Pressemitteilung

Wichtige Frist für KRITIS-Betreiber

30. März 2023

Ab 1. Mai 2023 müssen Systeme zur Angriffserkennung implementiert und von unabhängiger Seite geprüft sein

München. 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.

TÜV SÜD erinnert die Betreiber von Kritischen Infrastrukturen (KRITIS) daran, dass die Frist zur Implementierung von Systemen für Angriffserkennung (SzA) in Kürze ausläuft. Das „Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“, oft auch als IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) bezeichnet, mit dem u.a. 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. „Die verpflichtende Einführung von Systemen zur Angriffserkennung ist die logische Reaktion auf diese Entwicklung, denn diese Systeme erhöhen die Widerstandsfähigkeit der Betreiber – sofern sie richtig aufgesetzt und betrieben werden.“ Damit der Nachweis fristgemäß erfolgen kann, rät Häußler den Betreibern dazu, so schnell wie möglich aktiv zu werden und die Funktionstüchtigkeit der SzA von unabhängigen Experten prüfen und bestätigen zu lassen, wie das im Gesetz vorgeschrieben ist.

Weitere Informationen zu Prüfungen und Zertifizierungen von TÜV SÜD KRITIS-Betreiber gibt es unter www.tuvsud.com/ms-kritis.

Hinweis für Redaktionen: Die Pressemeldung und das Bild von Alexander Häußler in reprofähiger Auflösung gibt es unter www.tuvsud.com/presse

Pressekontakt:

Sabine Krömer TÜV SÜD AG Unternehmenskommunikation Westendstr. 199, 80686 München	Tel. +49 (0) 89 / 57 91 – 29 35 Fax +49 (0) 89 / 57 91 – 22 69 E-Mail sabine.kroemer@tuvsud.com Internet www.tuvsud.com/de

Im Jahr 1866 als Dampfkesselrevisionsverein gegründet, ist TÜV SÜD heute ein weltweit tätiges Unternehmen. Mehr als 25.000 Mitarbeiter sorgen an über 1.000 Standorten in rund 50 Ländern für die Optimierung von Technik, Systemen und Know-how. Sie leisten einen wesentlichen Beitrag dazu, technische Innovationen wie Industrie 4.0, autonomes Fahren oder Erneuerbare Energien sicher und zuverlässig zu machen. www.tuvsud.com/de