



**DOK FORUM
ICT TRENDS 2023
27. SEPTEMBER 2023**

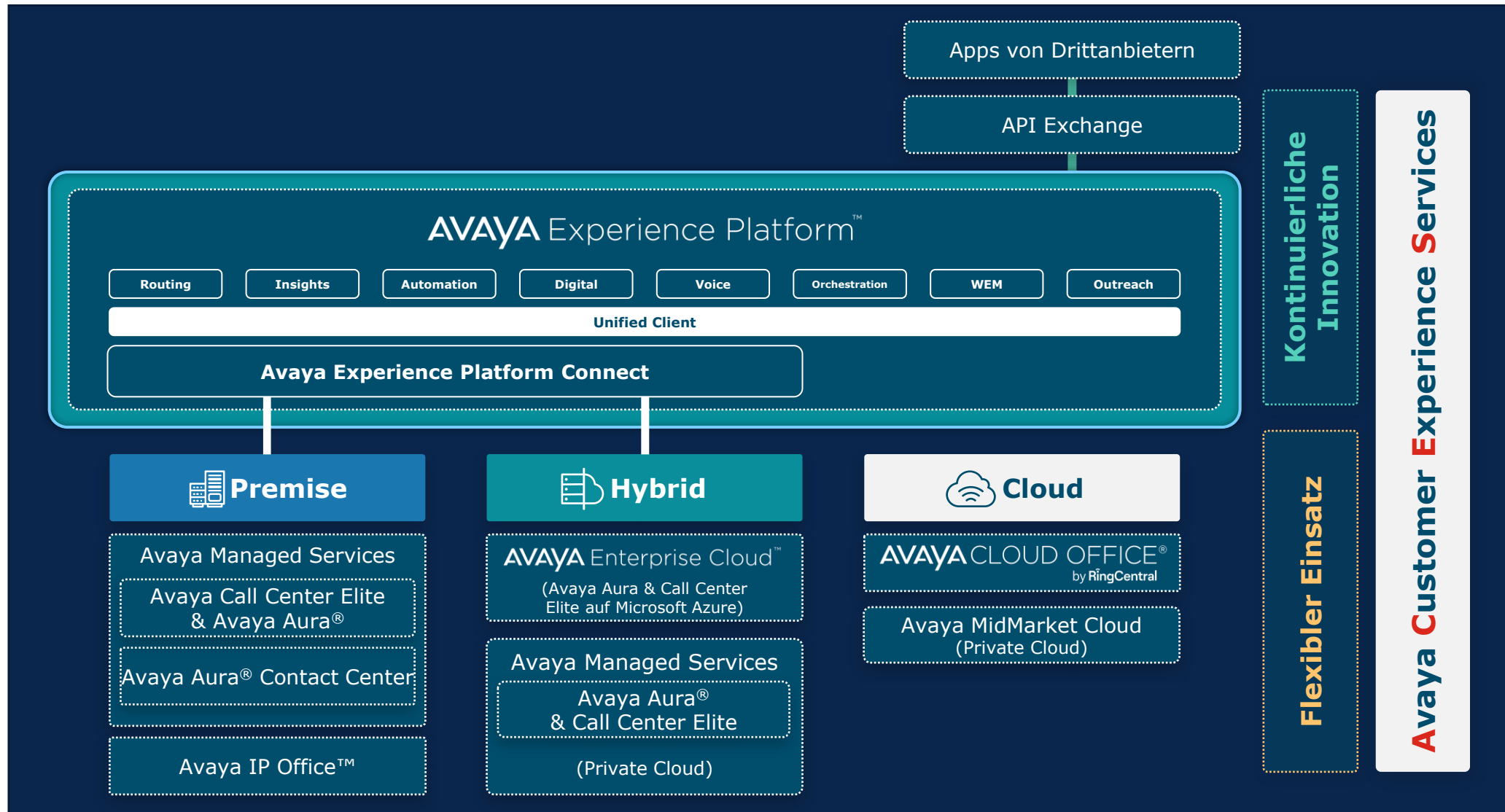
IT-SICHERHEIT IN DER TELEKOMMUNIKATION

**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 Disruption



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

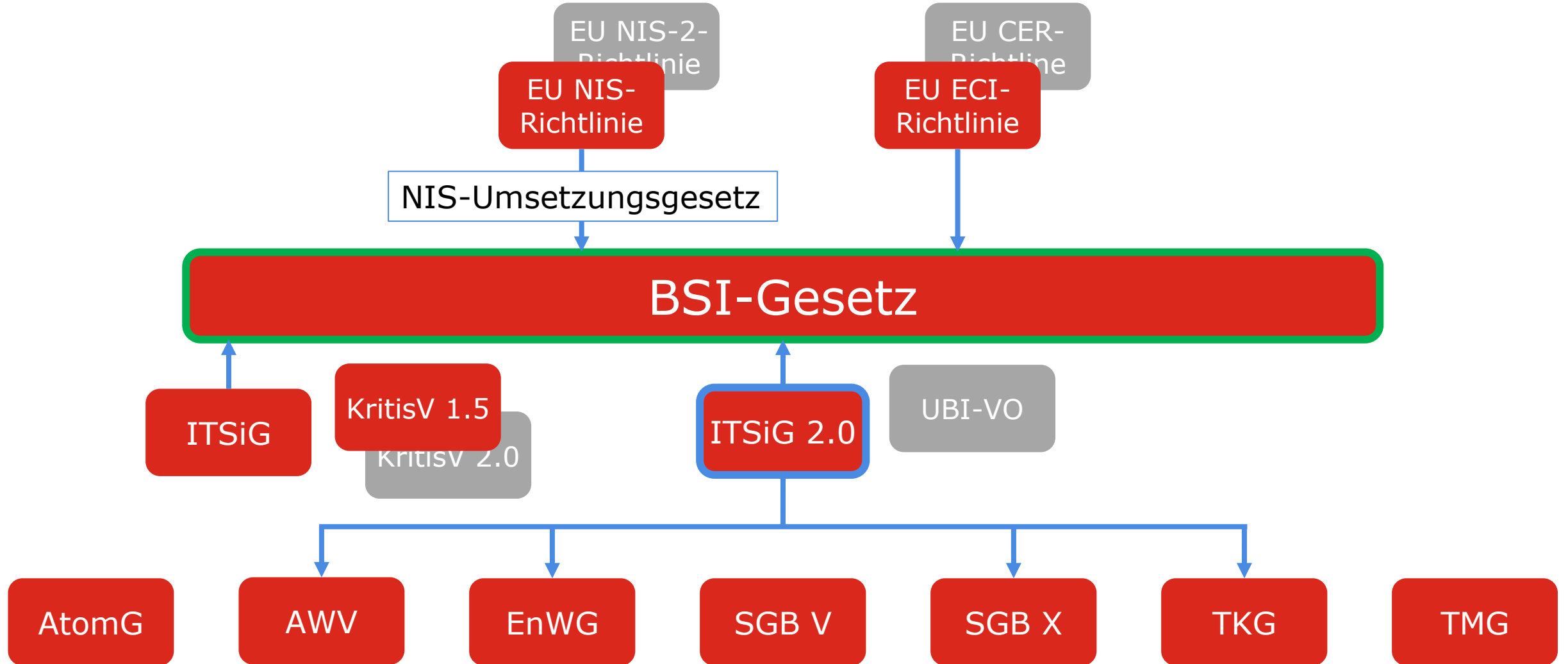
Empfohlene Schutzmaßnahmen

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

**Warum sollten Sie
sich mit diesem
