

TELENOT

KRITIS, NIS-2 und Co.

Was nun? Was tun?

Creating Your Security

Öffentlich

Agenda

01 Themenkreis

02 KRITIS-DachG

03 NIS-2

04 DORA

05 CRA

06 ISO 27001

07 Was nun? Was tun?

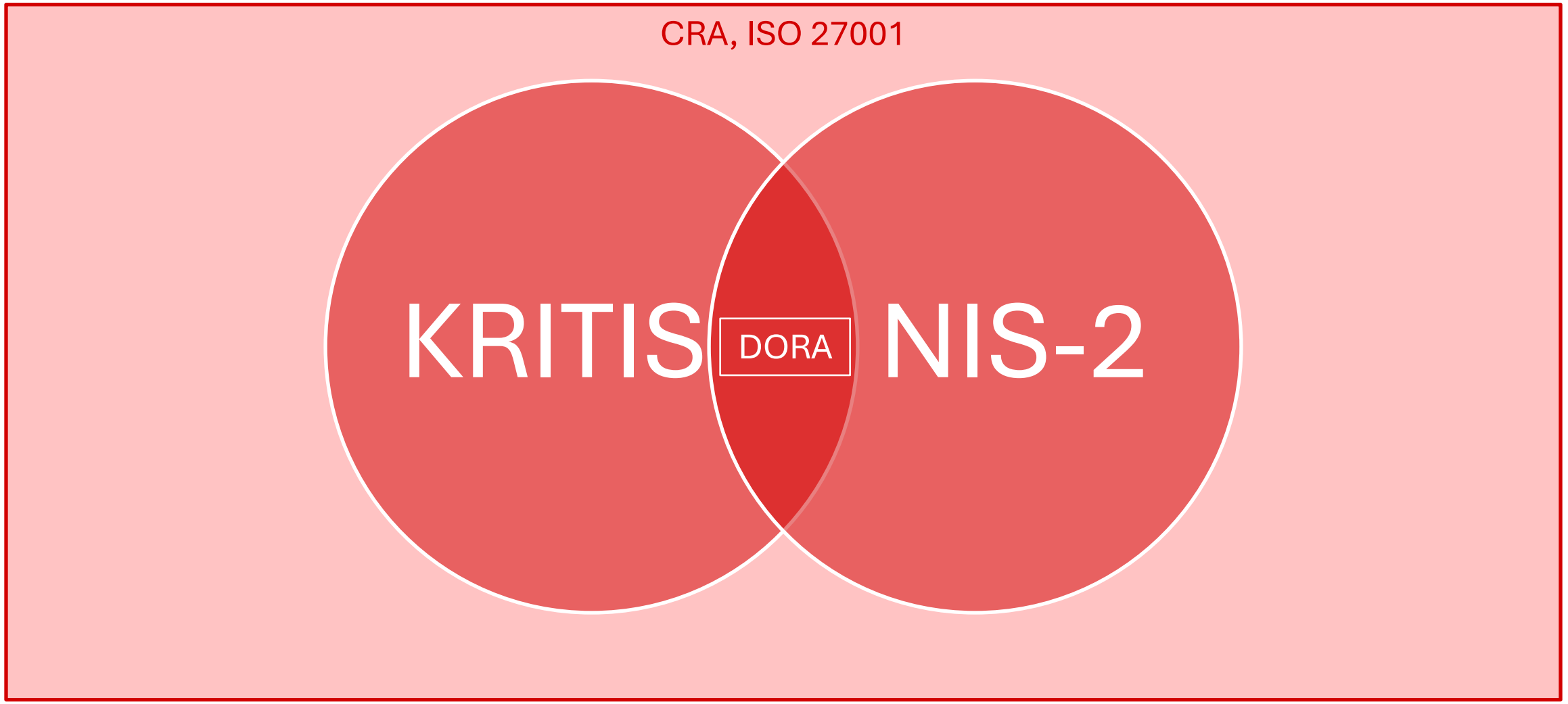
08 Fazit

Öffentlich

Themenkreis



Heutiger Themenkreis



Begriffe und Abkürzungen

KRITIS / Kritische Infrastruktur

Sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe,erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

KRITIS-Dachgesetz

Reguliert die Resilienz und physische Sicherheit Kritischer Infrastrukturen. Das Gesetz setzt die EU-Direktive RCE in Deutschland durch zusätzliche Pflichten (Meldepflichten, BCM/Betriebliches Kontinuitätsmanagement, physische Sicherheit, Personal und Krisen-management) für Betreiber kritischer Anlagen um. In Kraft getreten am 16. März 2026.

BBK / Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Aufsichtsbehörde für KRITIS-DachG

BSI / Bundesamt für Sicherheit und Informationstechnik

Aufsichtsbehörde für NIS-2

Begriffe und Abkürzungen

NIS-2 / Network and Information Systems Direktive / NIS-2 Umsetzungs- und Cybersicherheits-Stärkungsgesetz

Schwerpunkt Cybersicherheit. Das Gesetz wurde am 5. Dezember 2025 im Bundesgesetzblatt veröffentlicht und trat nach seinem Art. 30 am 6. Dezember 2025 in Kraft.

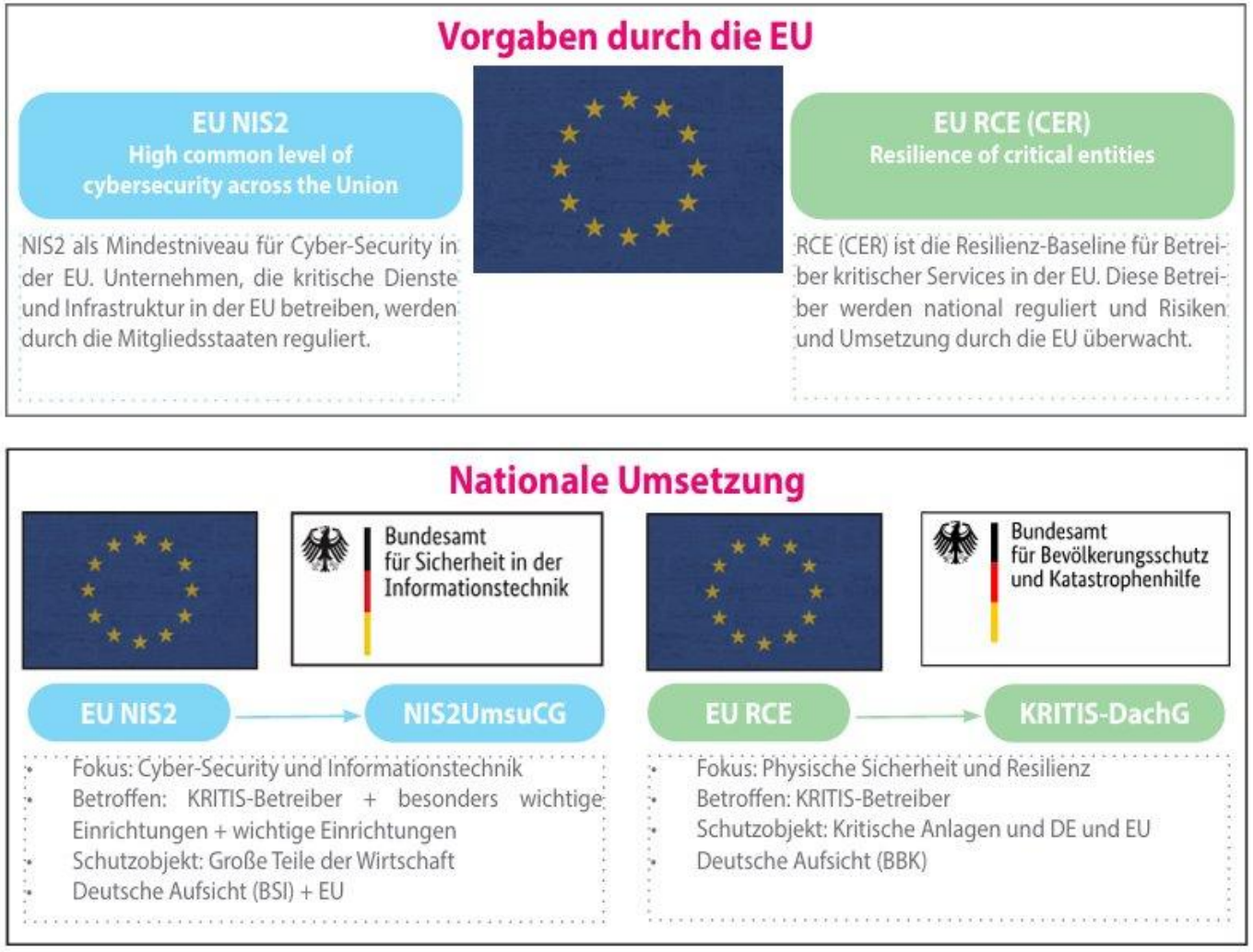
CRA / Cyber Resilience Act

EU-Verordnung zu Cybersicherheits-Anforderungen für Produkte. Teil von CE-Kennzeichnung eines Herstellers.

