TÜV Süd

KRITIS-Strukturen bis Mai sichern

[04.04.2023] Ab 1. Mai 2023 müssen Systeme zur Angriffserkennung implementiert und von unabhängiger Seite geprüft sein. Darauf weist der TÜV Süd hin.

KRITIS-Betreiber müssen Systeme zur Angriffserkennung etablieren, um ihre Widerstandsfähigkeit gegen Cyber-Attacken zu verbessern. Das schreibt das IT-Sicherheitsgesetz 2.0 vor. Für die Betreiber ist Eile geboten, denn das Gesetz verlangt einen Nachweis der unabhängigen Prüfung der Systeme, so der TÜV Süd.

Das „Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“, oft auch als IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) bezeichnet, mit dem BSIG und EnWG geändert wurden, hat entsprechende Regelungen geschaffen. Nach dem IT-SiG 2.0 müssen betroffene Unternehmen bis zum 1. Mai 2023 ein solches System etablieren. Zudem sind KRITIS-Betreiber dazu verpflichtet, die neuen Systeme von unabhängiger Seite prüfen zu lassen und dem Bundesministerium für Sicherheit in der Informationstechnik (BSI) einen entsprechenden Nachweis der Funktionstüchtigkeit vorzulegen.

Das IT-SiG 2.0 wurde im April 2021 verabschiedet. Es dient der Modernisierung und Verbesserung informationstechnischer Systeme von KRITIS-Betreibern. Das Gesetz verpflichtet die Betreiber dazu, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Das IT-Sicherheitsgesetz 2.0 ergänzt § 8a BSIG um den Absatz 1a, der ausdrücklich den Einsatz von Systemen zur Angriffserkennung als effektive Maßnahme zur frühzeitigen Erkennung von Cyber-Angriffen sowie zur Schadensreduktion und Schadensvermeidung fordert.

Betreiber von Energieversorgungsnetzen und Energieanlagen, die nach § 10 Absatz 1 BSIG als Kritische Infrastruktur gelten, müssen zum 1. Mai 2023 ein implementiertes System zur Angriffserkennung (SzA) gemäß § 11 Absatz 1f EnWG nachweisen. Diese Frist gilt unabhängig von laufenden oder geplanten Zertifizierungsverfahren nach den IT-Sicherheitskatalogen der Bundesnetzagentur. Grundsätzlich gilt, dass die regelmäßig zu erbringenden Nachweise der KRITIS-Betreiber ab diesem Datum auch eine Aussage zu SzA enthalten müssen.

„Kritische Infrastrukturen stehen mehr denn je im Fokus von Hackern – das gilt für kommunale Wasserversorger genauso wie für bundesweite Stromanbieter“, sagt Alexander Häußler, Global Product Performance Manager IT and Lead Auditor der TÜV SÜD Management Service GmbH.

(ur)

Weitere Informationen zu Prüfungen und Zertifizierungen von TÜV SÜD KRITIS-Betreiber gibt es hier.

Stichwörter: Informationstechnik, KRITIS-Strukturen´