TÜVNORD

KRITIS und das neue IT-Sicherheits-gesetz 2.0

TÜV NORD CERT

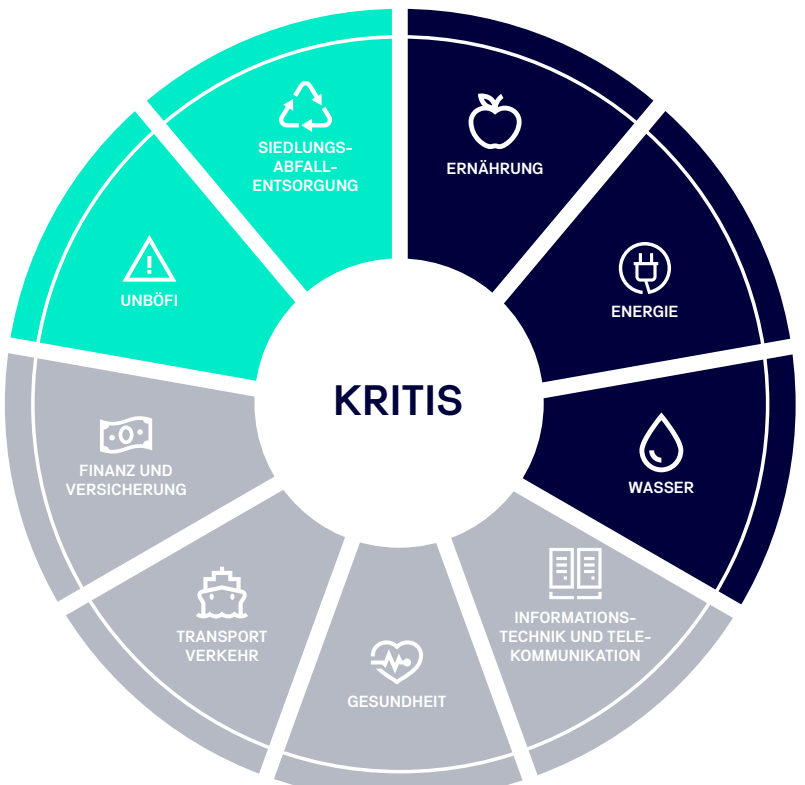
KRITIS und das neue IT-Sicherheitsgesetz 2.0

In einer digital vernetzten Welt ist eine sichere IT-Infrastruktur wichtiger denn je. Insbesondere Unternehmen, die zu den „kritischen Infrastrukturen“ (KRITIS) zählen, gelten als besonders schützenswert. Kommt es zum Ausfall eines KRITIS-Unternehmens, können nachhaltige Versorgungsengpässe entstehen, und auch die öffentliche Sicherheit kann in Gefahr geraten.

Bis vor Kurzem gehörten in Deutschland sieben verschiedene Sektoren der KRITIS an. Dazu zählen beispielsweise die Branchen Energie, Wasser, Ernährung, Telekommunikation oder das Gesundheits- und Finanzwesen.

Im Rahmen des IT-Sicherheitsgesetzes 2.0 (IT-Sig 2.0) sind nun auch die Sektoren Siedlungsabfallentsorgung und Unternehmen im besonderen öffentlichen Interesse (UBI/UNBÖFI) neu hinzugekommen.

Das IT-SiG 2.0 nimmt mit Senkung der Schwellenwerte in der KRITIS-Verordnung nun deutlich mehr Organisationen in die Pflicht, wirksame Maßnahmen zur Erhöhung ihrer IT-Sicherheit zu ergreifen. Dabei geht es grundsätzlich darum, alle Unternehmen zu erfassen, die mit ihren Dienstleistungen und Produkten mehr als 500.000 Personen versorgen.

