TÜV Rheinland: IT-Sicherheitsgesetz schützt kritische Infrastruktur

02.06.2020 | Köln

Energie, Transport und Verkehr, Ernährung oder Gesundheit sind Beispiele für kritische Infrastrukturen (KRITIS). Dienstleistungen, die zwingend für die Versorgung der Bevölkerung benötigt werden. Zu vier Fünfteln werden sie, laut Bundesamt für Sicherheit in der Informationstechnik (BSI), von privaten Unternehmen erbracht. „Auch kritische Infrastrukturen erfahren eine zunehmende Digitalisierung und Vernetzung und müssen aufgrund ihrer Bedeutung ganz besonders durch moderne Cybersecurity geschützt werden“, sagt Wolfgang Kiener, Leiter des Center of Excellence Advanced Threat im Bereich Cybersecurity bei TÜV Rheinland. Dabei im Fokus: die operationale Betriebstechnik, auch Operational Technology (OT) genannt. Denn IT-Standards reichen zur Risikobewertung nicht aus. Die Sicherheitslücken sind zahlreich und die Angriffe durch Cyberkriminelle häufen sich.

Schadsoftware kann

Produktionsanlagen zerstören

Der Triton-Angriff auf die Ölindustrie in Saudi-Arabien aus dem Jahr 2017 zeigt, welchen Risiken kritische Infrastrukturen ausgesetzt sind. Der Virus wurde eigens für ein spezielles Steuerungsmodul entwickelt, das weltweit in Kraftwerken zum Einsatz kommt. Bleibt er unentdeckt, kann er ganze Produktionsanlagen zerstören, Menschenleben gefährden oder sogar Umweltkatastrophen hervorrufen. Mit dem seit Juli 2015 gültigen IT-Sicherheitsgesetz sollen kritische Infrastrukturen in Deutschland besser geschützt werden. Es legt unter anderem fest, dass Betreiber erhebliche IT-Störungen beim BSI melden müssen. Zudem muss eine zu jeder Zeit erreichbare Kontaktstelle benannt werden, über die beispielsweise Sicherheitsinformationen des Ministeriums übermittelt werden können.

Nachweis über erforderliche Maßnahmen

Das IT-Sicherheitsgesetz schreibt außerdem den stets aktuellen Stand der Technik der jeweiligen Anlage vor sowie einen Nachweis über alle erforderlichen Maßnahmen, der alle zwei Jahre zu erbringen ist. In beiden Fällen können unabhängige Prüfdienstleister wie TÜV Rheinland zurate gezogen werden. „Wir unterstützen Unternehmen bei der Umsetzung eines ganzheitlichen Cybersecurity-Managements. Unsere Experten wissen, wie sich Unternehmen auch vor komplexen Cyberangriffen schützen können“, so Kiener. Etwa beim Aufbau und Betrieb von Leitständen zum Überwachen, Erkennen und Beheben von Cyberangriffen vor allem in der operationalen Betriebstechnik. Diese Fähigkeiten sind in kritischen Infrastrukturen unabdingbar, um größere Schäden und Katastrophen zu verhindern.

Mehr Informationen rund um das Thema Operational Technology und Cybersecurity stehen unter www.tuv.com/fscs-de zur Verfügung.

Kontakt für Journalisten: Norman Hübner
Telefon: +49 221 806 - 3060
E-Mail: norman.huebner@de.tuv.com

****

TÜV Rheinland ist ein weltweit führender unabhängiger Prüfdienstleister mit fast 150 Jahren Tradition. Im Konzern arbeiten über 20.000 Menschen rund um den Globus. Sie erwirtschaften einen Jahresumsatz von 2 Milliarden Euro. Die unabhängigen Fachleute stehen für Qualität und Sicherheit von Mensch, Technik und Umwelt in fast allen Wirtschafts- und Lebensbereichen. TÜV Rheinland prüft technische Anlagen, Produkte und Dienstleistungen, begleitet Projekte, Prozesse und Informationssicherheit für Unternehmen. Die Experten trainieren Menschen in zahlreichen Berufen und Branchen. Dazu verfügt TÜV Rheinland über ein globales Netz anerkannter Labore, Prüfstellen und Ausbildungszentren. Seit 2006 ist TÜV Rheinland Mitglied im Global Compact der Vereinten Nationen für mehr Nachhaltigkeit und gegen Korruption.

Website www.tuv.com