Lebensmittelhandel

- Banken
- Börsen
- Finanzdienstleister
- Versicherungen

- Arzneimittel und Impfstoffe
- Labore
- Medizinische Versorgung

- Informationstechnik
- Telekommunikation

- Presse
- Kulturgut
- Rundfunk (TV und Radio)
- Symbolträchtige Bauwerke

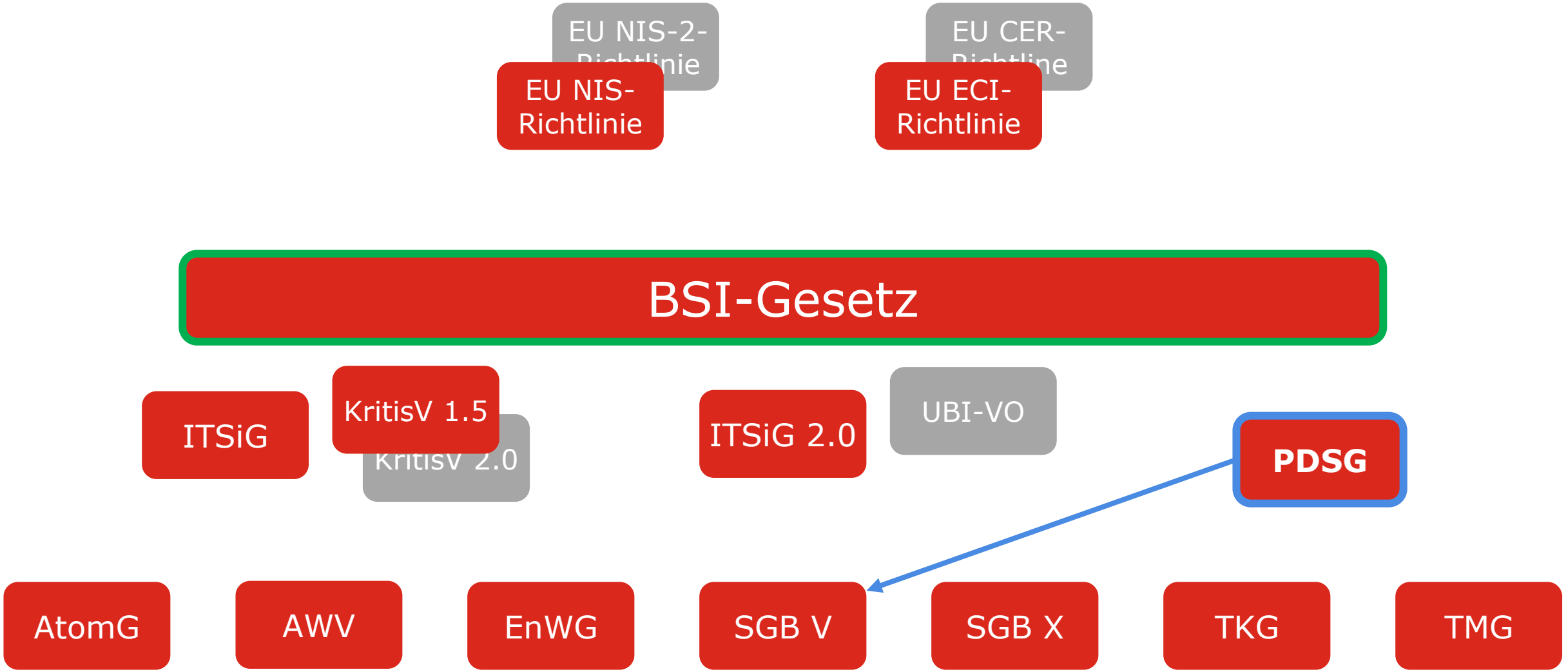
- Justizeinrichtungen
- Notfall-/Rettungswesen
- Parlament
- Regierung und Verwaltung

- Binnenschifffahrt
- Logistik
- Luftfahrt
- Schienenverkehr
- Seeschifffahrt
- Straßenverkehr

Diese 8 Sektoren
unterliegen dem
BSI-Gesetz

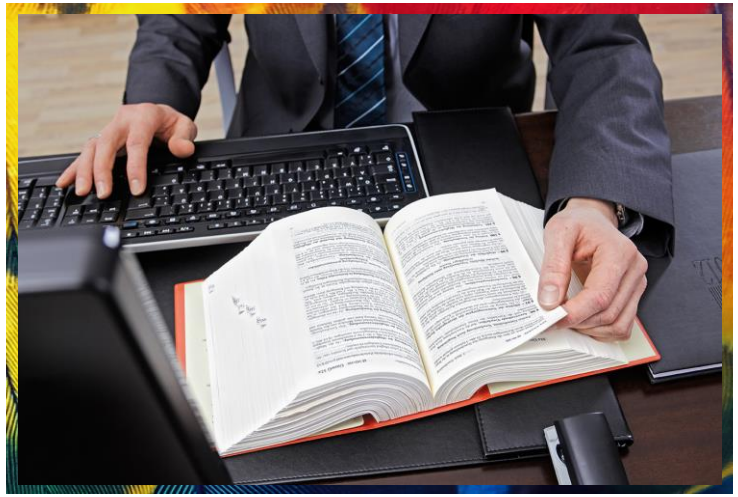
AVAYA

IT-Sicherheit in Krankenhäusern



AVAYA

§ 75c SGB V „IT-Sicherheit in Krankenhäusern“



Das Fünfte Buch Sozialgesetzbuch wurde durch das Patientendaten-Schutz-Gesetz u. a. um § 75c erweitert:

(1) Pflicht zu organisatorischen und technischen Vorkehrungen nach dem Stand der Technik zur Vermeidung von Störungen

(2) Eignung des Branchensicherheitsstandards (B3S) für die IT-Sicherheit der Gesundheitsversorgung im Krankenhaus vom BSI festgestellt

(3) Die Verpflichtung nach Absatz 1 gilt für alle Krankenhäuser

⇨ IT-Sicherheit ist seit dem 01.01.2022 gesetzliche Pflicht – auch für Krankenhäuser, die keine Betreiber einer „Kritische Infrastruktur“ sind!

