Pflichten für KRITIS-Betreiber

+ **Benennung einer Kontaktstelle**
  KRITIS-Betreiber sind verpflichtet gegenüber dem BSI eine Kontaktstelle zu benennen.
+ **Meldepflicht**
  Kommt es zu außergewöhnlichen IT-Störungen oder Sicherheitsvorfällen, müssen diese unverzüglich dem BSI gemeldet werden.
+ **Umsetzung des Stands der Technik**
  Dieser kann über eine Zertifizierung nach ISO 27001, BSI Grundschutz oder einen vom BSI genehmigten brachenspezifischen Sicherheitsstandard (B3S) erfolgen. Die Etablierung eines ISMS ist in manchen Sektoren verpflichtend.
+ **Ausarbeitung von Notfallplänen**
  Um die Versorgungssicherheit sicherzustellen, sind Betreiber verpflichtet, Maßnahmenkataloge auszuarbeiten und Prozesse zu etablieren, die dazu geeignet sind, Störungen schnellstmöglich zu beseitigen.
+ **Regelmäßige Sicherheitsaudits**
  Die Einhaltung des aktuellen technischen Stands und die allgemeine Sicherheit der eingesetzten Systeme und Dienste müssen alle zwei Jahre durch ein Sicherheitsaudit gegenüber dem BSI nachgewiesen werden.
+ **Nutzung von Systemen zur Angriffserkennung und zum Monitoring**
  Systeme zur Angriffserkennung und geeignete Monitoringsysteme, wie etwa ein SIEM, gehören ausdrücklich zu den technischen und organisatorischen Sicherheitsvorkehrungen, die ein Betreiber treffen muss.
+ **Meldung kritischer Komponenten**
  Werden durch Gesetz definierte kritische Komponenten eingesetzt, ist deren Verwendung anzuzeigen.

KORAMIS
Cybersecurity by telent

telent GmbH
Gerberstraße 34
71522 Backnang
Tel.: +49 7191 900-0
E-Mail: info.germany@telent.de

telent
service • commitment • value

www.telent.de

Copyright © telent GmbH. Alle Rechte vorbehalten.

Kritische Infrastrukturen vor neuen Herausforderungen

Sicherheitslösungen für KRITIS-Betreiber

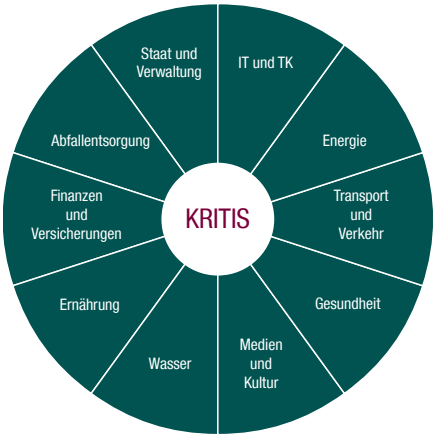
Durch Anpassungen der bestehenden IT-Sicherheitsgesetze und die Ausweitung der KRITIS-Sektoren ändern sich auch die Sicherheitsanforderungen an Betreiber Kritischer Infrastrukturen. Wir bieten mit unserer Marke „KORAMIS - Cybersecurity by telent“ umfassende Security-Lösungen und -Services, um unter die KRITIS-Gesetzgebung fallenden Unternehmen höchstmöglichen Schutz, bei gleichzeitiger Erfüllung der aus den Regularien ergehenden Anforderungen, zu bieten.

Was bedeutet KRITIS?

Der Gesetzgeber definiert KRITIS folgendermaßen:

„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.“

Derzeit werden zehn Sektoren den Kritischen Infrastrukturen zugerechnet. Damit fallen Unternehmen aus diesen Sektoren erst einmal unter die Bestimmungen des *Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme* - kurz auch IT-SiG 2.0 - und der dem Gesetz zugehörigen Verordnungen.



KRITIS Sektoren

Mit dem IT-SiG 2.0 fallen, unabhängig von der Zugehörigkeit zu den KRITIS-Sekoren, weitere „Unternehmen im besonderen öffentlichen Interesse (UNBÖFI)“ und gegebenenfalls deren Zulieferer, unter die KRITIS-Gesetzgebung.
Hierzu zählen insbesondere die Rüstungsindustrie und Unternehmen, sowie deren Zulieferer, denen eine erhebliche volkswirtschaftliche Bedeutung beigemessen wird.
Ebenso unter die UNBÖFI fallen Unternehmen, die im Gefahrstoffbereich der oberen Klasse tätig sind.
Diese Unternehmen sind dazu verpflichtet, bestimmte Auflagen hinsichtlich der IT-Sicherheit zu erfüllen.
Ob ein Unternehmen unter die KRITIS-Gesetzgebung fällt und die Auflagen erfüllen muss, wird anhand einer Schwellenwertanalyse festgestellt.

