Digitale Sicherheit für überwachungsbedürftige Anlagen

Cybersicherheit ganzheitlich denken und umsetzen

Während zahlreiche neue regulatorische Anforderungen für Cybersicherheit entstehen, fehlt in der Praxis oft ein koordinierter Ansatz, der verschiedene Schutzziele vereint und unterschiedliche Nachweispflichten integriert. Zugelassene Überwachungsstellen leisten ihren Beitrag zur rechtssicheren und wirtschaftlichen Umsetzung komplexer Vorgaben.

Betreiber überwachungsbedürftiger Anlagen müssen ihre Daten vor Cyberangriffen schützen, an erster Stelle aber die Sicherheit von Menschen im Umfeld ihrer Anlagen gewährleisten. Und das auch nachweisen – am besten nur einmal. Die Realität sieht allerdings mitunter anders aus.

Regelmäßig berichteten Betreiber von Mehrfachanforderungen aus verschiedenen Regulierungsbereichen, sagt Jörg Becker, Leiter des Kompetenzzentrums für Cybersicherheit bei TÜV SÜD Industrie Service. Dies führe zu Verwirrung. Das Problem: Je nach Anlagentyp und Branche müssen verschiedene Regulierungsbereiche berücksichtigt werden – von den Anforderungen an die kritische Infrastruktur und die kommende NIS2-Regulierung über die Störfallverordnung bis hin zu den Regeln für Betriebssicherheit wie der TRBS 1115 Teil 1.

Jede dieser Vorschriften stellt Anforderungen an die Cybersicherheit – allerdings mit unterschiedlichen Schwerpunkten. Becker: „Das grundsätzliche Konzept in den verschiedenen Rechtsgebieten ist zwar identisch, doch die konkreten Anforderungen sind teilweise sehr unterschiedlich." Der Grund hierfür liegt in den jeweiligen Schutzzielen, die mit den Anforderungen an die Cybersicherheit erreicht werden sollen. „Je nach Regulierung werden die klassischen Grundschutzziele – Vertraulichkeit, Integrität und Verfügbarkeit – unterschiedlich gewichtet", erklärt Becker. Das könne in Einzelfällen sogar zu widersprüchlichen Anforderungen führen: Während aus Arbeitssicherheitsperspektive eine sofortige Abschaltung im Gefahrenfall optimal wäre, steht dies im Widerspruch zu Anforderungen an eine kritische Infrastruktur, die auf Verfügbarkeit und Kontinuität ausgerichtet sei.

