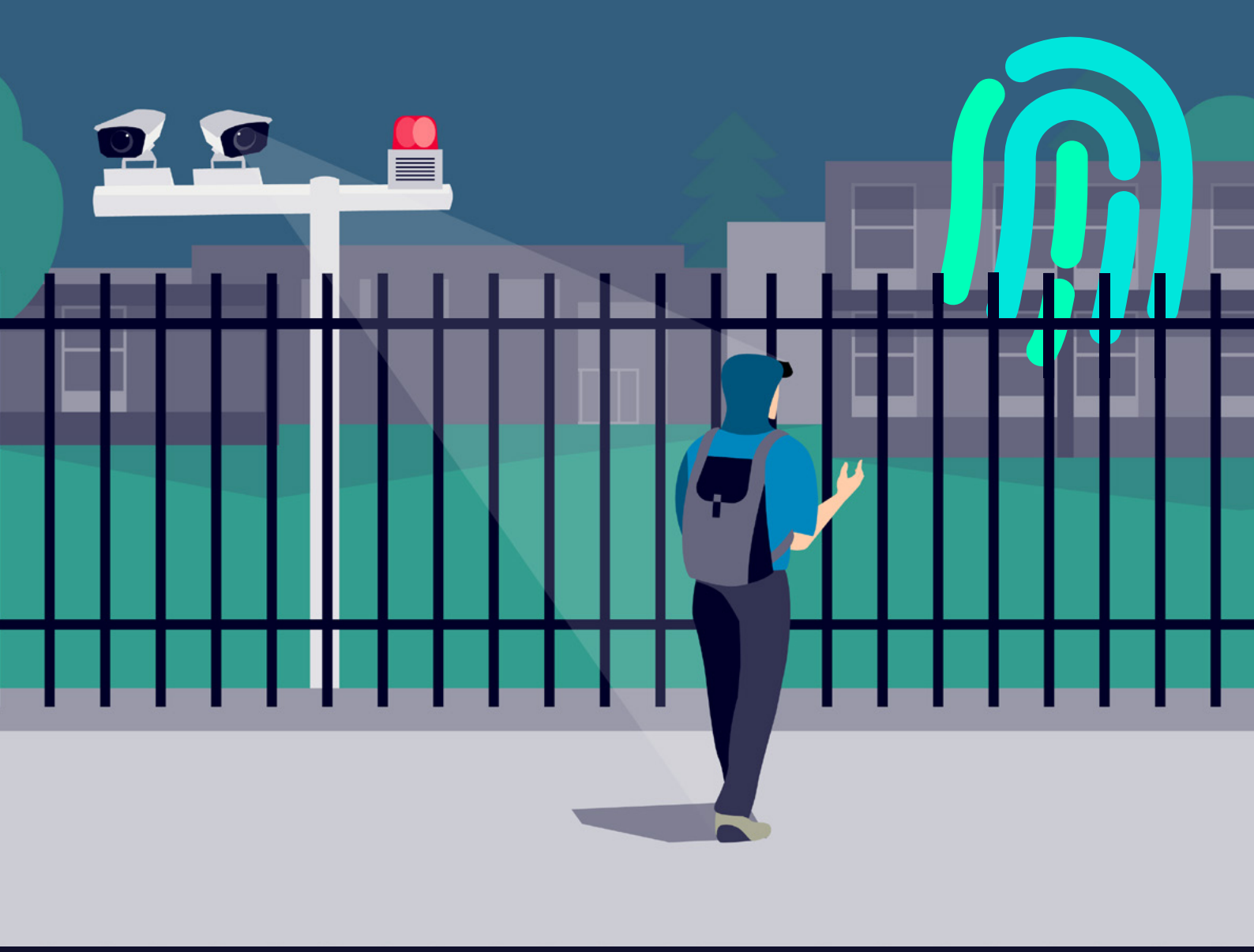


KRITIS und NIS2: Fragen und Antworten

Gesammelte Q&As zu Gebäudeinfrastruktur und Liegenschaften aus Webinaren, Kundengesprächen und der Praxis.

siemens.de/kritis-dachgesetz

SIEMENS



Einleitung

Das KRITIS-Dachgesetz und NIS2-Umsetzungsgesetz sind für viele Unternehmen bereits fester Bestandteil der Agenda.