Thema befassen?**



IT-Sicherheit – Kritische Infrastrukturen



KRITIS

10 Sektoren
32 Branchen

- Öffentl. Wasserversorgung
- Öffentl. Abwasserbeseitigung
- Elektrizität
- Fernwärme
- Gas
- Mineralöl

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

- Ernährungswirtschaft
- Lebensmittelhandel

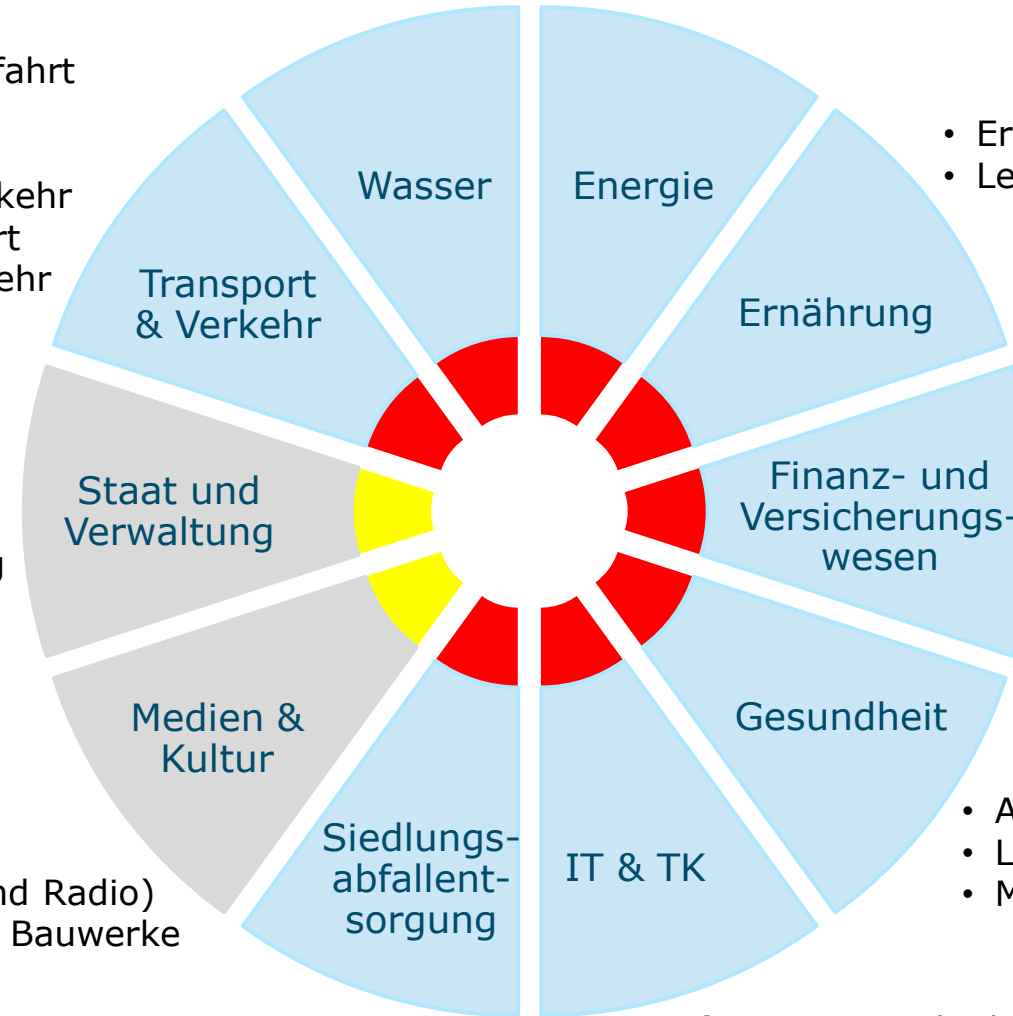
- Justizeinrichtungen
- Notfall-/Rettungswesen
- Parlament
- Regierung und Verwaltung