DORA / Digital Operational Resilience Act

Mit der Verordnung (EU) 2022/2554 verpflichtet die Europäische Union Finanzunternehmen zur Stärkung ihrer digitalen operationalen Resilienz.

Vorgaben durch die EU



Unterschied KRITIS und NIS-2



KRITIS-Dachgesetz konzentriert sich auf physische Sicherheit kritischer Infrastruktur

- Zutritt, Sabotage, Diebstahl, Brand,…



NIS-2 Umsetzungsgesetz konzentriert sich darauf, die digitale Sicherheit zu erhöhen

- IT-Systeme, Cybersicherheit,…
- Physische Sicherheit ist hier nur ein Teilthema davon

KRITIS

KRITIS-Dachgesetz



Warum das KRITIS-Dachgesetz?

- Kritische Infrastruktur gewährleistet das alltägliche Funktionieren der Gesellschaft
- Bei einem Ausfall ist die Sicherheit und Ordnung gefährdet
- Störungen führen zu Engpässen bei lebenswichtigen Gütern

KRITIS: Wer ist betroffen?

- Einrichtungen, die für das Funktionieren von Gesellschaft, Staat und Wirtschaft essenziell sind
- 10 Sektoren
- Betrifft ca. **2.000 Betreiber** in Deutschland
  - Versorgung von > 500.000 Menschen
  - Anlagen von "besonderer Bedeutung für Europa"



[1] Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende

Öffentlich

KRITIS: Was muss der Betreiber tun?

Beim BBK registrieren und eine 24h-Kontaktstelle für die betriebene Kritische Infrastruktur melden

Risiken bewerten & Resilienzpläne erstellen

- Naturbedingte, klimatische und vom Menschen verursachte Risiken
- Geeignete sicherheitsbezogene, technische und organisatorische Maßnahmen zur Gewährleistung der Resilienz planen (physischer Schutz gemäß „Stand der Technik“)

Umgehend erhebliche Störungen melden

Im Turnus von zwei Jahren alles dem BBK nachweisen

NIS-2

Network and Information Systems Direktive / NIS-2 Umsetzungs- und Cybersicherheits-Stärkungsgesetz



Warum NIS-2 Umsetzungsgesetz?

- Um eine sichere und stabile IT-Infrastruktur für Unternehmen zu gewährleisten
- Um Cyber-Angriffe oder technische Ausfälle, die den Betrieb erheblich stören zu verhindern

NIS-2 Umsetzungsgesetz

- Die NIS2-Richtlinie und das folgende Gesetz soll ein Mindestmaß an **Cybersicherheit in der gesamten EU** gewährleisten

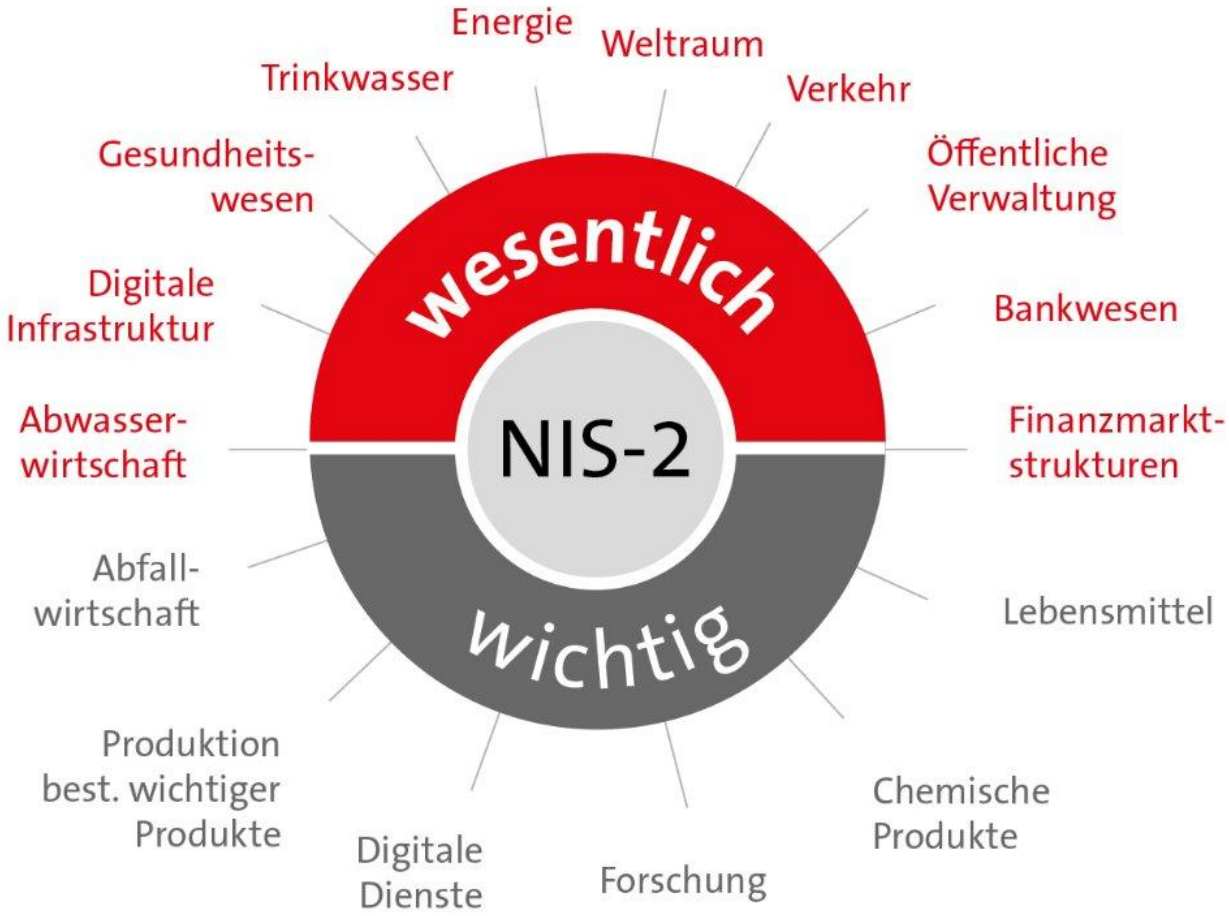
- Sie gilt für alle Unternehmen und Einrichtungen, die kritische Dienste und Infrastrukturen betreiben. Die Mitgliedstaaten müssen sicherstellen, dass diese Betreiber ihre Netze und IT-Systeme gegen Cyber-Angriffe schützen

- In Deutschland erfolgte die Umsetzung der NIS2-Richtlinie durch das NIS2-Umsetzungsgesetz (NIS2UmsuCG), die Aufsicht übernimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI)

NIS-2: Wer ist betroffen?

- Unternehmen die entgeltlich in abgebildeten Sektoren tätig sind

- In Deutschland sind ca. **30.000 Unternehmen** betroffen
  - Anzahl Mitarbeiter > 50
  - Jahresumsatz und Jahresbilanzsumme > 10 Millionen Euro



NIS-2: Was muss der Betreiber tun?