AVAYA

Warum sollten Sie sich mit diesem Thema befassen?

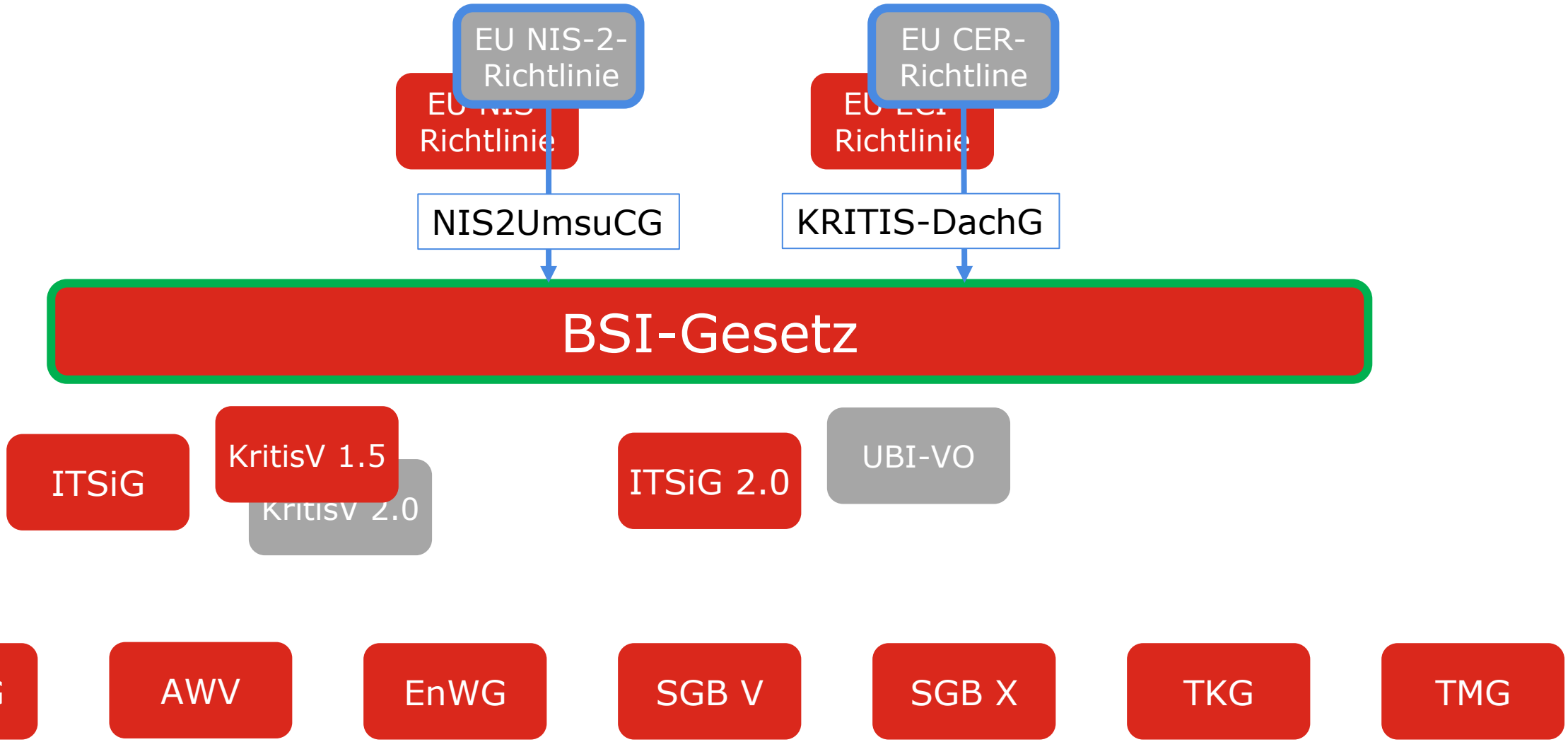
- Für Betreiber Kritischer Infrastrukturen ist IT-Sicherheit durch das BSI-Gesetz gesetzlich verpflichtend
- Für alle Krankenhäuser ist IT-Sicherheit durch § 75c SGB V gesetzlich verpflichtend

Was gilt für andere Unternehmen?

- Prüfen Sie, ob es für Sie eine gesetzliche Pflicht zur IT-Sicherheit gibt
- Für nicht betroffene Unternehmen ist IT-Sicherheit optional – jedoch zum Schutz vor wirtschaftlichem Schaden dringendst empfohlen

Aber es geht weiter ...

