ABUS SECURITY CENTER

DIE RELEVANZ VON ZUTRITTSKONTROLLLÖSUNGEN IM HINBLICK AUF DIE ERFÜLLUNG REGULATORISCHER VORGABEN AUS NIS-2 UND KRITIS

Überarbeitete Version 2.0 | Stand Februar 2026

ABUS I Security Center GmbH & Co. KG | Linker Kreuthweg 5, 86444 Affing | Germany | Tel: +49 8207 959 90-0 | sales@abus-sc.com | abus.com

INHALT

1. Einleitung

Um den Schutz der kritischen Infrastruktur in Deutschland zu erhöhen und deren Resilienz zu steigern, existieren unterschiedliche Regelwerke, die parallel gelten und sich gegenseitig ergänzen.

Die **KRITIS-Regularien** werden **im Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITISDachG)** geregelt. Das Gesetz wurde am 29.01.2026 mit Zustimmung des Bundesrats durch den Bundestag beschlossen.

Mit der Verabschiedung des KRITIS-Dachgesetzes hat der Bundestag erstmals einen bundeseinheitlichen, sektorübergreifenden Rechtsrahmen zum Schutz kritischer Infrastrukturen geschaffen. Ziel ist es, die Resilienz zentraler Versorgungsstrukturen gegenüber physischen, organisatorischen, hybriden und natürlichen Gefahren zu stärken.

Mit dem Gesetz wird die EU-Richtlinie 2022/2557 über die Resilienz kritischer Einrichtungen, die sogenannte CER-Richtlinie, in deutsches Recht umgesetzt. Der Fokus des Gesetzes liegt auf dem physischen Schutz kritischer Infrastrukturen und der Ergänzung bestehender IT- und Cyber-Sicherheitsregelungen. Grundlage ist ein All-Gefahren-Ansatz, der sowohl Cyber-Angriffe als auch physische, natürliche und technische Risiken umfasst.

Die europaweit geltende NIS-2-Richtlinie greift deutlich weiter. Zum einen betrifft die Richtlinie nicht nur die Betreiber der kritischen Infrastruktur, sondern auch „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ zu denen Unternehmen gehören, die in bestimmten Sektoren tätig sind und dabei definierte Schwellenwerte im Hinblick auf Mitarbeiteranzahl sowie Umsatz- und Bilanzsumme überschreiten. Neben strengeren Anforderungen zu physischen und technischen Schutzmaßnahmen fordert NIS-2 darüber hinaus ein systematisches Cyber-Risikomanagement und konkretisiert Anforderungen zur Abwehr von Risiken, die sich aus dem Unternehmensumfeld, wie z. B. Lieferketten, ergeben können.

Die Umsetzung der EU-weit gültigen NIS-2-Richtlinie in und für Deutschland obliegt dem Bundesamt für Sicherheit in der Informationstechnik (nachfolgend als BSI bezeichnet) und erfolgte insbesondere durch eine Novellierung des BSI-Gesetzes in Form des Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (nachfolgend als NIS-2-Umsetzungsgesetz bezeichnet).

Mit der Verabschiedung des NIS-2-Umsetzungsgesetzes am 05.12.2025 und des KRITIS-Dachgesetzes am 29.01.2026 durch den Bundestag traten ab diesem Zeitpunkt umfangreiche Anforderungen an die Cyber-Sicherheit der Bundesverwaltung sowie bestimmter Unternehmen in Kraft.

Vor Inkrafttreten der neuen Gesetzesvorgaben waren ca. 4.500 Einrichtungen und Unternehmen durch das BSI-Gesetz reguliert. Zu diesen zählten insbesondere Betreiber kritischer Infrastrukturen (nachfolgend als KRITIS bezeichnet), Anbieter digitaler Dienste und Unternehmen von besonderem öffentlichen Interesse, welche jetzt über das KRITIS-Dachgesetz geregelt werden.

Das NIS-2-Umsetzungsgesetz erweitert den Geltungsbereich um Unternehmen, die in bestimmten Sektoren tätig sind und dabei festgelegte Schwellenwerte überschreiten. Insgesamt ca. 29.500 Einrichtungen und Unternehmen stehen damit ab sofort unter der Aufsicht des BSI.

Unternehmen müssen selbstständig prüfen, ob sie unter die NIS-2-Richtlinie fallen und sich – falls sie betroffen sind – eigenständig beim BSI registrieren.

Dazu bietet das BSI online die Möglichkeit einer NIS-2-Betroffenheitsprüfung sowie einen digitalen Dienst mit einem zweistufigen Registrierungsprozess für betroffene Unternehmen.

1.1 Differenzierung KRITIS und NIS-2

Der Begriff KRITIS steht für „kritische Infrastrukturen" und wird vom BSI wie folgt definiert:

„Kritische Infrastrukturen (KRITIS) sind Organisationen und 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." (Quelle: BSI)

Das KRITIS-Dachgesetz definiert den Geltungsbereich für KRITIS in Deutschland.

Für Sicherheitsverantwortliche und die Sicherheitswirtschaft steigen damit die Anforderungen an integrierte Sicherheits-, Risiko- und Resilienzkonzepte.