Registrierung beim BSI

Umgehend erhebliche Sicherheitsvorfälle melden

Risikomanagement bewerten

Risikoanalyse, Incident Response, Absicherung der Lieferkette, Einsatz von Verschlüsselung, Multi-Faktor Authentifizierung, Zugriffs- und Zutrittskontrollen, Schulungen

DORA

Digital Operational Resilience Act (nur Finanzsektor)



EU-Verordnung DORA
Auswirkungen auf Errichter mit Kunden aus dem Finanzsektor

- Mit der Verordnung sollen die **Anforderungen des Finanzsektors im Umgang mit den Themen Cybersicherheit und IKT-Risiken** wesentlich verschärft und gleichzeitig ein neuer Aufsichtsrahmen für IKT-Dienstleister geschaffen werden (digitale operationale Resilienz).

- DORA wurde deshalb im Verhältnis zur Richtlinie NIS-2 als spezielleres Recht (lex specialis) eingestuft und ist folglich vorrangig vor NIS-2 anzuwenden. Die für sicherheitstechnische Unternehmen entscheidendste Neuregelung bezieht sich auf die kritischen IKT-Dienstleister, die nun unter die Aufsicht einer der drei europäischen Aufsichtsbehörden EBA, ESMA oder EIOPA gestellt werden.

- DORA findet seit dem 17. Januar 2025 unmittelbare Anwendung.

EU-Verordnung DORA
Empfehlungen

- **Zunächst kein Handlungszwang für sicherheitstechnische Unternehmen**, die für Finanzunternehmen tätig sind

- Finanzunternehmen sind zur Umsetzung verpflichtet

- Finanzunternehmen übernehmen Ausgestaltung des erforderlichen Regelwerkes gemäß DORA

CRA

Cyber Resilience Act



Cyber Resilience Act

- Teil der **CE-Kennzeichnung** eines Herstellers
- **Produkte mit digitalen Elementen** (Hard- und Software) – Direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz
- „Security by Design“ als Lebenszyklusanforderung (EoL)
- Risikobewertung und Dokumentationspflichten beim Hersteller
- Schutz der Lieferkette unter Einbeziehung von Produkten aus Drittstaaten
- Pflicht zu **Sicherheitsaktualisierungen** „by default“

Cyber Resilience Act

Wichtige Termine

- 10. Dezember 2024: Inkrafttreten der Verordnung
- 11. September 2026: Beginn der Meldepflicht
- **11. Dezember 2027:** Verpflichtungen treten in Kraft

- **Das heißt, ab dem 11.12.2027 dürfen keine Produkte mehr (neu) verbaut werden, die dem CRA nicht entsprechen!**



ISO 27001



ISO 27001

- Die ISO 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS).
- Sie definiert den systematischen Rahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmensdaten.
- Ziel ist es, Risiken systematisch zu erkennen und zu steuern, um Informationswerte und Geschäftsprozesse angemessen zu sichern und rechtliche sowie vertragliche Anforderungen zu erfüllen.
- TELENOT aktuell in der finalen Auditphase – das heißt, auch hier ein verlässlicher Partner für Betreiber, Fachbetriebe, baunahe Gewerke

Was nun? Was tun?



Was ist zu tun?

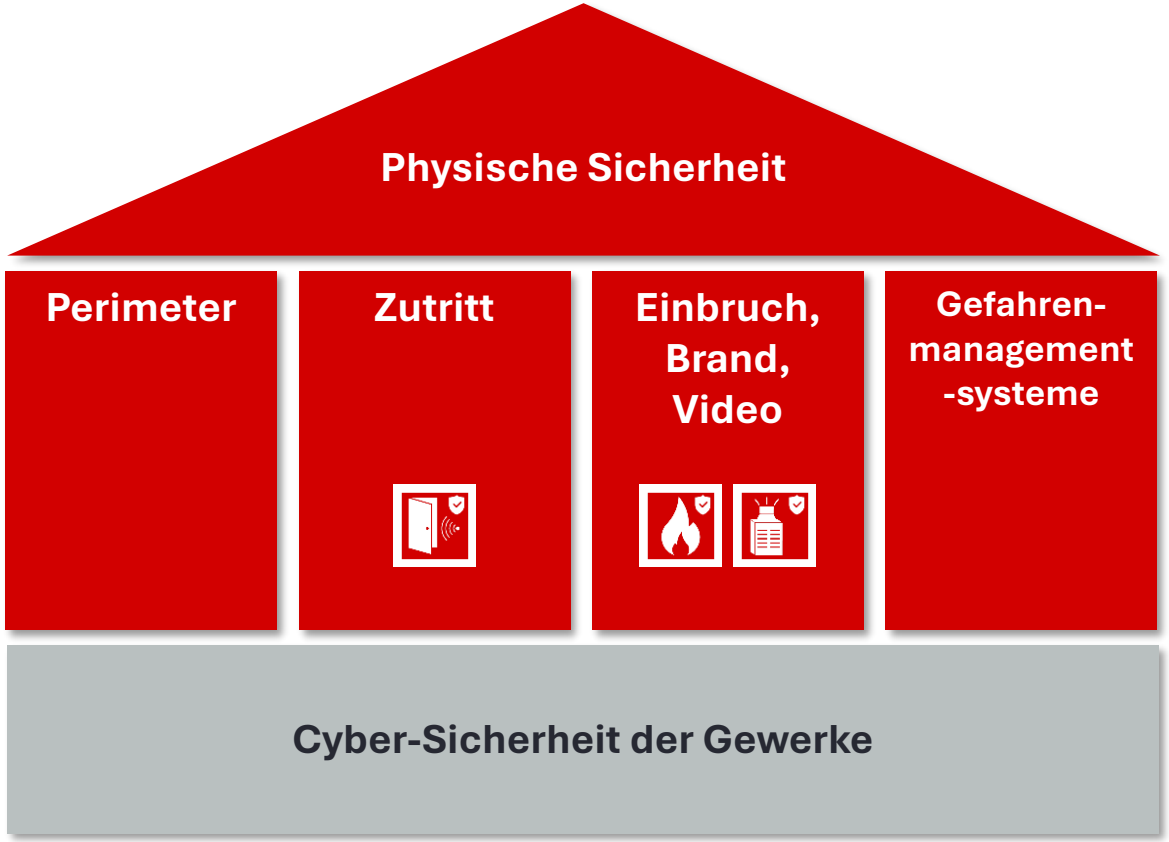
- **Ganzheitliche Sicherheitskonzepte**: Kombination von physischen Schutzmaßnahmen und Cyber-Security-Anforderungen
- Resilienz-Betrachtung: Wie kann die Widerstandsfähigkeit gegen Bedrohungen erhöht und die Zeit zur Wiederherstellung kurz gehalten werden?
- Risikobewertung: Passen die gewählten Schutzmaßnahmen zum Objekt?
- **Beachtung technischer Standards und Normen / Richtlinien: „Stand der Technik“**

Der Risikomanagementprozess



Öffentlich

Physische Schutzmaßnahmen



- **Perimeterschutz**
  - Physischer Schutz und Detektion
- **Zutritts- und Zugangssteuerung**
  - Zufahrts- und Zugangsschutz der Ein- und Ausfahrten, Ein- und Ausgänge, Schranken und Schleusen
- **Einbruchmeldeanlagen, Brandmeldeanlagen und Videosicherheitssysteme**
  - Schutz der Gebäude und Gelände – Detektion
- **Gefahrenmanagementsysteme**
  - Notfallmanagement (Standard-Handlungsabläufe)
  - Abarbeitung organisatorischer Maßnahmen – auch in Krisensituationen
  - Vorausschauender Überblick zur Sicherheitslage und „Systemgesundheit“

Physischer Schutz von Gebäuden im Themenkreis mit TELENOT



- Damit Betreiber von kritischen Infrastrukturen die Resilienz ihrer Anlagen zuverlässig gewährleisten können, wird **unsere elektronische Sicherheitstechnik** (Einbruch, Brand, Zutritt) auf Herz und Nieren geprüft sowie entsprechend der deutschen und **europäischen Normen und Richtlinien zertifiziert**.

