Häufige gestellte Fragen
zur KRITIS-Prüfung

FAQ

KRITIS-Prüfung

Sie möchten Ihr Unternehmen vor IT-Ausfällen und unberechtigten IT-Zugriffen schützen sowie alle Vorgaben gemäß der BSI-KRITIS-Verordnung erfüllen? Aus diesem Grund möchten Sie gern mehr zur Prüfung nach KRITIS und dem IT-Sicherheitskatalog 2.0 erfahren? Nachfolgend haben wir die häufigsten Fragen und Antworten zum Thema für Sie zusammengefasst.

1. Wofür steht KRITIS?

KRITIS steht für „kritische Infrastrukturen" und bezeichnet alle Infrastrukturen, deren Einrichtungen, Anlagen oder Teile aufgrund von Vernetzungsgröße und -grad eine hohe Bedeutung für das staatliche Gemeinwesen haben und bei deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe, Einschränkungen der öffentlichen Sicherheit oder andere dramatische Folgen drohen.

2. Was ist die KRITIS-Verordnung?

Basierend auf dem IT-Sicherheitsgesetz (IT-SiG) von 2015, das 2021 novelliert wurde, ergänzte und erweiterte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Verordnung zu den kritischen Infrastrukturen (KRITIS). Darin wurde festgelegt, dass KRITIS-Betreibende sowohl IT-Systeme als auch KRITIS-Kernkomponenten angemessen zu schützen haben, Ausfälle melden müssen und die Erfüllung der Anforderungen im zweijährigen Turnus nachweisen müssen.

3. Welche Sektoren sind von der KRITIS-Verordnung betroffen?

Folgende Sektoren werden gemäß der aktuellen Gesetzeslage als kritische Infrastrukturen eingestuft:

- Energie (Betrieb, Erzeugung und Versorgung)
- IT und Telekommunikation
- Ernährung
- Wasser/Abwasser
- Transport und Verkehr
- Gesundheit
- Finanz- und Versicherungswesen
- Entsorgung von Siedlungsabfälle
- Unternehmen im besonderen öffentlichen Interesse

4. Welche Ziele verfolgt die KRITIS-Prüfung?

Mit einer KRITIS-Prüfung stellen Sie sicher, dass Ihr Unternehmen alle branchenspezifischen Sicherheitsstandards gemäß der BSI-KRITIS-Verordnung und dem IT-Sicherheitsgesetz 2.0 erfüllt. In diesem Zusammenhang prüfen unsere Sachverständigen, ob alle Sicherheitsziele und deren praktische Umsetzung, in Ihrem Unternehmen gemäß der KritisV und branchenspezifischer Vorgaben erfasst und ausreichend umgesetzt werden.

5. KRITIS-Unternehmen sollen den „Stand der Technik“ einhalten. Was ist damit gemeint und wer legt den aktuellen Stand fest?

Der sogenannte „Stand der Technik“ meint, dass innerhalb eines Unternehmens alle Maßnahmen zum Schutz der IT-Systeme, Komponenten und Prozesse den fortschrittlichsten Verfahren, Ausstattungen und Betriebsweisen entsprechen müssen. Hierbei ist zu beachten, dass der jeweilige aktuelle Stand den entsprechenden nationalen, internationalen und europäischen Normen und Standards entspricht und erfolgreich in der Praxis erprobt wurde.

Konkrete Vorgaben und Leitfäden hierzu werden durch die jeweiligen Branchen im Rahmen der B3S – branchenspezifische Sicherheitsstandards – vorgeschlagen und durch das BSI geprüft und veröffentlicht. Das BSI ist zudem für die weitere Konkretisierung des neuesten „Stands der Technik“ für IT-Sicherheitsprodukte zuständig und besitzt zukünftig auch die Befugnis, selbst Sicherheitsrisiken zu detektieren.