Betreiber kritischer Infrastrukturen werden verpflichtet, Risikoanalysen durchzuführen, Resilienzmaßnahmen umzusetzen, Vorfälle zu melden und sich beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zu registrieren. Ergänzend sind nationale Risikoanalysen vorgesehen. Das Gesetz fokussiert insbesondere den physischen Schutz und ergänzt bestehende IT- und Cyber-Sicherheitsregelungen (z. B. NIS-2). Es folgt einem All-Gefahren-Ansatz, der auch Sabotage, Terror, Naturereignisse und technisches Versagen einbezieht.

NIS ist eine EU-weite Richtlinie zur Netzwerk- und Informationssicherheit. Sie hat zum Ziel, die Cyber-Sicherheit in Europa zu stärken, die Zusammenarbeit in der EU diesbezüglich zu vereinheitlichen und klare Meldepflichten bei Sicherheitsvorfällen einzuführen. Die ursprüngliche NIS-1-Verordnung stammt von 2016, die aktuell geltende NIS-2-Richtlinie wurde am 27.12.2022 im Amtsblatt L333 der Europäischen Union veröffentlicht.

Am 05.12.2025 wurde im Bundesgesetzblatt Jahrgang 2025 Teil I Nr. 301 das NIS-2-Umsetzungsgesetz veröffentlicht.

Somit ist die Umsetzung in deutsches Recht erfolgt und wird wie in anderen Staaten innerhalb der EU angewendet. Da es nach der Verabschiedung des nationalen Gesetzes keine Übergangszeit gibt, sind alle Rechte und Pflichten sofort gültig.

Welche Sektoren und damit Organisationen und Einrichtungen unter KRITIS oder NIS-2 fallen, werden in den folgenden Unterkapiteln unter 2.1 und 2.2. beschrieben. Die Sektoren können sich überschneiden und somit gleichzeitig unter NIS-2 und KRITIS fallen.

Mit dem Inkrafttreten des NIS-2-Umsetzungsgesetzes und des KRITIS-Dachgesetzes sind die Anforderungen an die physische und digitale Sicherheit in Unternehmen – insbesondere in jenen Unternehmen, die zum Bereich der kritischen Infrastrukturen gehören – umfassend geregelt.

Das Thema Zutrittskontrolle ist ein wesentliches Element, das die von den Regulierungen betroffenen Unternehmen benötigen, um die Anforderungen aus NIS-2 und KRITIS zu erfüllen.

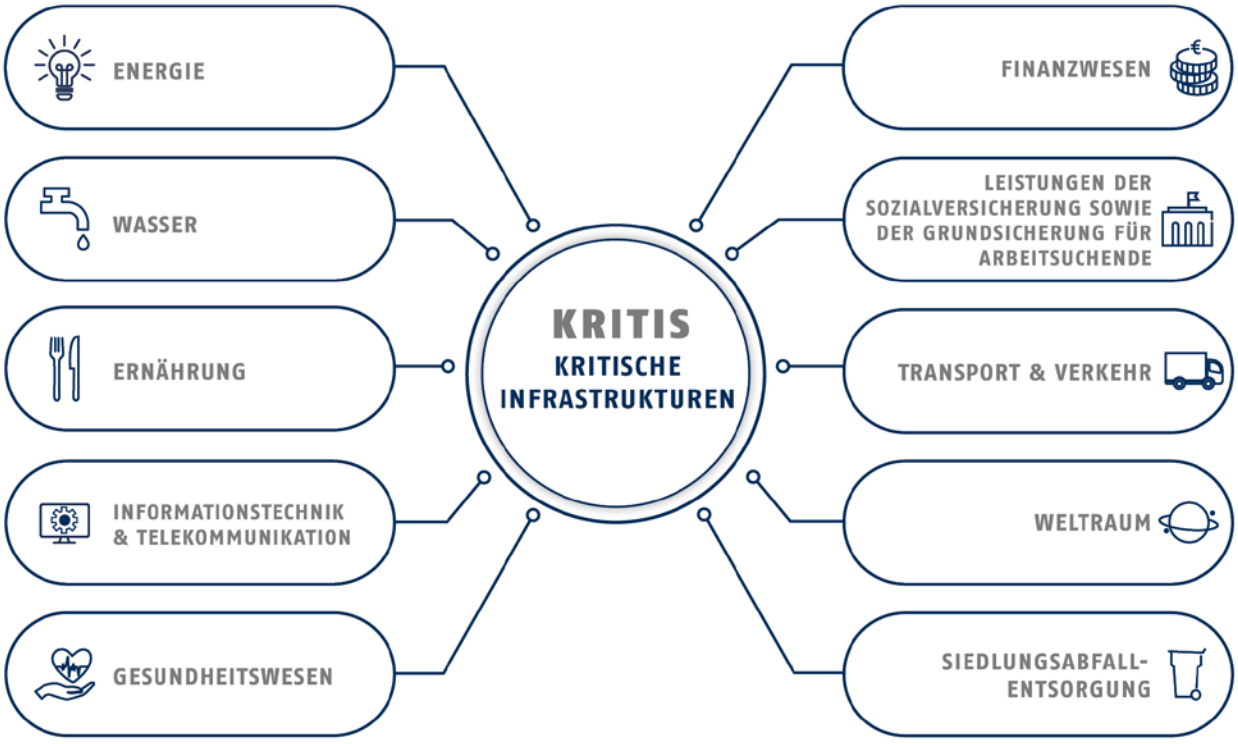
Dieses Whitepaper zeigt, wie mechanische, elektronische und hybride ABUS Zutrittslösungen Unternehmen effektiv dabei unterstützen können, regulatorische Vorgaben umzusetzen, Risiken zu minimieren und Resilienz zu stärken.