Sicherheitsrisiken in KMU häufig unterschätzt

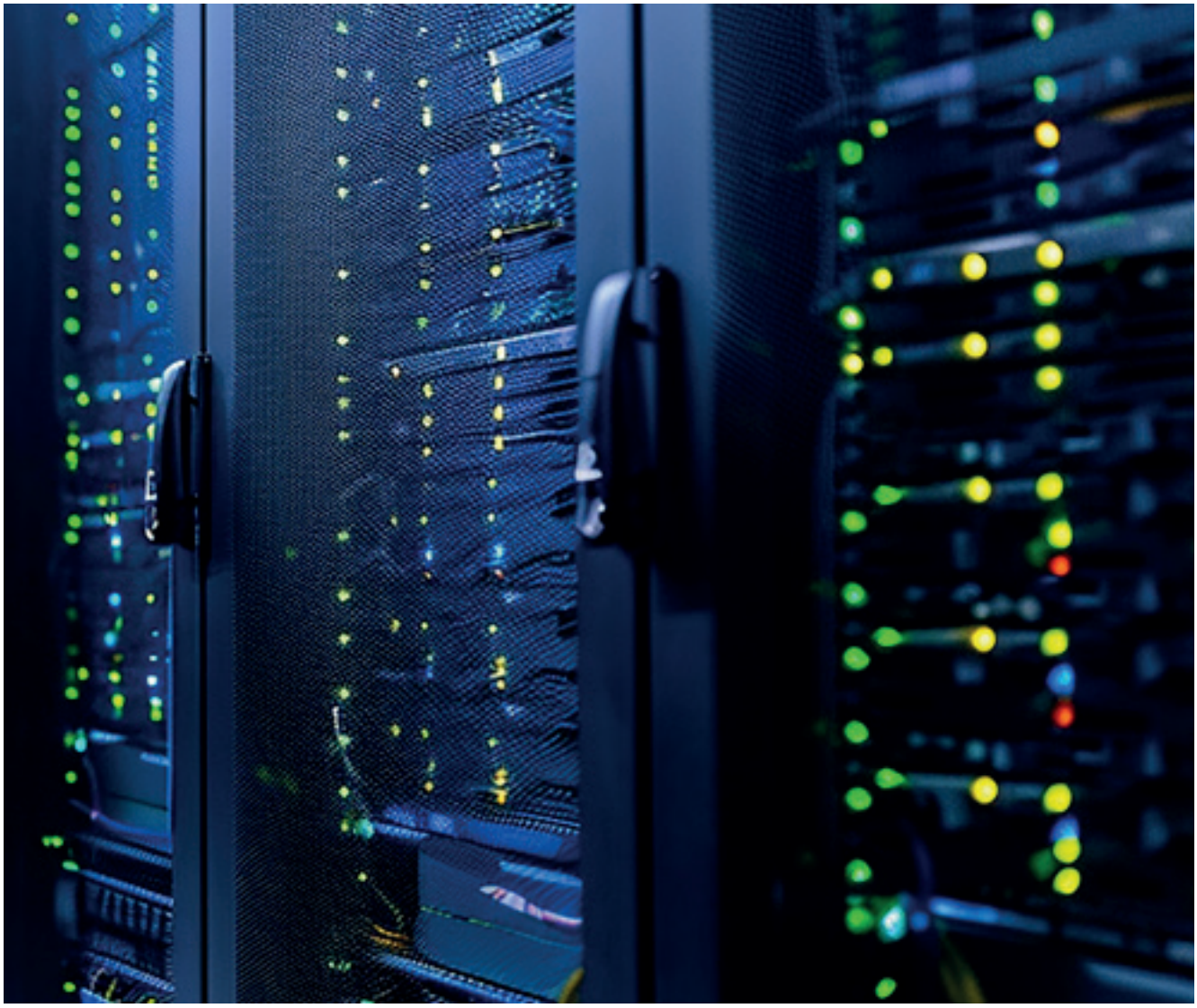
Während das allgemeine Bewusstsein für Cybersicherheit in den vergangenen Jahren deutlich gewachsen ist, zeigt sich in der Praxis noch eine erhebliche Diskrepanz zwischen dem Wissen und der konkreten Umsetzung von Schutzmaßnahmen. Boris Göppert, Leiter des Competence Centers Elektro- und Tanktechnik der TÜV

NORD Systems GmbH & Co. KG stellt immer wieder fest, dass Unternehmen die Bedeutung digitaler Sicherheit immer noch unterschätzen. Das gilt nach seiner Einschätzung vor allem für kleine und mittlere Unternehmen (KMU). Viele Betriebe argumentieren mit der fehlenden direkten Internetanbindung ihrer Produktionssysteme und leiten daraus irrtümlich ab, nicht von Cyberattacken betroffen sein zu können. „Dabei werden indirekte Angriffswege über Wartungsrechner, USB-Sticks oder temporäre Verbindungen unterschätzt", sagt Göppert. „Zudem können eigene Mitarbeiter oder Mitarbeiter von Wartungsfirmen unbeabsichtigt Sicherheitsrisiken schaffen, wenn sie mit kompromittierten Werkzeugen arbeiten."

Der ganzheitliche Ansatz als Schlüssel

Angesichts der vielfältigen Anforderungen und des Mangels an verfügbaren Experten im Bereich der industriellen Cybersicherheit stellt sich die Frage: Wie können Betreiber effizient und rechtskonform handeln und die Nachweisführung gestalten, ohne sich in den verschiedenen Regulierungsbereichen zu verlieren? Der Schlüssel dafür ist ein ganzheitlicher Cybersicherheitsansatz. „Der grundlegende Prozess der Cybersicherheit folgt immer den gleichen Schritten", so Jörg Becker. Zunächst werden relevante Anlagen und Systeme identifiziert. Dann folgt eine Einschätzung des Schutzbedarfs auf Basis einer Analyse möglicher Bedrohungen und ihrer potenziellen Auswirkungen, bevor die nötigen Cybersicherheitsmaßnahmen festgelegt und umgesetzt werden.