- Banken
- Börsen
- Finanzdienstleister
- Versicherungen

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

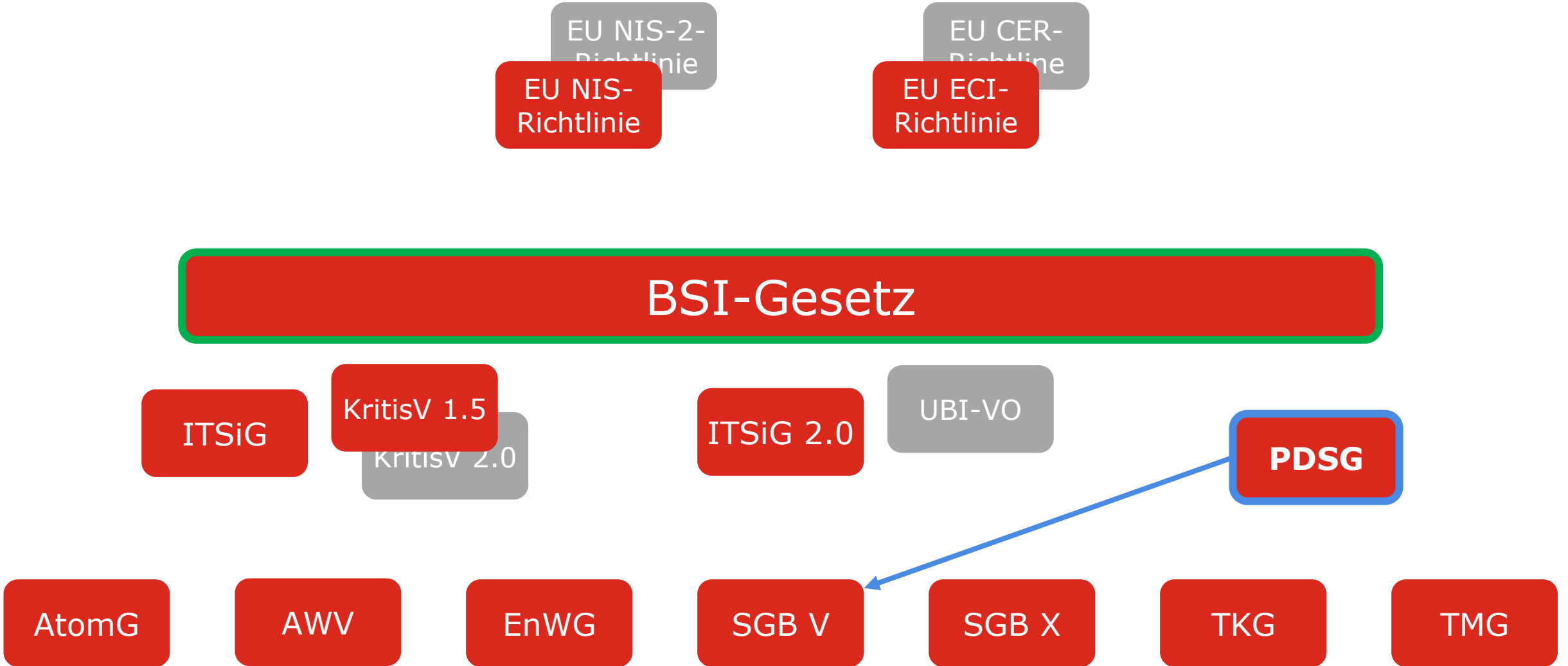
- Arzneimittel und Impfstoffe
- Labore
- Medizinische Versorgung

- Informationstechnik
- Telekommunikation



Diese 8 Sektoren
unterliegen dem
BSI-Gesetz

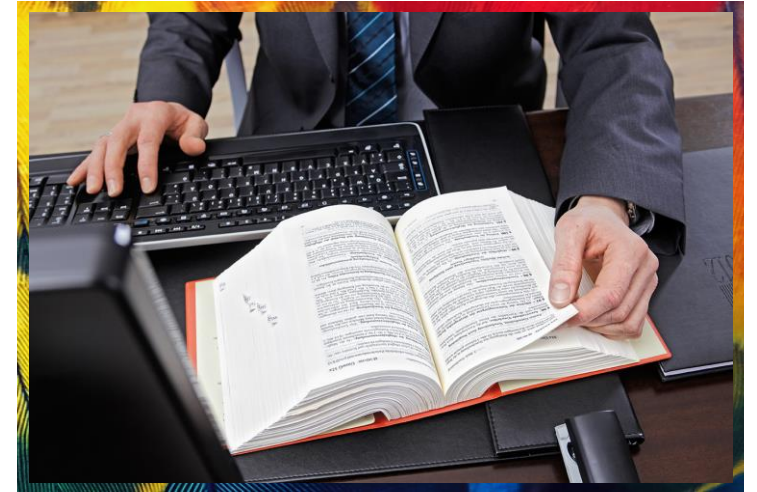
IT-Sicherheit in Krankenhäusern



§ 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!



Warum sollten Sie sich mit diesem Thema befassen?

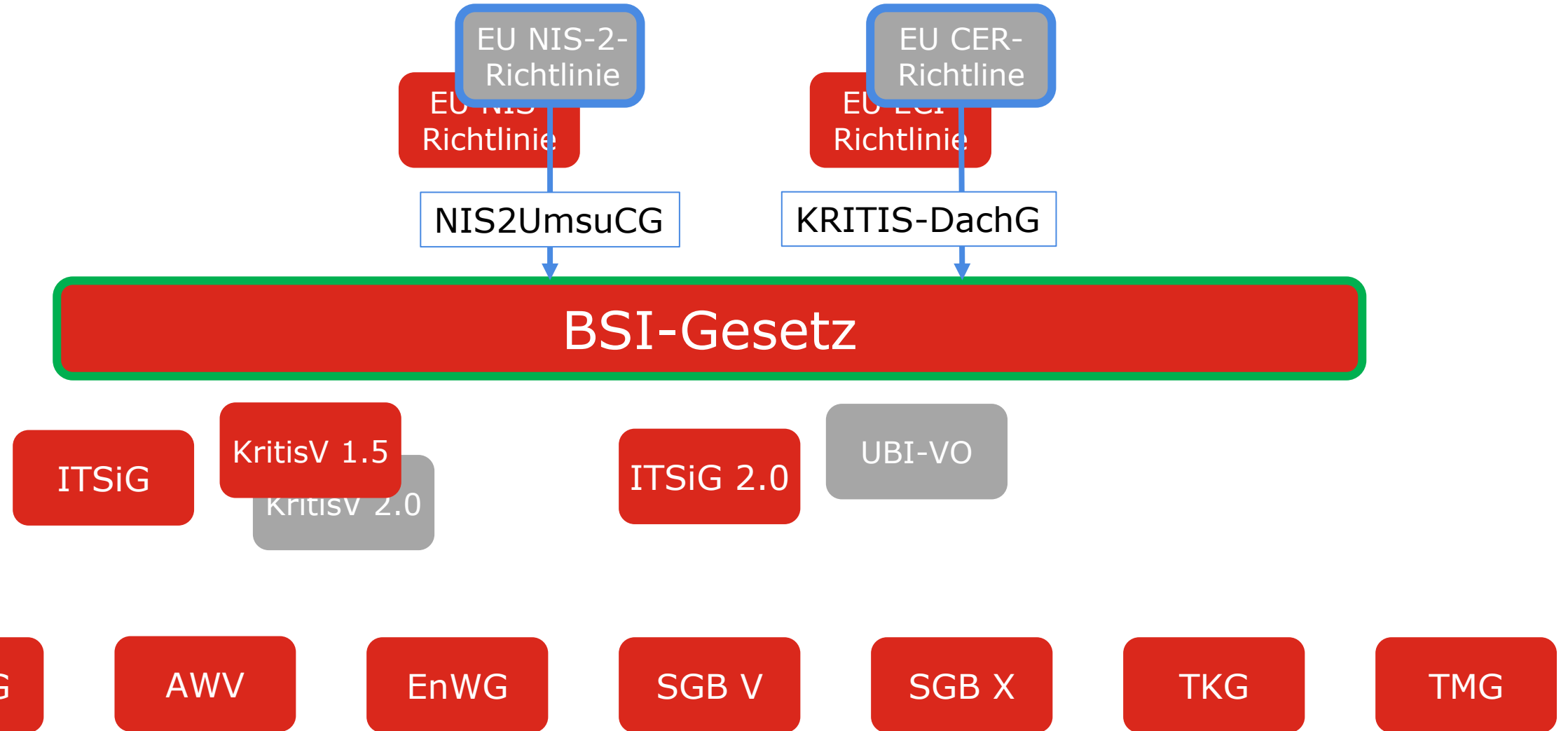
- Für Betreiber Kritischer Infrastrukturen ist IT-Sicherheit durch das BSI-Gesetz gesetzlich verpflichtend
- Für alle Krankenhäuser ist IT-Sicherheit durch § 75c SGB V gesetzlich verpflichtend