2. Regulatorischer Rahmen: KRITIS & NIS-2 im Überblick

2.1 KRITIS-Dachgesetz | Nationale Ausgestaltung Deutschland

Als **Betreiber kritischer Anlagen** gelten gemäß § 2 KRITIS-Dachgesetz natürliche oder juristische Personen beziehungsweise organisatorische Einheiten, die maßgeblichen Einfluss auf **kritische Anlagen** ausüben. Kritische Anlagen sind solche, die wesentlich für die Erbringung kritischer Dienstleistungen sind. **Kritische Dienstleistungen** wiederum sind grundlegende Versorgungsleistungen für die Allgemeinheit in **zentralen Sektoren (KRITIS-Sektoren).**

§ 4 Absatz 1 KRITIS-Dachgesetz definiert insgesamt zehn KRITIS-Sektoren. Diese **KRITIS-Sektoren** sind:



Das KRITIS-Dachgesetz konkretisiert auf Basis von Schwellenwerten, was kritische Anlagen und Betreiber kritischer Anlagen sind. Der Regelwert für Schwellenwerte nach § 5 Absatz 2 Satz 6 beträgt grundsätzlich 500.000 von einer Anlage zu versorgende Einwohner.

Pflichten für betroffene Organisationen und Einrichtungen gemäß KRITIS-Dachgesetz
Betreiber kritischer Anlagen sind verpflichtet:

- zur **Registrierung beim BBK bzw. BSI** (gemäß § 8 Absatz 1)

- **Risikoanalysen und Risikobewertungen durchzuführen** – mindestens alle 4 Jahre sowie im Bedarfsfall (gemäß § 12 Absatz 1)

- folgende **verpflichtende Maßnahmen** durchzuführen (gemäß § 13 Absatz 1):
  - o das Auftreten von Vorfällen zu verhindern
  - o einen angemessenen physischen Schutz von Liegenschaften und kritischen Anlagen zu gewährleisten
  - o auf Vorfälle zu reagieren, sie abzuwehren und die negativen Auswirkungen solcher Vorfälle zu begrenzen
  - o nach Vorfällen die zügige Wiederherstellung der kritischen Dienstleistung zu gewährleisten

Um die Ziele aus den verpflichtenden Maßnahmen zu erreichen, sollten gemäß § 13 folgende Maßnahmen unternommen werden:

- Maßnahmen der Notfallversorgung
- Maßnahmen der baulichen und technischen Sicherung und des organisatorischen Schutzes (Objektschutz)
- Instrumente und Verfahren für die Überwachung der Umgebung
- der Einsatz von Detektionsgeräten und
- Zugangskontrollen
- Maßnahmen zur Aufrechterhaltung des Betriebs (z. B. Notstromversorgung)
- Ermittlung alternativer Lieferketten
- Angemessenes Sicherheitsmanagement hinsichtlich Mitarbeiter und Dienstleister
- Schulung des Personals hinsichtlich der durchzuführenden Maßnahmen
- Erstellung eines Resilienzplans

2.2 NIS-2-Richtlinie | Cybersecurity auf EU-Ebene

Die **NIS-2-Richtlinie** (EU 2022/2555) ist die überarbeitete Fassung der ursprünglichen NIS-Richtlinie (2016). Sie zielt darauf ab, die Cyber-Resilienz von Unternehmen und Organisationen in der gesamten EU zu verbessern – insbesondere in Sektoren, die als kritisch für das öffentliche Leben gelten.

Die Umsetzung der EU-weiten NIS-2-Richtline für und in Deutschland wird durch das NIS-2-Umsetzungsgesetz geregelt. Das Gesetz wurde am 05.12.2025 im Bundesgesetzblatt Teil 1 Nr. 301 Jahrgang 2025 veröffentlicht.

Definition relevanter Sektoren unter der NIS-2-Richtlinie und dem NIS-2-Umsetzungsgesetz:

Bei den unter NIS-2 relevanten Sektoren in Deutschland wird gemäß § 28 und § 29 des NIS-2-Umsetzungsgesetzes unterschieden zwischen „Sektoren besonders wichtiger Einrichtungen", „Sektoren wichtiger Einrichtungen" und „Einrichtungen der Bundesverwaltung" (Stand Dezember 2025):

- **Sektoren besonders wichtiger Einrichtungen**
  - **Energie**
    - Stromversorgung, Fernwärme- oder Fernkälteversorgung, Kraftstoff- oder Heizölversorgung, Gasversorgung
  - **Transport und Verkehr**
    - Luft- und Schienenverkehr, Schifffahrt und Straßenverkehr
  - **Finanzwesen**
    - Bankwesen, Finanzmarktinfrastrukturen
  - **Gesundheitswesen**
  - **Wasser**
    - Trinkwasserversorgung, Abwasserbeseitigung
  - **Digitale Infrastruktur**
  - **Weltraum**