In der praktischen Umsetzung ergeben sich dabei häufig ähnliche Fragen:

- Welche Anforderungen sind zu erfüllen?
- Welche Risiken bestehen in der Lieferkette?
- Wie kann die Umsetzung sinnvoll gestartet oder weiterentwickelt werden?

Dieses FAQ-Dokument bündelt zentrale Fragen aus Webinaren, Kundengesprächen und aktuellen Praxisfällen. Es bietet eine erste Orientierung, hilft bei der Einordnung der Themen und unterstützt dabei, die nächsten Schritte strukturiert anzugehen.

Inhalt

1 **Einführung und Einordnung – KRITIS und NIS2** 03

2 **Betroffenheit und Relevanz** 06

3 **Pflichten und Verantwortung** 07

4 **Umsetzung in der Praxis** 09

5 **Ausblick** 11

6 **Fazit und Kontakt** 12

7 **Weiterführende Materialien** 13

1

Einführung und Einordnung – KRITIS und NIS2

01 | Was regelt das KRITIS-Dachgesetz?

Das KRITIS-Dachgesetz schafft den rechtlichen Rahmen für den Schutz kritischer Infrastrukturen in Deutschland. Der Fokus liegt hierbei auf physischer Sicherheit und betrachtet alle denkbaren Risiken, die durch technische Ausfälle oder gezielte Angriffe entstehen können.

Das Gesetz legt zunächst fest, welche Sektoren und Branchen als kritische Infrastrukturen gelten, wie etwa die Bereiche Energie, Wasser, Verkehr, Gesundheit, Informationstechnik und Telekommunikation. Für diese Bereiche definiert das KRITIS-Dachgesetz Mindeststandards und Schutzanforderungen, die Betreiber erfüllen müssen, um die Funktionsfähigkeit im Krisenfall sicherzustellen.

Zudem regelt das Gesetz Meldepflichten: Betreiber kritischer Infrastrukturen sind verpflichtet, Störungen und Ausfälle, die zu erheblichen Versorgungsengpässen führen können, an zuständige Behörden (bei KRITIS das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: BBK) zu melden.

Nicht zuletzt sieht das Gesetz auch Sanktionen bei Verstößen gegen die Schutzanforderungen vor, etwa in Form von Bußgeldern.

Insgesamt zielt das KRITIS-Dachgesetz darauf ab, die Infrastrukturen Deutschlands besser vor Ausfällen, Störungen und Angriffen zu schützen und so die Versorgungssicherheit der Bevölkerung zu gewährleisten. Dabei ist der All-Gefahren-Ansatz ein grundlegendes Prinzip, das Betreiber kritischer Infrastrukturen berücksichtigen müssen.



02 | Was ist die NIS2-Richtlinie und was bedeutet das NIS2-Umsetzungsgesetz?

Die NIS2-Richtlinie (Network and Information Security Directive 2) ist eine überarbeitete EU-Richtlinie, die im Jahr 2022 verabschiedet wurde.

Sie dient der Stärkung der Cybersicherheitsmaßnahmen in Unternehmen und öffentlichen Einrichtungen innerhalb der EU mit dem Ziel, die Resilienz und die Sicherheitsanforderungen für kritische Infrastrukturen und wichtige Unternehmen zu erhöhen, um sich besser gegen Cyberangriffe zu schützen.

Das NIS2-Umsetzungsgesetz (NIS2-UmsuCG) überträgt die Anforderungen der NIS2-Richtlinie in nationales Recht und legt fest, welche Unternehmen und Einrichtungen diese Anforderungen erfüllen müssen. Es bestimmt außerdem die Sicherheitsmaßnahmen, die ergriffen werden müssen, um die Cybersicherheit zu verbessern.

Diese Vorgaben sollen insbesondere in kritischen Infrastrukturen, wesentlichen und wichtigen Sektoren angewendet werden, um besser gegen Risiken und Bedrohungen der digitalen Infrastruktur gerüstet zu sein.

03 | Wann treten das KRITIS-Dachgesetz und das NIS2-Umsetzungsgesetz in Kraft?

Das NIS2-Umsetzungsgesetzt ist bereits am 6. Dezember 2025 in Kraft getreten. Das KRITIS-Dachgesetz folgte am 17. März 2026.