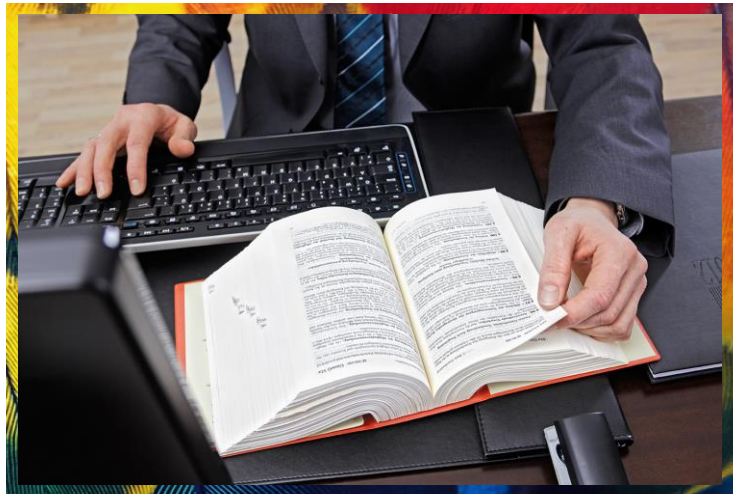
IT-Sicherheit – EU-Richtlinie NIS-2



AVAYA

EU-Richtlinie NIS-2

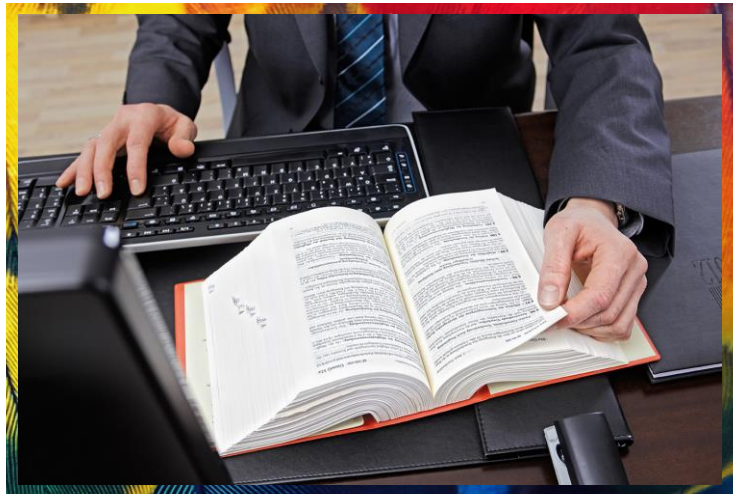
Richtlinie (EU) 2022/2555 vom 14.12.2022



- Erweiterte Betroffenheit
  - Bisher: 8 regulierte KRITIS-Sektoren mit Schwellenwerten
  - Jetzt: 11 Sektoren hoher Kritikalität („wesentliche Einricht.“) und 7 sonstige kritische Sektoren („wichtige Einrichtungen“)
  - Unabhängig von spezifischen Schwellenwerten
  - Pflichten bereits für mittelgroße Unternehmen ab 50 Mitarbeiter und mehr als 10 Mio. Euro Jahresumsatz
- Pflicht zur IT-Sicherheit und neuen Cybersicherheits-Pflichten
- Hohe Bußgelder: Je nach Sektor bis zu 10 Mio. Euro oder 2 % des Jahresumsatzes
- Leitungsorgane können für Verstöße persönlich haftbar gemacht werden
- EU-Mitgliedstaaten müssen NIS-2 bis 17.10.2024 umsetzen