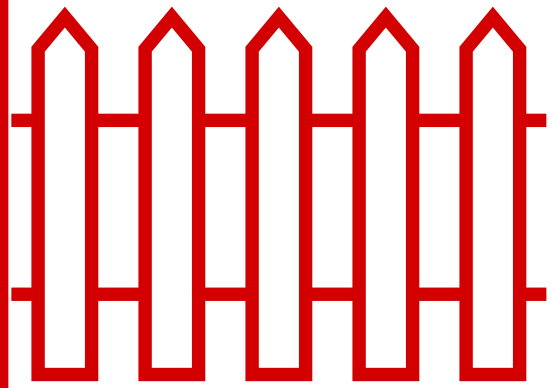
- Mit **unseren Produkten kann das Thema in Bezug zur physischen Sicherheit** umfangreich aus einer Hand gelöst werden – denn wir bieten Ihnen als Systemanbieter alles.

Was nun? Was tun!

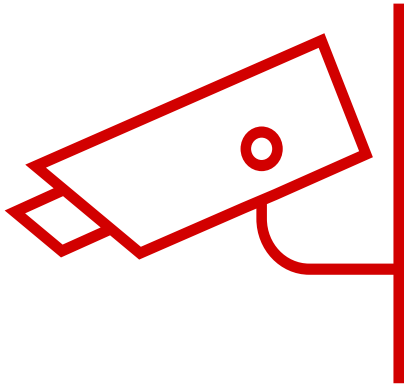
Perimetersicherung

- Äußerste Hürde
- Einsatz von Zäunen, Schranke, mechanische Barrieren
- Kombiniert mit Videosystemen

	Dokument	Typ	Titel
1	DIN CLC/TS 50661-1 (VDE V 0830-100-1)	Technische Spezifikation / Vornorm	Alarmanlagen - Externe Perimeter-Sicherheitsanlagen Teil 1: Systemanforderungen
2	DIN VDE V 0826-20	Vornorm	Überwachungsanlagen - Teil 20: Externe Perimeter Sicherheitsanlagen - Anwendungsregeln



Was nun? Was tun!



Videosicherheitssysteme

- Ergänzung zu anderen Sicherheitstechniken
- Beobachtung des Geschehens vor Ort

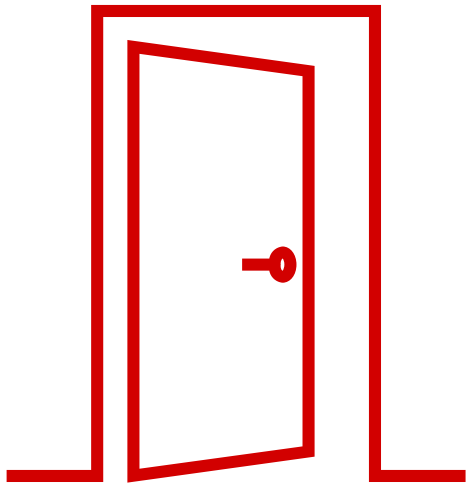
	Dokument	Typ	Titel
1	DIN EN 62676-1-2 VDE 0830-7-5-12	Norm	Videoüberwachungsanlagen für Sicherungsanwendungen Teil 1-2: Systemanforderungen – Allgemeine Anforderungen an die Videoübertragung
2	DIN EN 62676-4	Norm	Anwendungsregeln für Videosysteme in Sicherheitsanwendungen

Was nun? Was tun!

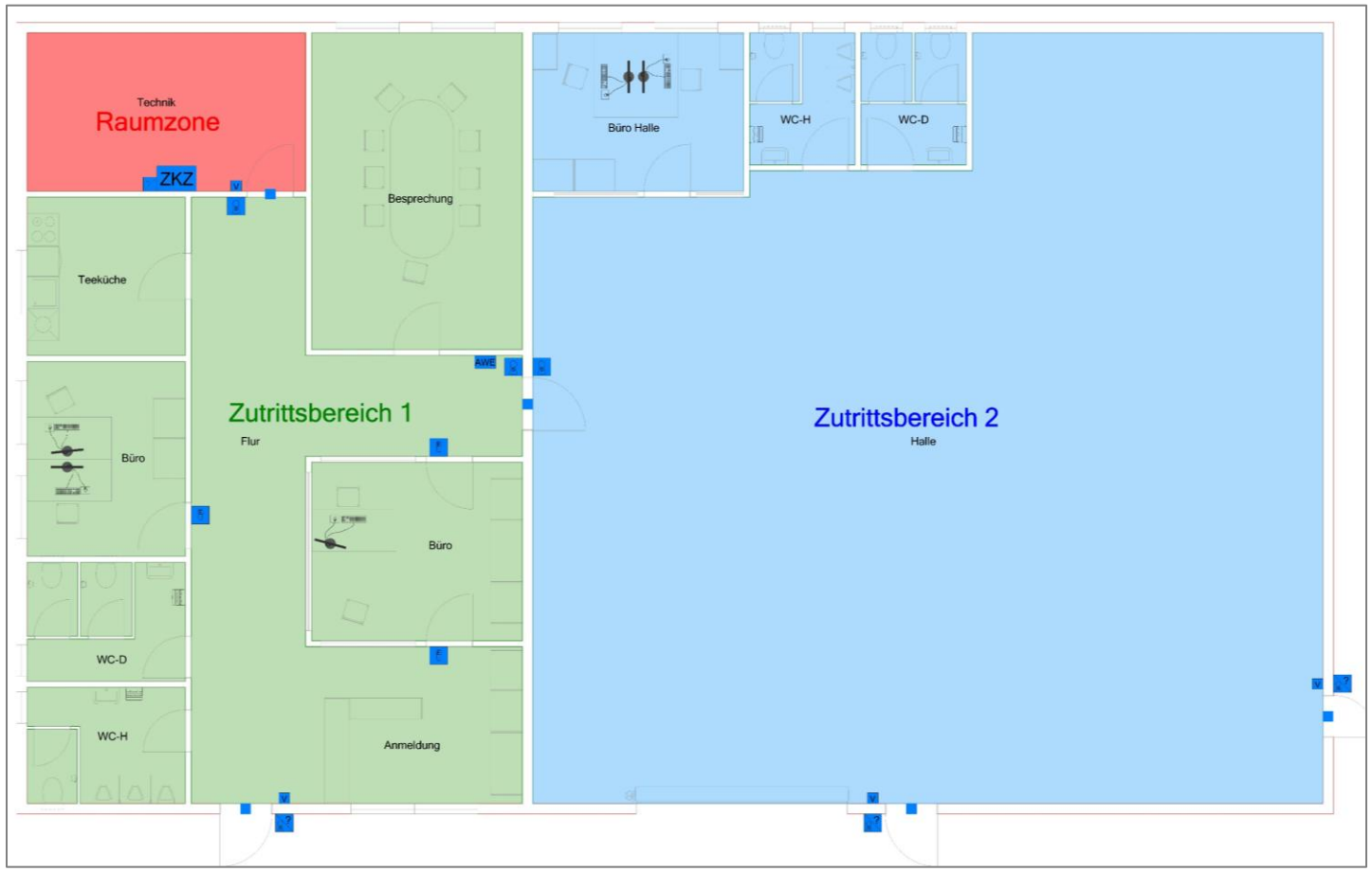
Zutritts- und Zugangssteuerung

- Regelung von Zutritten in schutzbedürftige Bereiche
- Einsatz von RFID-Lesern, Elektromechanische Zylinder / Türdrücker, Smartphones, Biometrie,...