04 | Gehören Krankenhäuser grundsätzlich zu KRITIS?

Krankenhäuser gehören grundsätzlich zu KRITIS, wenn sie die dafür vorgesehenen Schwellenwerte erreichen bzw. überschreiten oder/und weitere Parameter zusätzlich erfüllen. Der Versorgungsgrad, also die Bedeutung einer Dienstleistung für die Versorgung, muss anhand branchen-spezifischer Schwellenwerte bestimmt werden. Dies gilt für alle Dienstleistungen, die als kritisch eingestuft werden. Ergänzend kann der branchenspezifische Sicherheitsstandard B3S als Orientierung für angemessene Sichehits-maßnahmen herangezogen werden.

05 | Was bedeutet BSI-Zertifizierung?

Die BSI-Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik in Deutschland gewährleistet, dass IT-Produkte und -Prozesse bestimmte Sicherheitsstandards erfüllen. Im Zusammenhang mit dem KRITIS-Dachgesetz und der NIS2-Richtlinie spielt die BSI-Zertifizierung eine wichtige Rolle, da sie die Einhaltung von Cybersicherheitsstandards für Betreiber kritischer Infrastrukturen und wesentlicher Dienste gewährleistet. Für Unternehmen, die Teil kritischer Infrastrukturen sind, kann die BSI-Zertifizierung ein wichtiger Nachweis für die Erfüllung gesetzlicher und regulatorischer Sicherheitsvorgaben sein.

06 | Was steckt hinter dem Cyber Resilience Act der EU?

Der Cyber Resilience Act (CRA) ist die erste europäische Regelung, die Cybersicherheitsanforderungen für sowohl vernetzte als auch nicht vernetzte Produkte festlegt. Voraussetzung ist, dass die Produkte über eine Schnittstelle verfügen. Die Regulierung trat am 10. Dezember 2024 in Kraft. Erste Berichtspflichten müssen ab dem 11. September 2026 erfüllt werden, während der CRA ab dem 11. Dezember 2027 vollständig gilt. Besonders betroffen sind Hersteller von Hardware- und Software-Produkten, die nachweisen müssen, dass ihre Systeme die festgelegten Anforderungen erfüllen.

07 | Was macht das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)?

Das BBK ist die zentrale deutsche Behörde, die für den Bevölkerungsschutz und Katastrophenschutz zuständig ist. Ihre Aufgaben umfassen die Vorbereitung und Koordination von Maßnahmen zum Schutz und zur Unterstützung der Bevölkerung bei größeren Gefahrenlagen und Katastrophen. Für KRITIS und die NIS2 ist das BBK von Bedeutung, da es sich mit der Resilienz und dem Schutz kritischer Infrastrukturen befasst. Kritische Infrastrukturen sind essenziell für das Funktionieren der Gesellschaft und Wirtschaft, und ihre Störung kann schwere Auswirkungen haben. Das BBK arbeitet daran, diese Infrastrukturen widerstandsfähiger gegen Bedrohungen und Angriffe zu machen, indem es Sicherheits-strategien entwickelt.



2

Betroffenheit und Relevanz

08 | Wer muss die NIS2-Richtlinie umsetzen?

Die neue EU-Richtlinie NIS2 ergänzt das KRITIS-Dachgesetz und wird in Deutschland durch das NIS2-Umsetzungsgesetz (NIS2-UmsuCG) umgesetzt. Während das deutsche Gesetz sich primär auf die klassischen kritischen Infrastrukturen wie Energie, Wasser oder Verkehr konzentriert, greift die EU-Richtlinie NIS2 wesentlich weiter. Grundsätzlich lässt sich sagen, dass KRITIS-Betreiber immer die NIS2-Richtlinie beachten müssen. Es fallen aber nicht nur die traditionellen kritischen Sektoren unter das neue EU-weite Kontrollsystem, sondern auch eine Vielzahl weiterer Unternehmen und Dienstleister, die als „wesentliche“ oder „wichtige“ Einrichtungen definiert werden. Dazu gehören zum Beispiel die Trink- und Abwasserversorgung, Lebensmittelproduktion, Computer- und Elektronikindustrie oder die Automobilindustrie.



09 | Was sind mögliche physische Gefahren, die zu bewerten sind?