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 ...

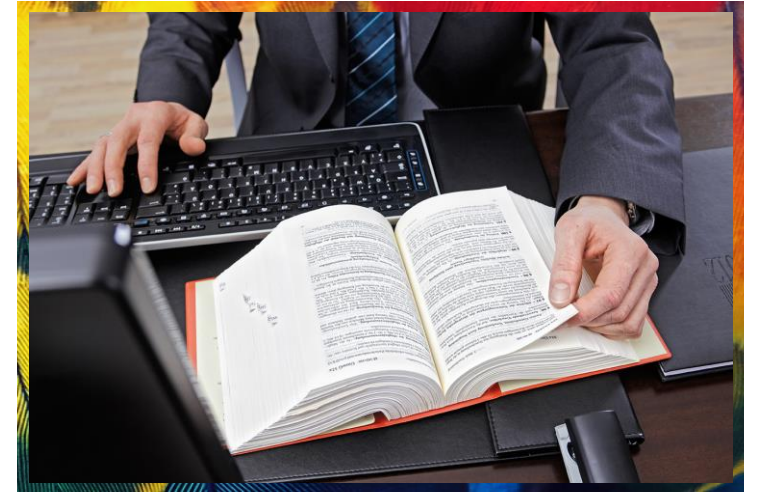
IT-Sicherheit – EU-Richtlinie NIS-2



EU-Richtlinie NIS-2

Richtlinie (EU) 2022/2555 vom 14.12.2022

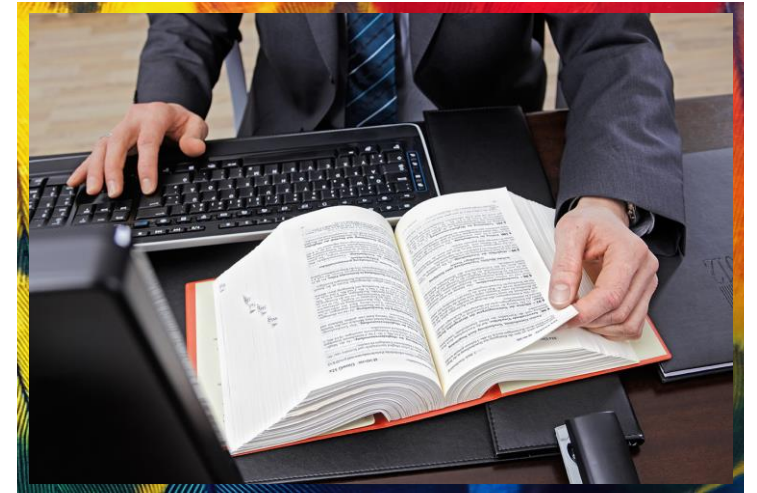
- Erweiterte Betroffenheit
 - Bisher: 8 regulierte KRITIS-Sektoren mit Schwellenwerten
 - Jetzt: 11 Sektoren hoher Kritikalität („wesentliche Einricht.“) und 7 sonstige kritische Sektoren („wichtige Einrichtungen“)
 - Unabhängig von spezifischen Schwellenwerten
 - Pflichten bereits für mittelgroße Unternehmen 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