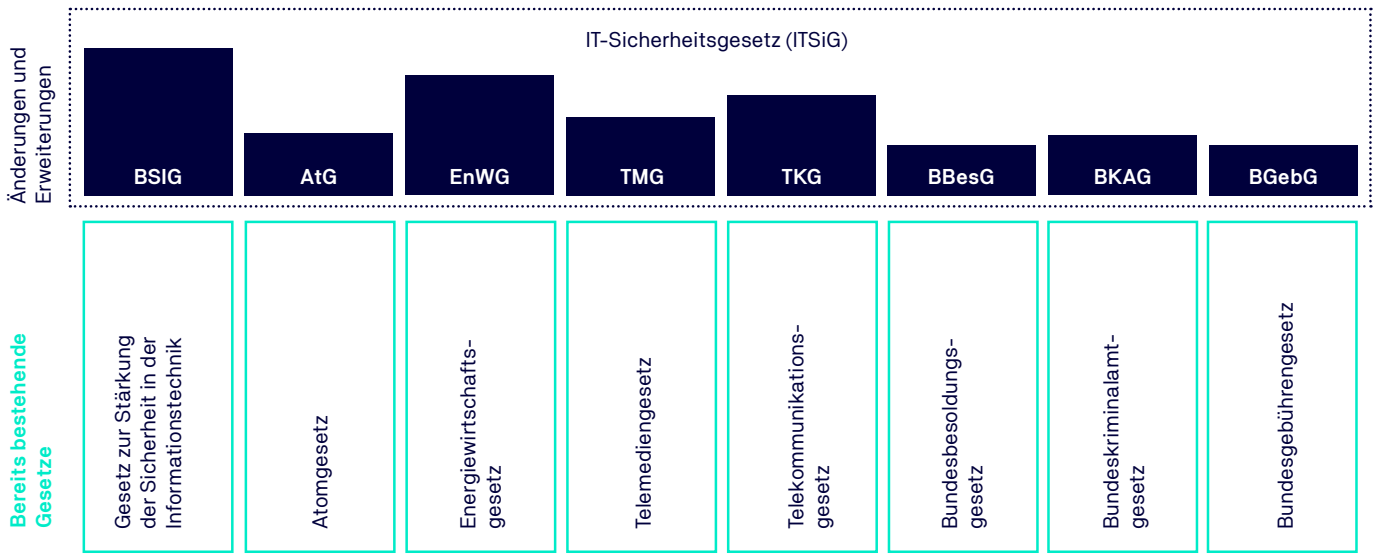


Die KRITIS-Verordnung 2021

Die Verordnungen zu den kritischen Infrastrukturen (KRITIS) des Bundesamts für Sicherheit in der Informationstechnik (BSI) ergänzen das seit Juli 2015 gültige IT-Sicherheitsgesetz.

Das IT-Sicherheitsgesetz ist an sich kein eigenständiges Gesetz, sondern ein Artikelgesetz, das als Sammlung von Änderungen und Erweiterungen bereits bestehender Gesetze zu betrachten ist.

Die Regierung hat nach dem IT-Sicherheitsgesetz 2.0 eine aktualisierte KRITIS-Verordnung 2021 beschlossen und zum 1. Januar 2022 in Kraft gesetzt. Sie konkretisiert die Ausführungen des IT-Sicherheitsgesetzes und definiert Schwellenwerte, Anlagen und Vorgaben zur Umsetzung. Diese Schwellenwerte sollten von Unternehmen im Grenzbereich in regelmäßigen Abständen auf Aktualisierungen geprüft werden. Der Pflicht bezüglich hoher Anforderungen im Bereich der IT-Sicherheit soll nachgekommen und Störungen der IT-Systeme sollen direkt dem BSI gemeldet werden.



Die Fristen durch die neue KRITIS-Verordnung 1.5

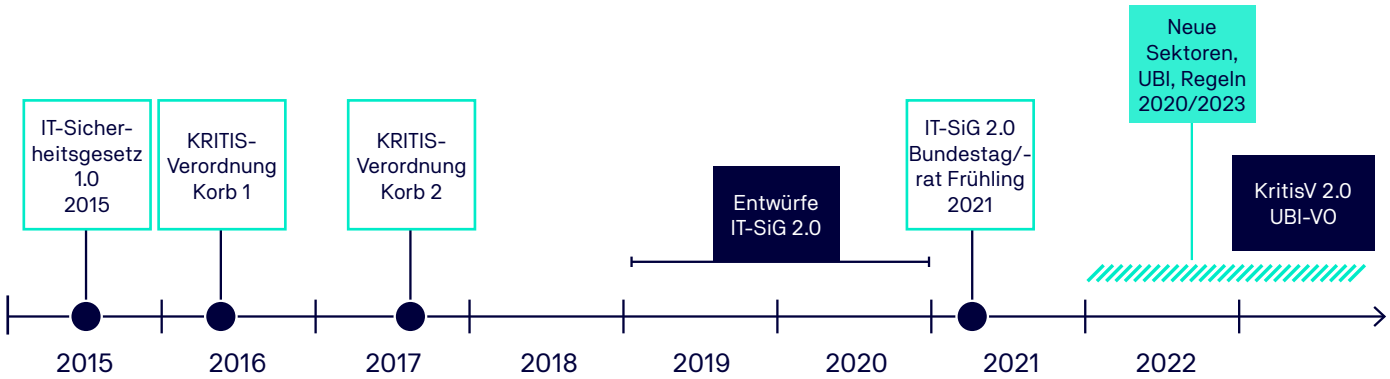
Die **neue Verordnung ist am 1. Januar 2022 in Kraft getreten.**