Die vollständige Aufzählung würde den Rahmen des Dokuments sprengen. Das BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) hat einen Kennziffernkatalog der bundeseinheitlichen Gefährdungsabschätzungen erstellt.

Dieser ist hier online abrufbar

10 | Welche Industriezweige müssen eine Betrachtung/Bewertung gemäß KRITIS-Dachgesetz durchführen?

Die beteffenden Sektoren sind im § 4 des KRITIS-Dachgesetzes benannt, die da wären:

- Energie
- Transport und Verkehr
- Finanzwesen
- Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende
- Gesundheitswesen
- Wasser
- Ernährung
- Informationstechnik und Telekommunikation
- Weltraum
- Siedlungsabfallentsorgung

sowie definierte Zuflieferer und Dienstleister der kritischen Infrastruktur, die für den Betrieb unabdingbar sind. Diese werden entweder von der Regierung zusätzlich bestimmt, von den Betreibern der kritischen Infrastruktur benannt, oder melden sich selbst, wenn sie wissen, dass sie als Lieferrant oder Dienstleister für eine kritische Infrastruktur fungieren.

11 | Ist es richtig, dass das KRITIS-Dachgesetz und die NIS2-Richtlinie für die öffentliche Verwaltung (bspw. Hochschulen) noch nicht gilt?

Bei dem Referentenentwurf für das KRITIS-Dachgesetz waren anfänglich 12 Sektoren vorgesehen, die betroffen sind. Diese wurden im Nachgang auf 10 Sektoren reduziert (vgl. Frage 10).

Verbände wie zum Beispiel der ZVEI, und BDI haben in einem Schreiben Einspruch dagegen erhoben und gefordert das die Beiden Sektoren „Medien und Kultur“ und „Öffentliche Verwaltung“ wieder in die zu betrachtenden Sektoren der KRITIS mit aufgenommen werden, daher auch auf der Präsentation ausgegraut dargestellt. Das KRITIS-Dachgesetz ist auch mit einem Anhang von Aufgaben verabschiedet worden, die im Nachgang noch bearbeitet werden, unter anderem die in der Präsentation ausgegrauten Sektoren.

3

Pflichten und Verantwortung

12 | Ich bin von der NIS2 betroffen. Muss ich auch das KRITIS-Dachgesetz erfüllen? Wie hängen die beiden zusammen?

Das Zusammenspiel der beiden Gesetze funktioniert genau andersherum: Wenn die Vorraussetzungen für die Bezeichnung „kritische Infrastruktur“ (KRITIS) erfüllt sind, dann muss automatisch auch das NIS2-Umsetzungsgesetz erfüllt werden. Das bedeutet: Alle vom KRITIS-Dachgesetz betroffenen Unternehmen müssen das NIS2UmsuCG erfüllen. Doch nicht alle wichtigen und besonders wichtigen Einrichtungen, die das NIS2UmsuCG erfüllen müssen, sind vom KRITIS-Dachgesetz betroffen.

13 | Welche Pflichten kommen auf betroffene Unternehmen konkret zu?

Betroffene Unternehmen müssen in der Regel angemessene technische, organisatorische und – je nach Anwendungsbereich – auch physische Schutzmaßnahmen umsetzen, zum Beispiel Perimeterschutz- und Einbruchmeldesysteme, Videosicherheits- oder Zutrittskontrollsysteme. Darüber hinaus gehören unter anderem auch dazu: Risikoanalysen, Maßnahmen zum Umgang mit Vorfällen, Vorkehrungen zur Aufrechterhaltung des Betriebs, die Absicherung von Lieferketten, der Umgang mit Schwachstellen, Zugriffsregelungen sowie gegebenenfalls Nachweis- und Meldepflichten. Welche Anforderungen im Einzelfall gelten, hängt davon ab, ob ein Unternehmen unter das NIS2UmsuCG, das KRITIS-Dachgesetz oder beide Regelwerke fällt.

14 | Welche Vorfälle müssen gemeldet werden und in welchen Fristen?

Grundsätzlich müssen erhebliche Sicherheitsvorfälle gemeldet werden, insbesondere wenn sie die Verfügbarkeit, Integrität, Vertraulichkeit oder Authentizität von Systemen, Daten oder Dienstleistungen beeinträchtigen oder beeinträchtigen können. Entscheidend ist, ob der Vorfall relevante Auswirkungen auf den Betrieb, die Versorgung oder die Sicherheit hat. Da für Meldungen kurze Fristen gelten können, sollten Unternehmen frühzeitig klare interne Melde- und Eskalationsprozesse festlegen.