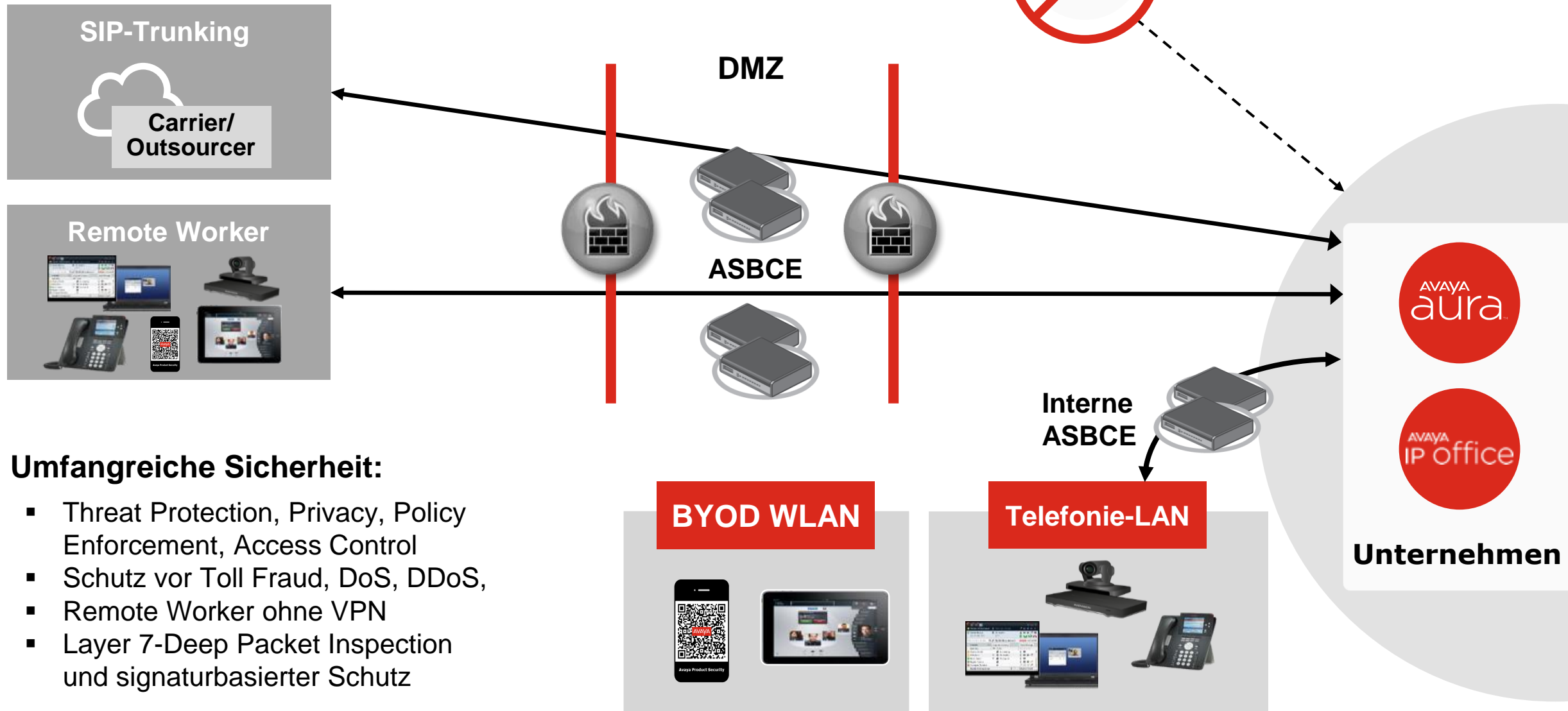
- Erste inoffizielle Referentenentwürfe vom 03.04.2023 und 03.07.2023
- Anpassungen der deutschen Gesetzgebung zur Umsetzung der NIS-2-EU-Richtlinie
- NIS2UmsuCG ist ein Artikelgesetz:
 - Regelungen werden in verschiedenen Gesetzen geregelt
 - BSIG soll das „allgemeine“ Gesetz der IT-Sicherheitsgesetzgebung 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?



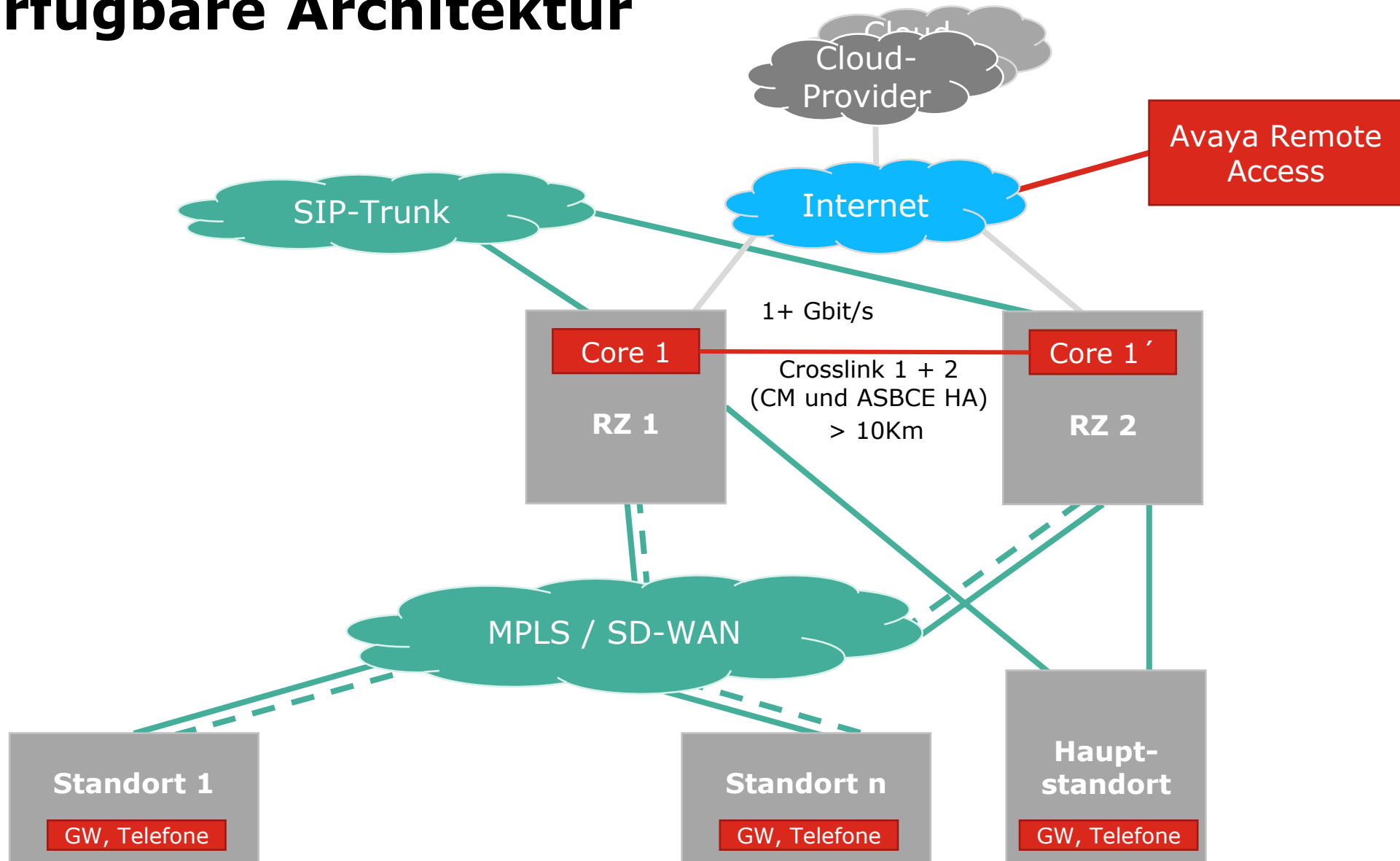
Session Border Controller



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

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)

AVAYA Support Portal

Product Support ▾ My Information ▾ Diagnostics & Tools ▾ Service / Parts Requests ▾ Help ▾ Sign In 🔍

Help Center

Avaya Product Security

Security Support Policies

- Avaya's Product Security Vulnerability Response Policy
- Avaya's Security Vulnerability Classification
- Maintenance Contract Requirements for Product Support
- Avaya Product Security Support Flow
- Security Vulnerability Escalation Prerequisites
- Avaya Product Port Matrix Documents

Current Vulnerability

- > Apache Log4j Vulnerabilities
- > Spring4Shell Vulnerabilities

Avaya Security Advisories by Year


- [Security Advisories for 2023](#)
- [Security Advisories for 2022](#)
- [Security Advisories for 2021](#)
- [Security Advisories for 2020](#)
- [Security Advisories for 2019](#)

Important Note: Avaya Security Advisories (ASA) are posted for vulnerable applications/packages (e.g. Red Hat kernel, Apache Tomcat, etc.) determined to impact Avaya products. An ASA will not be posted if the vulnerable application/package is not installed by default.