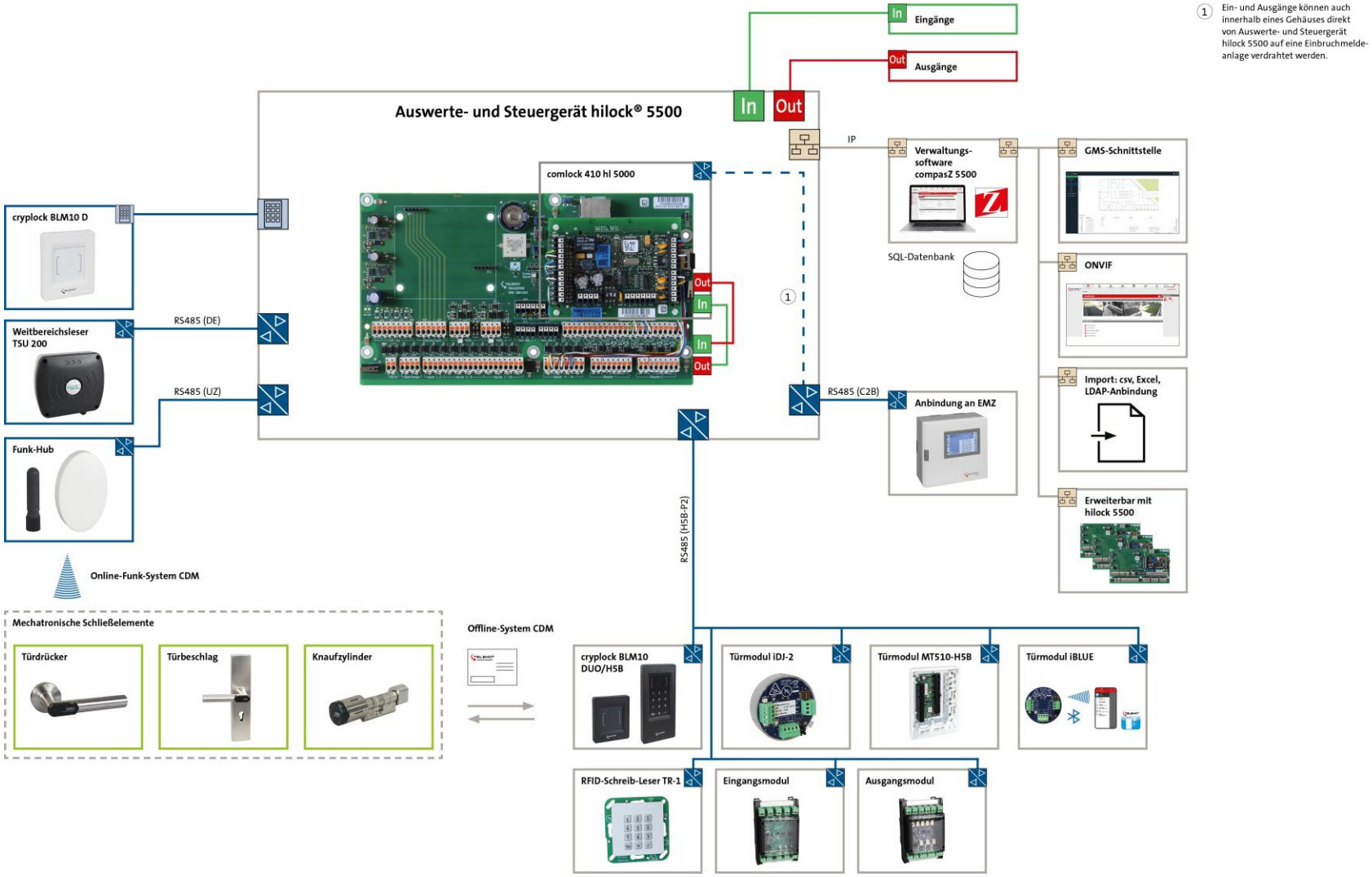
	Dokument	Typ	Titel
1	DIN EN 60839-11-1	Technische Spezifikation	Alarmanlagen - Teil 11-1: Elektronische Zutrittskontrollanlagen - Anforderungen an Anlagen und Geräte
2	DIN EN 60839-11-2	Anforderungen an den Betrieb	Alarmanlagen - Teil 11-2: Elektronische Zutrittskontrollanlagen - Anwendungsregeln



Was nun? Was tun!
Zutrittskontrolltechnik von TELENOT



Was nun? Was tun!
Zutrittskontrolltechnik von TELENOT



Öffentlich

Was nun? Was tun!

Einbruchmeldeanlagen

- Sicherung von Diebstahl und Schutz von Personen als auch Geschäftsgeheimnisse innerhalb von Gebäuden und Anlagen
- Einsatz von Bewegungsmeldern, Magnetkontakten, Glasbruchsensoren,...

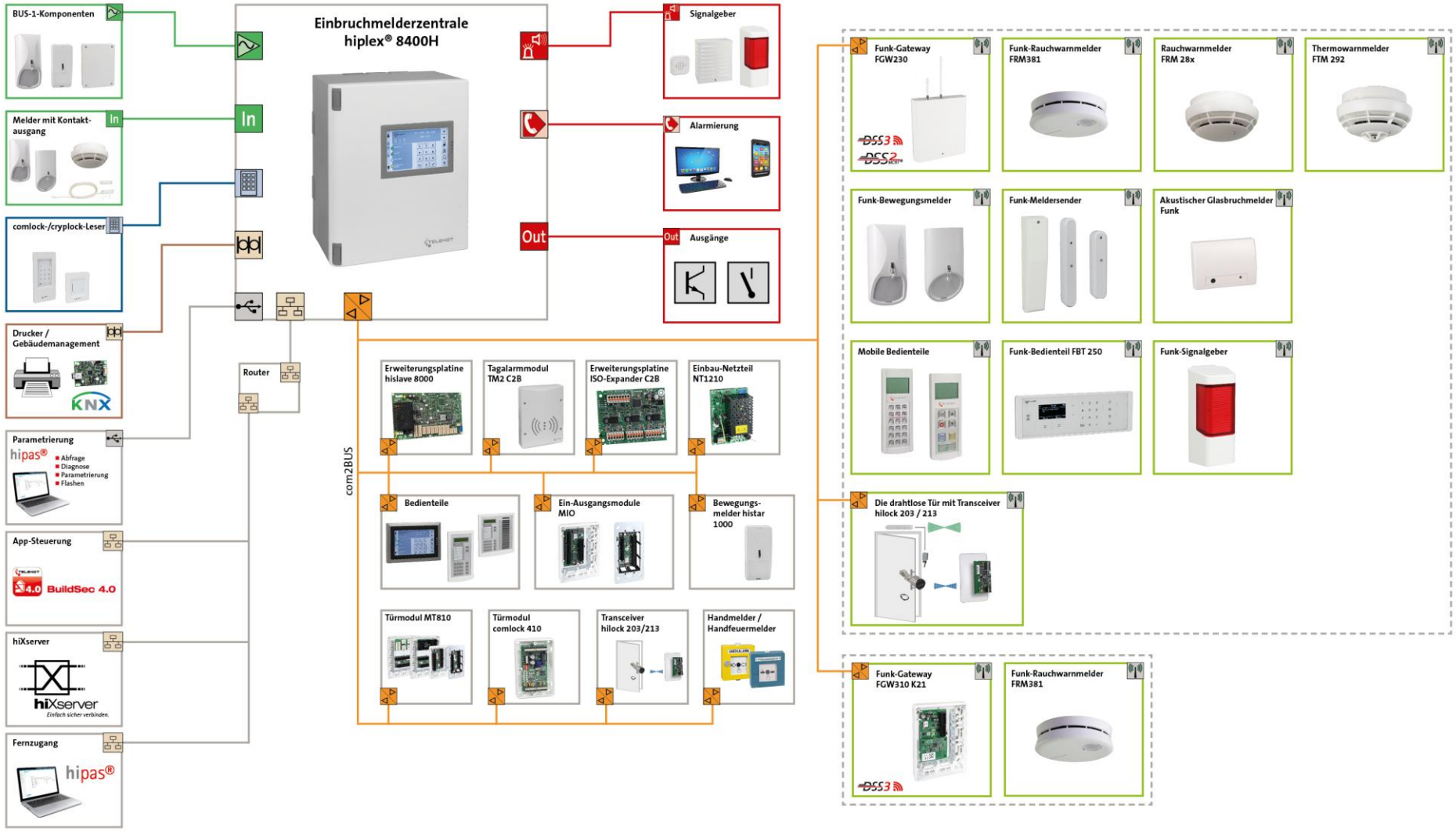
	Dokument	Typ	Titel
1	DIN VDE 0833-1	Norm	Gefahrenmeldeanlagen für Brand, Einbruch und Überfall - Teil 1: Allgemeine Festlegungen
2	DIN VDE 0833-3	Norm	Festlegungen für Einbruch- und Überfallmeldeanlagen
3	DIN EN 50131	Normenreihe	Alarmanlagen - Einbruch- und Überfallmeldeanlagen
4	VdS 2311*)	Richtlinie	Einbruchmeldeanlagen, Planung und Einbau
5	VdS 2347*)	Richtlinie	Integrierte Gefahrenmeldeanlagen - Anforderungen



