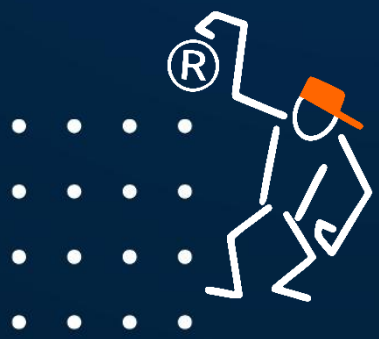
KRITIS/ NIS2 Checkliste

RISIKEN MINIMIERN UND IHR UNTERNEHMEN SCHÜTZEN



Inhaltsverzeichnis

Greizer Straße 7
08427 Fraureuth, Sachsen

+49 (0) 3761 70947-60
frrth@ape-soft.de

KRITIS und die Bedeutung für die Sicherheit

Das **Gesetz zum Schutz Kritischer Infrastrukturen** (KRITIS) zielt darauf ab, Organisationen und Einrichtungen, deren Ausfall oder Beeinträchtigung gravierende Folgen für das staatliche Gemeinwesen haben könnte, zu schützen. Darunter fallen insbesondere Bereiche wie Telekommunikation, Strom- und Wasserversorgung, die zu den größten und am stärksten gefährdeten Sektoren der Kritischen Infrastruktur zählen.

Kritische Infrastrukturen sind von **zentraler Bedeutung** für die öffentliche Sicherheit, das Wohlstandsniveau und die Funktionsfähigkeit des Staates. Um diese Schutzwürdigkeit zu gewährleisten, legt das KRITIS-Gesetz Standards fest, die sicherstellen sollen, dass **notwendige Maßnahmen ergriffen werden**, um diese Einrichtungen vor digitalen Bedrohungen und Angriffen zu schützen.

Die Rolle von NIS2 für Unternehmen im Bereich KRITIS

Die **NIS2-Richtlinie** (Netzwerk- und Informationssicherheit) ist eine EU-weite Gesetzgebung, die einen harmonisierten Rahmen für die Cybersicherheit von kritischen Infrastrukturen schaffen soll. Sie betrifft vor allem Organisationen, die als Betreiber von wesentlichen und digitalen Diensten gelten. Ziel ist es, den **Schutz vor Cyberangriffen** zu erhöhen, die Sicherheit von Netzwerk- und Informationssystemen zu stärken und die Resilienz kritischer Infrastrukturen zu fördern.

Für Unternehmen im Bereich KRITIS bedeutet dies, dass Sie:

- Verpflichtungen zur Erhöhung der Cybersicherheit erfüllen müssen.
- Notfall- und Wiederherstellungspläne für den Fall eines Sicherheitsvorfalls entwickeln.
- Berichtspflichten hinsichtlich von Sicherheitsvorfällen einhalten müssen.

Betroffene Bereiche und rechtliche Konsequenzen

Welche Organisationen sind betroffen?
Die Anforderungen aus dem KRITIS-Rahmen sowie der NIS-2-Richtlinie gelten für eine Vielzahl von Sektoren, deren Ausfall erhebliche Auswirkungen auf das Gemeinwesen haben könnte. Betroffene Bereiche sind unter anderem:

Sektoren mit hoher Kritikalität[1]:

- Abwasser
- Bankwesen
- digitale Infrastruktur
- Energie
- Finanzmarktinfrastruktur
- Gesundheitswesen
- öffentliche Verwaltung
- Trinkwasser
- Verkehr
- Verwaltung
- Weltraum

Sonstige kritische Sektoren[2]:

- Abfallbewirtschaftung
- Anbieter digitaler Dienste
- Forschung
- Post & Kurierdienste
- Produktion, Herstellung & Handel mit chemischen Stoffen
- Produktion, Verarbeitung & Vertrieb von Lebensmittel
- Vertreibendes Gewerbeherstellung von Waren

Hinweis: NIS 2 erweitert den Anwendungsbereich deutlich. Auch mittlere Unternehmen können betroffen sein, wenn sie als „wichtige Einrichtungen“ gelten.

[1] Vgl. Richtlinie (EU) 2022/2555, Anhang I
[2] Vgl. Richtlinie /EU) 2022/2555, Anhang II

Was droht bei Verstößen?
Unternehmen, die ihren Pflichten nicht nachkommen, müssen mit folgenden Konsequenzen rechnen:

- Hohe Bußgelder:
  - Für „wesentliche Einrichtungen[i]“: bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes
  - Für „wichtige Einrichtungen[ii]“: bis zu 7 Mio. € oder 1,4 % des weltweiten Umsatzes
- Verwaltungsmaßnahmen: z. B. behördliche Anordnungen zur Behebung von Mängeln
- Persönliche Haftung der Geschäftsleitung: Bei grober Fahrlässigkeit oder Pflichtverletzung kann die Verantwortung direkt bei der Leitungsebene liegen
- Reputationsschäden: Öffentliche Bekanntmachung von Sicherheitsverstößen oder Datenpannen

Massgeschneiderte Lösungen für Ihr Unternehmen

Die APE Software GmbH bietet **umfassende Zutritts- und Sicherheitslösungen**, die speziell auf die Bedürfnisse kritischer Infrastrukturen ausgerichtet sind. Unsere Systeme sorgen dafür, dass nur autorisierte Personen Zugang zu sensiblen Bereichen erhalten und tragen somit zur Erhöhung Ihrer Sicherheitsvorkehrungen bei.