Notifications can be provided for new and updated Avaya Security Advisories via subscribing to **E-Notifications**, must have an Avaya Support account and login into the account.

[^ Back to top](#)

Feedback



Avaya Product Security

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



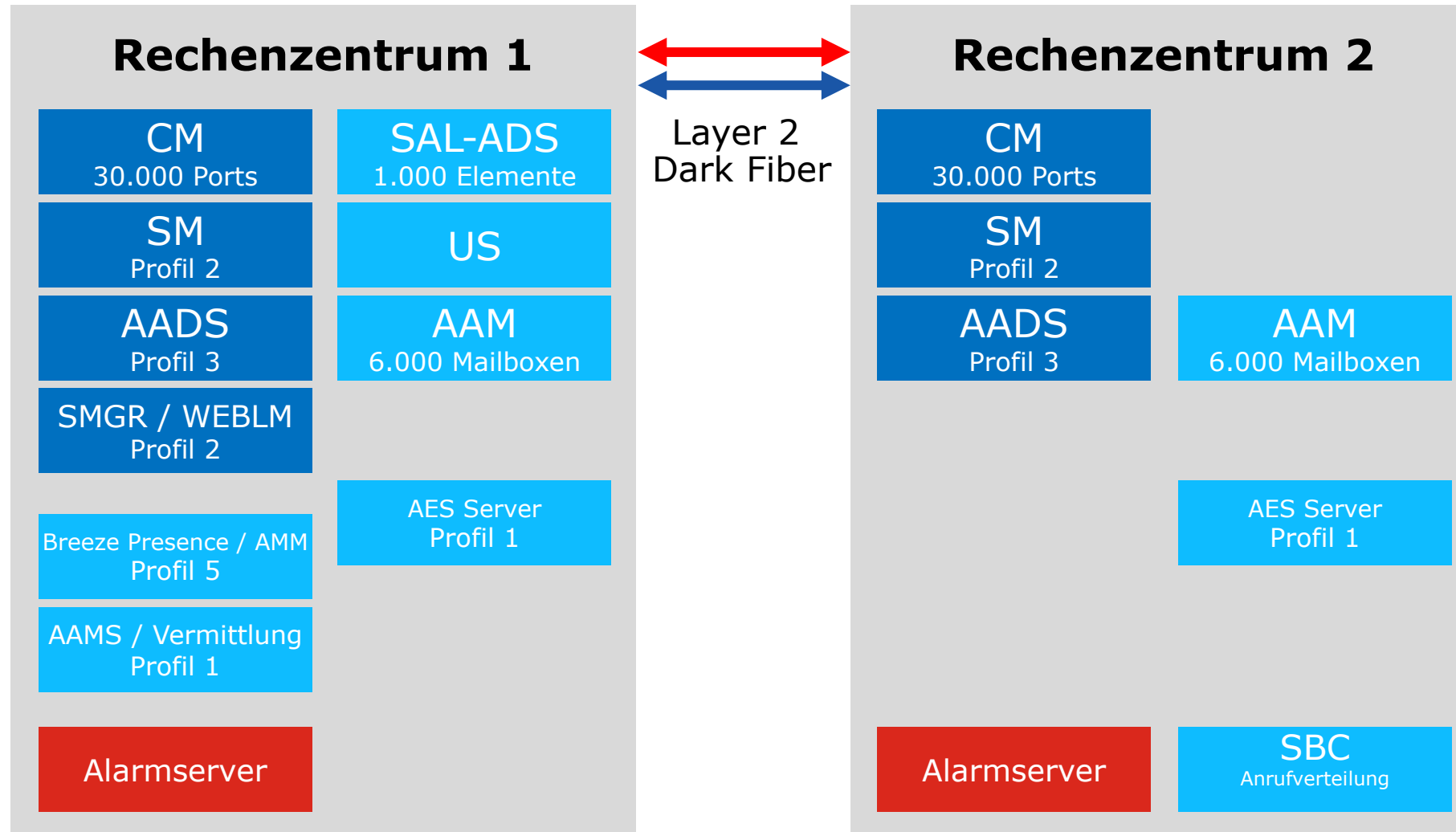
<https://support.avaya.com/support/en/helpcenter/GenericDetail/C2009223125237478059>