Was nun? Was tun!
Einbruchmeldetechnik von TELENOT



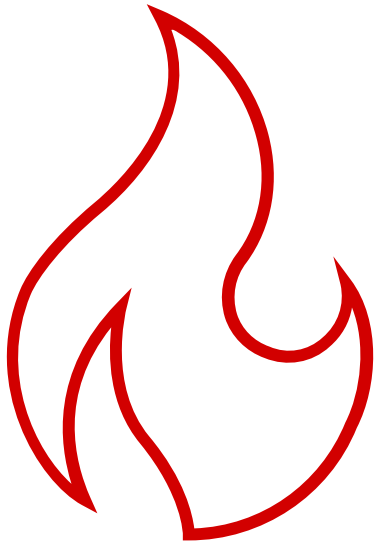
Was nun? Was tun!
Einbruchmeldetechnik von TELENOT



Was nun? Was tun!

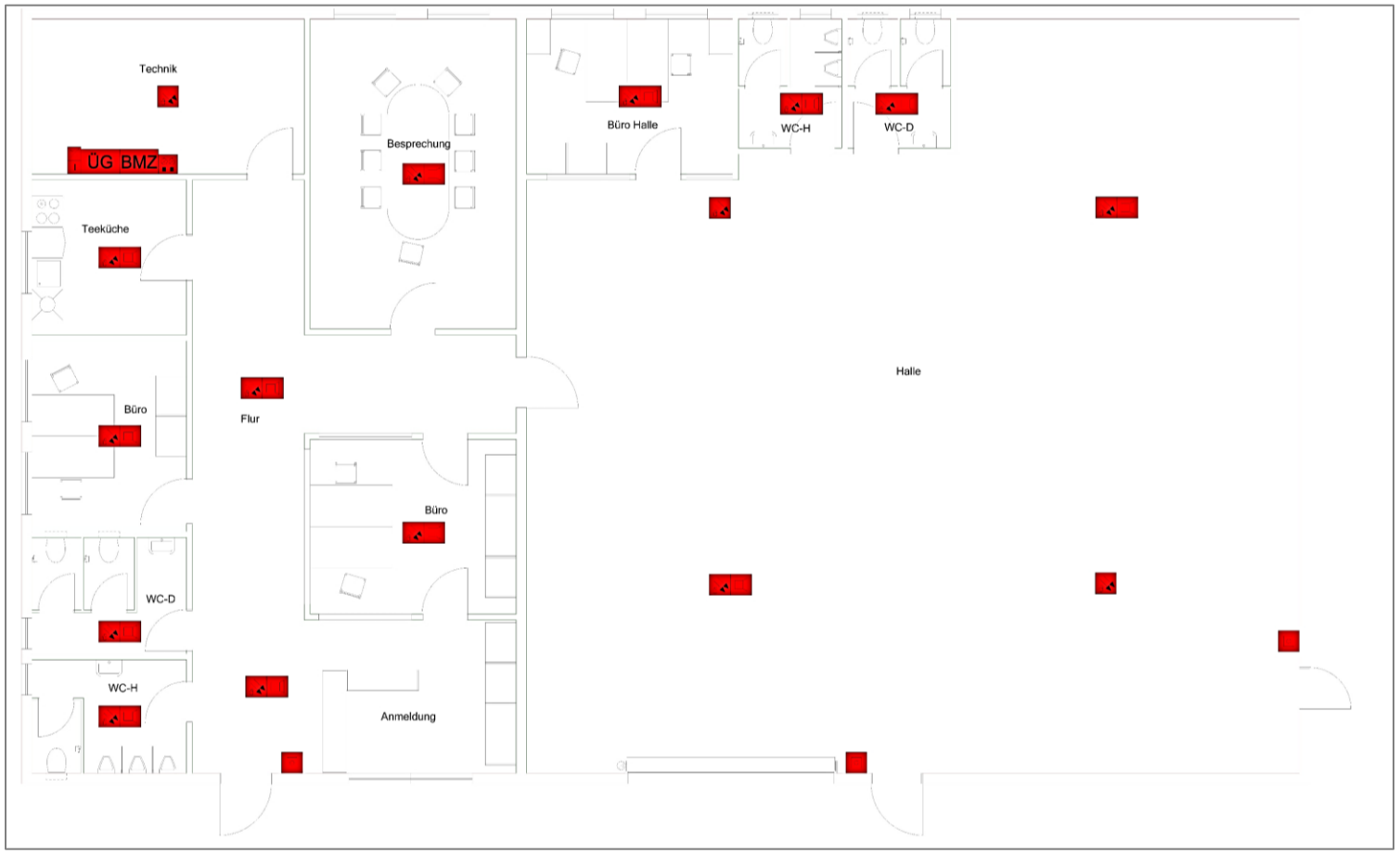
Brandmeldeanlagen

- Schutz von Gebäuden, Anlagen und Geräten vor Schäden durch Brand sowie Schutz von Personen
- Einsatz von Brandmeldern, Handfeuermeldern, Rauchansaugsysteme,...