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Kurz: NIS2UmsuCG

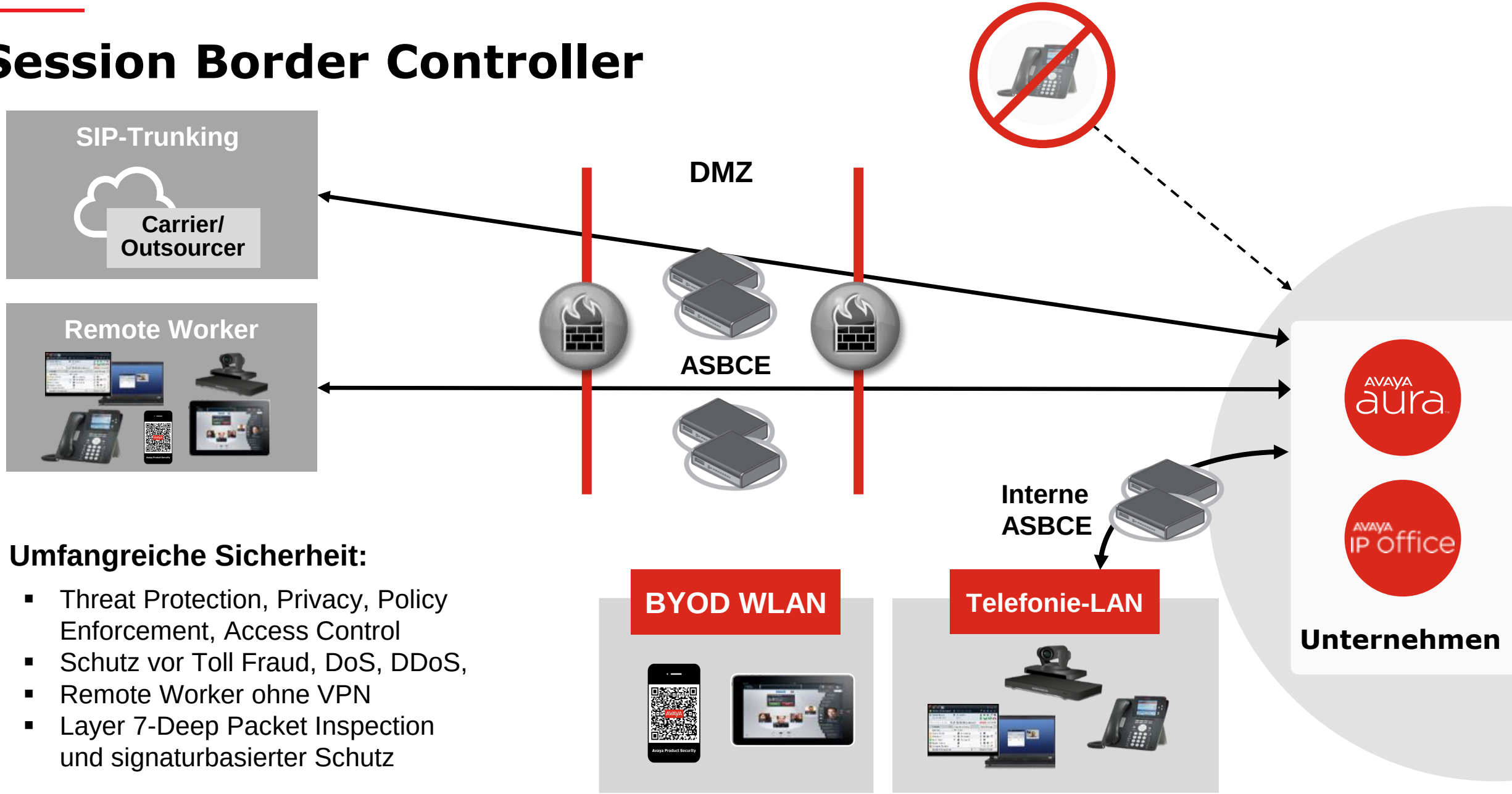


- Erste inoffizielle Referentenentwürfe vom 03.04.2023 und 03.07.2023
- Anpassungen der deutschen Gesetzgebung zur Umsetzung der NIS-2-EU-Richtlinie
- NIS2UmsuCG ist ein Artikelgesetz:
  - Regelungen werden in verschiedenen Gesetzen geregelt
  - BSIG soll das „allgemeine" Gesetz der IT-Sicherheitsgesetzgebung bleiben
- Das BSIG soll von aktuell 15 Paragrafen auf zukünftig 65 Paragrafen anwachsen
  - § 28 BSIG: Anwendungsbereichs mit deutlichen Ausweitung des Adressatenkreises
  - §§ 30 ff. BSIG: Pflichten der Adressaten
- NIS2UMsuCG soll im März 2024 verkündet werden und am 01.10.2024 in Kraft treten

Wie können Sie Ihre Telekommunikation sicherer machen?

AVAYA

Session Border Controller

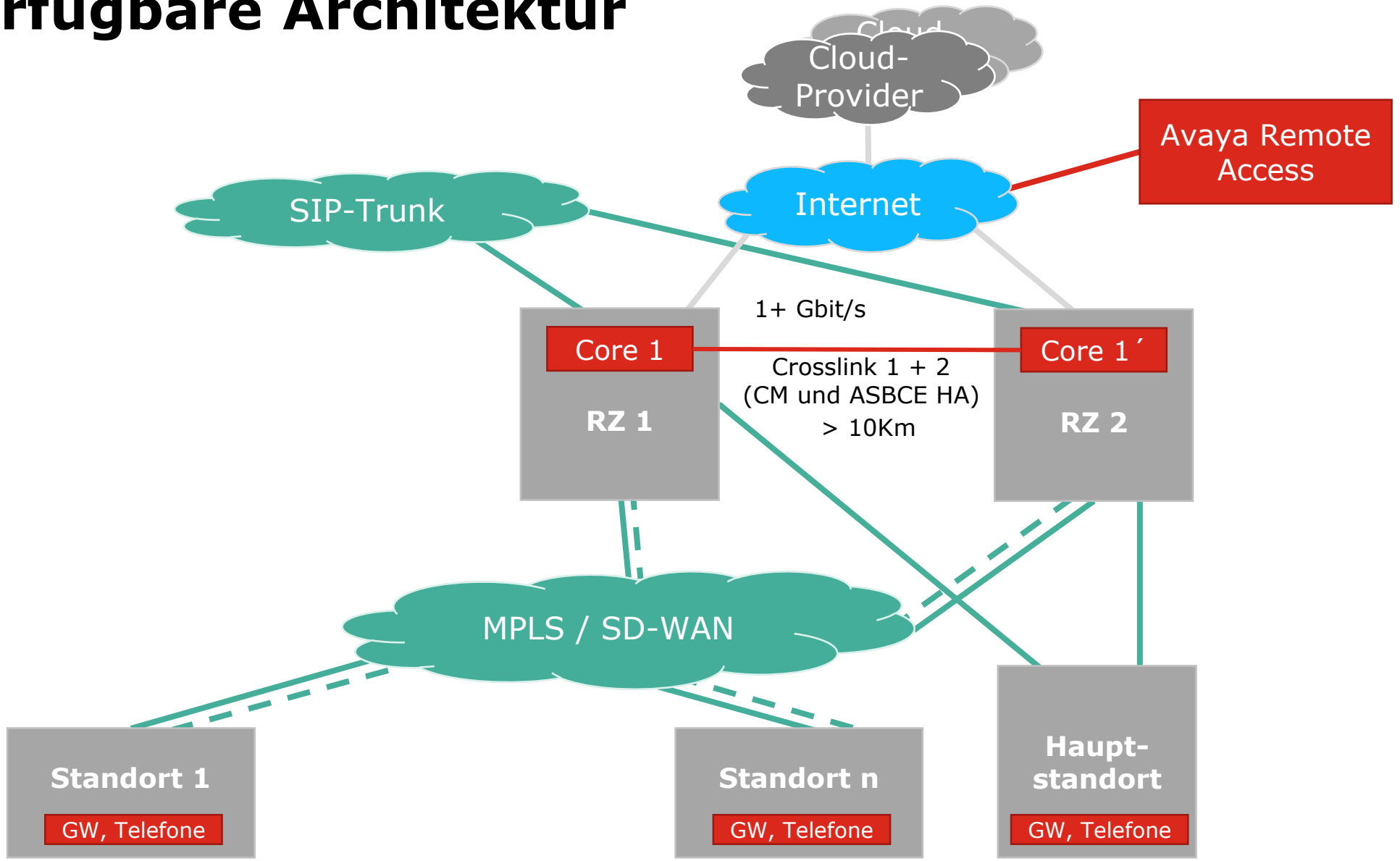


Umfangreiche Sicherheit:

- Threat Protection, Privacy, Policy Enforcement, Access Control
- Schutz vor Toll Fraud, DoS, DDoS,
- Remote Worker ohne VPN
- Layer 7-Deep Packet Inspection und signaturbasierter Schutz