Neue und alte Anlagen, die die (neuen) Schwellenwerte 2021 überschreiten, müssen **spätestens zum 1. April 2022 registriert werden.**

Die Umsetzung von Cyber-Security-Maßnahmen nach § 8a BSIG muss **zum 1. April 2022 erfolgt sein.**

Ein Nachweis der Umsetzung durch KRITIS-Prüfungen ist spätestens **zum 1. April 2024** zu erbringen.

Der KRITIS-Sektor **Siedlungsabfallentsorgung und die UBI/ UNBÖFI werden 2022** noch in einer separaten KRITIS-Verordnung 2.0 und einer UBI-Verordnung **definiert**.



Anforderungen

Das BSI verpflichtet Betreiber von kritischen Infrastrukturen, bestimmte Anforderungen zu erfüllen. Hier finden Sie eine Übersicht der zu implementierenden Maßnahmen:

Registrierung
Unternehmen müssen sich unmittelbar nach Feststellung als KRITIS-Betreiber beim BSI registrieren und eine Kontaktstelle benennen. Das BSI darf Betreiber selbstständig als kritische Infrastruktur registrieren und bei bestimmten Sachverhalten Einblick in Unterlagen verlangen, wenn sie ihrer Registrierungspflicht nicht nachkommen.

Angriffserkennung
Mit IT-SiG 2.0 gehören Systeme zur Angriffserkennung nun ausdrücklich zu den technischen und organisatorischen Sicherheitsvorkehrungen in KRITIS-Anlagen.
Sie müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Die Umsetzung dieser Forderung kann z.B. mittels Security Operation Center (SOC) oder Security Information and Event Management (SIEM) realisiert werden. Ihr Einsatz ist spätestens ab dem 1. Mai 2023 verpflichtend.

Meldepflichten
KRITIS-Betreiber und Unternehmen im besonderen öffentlichen Interesse sind verpflichtet, bei erheblichen Störungen dem BSI auf Nachfrage Informationen zur Verfügung zu stellen, die für die Störungsbewältigung notwendig sind.

Einsatz von kritischen Komponenten
Unternehmen müssen den Einsatz von kritischen Komponenten bestimmter Sektoren melden. Der Einsatz solcher Komponenten darf untersagt werden. Kritische Komponenten sind nach § 2 IT-SiG IT-Produkte, deren Ausfall die Funktion der Anlage erheblich beeinträchtigen würde. Diese Komponenten werden noch für die jeweiligen Sektoren definiert.

Inventarisierung
Betreiber müssen kritische IT-Produkte in KRITIS-Anlagen inventarisieren — mit aktuellen Informationen zu Herstellern und Typen der Produkte. Bislang galt das nur für den KRITIS-Sektor Telekommunikation.

Aufrechterhaltung der kritischen Infrastruktur
Die KRITIS-Schutzziele (Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität) müssen anhand der betriebsrelevanten Teile festgelegt, in die Risikobetrachtung aufgenommen und durchgängig in allen Prozessen betrachtet werden. Anhaltspunkt für das Ausmaß eines Risikos für die Allgemeinheit sollten die Auswirkungen auf die Funktionsfähigkeit der kritischen Infrastruktur und der kritischen Dienstleistung sein.

Sind Sicherheitsvorkehrungen nach dem jeweils aktuellen Stand der Technik möglich und angemessen, muss der Betreiber sie umsetzen. Grundsätzlich gilt: Ein Transfer der Risiken z. B. auf Versicherungen ist nicht möglich und kein Ersatz für Sicherheitsvorkehrungen. Eine rein betriebswirtschaftliche Risikobetrachtung reicht in der Regel nicht aus.

Prüfung der Absicherung
In Form von Sicherheitsaudits müssen KRITIS-Betreiber alle zwei Jahre dem BSI die Umsetzung angemessener Maßnahmen und die Einhaltung der Technikstandards nachweisen, so § 8a III BSIG.

Wie kann die Einhaltung der Maßnahmen nach dem Stand der Technik nachgewiesen werden?