Unsere Lösungen bieten:

- Höchste Sicherheitsstandards und Konformität mit den relevanten Normen und Vorschriften.
- Sichere Zonen sowohl im Außenbereich als auch in internen Bereichen.
- Zutrittsprotokolle zur Überwachung und Dokumentation von Zugriffsereignissen.
- Langfristige Partnerschaft für regelmäßige Anpassungen und Updates.

Durch **maßgeschneiderte Lösungen** reduzieren wir Sicherheitsrisiken, optimieren Ihre betrieblichen Abläufe und steigern die Effizienz!

KRITIS & NIS2 Checkliste:

1. Informationssicherheitsmanagement und Compliance

- **Sicherheitsstandards in der Lieferkette**: Sicherstellung, dass Geschäftspartner und Dienstleister angemessene Sicherheitsvorkehrungen getroffen haben (z.B. durch Zertifikate wie ISO/IEC 27001, SOC 2, TISAX®).
- **Sicherheitsrichtlinien und Risikomanagement**: Entwicklung und Umsetzung der Richtlinien für Risiken und Informationssicherheit, sowie Definition von Regeln zum Umgang mit Cyber-Sicherheitsrisiken.
- **Meldung und Behandlung von Sicherheitsvorfällen**: Sicherstellen, dass Vorfälle gemeldet und angemessen behandelt werden.
- **Compliance**: Einhaltung von NIS 2.0-Anforderungen, regelmäßige Audits zur Überprüfung gesetzlicher Vorgaben, und Dokumentation der Sicherheitsvorkehrungen für Prüfbehörden.
- **Zertifizierungen**: Zusammenarbeit mit zertifizierten Partnern und Technologien.

2. Technische Sicherheitsmaßnahmen

- **Schutz vor Cyberangriffen**: Absicherung von Systemen durch Firewalls, regelmäßige Audits und Sicherheitsupdates für alle relevanten Systeme.
- **Zutrittskontrolle**: Einsatz moderner Zutrittslösungen wie biometrische Systeme oder RFID-Karten, regelmäßige Prüfung und Aktualisierung von Zugangsrechten, sowie besondere Absicherung sensibler Bereiche (z.B. Serverräume).
- **Videoüberwachung**: Sicherstellung, dass Kameras funktionstüchtig sind, kritische Bereiche überwachen und Videoaufzeichnungen DSGVO-konform gespeichert sowie regelmäßig überprüft werden.
- **Authentifizierung**: Einführung von Multi-Faktor-Authentifizierung (MFA) und Single Sign-On (SSO) für sicheren Zugang zu Systemen.

3. Business Continuity Management (BCM)

- **Backup-Management**: Sicherstellung einer redundanten Datenhaltung für den Notfall und Ausarbeitung einer Wiederherstellungsstrategie.
- **Notfallmanagement**: Entwicklung von Notfallplänen, um die Aufrechterhaltung kritischer Dienstleistungen auch im Falle eines Cyber-Sicherheitsvorfalls zu gewährleisten.

4. Personal und Schulungen

- **Schulungen und Awareness-Training**: Regelmäßige Schulung des Personals zu Sicherheitsrichtlinien, Passwortmanagement, Erkennen von Phishing-Mails und sicherem Umgang mit IT-Systemen.
- **Zugangskontrollen für sensible Daten**: Sicherstellen, dass nur berechtigtes Personal Zugang zu kritischen Systemen und Daten hat und die Verwaltung dieser Anlagen ordnungsgemäß erfolgt.

5. Zusammenarbeit mit Partnern und Dienstleistern

- **Integration von Partnern in die Sicherheitsstrategie**: Sicherstellung, dass Partner in die Sicherheitsstrategie eingebunden sind.
- **Externe Dienstleister**: Regelmäßige Überprüfung und Schulung externer Dienstleister, um die Datensicherheit auch außerhalb des Unternehmens zu gewährleisten.
- **Vereinbarungen zur Datensicherheit**: Klare Vereinbarungen zur Datensicherheit mit allen Partnern und Dienstleistern, um Sicherheitslücken zu vermeiden.

Ihre nächsten Schritte:

1. **Überprüfen Sie den Status Quo:**
   Welche Punkte sind erfüllt? Wo gibt es Nachholbedarf?
2. **Beratung anfordern:**
   Kontaktieren Sie uns, um Ihre Sicherheitsstandards auf KRITIS & NIS 2 vorzubereiten.
3. **Setzen Sie auf langfristige Sicherheit:**
   Arbeiten Sie mit uns an einer für Sie maßgeschneiderten Lösung!

Sicherheit durch innovative Zutrittslösungen – Nehmen Sie mit uns Kontakt auf

Der Schutz kritischer Infrastrukturen ist eine wichtige Aufgabe, die nicht nur gesetzlich vorgeschrieben ist, sondern auch das Vertrauen Ihrer Kunden stärkt. Die **APE Software GmbH** bietet Ihnen die passenden Lösungen, um Ihr Unternehmen vor digitalen und physischen Bedrohungen zu schützen und die Anforderungen des KRITIS-Gesetzes sowie der NIS2-Richtlinie zu erfüllen.

Kontaktieren Sie uns, um Ihre maßgeschneiderte Sicherheitslösung zu finden:

- **Telefon:** +49 (0) 3761 70947-60
- **E-Mail:** frrth@ape-soft.de
- **Website:** www.ape-soft.de
- **Adresse:** Greizer Straße 7, 08427 Fraureuth

[i] Große Unternehmen = >250 Beschäftigte oder >50 Mio. Euro Jahresumsatz
[ii] Mittlerer Unternehmen = >50 Beschäftigte oder > 10 Mio. Euro Jahresumsatz