- **Sektoren wichtiger Einrichtungen**
  - **Transport & Verkehr**
    - Post- und Kurierdienste
  - **Abfallbewirtschaftung**
  - **Produktion, Herstellung und Handel mit chemischen Stoffen**
  - **Produktion, Verarbeitung und Vertrieb von Lebensmitteln**
  - **Verarbeitendes Gewerbe/Herstellung von Waren**
    - Herstellung von Medizinprodukten und In-vitro-Diagnostika, Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen, Herstellung von elektrischen Ausrüstungen, Maschinenbau, Herstellung von Kraftwagen und Kraftwagenteilen, sonstiger Fahrzeugbau
  - **Anbieter digitaler Dienste**
  - **Forschung**

- **Einrichtungen der Bundesverwaltung***
  - **Bundesbehörden**
  - **öffentlich-rechtlich organisierte IT-Dienstleister** der Bundesverwaltung
  - **weitere Körperschaften**, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen

* mit Ausnahme der Institutionen der Sozialen Sicherung und der Deutschen Bundesbank sowie die in § 29 Absatz 3 aufgeführten Bundeseinrichtungen

Zur Ermittlung, ob ein Unternehmen von den Regulierungen nach dem NIS-2-Umsetzungsgesetz betroffen ist, bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf seiner Webseite die Möglichkeit zur Durchführung einer NIS-2-Betroffenheitsprüfung.

Mit dem NIS-2-Umsetzungsgesetz wurde die Definition und die Zahl der Sektoren um mittelgroße Unternehmen und Großunternehmen als „Einrichtung" erweitert. Zudem wurden die Sektoren durch das NIS-2-Umsetzungsgesetz in zwei Gruppen klassifiziert: Die „besonders wichtigen Einrichtungen" und die „wichtigen Einrichtungen".

Gemäß § 28 des **NIS-2-Umsetzungsgesetzes** gelten folgende Einrichtungen als besonders wichtig oder wichtig:

Klassifizierung	Einrichtung	Anzahl Mitarbeiter	a) Jahresumsatz b) Jahresbilanzsumme
Besonders wichtige Einrichtungen	Bertreiber kritischer Anlagen	unabhängig	unabhängig
	qualifizierte Vertrauensdienste-anbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter	unabhängig	unabhängig
	Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze	≥ 50 ODER	a) > 10 Mio. EUR UND b) > 10 Mio. EUR
	Unternehmen	≥ 250 ODER	a) > 50 Mio. EUR UND b) > 43 Mio. EUR
Wichtige Einrichtungen	Vertrauensdiensteanbieter	unabhängig	unabhängig
	Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze	< 50 UND	a) ≤ 10 Mio. EUR ODER b) ≤ 10 Mio. EUR
	Unternehmen	≥ 50 ODER	a) > 10 Mio. EUR UND b) > 10 Mio. EUR

§ 30 Absatz 2 des NIS-2-Umsetzungsgesetzes definiert insgesamt zehn Risikomanagement-Maßnahmen im Bereich der Cyber-Sicherheit, die betroffene Unternehmen mindestens ergreifen müssen, um die Auswirkung von Sicherheitsvorfällen möglichst gering zu halten. Diese sind:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik

2. Bewältigung von Sicherheitsvorfällen

3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall und Krisenmanagement

4. Sicherheit in der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern

5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen

6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagement-Maßnahmen im Bereich der Sicherheit der Informationstechnik

7. Grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik

8. Konzepte und Verfahren für den Einsatz von kryptografischen Verfahren

9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen

10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Darüber hinaus konkretisiert insbesondere § 31 des NIS-2-Umsetzungsgesetzes die besonderen Anforderungen an die Risikomanagement-Maßnahmen sogenannter „Betreiber kritischer Infrastrukturen" für Deutschland. § 32 definiert die Meldepflichten für „besonders wichtige Einrichtungen" und „wichtige Einrichtungen" bei Auftreten von Sicherheitsvorfällen.

2.3 Die Relevanz von Zutrittskontrolllösungen im Kontext der NIS-2-Richtlinien und des KRITIS-Dachgesetzes

Ein zentraler Aspekt aus dem NIS-2-Umsetzungsgesetz und dem KRITIS-Dachgesetz liegt in der effektiven Steuerung und Kontrolle physischer Zutritte zu sicherheitskritischen Bereichen.

Dazu zählt in erster Linie das systematische Zutrittsmanagement für Betriebsgebäude, technische Anlagen und insbesondere IT-Infrastrukturen wie Serverräume oder Leitstände. Eine klare Trennung von Zugriffsrechten, revisionssicherer Protokollierung und Schutz vor Manipulation sind genauso essenziell wie die Identifikation und Authentifikation der jeweiligen Person vor dem Zutritt. Nur autorisierte Personen dürfen Zutritt zu diesen sensiblen Bereichen erhalten – und dies ausschließlich auf Grundlage klar definierter Rollen und Verantwortlichkeiten.

Konkret bezogen auf die im KRITIS-Dachgesetz und NIS-2-Umsetzungsgesetz genannten Anforderungen für Organisationen und Einrichtungen bedeutet dies:

2.3.1 Unterstützung zur Erfüllung von Anforderungen im Kontext des KRITIS-Dachgesetzes durch den Einsatz geeigneter Zutrittskontrolllösungen

Gemäß den Anforderungen des KRITIS-Dachgesetzes § 16 Absatz 1 (mit Verweis auf das NIS-2-Umsetzungsgesetz § 39 Absatz 1) müssen Betreiber kritischer Infrastrukturen spätestens alle drei Jahre angemessene organisatorische und technische Schutzmaßnahmen nachweisen. Dieser Nachweis ist gegenüber dem BSI zu erbringen und umfasst unter anderem Sicherheitskonzepte, Pläne der Zutrittszonen, Prüfprotokolle sowie Regelungen zur Besucherverwaltung.