15 | Gelten für Social Engineering-Auswirkungen oder -Angriffe auch Meldepflichten?

Ein „Angriff“ umfasst Sabotageakte, die die physische Sicherheit betreffen. Social Engineering, also der gezielte Manipulationsversuch, um vertrauliche Informationen zu erlangen, sollte durch Maßnahmen wie Aufklärung und Schulung zur Datensicherheit innerhalb der Unternehmen verhindert werden. Wenn ein Angriff auf die IT-Infrastruktur erfolgt, der auf Informationen aus Social Engineering basiert, müssen die potenziell erheblichen Auswirkungen ebenfalls gemeldet werden.



16 | Wird die ISO 27001 Voraussetzung oder Pflicht für Betreiber und Zulieferer kritischer Infrastrukturen?

Das NIS2UmsuCG legt die Anforderungen fest, die von der Regierung per Gesetz definiert werden. Dabei wird „nur“ das Ziel beschrieben, das erreicht werden muss – nicht jedoch, wie dieses Ziel konkret umgesetzt werden soll. Daher enthält das Gesetz keine vorgeschriebenen Lösungen. Die ISO 27001:2022 bietet allgemein gültige Anforderungen für Informationssicherheitsmanagementsysteme (ISMS), die für jede Art von Organisation anwendbar sind. Sie kann daher als möglicher Ansatz und Hilfsmittel dienen, um die gesetzlichen Anforderungen zu erfüllen.

17 | Wer bestätigt zum Schluss die korrekte Einhaltung der Gesetze?

Das KRITIS-Dachgesetz definiert das im § 13 (4) Der Betreiber kritischer Anlagen muss die Maßnahmen nach Absatz 1 in einem Resilienzplan darstellen und diesen anwenden. Aus dem Resilienzplan müssen die den Maßnahmen zugrunde liegenden Erwägungen hervorgehen. Auf die Risikoanalyse und Risikobewertung des Betreibers ist Bezug zu nehmen. Der Resilienzplan ist bei Bedarf sowie nach Durchführung einer Risikoanalyse und Risikobewertung des Betreibers kritischer Anlagen zu aktualisieren. Die vom Betreiber festgelegten Maßnahmen überprüft das BBK (Bundesamt für Bevölkerungsschutz und Kathastrophenhilfe) alle 4 Jahre auf Wirksamkeit, wobei der Plan bei jeder wesentlichen Änderung der Risikolage angepasst werden muss. Bei der Durchführung der Überprüfung kann die zuständige Behörde sich eines qualifizierten unabhängigen Dritten bedienen.

18 | Welche Verantwortung und Haftung trägt die Geschäftsführung?

Die Geschäftsführung trägt Verantwortung dafür, dass angemessene Maßnahmen zur Erfüllung der gesetzlichen Anforderungen umgesetzt, überwacht und organisatorisch verankert werden. Dazu gehört insbesondere, Risikomanagement, Sicherheitsmaßnahmen, Meldeprozesse und interne Zuständigkeiten wirksam zu steuern. Bei Pflichtverletzungen können je nach Rechtslage und Einzelfall nicht nur Bußgelder gegen das Unternehmen, sondern auch persönliche Haftungsrisiken für Mitglieder der Geschäftsführung entstehen.

19 | Welche Aspekte der Lieferkettensicherheit sind im Kontext von KRITIS und NIS2 bei der Auswahl und Nutzung externer IT-Produkte und -Dienstleistungen relevant?

Die Geschäftsführung trägt Verantwortung dafür, dass angemessene Maßnahmen zur Erfüllung der gesetzlichen Anforderungen umgesetzt, überwacht und organisatorisch verankert werden. Dazu gehört insbesondere, Risikomanagement, Sicherheitsmaßnahmen, Meldeprozesse und interne Zuständigkeiten wirksam zu steuern. Bei Pflichtverletzungen können je nach Rechtslage und Einzelfall nicht nur Bußgelder gegen das Unternehmen, sondern auch persönliche Haftungsrisiken für Mitglieder der Geschäftsführung entstehen.