AVAYA

Hochverfügbare Architektur

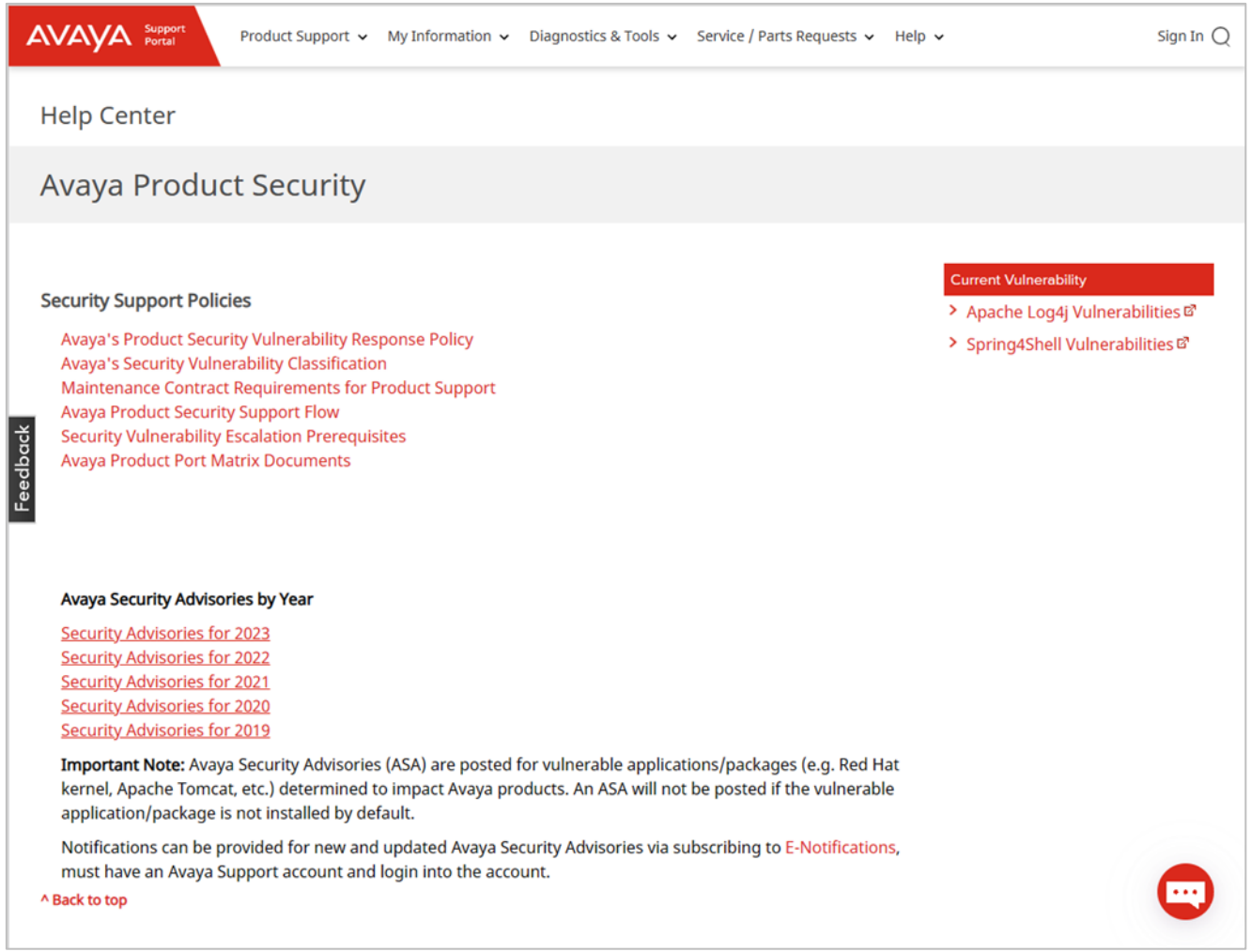


Systeme „auf dem Stand der Technik halten”

Patches und Updates

Avaya Aura Enterprise Updates ermöglichen Unternehmenskunden regelmäßige und planbare Wartungszyklen

- Security Updates
  - Updates für Linux und den Kernel
  - Jeden Monat
- Service Updates
  - Umfassende Korrekturen, kleinere Features und Interoperabilität
  - Alle 4 Monate
- Innovation Updates
  - Neue Funktionen und unter Umständen neue Betriebssysteme
  - Geplant alle 24 Monate (im letzten Quartal des Jahres)



https://support.avaya.com/support/en/helpcenter/GenericDetail/C2009223125237478059