Die physische Sicherheit stellt dabei einen wesentlichen Bestandteil des Gesamtschutzes dar. Betreiber sind verpflichtet, technische und organisatorische Maßnahmen zu ergreifen, um die physische Sicherheit ihrer Systeme zu gewährleisten. Zutrittskontrollsysteme gelten hierbei als zentrale Maßnahme. Diese beinhalten insbesondere den kontrollierten Zugang zu kritischen Bereichen ausschließlich durch autorisierte Personen, den Einsatz von Identifikations- und Authentifizierungsmethoden, die lückenlose Protokollierung aller Zutritte sowie die Vermeidung unkontrollierter Zugänge.

Darüber hinaus sollten Zutrittskontrollsysteme integraler Bestandteil eines ganzheitlichen Resilienzansatzes sein, das auf Grundlage des § 13 KRITIS-Dachgesetzes umgesetzt wird. In diesem Zusammenhang sind Prozesse wie die Vergabe von Zutrittsrechten, die regelmäßige Überprüfung und Freigabe von Zugängen sowie eine umfassende Dokumentation und Durchführung von Audits erforderlich.

2.3.2 Unterstützung zur Erfüllung von Anforderungen im Kontext der NIS-2-Richtlinien durch den Einsatz geeigneter Zutrittskontrolllösungen

§ 30 Absatz 1 des NIS-2-Umsetzungsgesetzes schreibt vor: „Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die in Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten."

§ 30 Absatz 2 konkretisiert: „Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen."

Hierbei sind Zutrittskontrolllösungen ein wesentlicher Bestandteil. Sie tragen zur Einhaltung der Anforderungen an physische Sicherheit, Zutrittskontrolle, Protokollierung, Kryptographie, Reaktionsfähigkeit und Risikomanagement bei.

3. Exkurs Sicherheitsstandards: BSI IT-Grundschutz und ISO/IEC 27001

Im Hinblick auf die Anforderungen aus dem NIS-2-Umsetzungsgesetz und dem KRITIS-Dachgesetz existieren Stand heute keine definierten Standards, die Betreiber betroffener Institutionen umsetzen könnten, um die Erfüllung der NIS-2- und KRITIS-Regularien sicherzustellen.

Einige nationale Regelwerke und international anerkannte Best-Practice-Standards bieten jedoch Leitplanken, die die Umsetzung und den Nachweis erleichtern können. Dazu gehören im Bereich Informationssicherheit der BSI IT-Grundschutz sowie die ISO/IEC 27001, die hier exemplarisch und mit Blick auf das Thema Zutrittskontrolle betrachtet werden.

3.1 BSI IT-Grundschutz | Maßnahmenempfehlungen für kritische Infrastrukturen

Der **BSI IT-Grundschutz** ist ein vom BSI entwickelter und frei verfügbarer ganzheitlicher Ansatz zur Informationssicherheit. Er ermöglicht kleinen Institutionen einen schnellen Einstieg und die Umsetzung grundlegender Sicherheitsanforderungen und bietet größeren Institutionen eine Basis zum Aufbau eines vollwertigen Informationssicherheit-Managementsystems (nachfolgend als ISMS bezeichnet). Dazu liefert der **BSI IT-Grundschutz** Anleitungen, Empfehlungen und Hilfestellungen in Form von Leitlinien und Checklisten.

Die Grundlage bilden die BSI-Standards. Sie erläutern, wie ein ISMS organisatorisch und systematisch aufgebaut werden kann. Ergänzend dazu liefert das IT-Grundschutz-Kompendium neben den IT-Grundschutz-Bausteinen auch Umsetzungshinweise zur Erreichung eines angemessenen Sicherheitsniveaus.

Zum Thema Zutrittskontrolle findet sich in den BSI IT-Grundschutz-Bausteinen unter anderem folgende relevante Abschnitte:

- **ORP.4 – Identitäts- und Berechtigungsmanagement:** Organisation und Dokumentation von Zutrittsrechten, physische Zutrittskontrolle, Besuchermanagement

- **INF.1 – Allgemeines Gebäude:** Einsatz von elektronischen Zutrittskontrollsystemen, regelmäßige Überprüfung und Anpassung von Zutrittsrechten, Protokollierung und Auswertung von Zutritten

- **INF.2 – Rechenzentrum sowie Serverraum:** mechanische Absicherung, Alarmierung bei Zutrittsversuchen, Zugriffsbeschränkung nach Rollen

- **INF.7 – Büroarbeitsplatz:** differenzierte Zutrittskontrolle auch für Bürobereiche mit sensiblen Daten

Daneben gelten auch die allgemeinen Anforderungen aus dem IT-Grundschutz:
- Einsatz von elektronischen Schließsystemen
- Alarmierung bei unbefugtem Zutritt
- regelmäßige Prüfung von Schließberechtigungen
- Nachvollziehbarkeit aller Zutritte über Protokolle

3.2 ISO/IEC 27001 | Zutrittskontrolle als Teil des ISMS

Die ISO/IEC 27001 ist der international führende Standard für ein ISMS.

Die Norm bietet einen strukturierten Rahmen für die Implementierung und den Betrieb eines wirksamen ISMS mit dem Ziel, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durch systematische Risikobetrachtung und -behandlung zu schützen.

