TÜV Rheinland: Neue Sicherheitsvorgaben für KRITIS-Unternehmen berücksichtigen

Oct 5, 2021 | Industrie & Digitalisierung

Kritische Infrastrukturen: IT-Sicherheitsgesetz 2.0 und KRITIS-Verordnung verabschiedet / Betroffene Unternehmen müssen Schutz kritischer Infrastrukturen gewährleisten / Analyse möglicher Lücken hilft bei Bestandsaufnahme / Informationen unter www.tuv.com/fscs-de

Ansprechpartner:

Norman Hübner
Pressesprecher IT und Cybersecurity
+49 221 806-3060
norman.huebner@de.tuv.com

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme ist bekannt als IT-Sicherheitsgesetz. Dieses zielt auf Betreiber von kritischen Infrastrukturen (KRITIS) ab – also auf Unternehmen, die eine wesentliche Rolle in der Versorgung der Bevölkerung mit wichtigen Gütern und Dienstleistungen spielen. Dazu gehören unter anderem Einrichtungen aus den Bereichen Energie, Gesundheit, Trinkwasserversorgung oder Transport und Verkehr. Das IT-Sicherheitsgesetz, das seit Mai 2021 in der neuesten Fassung 2.0 gilt, verpflichtet Unternehmen und Organisationen zur Einhaltung eines Mindestmaßes an IT-Sicherheit, die dem Stand der Technik entsprechen. Die neue Fassung setzt zudem in Sachen Cybersecurity ab 2023 eine Angriffserkennung voraus. Das ist im Bereich operativer Betriebstechnik (auch Operational Technology, kurz OT) von besonderer Bedeutung. OT bezeichnet Anlagen, Geräte oder Systeme, die industrielle Prozesse steuern.

Zahl der KRITIS-Betreiber steigt

Neu ist auch die Mitte August 2021 verabschiedete KRITIS-Verordnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die Verordnung tritt am 1. Januar 2022 in Kraft und erweitert den Geltungsbereich für in Frage kommende Unternehmen. Die entscheidende Neuerung ist der erweiterte Anwendungsbereich: Zu den bestehenden etwa 1.600 KRITIS-Betreibern werden weitere 250 Unternehmen hinzukommen. Unternehmen, die zuvor nicht betroffen waren, müssen jetzt höhere Anforderungen an den Schutz vor Hackerangriffen erfüllen und stehen damit vor neuen Herausforderungen.

Richtlinien des BSI

Eine Orientierung dazu, wie die erforderlichen Maßnahmen konkret aussehen, geben Dokumente des BSI. Dazu gehören die „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“ sowie die „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifischen Sicherheitsstandards (B3S)“. Diese Leitlinien liefern wertvolle Hilfestellungen für die Auswahl und konkrete Umsetzung von Sicherheitsmaßnahmen. „Die Dokumente helfen bei der Interpretation der sehr allgemein gehaltenen Vorgaben im IT-Sicherheitsgesetz und spielen damit eine wichtige Rolle bei der Konzeption und Planung eines KRITIS-Umsetzungsprojektes“, sagt Jörg Zimmermann, Fachmann für Informationssicherheit bei TÜV Rheinland. „Unternehmen, die vor einer solchen Aufgabe stehen, empfehlen wir, sich Experten zur Unterstützung ins Haus zu holen.“

Bestandsaufnahme und GAP-Analyse

Stellen Unternehmen fest, dass sie von der neuen KRITIS-Verordnung betroffen sind, empfiehlt TÜV Rheinland, eine Bestandsaufnahme und eine so genannte GAP-Analyse durchzuführen: Die Fachleute können durch eine solche Analyse mögliche Lücken zwischen dem Ist- und dem Soll-Zustand detailliert erfassen und bewerten. Auch kann auf diese Weise die Frage des betroffenen Geltungsbereichs in Organisationen und Einrichtungen näher beleuchtet werden. Um KRITIS-fest zu werden, müssen Unternehmen und Organisationen alle möglichen Risiken aufzeigen und dokumentieren sowie entsprechende Sicherheitsmaßnahmen umsetzen. Sobald klar ist, welche Maßnahmen umgesetzt werden sollen, ist eine zielgerichtete Kommunikation an die Belegschaft wichtig, da in der Regel alle Bereiche des Unternehmens betroffen sind.

Dazu Zimmermann: „Ein KRITIS-Projekt ist kein IT-Projekt, sondern ein Organisationsprojekt, in das alle Unternehmensbereiche integriert werden müssen. Es ist nicht damit getan, das Thema allein an die IT zu geben.“ Die erfolgreiche und wirksame Umsetzung von Sicherheitsmaßnahmen muss alle 2 Jahre durch ein Audit nachgewiesen werden. „Besonders Unternehmen, die sich bisher nicht haben zertifizieren lassen, müssen sich gründlich auf diese Audits vorbereiten und sollten vorab ein Test-Audit durchführen“, empfiehlt Zimmermann.

Weitere Informationen zum Thema kritische Infrastrukturen und Cybersecurity im OT-Umfeld gibt es unter www.tuv.com/fscs-de bei TÜV Rheinland.

Sicherheit und Qualität in fast allen Wirtschafts- und Lebensbereichen: Dafür steht TÜV Rheinland. Mit mehr als 20.000 Mitarbeiterinnen und Mitarbeitern und einem Jahresumsatz von 2 Milliarden Euro zählt das vor rund 150 Jahren gegründete Unternehmen zu den weltweit führenden Prüfdienstleistern. Die hoch qualifizierten Expertinnen und Experten von TÜV Rheinland prüfen rund um den Globus technische Anlagen und Produkte, begleiten Innnovationen in Technik und Wirtschaft, trainieren Menschen in zahlreichen Berufen und zertifizieren Managementsysteme nach internationalen Standards. Damit sorgen die unabhängigen Fachleute für Vertrauen entlang globaler Warenströme und Wertschöpfungsketten. Seit 2006 ist TÜV Rheinland Mitglied im Global Compact der Vereinten Nationen für mehr Nachhaltigkeit und gegen Korruption.
Website: www.tuv.com