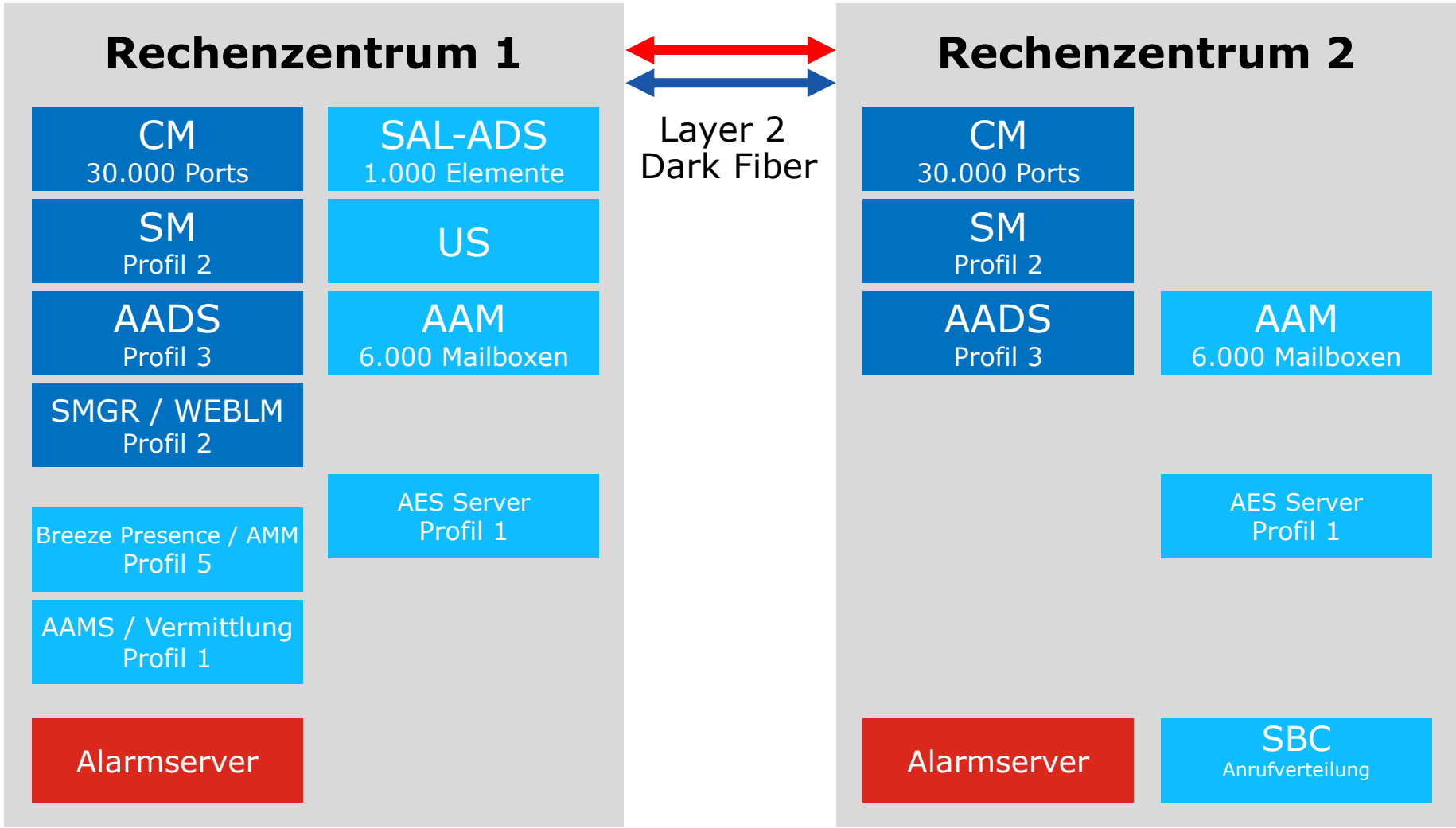
Avaya Product Security

Informationsseite im Avaya Support Portal mit wichtigen Hinweisen über aktuelle Bedrohungen und Abhilfen