Der PDCA-Zyklus (Plan-Do-Check-Act), auch bekannt als Deming-Kreis, ist ein zentrales Element der ISO/IEC 27001 und bildet das Fundament für den Aufbau, die Umsetzung und die kontinuierliche Verbesserung eines ISMS. Dieser iterative Prozess stellt sicher, dass Informationssicherheit systematisch und nachhaltig in einer Organisation verankert wird.

Relevante Maßnahmen zum Thema Zutrittskontrolle innerhalb der ISO/IEC 27001 finden sich in Anhang A der Norm (2024):

- **(A) 7.1 – Physische Sicherheitsperimeter:** Verhinderung des unbefugten physischen Zugriffs, der Beschädigung und des Eingriffs in die Informationen und anderen damit verbundenen Werte der Organisation.

- **(A) 7.2 – Physischer Zutritt:** Sicherstellung, dass nur autorisierter physischer Zugang zu den Informationen und anderen damit verbundenen Werten der Organisation erfolgt.

- **(A) 7.3 – Sichern von Büros, Räumen und Einrichtungen:** Verhinderung des unbefugten physischen Zugriffs, der Beschädigung und des Eingriffs in die Informationen und anderen damit verbundenen Werten der Organisation in Büros, Räumen und Einrichtungen.

- **(A) 7.4 – Physische Sicherheitsüberwachung:** Die Räumlichkeiten sollten ständig auf unbefugten physischen Zugang überwacht werden.

- **(A) 8.3 – Informationszugangsbeschränkung:** Der Zugang zu Informationen und anderen damit verbundenen Werten sollte in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.

- **(A) 8.15 – Protokollierung:** Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, sollten erstellt, gespeichert, geschützt und analysiert werden. Aufzeichnung von Ereignissen, Generierung von Beweisen, Sicherstellung der Integrität von Protokolldaten, Schutz vor unbefugtem Zugriff, Identifizierung von Informationssicherheitsereignissen, die zu einem Informationssicherheitsvorfall führen können, und Unterstützung von Untersuchungen.

Die Norm verlangt explizit, dass Zutrittsregelungen dokumentiert, überwacht und regelmäßig überprüft werden müssen.

4. Fazit zum regulatorischen Rahmen

Die Kombination aus **gesetzlichen Pflichten** (NIS-2-Umsetzungsgesetz, KRITIS-Dachgesetz) und **Best Practices** aus Normen wie **ISO/IEC 27001** und dem **BSI IT-Grundschutz** macht deutlich: Zutrittskontrolle ist keine optionale Maßnahme, sondern ein zentrales Element ganzheitlicher Sicherheitsarchitekturen.

5. Die Antwort von ABUS: ganzheitliche Zutrittskontrolllösungen

ABUS bietet Unternehmen ein umfangreiches Portfolio an Zutrittskontrolllösungen, die sich modular, skalierbar und sicher in bestehende Sicherheitskonzepte integrieren lassen.

Damit unterstützen ABUS Lösungen nicht nur die physische Sicherung sensibler Bereiche, sondern auch die dokumentierte Zugriffskontrolle im Sinne des NIS-2-Umsetzungsgesetzes, KRITIS-Dachgesetz, ISO/IEC 27001 und BSI-Grundschutz.

Die Erfüllung der Anforderungen aus KRITIS-Dachgesetz und NIS-2-Umsetzungsgesetz ist grundsätzlich mit mechanischen Schließsystemen möglich, erfordern jedoch einen erhöhten Aufwand insbesondere, wenn es um Ereignisprotokollierung oder dynamische Rechteverwaltung geht – wesentliche Anforderungen, die in beiden Regelwerken genannt werden.

Um eine höchstmögliche Konformität mit den Anforderungen aus dem NIS-2-Umsetzungsgesetz und dem KRITIS-Dachgesetz zu erreichen, ist es empfehlenswert, auf elektronische Lösungen zu setzen. Eine Alternative besteht darin, bestehende mechanische Systeme mit elektronischen Zutrittslösungen zu kombinieren. So entsteht eine hybride Sicherheitsarchitektur, die sowohl die physischen als auch die organisatorischen Anforderungen beider Regelwerke erfüllt.

5.1 Elektronische Lösungen von ABUS

Elektronische Zutrittssysteme von ABUS ermöglichen eine dynamische, zentral steuerbare und revisionssichere Verwaltung von Zutrittsrechten. Sie bieten maximale Transparenz und Kontrolle – wichtige Anforderungen aus dem NIS-2-Umsetzungsgesetz und dem KRITIS-Dachgesetz.

Kernvorteile elektronischer Zutrittskontrolllösungen:

1. **Rechteverwaltung:** Elektronische Systeme ermöglichen eine dynamische Vergabe und Änderung von Zutrittsrechten, was für die flexible Anpassung an sich ändernde Sicherheitsanforderungen essenziell ist.

2. **Ereignisprotokollierung:** Alle Zutrittsversuche werden automatisch protokolliert – sowohl erfolgreiche als auch fehlgeschlagene – und bieten so eine detaillierte Nachvollziehbarkeit, die in den Sicherheitsanforderungen von NIS-2 und KRITIS-Regularien explizit gefordert wird. Der Zugriff auf personenbezogene Daten wird dabei geschützt und die Vorhaltezeit dieser Informationen kann definiert werden. Damit werden die gesetzlichen Anforderungen zum Schutz personenbezogener Daten eingehalten.