20 | Wann müssen die Maßnahmen spätestens umgesetzt werden?

Erste Maßnahmen zur Erhöhung der physischen Resilienz müssen im Rahmen der neuen Gesetze zeitnah nach deren jeweiligem Inkrafttreten (NIS2UmsuCG am 6. Dezember 2025 und KRITIS-Dachgesetz am 17. März 2026) vollumfänglich gelten.

4

Umsetzung in der Praxis

21 | Im Rahmen des KRITIS-Dachgesetzes und der NIS2-Richtlinie muss eine sogenannte Wirksamkeitsprüfung durchgeführt werden. Was wird dabei geprüft?

Bei der Wirksamkeitsprüfung wird der aktuelle Sicherheitszustand bewertet und mit dem Zustand vor der Umsetzung der Maßnahmen verglichen. Dabei wird überprüft, ob das festgelegte Schutzziel durch die definierten Schutz- und Abwehrmaßnahmen erreicht wurde. Das Ziel der Wirksamkeitsprüfung ist es, sicherzustellen, dass alle betroffenen Organisationen – unabhängig davon, ob sie zu KRITIS oder zu NIS2 gehören – ihre Sicherheitsmaßnahmen angemessen umgesetzt haben.

22 | Wie ist das Verbot der Überwachung des öffentlichen Raums durch Videosicherheitssysteme geregelt? Sind Liegenschaften, die die KRITIS-Kriterien erfüllen davon ausgenommen? Gibt es Sonderregelungen?

Bei der Kritischen Infrastruktur werden die Videosicherheitssysteme meist nicht im öffentlichen, sondern in Betriebsbereichen (privaten Bereichen) eingesetzt.
Es gelten jedoch auch hier Länderspezifische Datenschutzgesetze und die Datenschutz-Grundverordnung DSGVO.

Im KRITIS-Dachgesetz selbst wird hierzu nicht der Datenschutz von Videosicherheitssystemen geregelt.
Weitergehende Informationen sind auf der Seite des BfDi (Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit www.bfdi.bund.de) „Videoüberwachung und das Datenschutzrecht“ zu finden.



23 | Gibt es denn Vorgaben, Richtlinien o.ä., wie der physische Schutz auszusehen hat / welche Kriterien diese erfüllen müssen oder gibt es bereits Pläne diese zu definieren?

Das KRITIS-Dachgesetz definiert im § 13 Absatz 2 einen angemessenen physischen Schutz von Liegenschaften und kritischen Anlagen zu gewährleisten. Der Gesetzgeber schreibt nicht vor wie dies zu erledigen ist, sondern was er umgesetzt haben möchte. Das WIE sollen die Verbände, Hersteller und die Industrie definieren, die auch vereinzelt schon Handreichungen und Handlungsempfehlungen am Erarbeiten sind. Siemens unterstützt hierbei auch in der Verbandarbeit und arbeitet dort mit. Da es keine KRITIS-Norm gibt, gelten für die Realisierung der Maßnahmen die geltenden Normen sowie der „Anerkannten Regeln der Technik" und der „Stand der Technik". Zur besseren Orientierungshilfe kann ebenfalls die Norm DIN SPEC 14027 herangezogen werden. Die DIN SPEC wurde vom Bundesministerium des Inneren (BMI) initiiert und finanziert und ist unter dem folgenden Link kostenlos verfügbar.

Jetzt kostenlos downloaden

24 | Wie sollten Unternehmen jetzt konkret starten, wenn noch keine vollständige Umsetzung erfolgt ist?

Ein sinnvoller Start ist eine strukturierte Bestandsaufnahme. Unternehmen sollten zunächst prüfen, ob und in welchem Umfang sie betroffen sind. Anschließend sollten relevante Systeme, Anlagen, Prozesse, Dienstleister und Abhängigkeiten erfasst sowie bestehende Schutzmaßnahmen bewertet werden. Auf dieser Grundlage lassen sich Risiken, Lücken und Prioritäten ableiten, um daraus einen realistischen Umsetzungsplan mit klaren Verantwortlichkeiten und Maßnahmen zu entwickeln. Ein Gap Assessment oder eine Gap Analyse, wie wir es in Projekten einsetzen, kann dabei unterstützen, den Status quo strukturiert zu bewerten und Sicherheitslücken frühzeitig zu identifizieren.