Erfahrungen

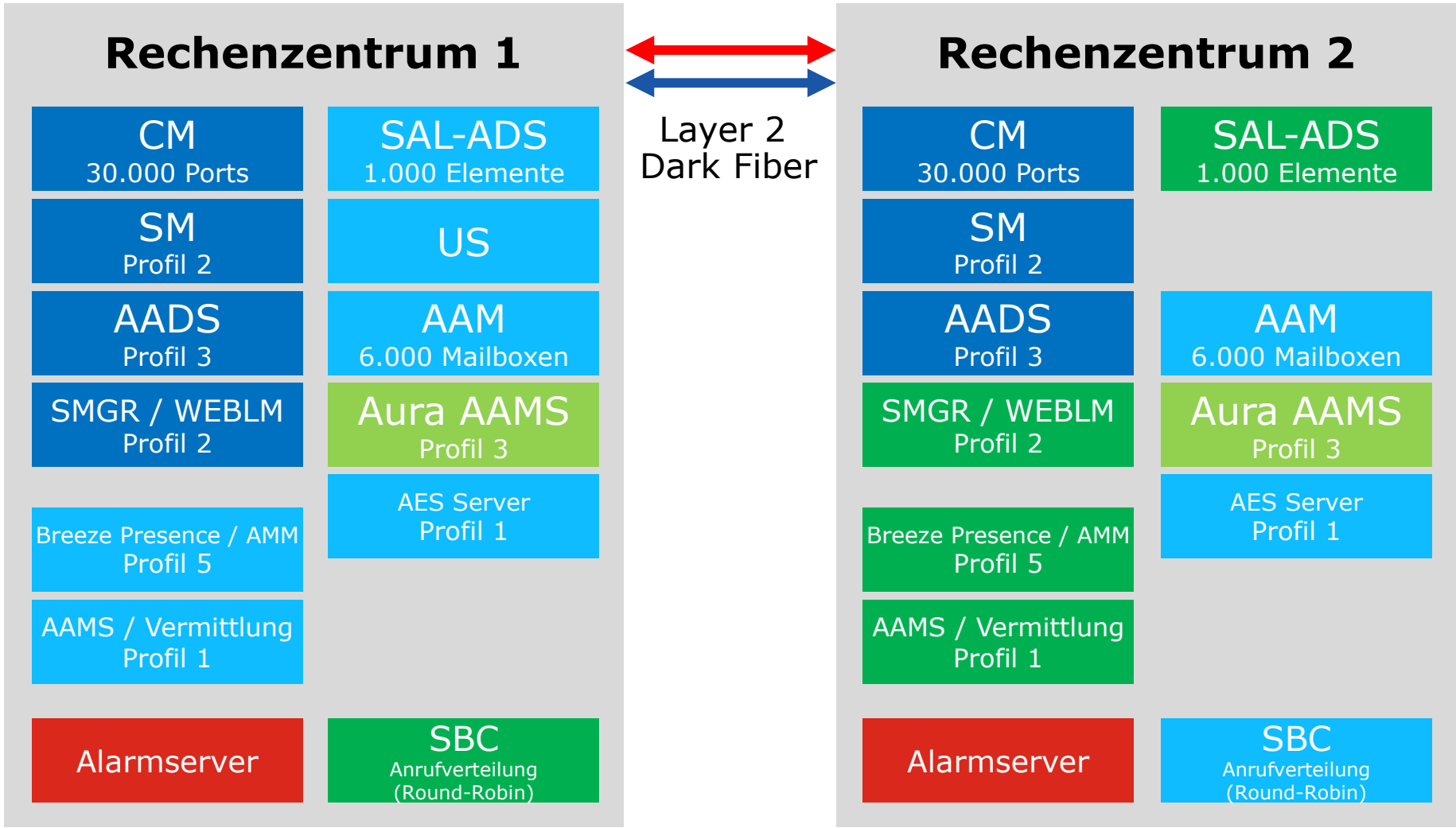
KRITIS-Audit bei einem realen Kunden

Ursprüngliches Avaya Aura Core-Design



AVAYA

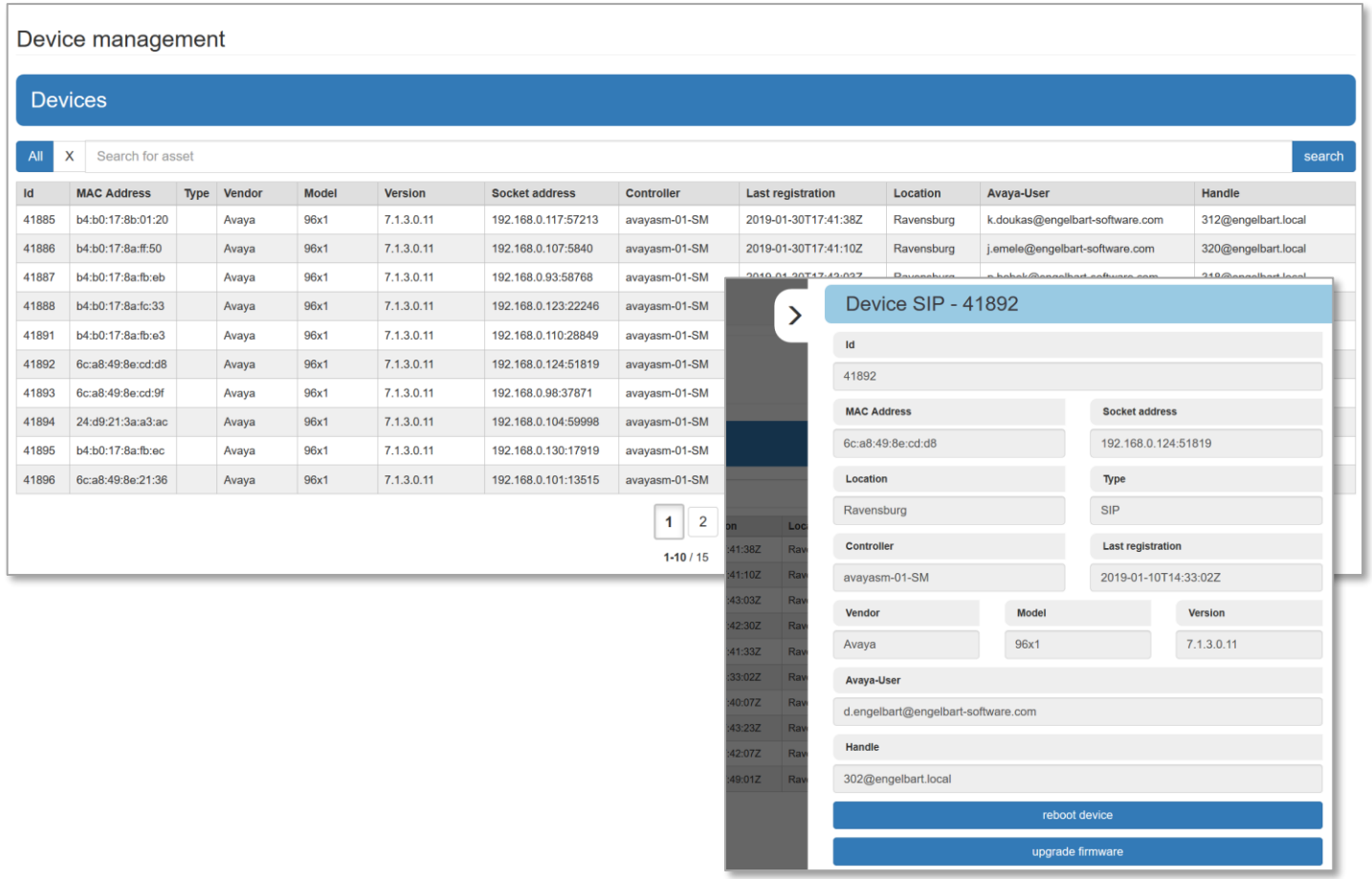
Erweiterung des Avaya Aura Core-Designs



Neue Lizenzen

AVAYA

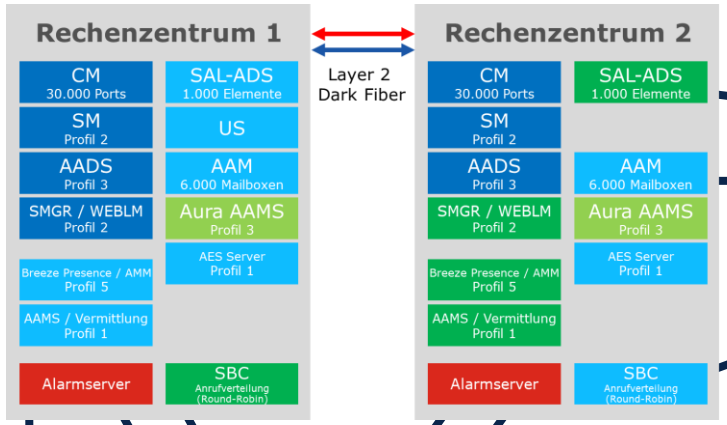
Avaya Asset Tracking



- Unterstützung der Dokumentation, in der Betriebsphase – und auch für Audits
- Asset-Management ist für KRITIS-Einrichtungen verpflichtend

BSI-ID	Anforderung
BSI-5	Asset Inventar und Prozesse
BSI-6	Zuweisung von Asset Verantwortlichen
BSI-7	Nutzungsanweisungen für Assets
BSI-8	Ab- und Rückgabe von Assets
BSI-12	Überführung und Entfernung von Assets