3. **Einbindung in ein ISMS:** Durch die Möglichkeiten, die eine elektronische Zutrittslösung bietet, können die regulatorischen Anforderungen eines ISMS im Hinblick auf Zutrittssteuerung und Protokollierung erfüllt werden.

4. **Zentralisierte Verwaltung:** Durch die zentrale Verwaltung von Zutrittsrechten können Unternehmen steuern, dass sicherheitskritische Bereiche nur von autorisierten Personen betreten werden.

5. **Skalierbarkeit und Flexibilität:** Elektronische Systeme können an die spezifischen Bedürfnisse eines Unternehmens angepasst und bei Bedarf skaliert werden, ohne die Sicherheit zu beeinträchtigen.

6. **Hohe Sicherheitsstandards:** Elektronische Lösungen verfügen über eine End-to-End-Verschlüsselung.

7. **Ganzheitliches Sicherheitskonzept:** Durch die Kombination und Integration unserer elektronischen Zutrittskontrolllösungen mit unseren professionellen Videoüberwachungs- und Alarmsystemen entsteht ein ganzheitliches Sicherheitskonzept. Sicherheitsvorfälle können schneller erkannt und Reaktionszeiten darauf verkürzt werden. Videoaufzeichnungen dienen zudem der Beweissicherung und Rekonstruktion von Vorfällen. Rund-um-Sicherheit aus einer Hand.

Elektronische Zutrittskontrolllösungen bieten eine hochgradige Flexibilität und Transparenz, die für die Erfüllung der Anforderungen aus dem NIS-2-Umsetzungsgesetz und dem KRITIS-Dachgesetz notwendig sind. Sie sind besonders geeignet für den Einsatz in kritischen Infrastrukturen, da sie sowohl physische als auch digitale Sicherheitsaspekte berücksichtigen.

Für Unternehmen, die die Vorgaben aus dem NIS-2-Umsetzungsgesetz und dem KRITIS-Dachgesetz umsetzen müssen, bieten elektronische Zutrittslösungen eine zuverlässige und zukunftssichere Möglichkeit, Sicherheitsmaßnahmen effektiv zu implementieren.

5.2 Hybride Lösungen von ABUS

Hybride Zutrittskontrolllösungen von ABUS kombinieren mechanische und elektronische Komponenten und bieten – richtig geplant – eine flexible Sicherheitsarchitektur, die die Anforderungen aus dem NIS-2-Umsetzungsgesetz sowie dem KRITIS-Dachgesetz erfüllen kann.

Hybride Lösungen eignen sich insbesondere für Unternehmen, die eine schrittweise Umstellung von einer mechanischen auf eine digitale Lösung planen oder die eine Kombination aus verschiedenen Sicherheitsanforderungen umsetzen wollen.

Vorteile hybrider Zutrittskontrolllösungen:

1. **Stufenweise Integration:** Hybride Systeme ermöglichen es, bestehende mechanische Schließsysteme mit modernen elektronischen Zutrittslösungen zu kombinieren. Dies bietet Unternehmen die Möglichkeit, die Sicherheit in kritischen Infrastrukturen schrittweise zu digitalisieren, ohne die physischen Sicherheitsmaßnahmen zu gefährden. Dies ist insbesondere vorteilhaft für Unternehmen, die mehrere Standorte oder eine komplexe Infrastruktur haben. Sie ermöglichen eine stufenweise Integration und Anpassung an sich ändernde Sicherheitsanforderungen und wachsende Unternehmensstrukturen, ohne dass direkt eine vollständige Umstellung auf digitale Systeme notwendig ist.

2. **Zugangskontrolle und Ereignisprotokollierung**: Hybride Systeme bieten die Protokollierung und Zutrittsrechteverwaltung der elektronischen Systeme und kombinieren diese mit der physischen Sicherheit mechanischer Lösungen. Das ermöglicht eine Nachvollziehbarkeit und den sicheren Zugriff auf kritische Bereiche, was sowohl den Anforderungen aus dem NIS-2-Umsetzungsgesetz als auch dem KRITIS-Dachgesetz entspricht.

3. **Redundanz und Ausfallsicherheit:** Die Kombination von mechanischen und elektronischen Komponenten sorgt selbst bei einem Stromausfall oder einer Störung des elektronischen Systems dafür, dass der physische Schutz durch mechanische Lösungen gewährleistet bleibt.

4. **Integration in vorhandene IT-Infrastrukturen:** Hybride Lösungen bieten die Möglichkeit, sowohl mechanische als auch digitale Zutrittskontrollsysteme in vorhandene IT-Infrastruktur zu integrieren, was eine durchgehende Sicherheitsstrategie ermöglicht und die Einhaltung der Anforderungen aus dem NIS-2-Umsetzungsgesetz und dem KRITIS-Dachgesetz unterstützt.

5. **Einbindung in ein ISMS**: Durch die Möglichkeiten, die ein hybrides Zutrittskontrollsystem bietet, können die Anforderungen eines ISMS hinsichtlich Zutrittssteuerung und Protokollierung erfüllt werden.