6. Welche Vorteile bringt die KRITIS-Prüfung meinem Unternehmen?

Eine erfolgreiche Prüfung nach KritisV und IT-SiG 2.0 bietet Ihnen eine ganze Reihe von Vorteilen:

- Wirksame Informationssicherheit nach den jeweils gültigen Normen und branchenspezifische Standards (B3S)
- Effizienz und Kostenminimierung durch klare interne Prozesse und Verantwortlichkeiten
- Identifizierung und Beseitigung von Risiken und Schwachstellen
- Hohe Vertrauenswürdigkeit in Ihr Unternehmen bei Partnern, Kunden, Mitarbeitern und Öffentlichkeit
- Wettbewerbsvorteil gegenüber Mitbewerbern bei öffentlichen Ausschreibungen
- BSI-konformer Nachweis über die Erfüllung der Anforderungen gemäß des IT-Sicherheitsgesetzes
- Vermeidung von Bußgeldern durch eventuelle Verstöße

7. Mein Unternehmen verfügt bereits über eine ISO 27001 Zertifizierung. Ist diese ausreichend?

Nein. Die ISO 27001 Zertifizierung kann lediglich als Grundlage für den Nachweis gemäß §8a BSIG verwendet werden. Sie erfasst nicht

automatisch den gesamten relevanten Geltungsbereich (Scope) und deren zugehörige Umsetzungsmaßnahmen, die für den Nachweis notwendig sind. Es besteht hierbei das Risiko, dass relevante Schutzziele kritischer Infrastrukturen nicht ausreichend oder gar nicht erfasst werden. Es ist jedoch möglich eine vorhandene ISO 27001 Zertifizierung zu erweitern. Hierbei werden alle bisher ungeprüften Teile der kritischen Infrastruktur entsprechend der Anforderungen gemäß § 8a (1) und (3) BSIG geprüft, sowie bereits geprüfte Bereiche bezüglich der KRITIS-Schutzziele ergänzend beurteilt. Eine Zertifizierung nach ISO 27001 ist aber nicht zwingend notwendig. Sie haben alternativ auch die Möglichkeit eigene branchenspezifische Sicherheitsstandards (B3S) und Prüfkriterien zu definieren und diese vom BSI prüfen zu lassen. Damit wären ebenfalls alle gesetzlichen Anforderungen erfüllt. Gern unterstützen wir Sie hierbei und bieten Ihnen eine entsprechende Kombination unserer Leistungen an.

8. Wie ist der konkrete Ablauf einer KRITIS-Prüfung?

Die Zertifizierung wird in folgenden Schritten durch unsere Experten durchgeführt:

1. Prüfungsvorbereitung, inklusive der Wahl der Prüfungsgrundlage sowie der Prüfung des Geltungsbereichs
2. Erstellung des Prüfplans
3. Dokumentationsprüfung
4. Vor-Ort-Prüfung
5. Nachbereitung der Vor-Ort-Prüfung
6. Erstellung des Prüfberichts und der Mängelliste

9. Wie lange ist meine Zertifizierung gültig?

Die KRITIS-Zertifizierung ist zwei Jahre gültig und erfordert vor Ablauf von zwei Jahren eine erneute Überprüfung der IT-Sicherheit kritischer Komponenten und Systeme Ihres Unternehmens.

10. Welche relevanten Änderungen gab es mit der Novellierung der KritisV?

Mit der Veröffentlichung des IT-Sicherheitskataloges 2.0 (2021) wurde auch die KRITIS-Verordnung angepasst und erweitert. Die Änderungen umfassen vor allem Schwellenwerte, die in allen betroffenen Sektoren gesenkt wurde, und konkretisiert vorhandene Definitionen. Der Nachweis, dass die eigene Infrastruktur den Anforderungen entspricht, muss bis 1. April 2024 erbracht werden, die Umsetzung von neuen Cyber-Security-Maßnahmen bis 01. Mai 2023 und die Einhaltung der neuen Schwellenwerte bereits seit 2022.

Sie haben weitere Fragen zur KRITIS-Prüfung? Sprechen Sie uns an!

Wünschen Sie weitere Informationen?
Besuchen Sie unsere Website:

dekra-certification.de