Systemmeldungen – Workflow



SAL

Avaya Service

Unterstützt durch
Avaya Service Bot mit KI

Systemnachrichten

SMGR

Web-Benutzeroberfläche mit allen Meldungen

Weiterleitungen **aller Nachrichten** per SNMP

Weiterleitungen **aller Nachrichten** an ein E-Mail-Postfach

SNMP Traps

SNMP Traps

ZABBIX
Filtern der Meldungen

Weiterleitung wichtiger Meldungen **per E-Mail**
an interne Mailadressen z. B. die Kunden-IT

Meldungen von Problemen **per E-Mail** an Avaya
und automatisches Öffnen eines Service-Tickets

Kundeneigener SNMP-Server
Unterstützung durch Avaya

AVAYA

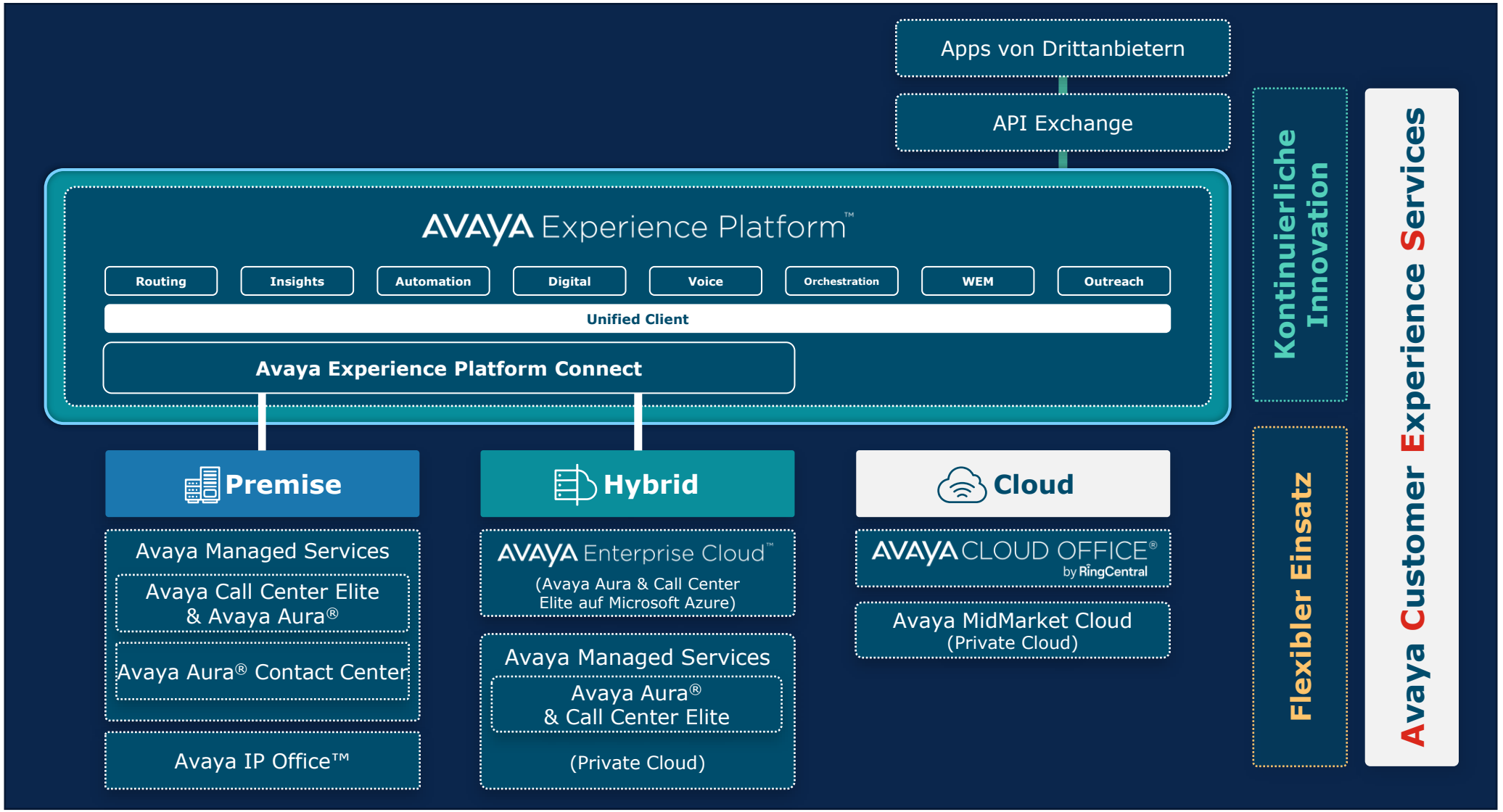
IT-Sicherheit in der Telekommunikation

Zusammenfassung

- IT-Sicherheit in der Telekommunikation ist eine anspruchsvolle, aufwendige und herausfordernde Aufgabe – aber unerlässlich!
- IT-Sicherheit möglichst bereits bei der Auswahl des Anbieters berücksichtigen – kommen Sie zu uns oder zu einem geeigneten Avaya-Partner
- Aktivieren und Nutzen Sie vorhandene Sicherheitsfunktionen
- Prüfen Sie Optionen für erweiterte Sicherheit
- Holen Sie sich bei Bedarf Professional Services-Unterstützung – z. B. von Avaya Customer Experience Services (ACES) oder einem Avaya-Partner
- Überprüfen Sie Ihre Systeme kontinuierlich auf Sicherheitsschwachstellen und halten Sie sie auf dem aktuellen Stand der Technik

Gibt es keinen einfacheren Weg?

Innovation Without Dispruption



Wir freuen uns auf Kontakt mit Ihnen

- Besuchen Sie unseren Stand hier auf dem DOK FORUM
- Nutzen Sie Kontakte zu Avaya oder Avaya-Partnern
- Kontaktieren Sie uns im Web https://avaya.com/de/contacts
- Oder wenden Sie sich direkt an

Guido Steffens
Channel Account Manager & Strategic Consultants
Avaya Deutschland GmbH

(069) 7505-7777
steffens@avaya.com

VIELEN DANK