Erfahrungen

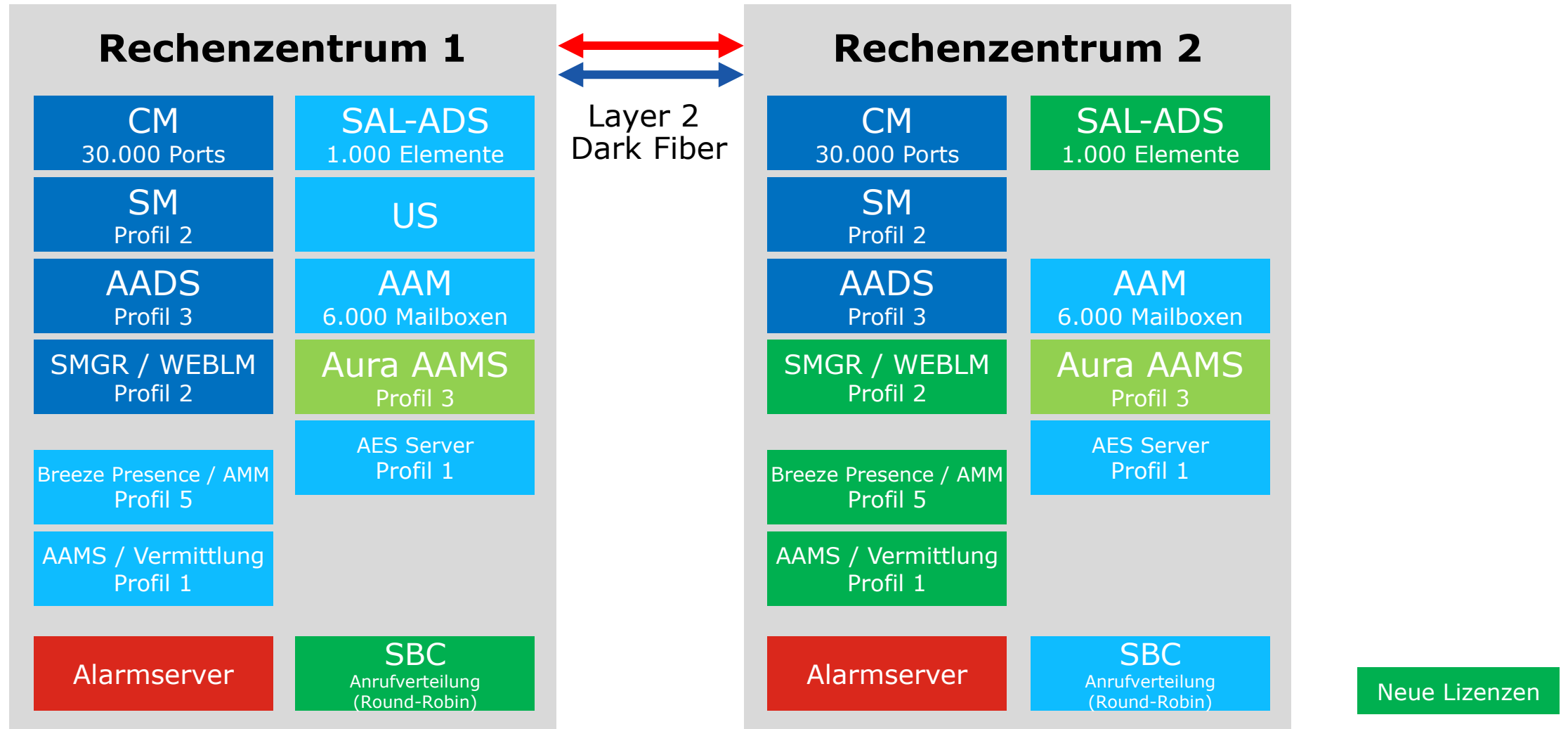
KRITIS-Audit bei einem realen Kunden



Ursprüngliches Avaya Aura Core-Design



Erweiterung des Avaya Aura Core-Designs



Avaya Asset Tracking

Device management

Devices

All X Search for asset search

Id	MAC Address	Type	Vendor	Model	Version	Socket address	Controller	Last registration	Location	Avaya-User	Handle
41885	b4:b0:17:8b:01:20		Avaya	96x1	7.1.3.0.11	192.168.0.117:57213	avayasm-01-SM	2019-01-30T17:41:38Z	Ravensburg	k.doukas@engelbart-software.com	312@engelbart.local
41886	b4:b0:17:8a:ff:50		Avaya	96x1	7.1.3.0.11	192.168.0.107:5840	avayasm-01-SM	2019-01-30T17:41:10Z	Ravensburg	j.emele@engelbart-software.com	320@engelbart.local
41887	b4:b0:17:8a:fb:eb		Avaya	96x1	7.1.3.0.11	192.168.0.93:58768	avayasm-01-SM	2019-01-30T17:42:02Z	Ravensburg	e.hobek@engelbart-software.com	319@engelbart.local
41888	b4:b0:17:8a:fc:33		Avaya	96x1	7.1.3.0.11	192.168.0.123:22246	avayasm-01-SM				
41891	b4:b0:17:8a:fb:e3		Avaya	96x1	7.1.3.0.11	192.168.0.110:28849	avayasm-01-SM				
41892	6c:a8:49:8e:cd:d8		Avaya	96x1	7.1.3.0.11	192.168.0.124:51819	avayasm-01-SM				
41893	6c:a8:49:8e:cd:9f		Avaya	96x1	7.1.3.0.11	192.168.0.98:37871	avayasm-01-SM				
41894	24:d9:21:3a:a3:ac		Avaya	96x1	7.1.3.0.11	192.168.0.104:59998	avayasm-01-SM				
41895	b4:b0:17:8a:fb:ec		Avaya	96x1	7.1.3.0.11	192.168.0.130:17919	avayasm-01-SM				
41896	6c:a8:49:8e:21:36		Avaya	96x1	7.1.3.0.11	192.168.0.101:13515	avayasm-01-SM				