KRITIS-Einordnung durch Schwellenwertanalyse

Gehört eine Anlage oder Teile davon zu den Kritischen Infrastrukturen, sind für sie Schwellenwerte festgelegt, bei deren Erreichen oder Überschreiten die KRITIS-Gesetzgebung greift. Diese Schwellenwerte sind sektorabhängig und betreffen z. B. die Trinkwassermenge in Millionen m^3/Jahr oder die Anzahl der Teilnehmer eines bestimmten Dienstes.

Bei der Schwellenwertanalyse setzt telent eine dreistufige Methodik ein:

1. Wir identifizieren die kritischen Dienstleistungen, die bei „Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen“ würden (vgl. BSI-KritisV, Paragraf 1).

2. Daraufhin werden die dafür notwendigen Anlagen bestimmt.

3. Abschließend können die Betreiber der Anlagen anhand der Schwellenwerte erkennen, ob ihre Anlage als kritische Infrastruktur einzustufen ist oder nicht.

Die Anhänge der Rechtsverordnung liefern tabellarische Angaben für alle Anlagentypen inklusive Schwellenwerte. Allerdings gibt es auch Branchen, für die es keine Schwellenwerte gibt; sie werden durch ihre Systeme identifiziert, wie z. B. die Verkehrssteuerungs- und Leittechnik für das Netz der Bundesautobahnen.

Lösungs- und Serviceportfolio von telent

telent stellt ein komplettes Portfolio von Produkten und Dienstleistungen bereit, mit deren Hilfe Betreiber von KRITIS den besonderen Sicherheitsanforderungen und Nachweispflichten gerecht werden können:

+ **Risiko- und Schwachstellenanalyse**
  Mit der Risikoanalyse werden Risiken bezüglich der IT-Sicherheit identifiziert und Maßnahmen abgeleitet, um nicht akzeptable Risiken zu reduzieren und zu kontrollieren. Wir unterstützen Sie über den gesamten Prozess: von der Analyse des IST-Zustandes bis hin zu Definitionen von Maßnahmen, bei der Abschätzung der Restrisiken bis hin zur kontinuierlichen Verbesserung der Sicherheitsarchitektur. Wir stützen uns dabei auf Standards, wie den ISO/IEC 27005 oder IEC 62443-3 und auf Best Practices.
  Die Schwachstellenanalyse hilft, die Sicherheit Ihrer technischen Anlagen und Prozesse und so den tatsächlichen Sicherheitsstand Ihrer Infrastruktur zu bestimmen. Schwachstellen werden dokumentiert und bewertet. Abweichungen von relevanten Sicherheitsstandards oder individuellen Vorgaben werden ausgewiesen und darauf aufbauend ein Maßnahmenplan erstellt.

+ **Informationssicherheitsmanagementsystem (ISMS)**
  Wir unterstützen Sie bei der Einführung und dem Aufbau Ihres ISMS. Dabei begleiten wir Sie von der Planung bis hin zum Regelbetrieb. Unsere Leistungen umfassen eine Definition der Regeln, Methoden und Abläufe zur Gewährleistung, Steuerung und Kontrolle der Informationssicherheit. Damit ist sichergestellt, dass Sie sich stets auf dem aktuellen Stand von gesetzlichen und regulatorischen Vorgaben und Technik befinden.
  Bei der Etablierung berücksichtigen wir Branchenstandards, Anforderungen aus den einschlägigen Normen, wie etwa ISO 27001, ISO 27019, IEC 62443, und natürlich Anforderungen aus dem BSI-Grundschutz.

+ **Systeme zur Angriffserkennung**
  Um den Betrieb hochkomplexer Systeme und Netzwerke zu gewährleisten, bedarf es eines Überblicks über die Assets. Zudem muss das Netzwerk fortlaufend überwacht werden, um Bedrohungen, fehlerhafte Kommunikation und kritische Schwachstellen jederzeit identifizieren und ein Höchstmaß an Netzwerksicherheit sicherstellen zu können. Genau hier setzt die Idee der Angriffserkennung, auch als Anomaly Detection bekannt, ein. Wir unterstützen Sie bei der Auswahl, Implementierung, Inbetriebnahme und optional auch dem Betrieb eines zu Ihren Anforderungen passenden Systems zur Angriffserkennung.

+ **SIEM / SOC - Managed Security Services**
  IT-Security stellt für mittelständische Unternehmen und Organisationen oftmals eine kaum zu bewältigende Aufgabe dar. Die damit verbundenen Kosten, Risiken und organisatorischen Herausforderungen sind unverhältnismäßig hoch. Mit unserer spezialisierten Marke „KORAMIS - Cybersecurity by telent“ unterstützen wir Sie bei den zu bewerkstelligenden Aufgaben und bieten 24/7-Lösungen und -Services.

+ **Sicherheits-Audit und Rezertifizierung**
  Wir unterstützen Unternehmen nicht nur beim Aufbau und der Aufrechterhaltung eines ISMS-Regelbetriebs nach ISO / IEC 27001, B3S oder Grundschutz, sondern begleiten diese bei allen Maßnahmen bis hin zum Audit durch eine anerkannte Prüfstelle.