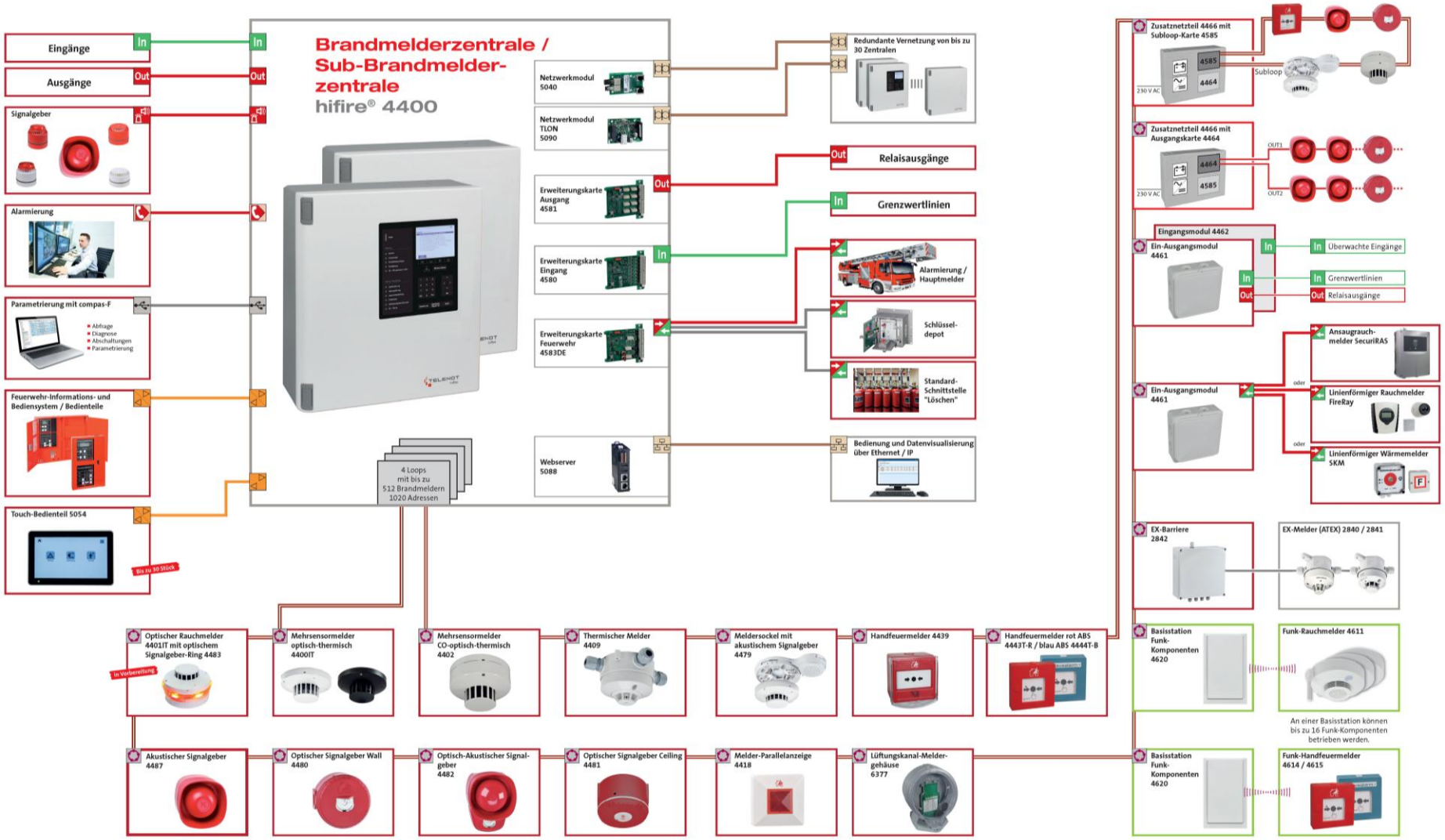


	Dokument	Typ	Titel
1	DIN VDE 0833-1	Norm	Gefahrenmeldeanlagen für Brand, Einbruch und Überfall - Teil 1: Allgemeine Festlegungen
2	DIN VDE 0833-2	Norm	Festlegungen für Brandmeldeanlagen
3	DIN 14675	Norm	Brandmeldeanlagen
4	VdS 2095	Richtlinie	Automatische Brandmeldeanlagen, Planung und Einbau

Was nun? Was tun!
Brandmeldetechnik von TELENOT



Was nun? Was tun!
Brandmeldetechnik von TELENOT

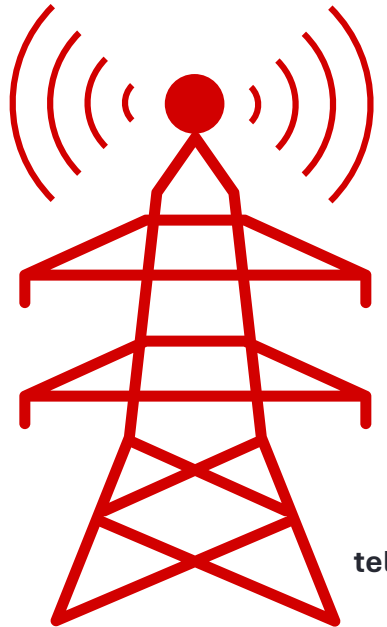


Was nun? Was tun!

Übertragungseinrichtungen

- Sichere Übertragung von Alarmen und Störungen zu hilfeleistenden Stellen

	Dokument	Typ	Titel
1	DIN EN 50136-1	Norm	Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen - Teil 1: Allgemeine Anforderungen an Alarmübertragungsanlagen
2	DIN EN 50136-2	Norm	Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen - Teil 2: Anforderungen an Übertragungseinrichtungen (ÜE)
3	DIN EN 50136-3	Norm	Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen - Teil 3: Anforderungen an Übertragungszentralen (ÜZ)
4	DIN EN 54-21	Norm	Brandmeldeanlagen - Teil 21: Übertragungseinrichtungen für Brand- und Störungsmeldungen
5	DIN EN 50131-1	Norm	Alarmanlagen – Einbruch- und Überfallmeldeanlagen - Teil 1: Systemanforderungen
6	DIN VDE 0833-1	Norm	Gefahrenmeldeanlagen für Brand, Einbruch und Überfall - Teil 1: Allgemeine Festlegungen
7	VdS 2465-1	Richtlinie	Übertragungsprotokoll für Gefahrenmeldungen
8	VdS 2465-2	Richtlinie	Übertragungsprotokoll für Gefahrenmeldungen mittels TCP/IP - Übertragungsprozedur und Protokollprozedur
9	VdS 2465-3	Richtlinie	Übertragungsprotokoll für Gefahrenmeldungen mittels TCP/IP - Allgemeiner Satzaufbau und Satztypenbeschreibungen
10	VdS 2311	Richtlinie	Einbruchmeldeanlagen, Planung und Einbau
11	VdS 3836	Richtlinie	Cyber-Sicherheit für vernetzte Produkte



Es gilt immer: Stand der Technik

Resilienz-Maßnahmen sind basierend auf den staatlichen und eigenen Risikoanalysen und -bewertungen unter Einhaltung des „Standes der Technik“ umzusetzen! Also mit Produkten, die gemäß vorgenannten Normen und Richtlinien zertifiziert, die Sicherheitslösung geplant, eingebaut und gewartet wird



Fazit

Rundum in den besten Händen bei TELENOT



Physischer (elektronischer) Schutz mit TELENOT und Partnern

Hier können TELENOT und seine Partner unterstützen – für **Gebäude, Räumlichkeiten und Personen**

Physischer Schutz

- Detektionsgeräte wie Alarmanlagen und deren Bewegungsmelder, Glasbruchmelder, …
- Zugangskontrolltechnik / Zutrittskontrolltechnik
- Zudem Brandmeldetechnik sowie rechtzeitige Alarmierung

Wiederherstellung

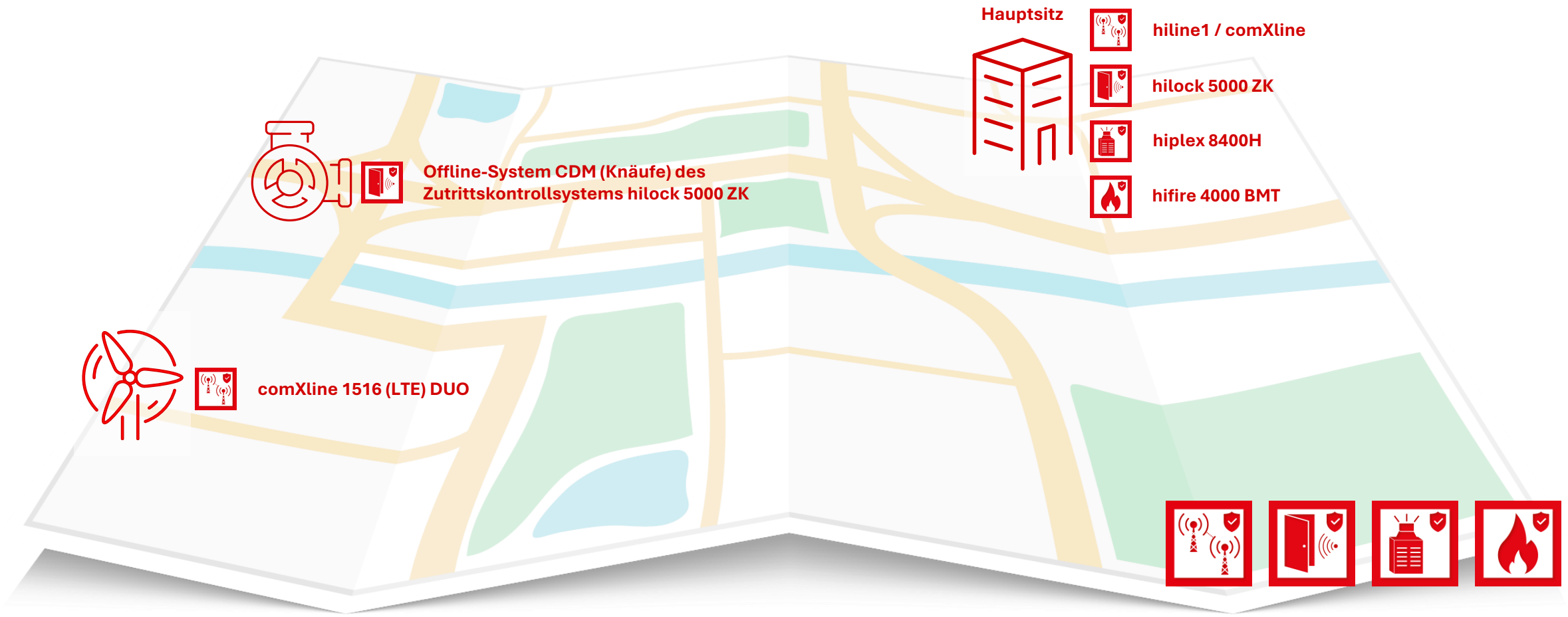
- Notstromversorgung durch Akkus in unseren Systemen
- Rechtzeitige Alarmierung beschleunigt die Wiederherstellung (BCM – Business Continuity Management)

Personalsicherheit

- Durch definierte Zugangsrechte und Transponder / Leser mittels moderner, skalierbarer Systeme und rechtzeitiger Alarmierung des Personals sowie Überfallmeldern

Anwendungsbeispiele unseres Leistungsspektrums

Umfangreiche Absicherung durch Einbruch-, Brand-, Übertragungs- und Zutrittskontrolltechnik – alles aus einer Hand!