1 2
1-10 / 15

Device SIP - 41892

Id: 41892

MAC Address: 6c:a8:49:8e:cd:d8 Socket address: 192.168.0.124:51819

Location: Ravensburg Type: SIP

Controller: avayasm-01-SM Last registration: 2019-01-10T14:33:02Z

Vendor: Avaya Model: 96x1 Version: 7.1.3.0.11

Avaya-User: d.engelbart@engelbart-software.com

Handle: 302@engelbart.local

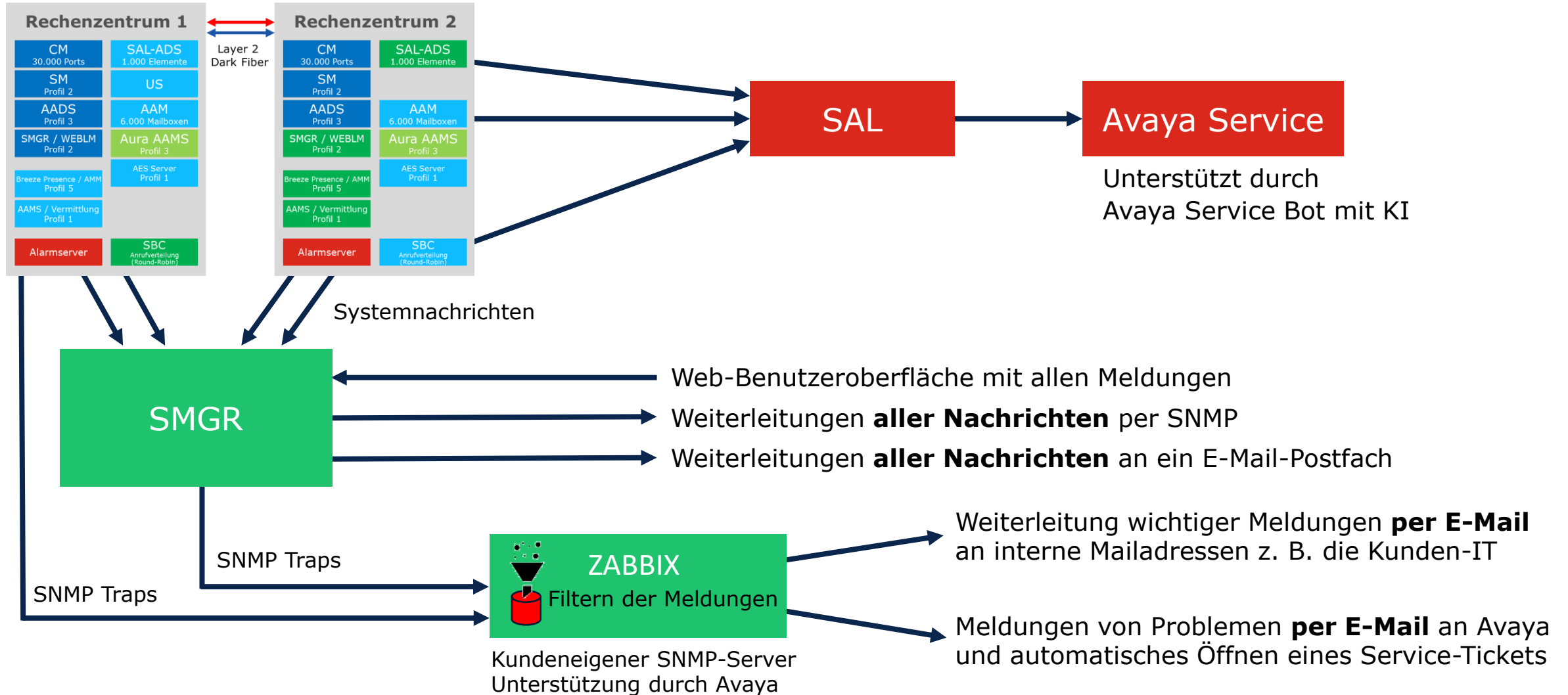
reboot device

upgrade firmware

- 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



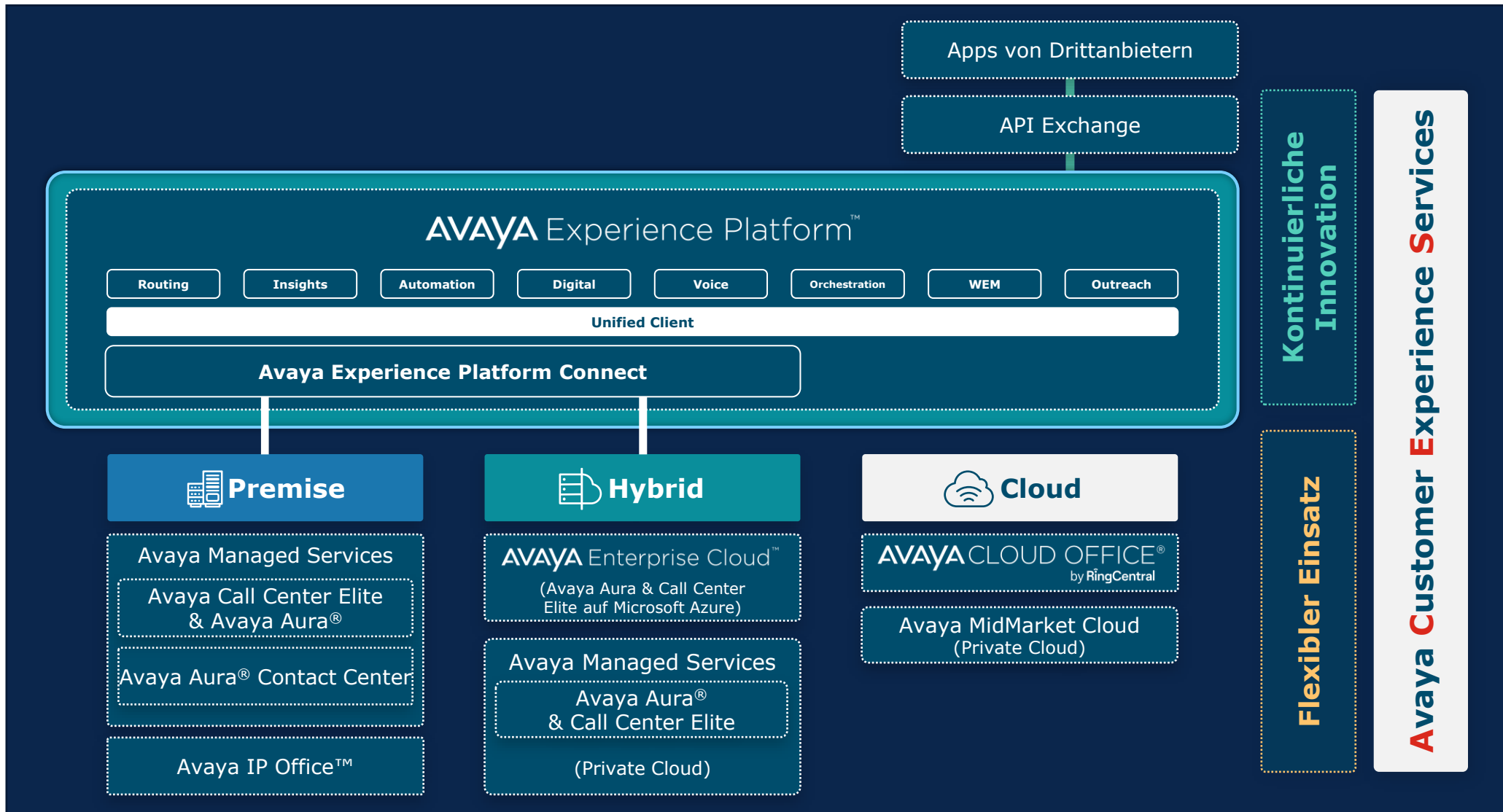
IT-Sicherheit in der Telekommunikation

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 Disruption



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

The Avaya logo is positioned on the left side of the slide. It features the word "AVAYA" in a stylized, multi-colored font. The letters are outlined and filled with a gradient of colors: red, orange, yellow, and blue. The 'A' at the end is blue. The logo is set against a white background with a colorful border on the left and bottom edges.

AVAYA

VIELEN DANK