25 | Was kann eine mögliche relevante Schwachstelle sein?

Eine Schwachstelle ist immer dann relevant, wenn die Ausnutzung der Schwachstelle eine realistische Bedrohung für die betroffene Umgebung darstellt. Stellen wir uns einen Schnittstellenwandler vor, der zwischen Ihrem Brandmeldesystem und der zugehörigen Management-Ebene eingesetzt wird. Es wird angenommen, dass dieses Gerät eine Schwachstelle besitzt, welche ohne viel Aufwand ausgenutzt werden kann. Bei Ausnutzung der Schwachstelle, meldet sich der Schnittstellenwandler weiterhin als aktiv bei dem Managementsystem – jedoch wird die Weitergabe von Statusmeldungen und Schaltbefehlen unterdrückt.
In Summe ist diese Schwachstelle durch existierende und funktionierende Rückfallebenen weniger kritisch als würde die gleiche Schwachstelle im Brandmeldesystem selbst existieren. Jedoch kann die beschriebene Schwachstelle schnell kritisch werden, wenn hierdurch im Ernstfall Unsicherheiten auftreten.



26 | Sind Siemens Software-Lösungen, wie zum Beispiel das Schwachstellenmanagement, primär für Siemens-Anlagen oder sind sie auch in Kombination mit anderen Hardware-Herstellern verwendbar?

Im Falle des Schwachstellenmanagement nutzen wir herstellerübergreifende Datenbanken sowie protokollbasierte Identifikationsmechanismen. Daher funktioniert diese Lösung im beschriebenen Leistungsumfang herstellerübergreifend. Für eine individuelle Beurteilung und Machbarkeitsstudie, kontaktieren Sie bitte Ihren Siemens-Ansprechpartner oder schreiben Sie eine E-Mail an:

kontakt.msm.de@siemens.com

5

Ausblick:
Resilienz erweitert sich um den Wirtschaftsschutz

Seit dem 06. März 2026 steht die Nationale Wirtschaftsschutzstrategie im Fokus: Sie verfolgt das Ziel, die Resilienz deutscher Unternehmen, ihrer Wertschöpfungs- und Lieferketten sowie von Forschung und Entwicklung gegenüber physischen, digitalen und hybriden Sicherheitsbedrohungen zu stärken. Dabei wird ein ganzheitlicher, integrierter All Gefahren Ansatz verfolgt, der physische, digitale und hybride Bedrohungen gleichermaßen berücksichtigt.

Wichtige Maßnahmen sind die Weiterentwicklung rechtlicher Rahmenbedingungen, die Förderung kollektiver Zusammenarbeit von Staat und Wirtschaft sowie die Unterstützung individueller Schutzmaßnahmen (z. B. DIN SPEC 14027 Corporate Security).





Relevanz für den Gebäudekontext

- **Physische Sicherheit**
  Abstimmung von Schutzkonzepten (z. B. Zutrittskontroll-, Videosicherheits- und Perimeterschutzsysteme) mit den neuen Schutzniveaus und Anforderungen.
- **Hybrid- und Digitalsicherheit**
  Verzahnung von Gebäudesystemen (z. B. Gebäudeautomation, Zutrittskontrolle) mit Cyber , IT- und OT Sicherheitsmaßnahmen.
- **Lieferketten und Forschung**
  Schutz sensibler Bereiche und sensibler Prozesse (Labore, F&E Standorte, Logistik) gegenüber Wirtschaftsspionage und Sabotage.

Nächste Schritte

- **Orientierung:**
  Die DIN SPEC 14027 Corporate Security ergänzt bestehende Standards und definiert Schutzniveaus zur praktischen Einordnung der eigenen Organisation.
- **Unterstützung:** Die DIN SPEC wurde vom BMI initiiert und finanziert und ist kostenlos verfügbar: https://www.dinmedia.de/de/technische-regel/din-spec-14027/400565136.
- **Umsetzung:**
  Prüfen Sie, ob bestehende Gebäudesicherheitskonzepte an die definierten Schutzniveaus angepasst werden müssen und stimmen Sie diese mit Ihrer Betriebssicherheit, Cybersecurity und dem entsprechenden Fachbereich ab.