Die Implementierung eines Information Security Management System, kurz ISMS, ist für Betreiber kritischer Infrastrukturen verpflichtend, um die neuen Sicherheitsstandards umsetzen zu können. Eine ISMS bezieht sich nicht nur auf die IT-Sicherheit des Unternehmens, sondern trägt auch zur Optimierung der Unternehmensprozesse und -strukturen bei, um Störungen und Risiken hinsichtlich des Informationssicherheitsmanagements zu reduzieren.

KRITIS-Betreiber können beispielsweise **durch eine Zertifizierung gemäß ISO 27001 mit den zusätzlichen Aspekten der KRITIS-Schutzziele gemäß § 8a BSIG** die Anforderungen des BSI erfüllen.

Eine andere Möglichkeit der Nachweiserbringung besteht darin, einen **vom BSI anerkannten branchenspezifischen Sicherheitsstandard (B3S) oder die Orientierungshilfe des BSI als Prüfgrundlage** zu verwenden.

Neuerungen im IT-Sicherheitsgesetz 2.0

Neue Pflichten für KRITIS-Betreiber

- Systeme zur Angriffserkennung
- kitische Komponenten
- mehr Meldepflichten

Mehr Betreiber in der Pflicht

- neue Sektoren
- sinkende Schwellenwerte
- mehr Anlagenkategorien

Mehr Sanktionen/ Bußgelder

- neue Tatbestände
- höhere Bußgelder
- vorsätzliche oder fahrlässige Verstöße

Mehr Befugnisse für das BSI

- zentrale Meldestelle
- BSI darf Betreiber selbst registrieren
- tiefere Untersuchungen

Warum TÜV NORD?

Wir sind Ihr unabhängiger, neutraler Gesprächspartner und Dienstleister mit über einem Jahrhundert Prüferfahrung. Zutiefst überzeugt von der Wirksamkeit der Zertifizierungen, erarbeiten wir immer wieder neue Lösungsmöglichkeiten und setzen sie mit Ihnen gemeinsam um.

Mit unserem exakt konzertierten Projektmanagement sparen wir Ihnen Zeit durch:

- straff projektierte Auditprogramme
- stringente Vorbewertung Ihrer Systeme und Prozesse
- abgestimmte Audittermine
- individuell vorbereitete, prozessorientierte Auditpläne

Bei Bedarf können wir noch mehr

Neben den Prüfungen der Nachweise bieten wir KRITIS-Betreibern weitere spezielle Dienstleistungen an, die auch kombiniert werden können, um:

- die Managementsysteme und ihre Prozesse noch wirksamer zu machen
- Synergien zu nutzen und den Aufwand für die Koordination und Abwicklung zu optimieren und
- letztlich die Planungs- und Rechtssicherheit zu erhöhen.

Am Anfang können gemeinsame Scoping-Workshops stehen, um die Ausgangssituation zu verstehen und zu analysieren. Dann erfolgt das Maßschneidern entsprechender Audit-Programme, die auf Wunsch auch Vor-Audits beinhalten können. Bei Mehr-Standort-Organisationen geht es darum entsprechende Stichprobenverfahren zu ermöglichen.

Größere und komplexere Vorhaben werden von erfahrenen Projekt-Managern gesteuert, die sich jederzeit um die Bedürfnisse unserer Auftraggeber kümmern; und das dauerhaft. Sie entscheiden, welche unserer Kompetenzen Sie für Ihr Unternehmen nutzen.

In Ergänzung bieten wir Zertifizierungen an nach

ISO 9001

ISO 50001

ISO 27001

und vielen weiteren Normen

Wir sind für Sie da.
Sprechen Sie uns gerne an.

ALEXANDER EBERT
Sales Manager Nord

TÜV NORD CERT GmbH
Große Bahnstraße 31
22525 Hamburg

+49 40 8557 1581
+49 160 888 4177

alebert@tuev-nord.de

ALEXANDER ENGEL
Stellv. Leiter ISMS

TÜV NORD CERT GmbH
Große Bahnstraße 31
22525 Hamburg

+49 40 8557 2312
+49 160 888 5312

alengel@tuev-nord.de

Weitere Informationen zu **KRITIS** und dem neuen **IT-Sicherheitsgesetz 2.0**.

Sie wollen sich weitergehend informieren? Wir bieten Ihnen mit unseren **Webinaren** die Möglichkeit dazu.

TÜVNORD

Inspired by
Knowledge

TÜV NORD CERT
Am TÜV 1
45307 Essen

T 0800 245-7457
F 0511 9986 69-1900

tuev-nord-cert.de

TÜV® 24-0556-03/23

TÜVNORDGROUP