Hybride Zutrittskontrolllösungen bieten eine Balance zwischen physischer Sicherheit und digitaler Flexibilität. Die Fähigkeit, mechanische Systeme mit elektronischen Funktionen zu kombinieren, macht hybride Lösungen zu einer zukunftssicheren Option für Unternehmen, die eine hohe Sicherheit und Skalierbarkeit wünschen, ohne sofort auf eine vollständige digitale Umstellung angewiesen zu sein.

6. Exkurs Zertifizierung: Zertifizierungen nach NIS-2, KRITIS, ISO/IEC 27001

Ein häufiger Irrtum besteht darin zu glauben, dass bestimmte Produkte – etwa Zutrittskontrollsysteme – **nach NIS-2, KRITIS oder ISO/IEC 27001 „zertifiziert“** werden können.

Tatsächlich ist dies zum aktuellen Zeitpunkt **nicht der Fall**, denn:

Diese Rechtsvorgaben und Normen zertifizieren keine Produkte – sondern Prozesse oder Organisationen

- **NIS-2** ist eine EU-Richtlinie, die Vorgaben an Sicherheitsmaßnahmen und Prozesse in Unternehmen formuliert – aber keine Produktzertifizierungen vorsieht.

- **KRITIS-Regularie**n (nach deutschem BSI-Gesetz) verlangen zum Beispiel den „Stand der Technik“, definieren aber keine Zulassung bestimmter Produkte oder Marken.

- **ISO/IEC 27001** ist ein Standard für ISMS. Eine Organisation kann sich danach zertifizieren lassen – nicht jedoch einzelne technische Komponenten wie Schlösser oder Zutrittsmedien.

Sicherheit ergibt sich aus dem Zusammenspiel aller Maßnahmen – nicht dem Einzelprodukt

Die Wirksamkeit von Zutrittskontrolllösungen hängt nicht nur von der Technik ab, sondern vom **gesamten organisatorischen und technischen Kontext.** Dazu zählen:

- Risikobewertung
- Rollen- und Rechtekonzepte
- Wartung und Betrieb der Systeme
- Schulung des Personals
- Dokumentation und Protokollierung

Konkret: Es existieren zum aktuellen Stand (Februar 2026) keinerlei Zertifizierungsmöglichkeiten für Produkte im Bereich Zutrittskontrolllösungen nach dem NIS-2-Umsetzungsgesetz, KRITIS-Dachgesetz, ISO/IEC 27001 oder dem BSI IT-Grundschutz!

Richtig ist: Zutrittskontrolllösungen sind ein wichtiger technischer Bestandteil, um die Anforderungen aus dem NIS-2-Umsetzungsgesetz, KRITIS-Dachgesetz und ISO/IEC 27001 umzusetzen. Sie können jedoch nicht für sich allein „zertifiziert“ werden – entscheidend ist, wie sie eingesetzt, gesteuert und dokumentiert werden.

Was bedeutet das für die Zutrittskontrolllösungen von ABUS?

ABUS selbst unterliegt als Unternehmen der NIS-2-Richtlinie (EU 2022/2555) bzw. dem NIS-2-Umsetzungsgesetz und somit den Anforderungen hinsichtlich Informationssicherheit und sichere Entwicklungspraktiken und bietet damit sich selbst und den durch Lieferung verbundenen Unternehmen ebenfalls das gesetzlich vorgeschriebene hohe Cyber-Sicherheitsniveau.

Mit Produkten made in Germany.

7. Kontakt, Beratung und Projektierung

Mit der zunehmenden Regulierung im Bereich der Informations- und Infrastruktursicherheit – insbesondere durch das NIS-2-Umsetzungsgesetz und den Anforderungen für kritische Infrastrukturen gemäß KRITIS-Dachgesetz – stehen Unternehmen vor der Aufgabe, ihre physischen Sicherheitsmaßnahmen neu zu bewerten und gezielt weiterzuentwickeln. Ein zentrales Element dabei ist die Zutrittskontrolle:
Wer darf wann wohin – und unter welchen Bedingungen?

ABUS unterstützt Unternehmen aus allen Branchen bei genau dieser Fragestellung – mit einem breiten Lösungsportfolio und einer eigenen Projektierungsabteilung, die Sie von der Planung bis zur Umsetzung begleitet. Ob rein elektronische oder hybride Lösungen – wir sind in der Welt der Zutrittskontrolle seit vielen Jahren zu Hause und beraten Sie individuell.

Nehmen Sie gerne Kontakt zu uns auf – wir hören zu, fragen nach und entwickeln gemeinsam mit Ihnen die für Sie passende Lösung.

Sprechen Sie uns gerne an! Fordern Sie hier direkt Ihren persönlichen Beratungstermin bei uns an!
abus.info/nis-2-kritis

Abkürzungs- & Link-Verzeichnis

Hinweise zu im Text verwendeten Abkürzungen und Hyperlinks.

A. Abkürzungsverzeichnis:

BSIG oder BSI-Gesetz – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik

BSI – Bundesamt für Sicherheit in der Informationstechnik

NIS-2-Umsetzungsgesetz – Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

KRITIS – kritische Infrastrukturen

ISMS – Informationssicherheit-Managementsystem

KRITISDachG – KRITIS-Dachgesetz – Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen

BBK – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

B. Link-Verzeichnis:

NIS-2-Umsetzungsgesetz: https://www.recht.bund.de/bgbl/1/2025/301/VO.html

NIS-2-Betroffenheitsprüfung: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html

NIS-2-Registrierung für betroffene Unternehmen: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html