6

Fazit

Für die Gebäudeinfrastruktur gilt: Physische Sicherheit und Cybersecurity sollten nicht getrennt betrachtet werden, da beide ineinandergreifen. Ein ganzheitlicher Blick auf Assets, Risiken und Schutzmaßnahmen ist eine wichtige Grundlage, um gesetzliche Anforderungen umzusetzen. Unsere Experten unterstützen Sie gerne bei der Einordnung von Handlungsbedarfen und der Umsetzung geeigneter Sicherheits-Maßnahmen.

Wenn Sie mehr erfahren möchten oder nächste Schritte planen, dann schreiben Sie uns:

kontakt.msm.de@siemens.com

Kontakt-formular

Die Grundlage für eine gute Cybersicherheit ist eine gute physische Sicherheit. Systeme zur physischen Sicherheit müssen auch Anforderungen der Cybersicherheit erfüllen.



7

Weiterführende Materialien

1. Quick-Check KRITIS/NIS2

Machen Sie den Test: Wo stehen Sie bei Cybersecurity und physischer Sicherheit?



Unsere Quick-Check für Cybersecurity und physische Sicherheit bieten eine erste Orientierung und Selbsteinschätzung, wie resilient Ihr Unternehmen aufgestellt ist.

Jetzt kostenlos testen

2. NIS2-Umsetzungsguide

NIS2-Anforderungen und -lösungen für die Gebäudetechnik

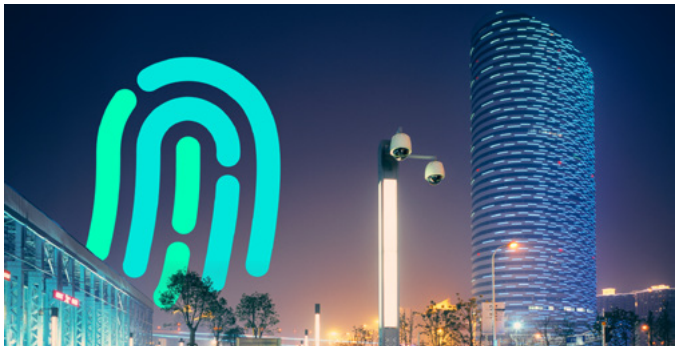


Unser NIS2-Umsetzungsguide bietet einen Überblick über regulatorische Anforderungen und zeigt mögliche Lösungen für ihre praktische Umsetzung.

Hier geht es zum Download

3. Webinar 26.03.26

KRITIS und NIS2: Ihr Fahrplan zur operativen Umsetzung in Gebäuden und Liegenschaften



Unsere Webinaraufzeichnung bietet eine kompakte regulatorische Einordnung und zeigt einen möglichen Fahrplan zur strukturierten Umsetzung in Gebäuden und Liegenschaften.

Hier geht es zur Aufzeichnung

4. Top-10

Sind Ihre OT-Systeme ausreichend geschützt oder gibt es Sicherheitslücken?



Unsere Übersicht zeigt die 10 häufigsten OT-Cybersecurity-Risiken in der Praxis – und wie Sie Ihre gebäudetechnischen Systeme digital und physisch besser schützen können.

Hier geht es zum Download

Smart Infrastructure verbindet die reale mit der digitalen Welt über Energiesysteme, Gebäude und Industrien hinweg, um unsere Lebens- und Arbeitsweise durch mehr Effizienz und Nachhaltigkeit zu verbessern.

Gemeinsam mit unseren Kunden und Partnern schaffen wir ein Ökosystem, das sowohl intuitiv auf die Bedürfnisse der Menschen reagiert als auch Kunden dabei unterstützt, ihre Geschäftsziele zu erreichen.

Ein Ökosystem, das unseren Kunden hilft zu wachsen, das den Fortschritt von Gemeinschaften fördert und eine nachhaltige Entwicklung begünstigt, um unseren Planeten für die nächste Generation zu schützen.

Herausgeber
Siemens AG

Smart Infrastructure
De-Saint-Exupéry-Straße 5–7
60549 Frankfurt am Main

Kundenbetreuungs-Center
Tel. 0800 100 76 39
info.de.sbt@siemens.com

Artikel-Nr. E10003-A38-H528 (Stand 10/2026)

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

© Siemens 2026