© stas111 & CS21NNN, Adobe Stock



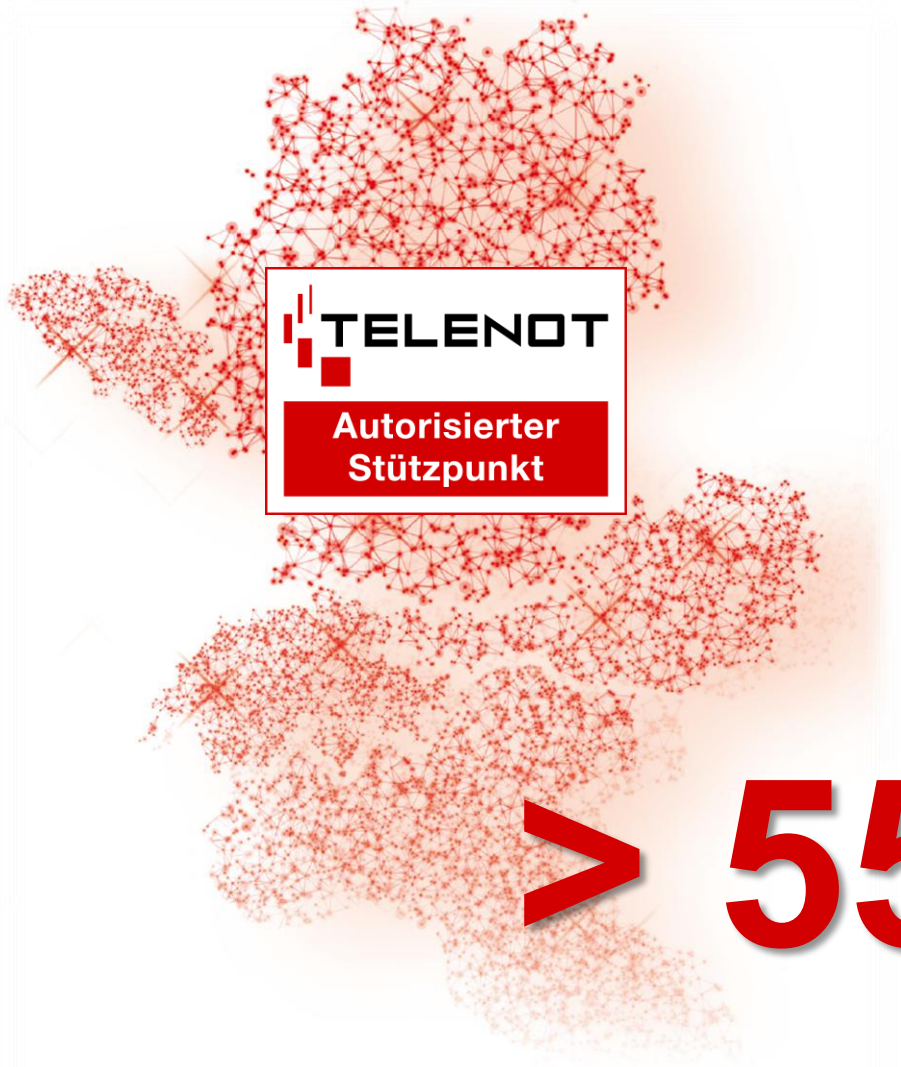
Der TELENOT Planungsservice

WIR PLANEN IHRE PHYSISCHE SICHERHEITSLÖSUNG!

Ihre Vorteile:

- Planungssicherheit
- Flexibilität
- Maximale, normgerechte Professionalität
- Gesteigerte Produktivität
- Kostensenkung

Bestes Netzwerk
für Sicherheit mit Brief und Siegel



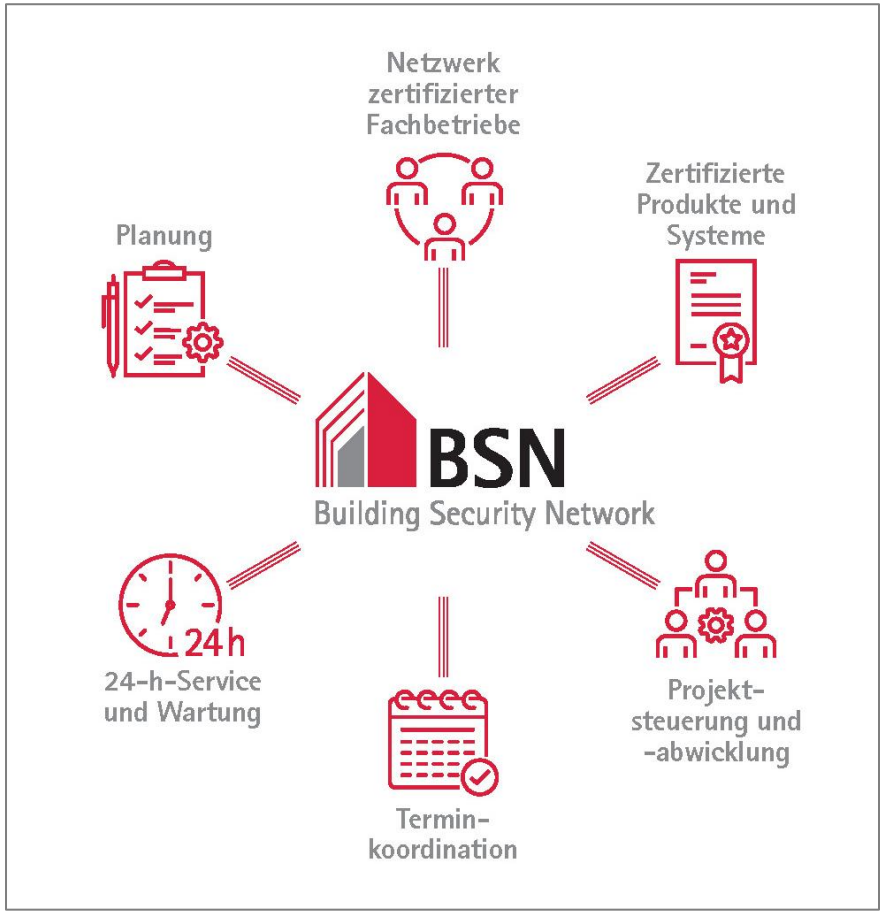
- Offiziell zertifizierte Fachbetriebe
- In Deutschland, Österreich, der Schweiz und Luxemburg – sowie weiteren europäischen Ländern
- Sicherstellung von Planung, Montage, Inbetriebnahme bis hin zu 24h-Service
- Herausragende Sicherheitslösungen und Topservice – auch in Ihrer Nähe!

> 550 AUTORISIERTE TELENOT-STÜTZPUNKTE

BSN – der Generalunternehmer für Ihre physische Sicherheit

- Fundament des Geschäftsmodells: Die BSN verfügt mit Ihren mehr als 550 Autorisierten TELENOT-Stützpunkten über das leistungsfähigste Netzwerk zertifizierter Fachbetriebe für Sicherheit mit Brief und Siegel in Europa

- National und international agierende Handelskonzerne, Unternehmen, Verbände und Organisationen





Fazit

Deshalb unser Angebot an Sie
– egal was auf Sie zukommt:

Mit uns sind Sie in Bezug auf die physische Sicherheit bestens gerüstet!