Wenn Betreiber einen Prozess etablieren, der von vornherein alle relevanten Schutzziele und regulatorischen Anforderungen integriert, können sie erhebliche Synergien nutzen. Konkret



bedeutet das: Die grundlegenden Prozessschritte der Cybersicherheit – von der Identifizierung schutzwürdiger Anlagen und Systeme, über die Risikoanalyse und die Festlegung von Schutzmaßnahmen bis zur Implementierung und Überprüfung – müssen in weiten Bereichen nur einmal durchlaufen werden. „Trotz der Vorteile wird dieser integrale Ansatz in der Praxis bisher kaum genutzt", berichtet Jörg Becker. Meist scheitere die Umsetzung daran, dass die spezifischen Anforderungen der verschiedenen Regulierungsbereiche nicht konkret genug berücksichtigt werden.

Prüforganisationen als Brückenbauer

Zugelassene Überwachungsstellen (ZÜS) stehen vor der Herausforderung, die Cybersicherheit von Anlagen prüfen zu müssen und gleichzeitig den Aufwand für die Betreiber der Anlagen möglichst gering zu halten. Die ZÜS müssen sicherstellen, dass alle relevanten Punkte abgedeckt sind – im Idealfall, ohne diese mehrfach bei derselben Anlage nach unterschiedlichen Regelwerken zu prüfen.

Das entspricht auch dem Selbstverständnis einer ZÜS, die für Sicherheit eintritt und durch optimierte Prüfprozesse Brücken zwischen rechtlichen Anforderungen und praxisnahen Prozessen der Betreiber baut. Denn systemische Ineffizienzen demotivieren letztlich alle Beteiligten und beeinträchtigen die inhaltliche Qualität des Vorgehens und dadurch die Sicherheit der Anlagen.

Boris Göppert unterstreicht die grundsätzliche Ausrichtung der Prüfdienstleister auf Effizienz und fachlich hochwertige Aussagen. Bei Audits liege der Fokus auch darauf, ob die Betreiber in ihren Risikoanalyseprozessen die verschiedenen regulatorischen An-

forderungen bereits integriert hätten. „Nicht selten besteht hier noch Optimierungspotenzial, das im Rahmen einer Prüfung aufgedeckt wird."

Pragmatisch und zielgerichtet vorgehen

Vor dem Hintergrund der komplexen Anforderungen ist die Auswahl pragmatischer Ansätze für die Cybersicherheit entscheidend. Jörg Becker vergleicht die Situation mit dem Erstellen eines universellen Kochbuchs – ein umfassendes Werk für alle Anwendungsfälle wäre unvermeidlich sehr umfangreich. Wer sich hingegen auf grundlegende Zutaten konzentriert und wie diese in Kombination funktionieren, kann bereits eine Menge Gerichte auf den Tisch bringen. Boris Göppert sagt dazu: „Wir müssen immer das Ziel im Blick behalten und dürfen uns nicht in Detaildiskussionen verlieren".

Einen zielgerichteten Zugang zur Cybersicherheit bieten die sechs fundamentalen Themen, die in der Technischen Regel für Betriebssicherheit 1115 Teil 1, Kapitel 4.5.2 (2) aufgeführt sind: Segmentierung und Fernzugriff, Zugangs- und Zugriffsschutz, Härtung von Komponenten, Unabhängigkeit von sicherheitsrelevanten Mess-, Steuer- und Regelungseinrichtungen sowie Überwachung und Notfallmanagement – verbunden mit dort genannten Grundprinzipien der Cybersicherheit.

Zusätzlich wird nun die TRBS 1115 Teil 1 um einen Anhang erweitert, der Betreibern eine erhebliche praktische Hilfe sein dürfte. „In diesem Anhang werden beispielhaft Maßnahmen dargestellt, wie sich Cybersicherheit bei überwachungsbedürftigen Anlagen umsetzen lässt, unabhängig davon, ob es sich um einen Aufzug oder eine Druckanlage handelt", erklärt Boris Göppert. „Entscheidend ist nur, welchen Grad der Vernetzung ein System hat." Das Spektrum reicht von isolierten Inselsystemen über Anlagen mit temporären Verbindungen bis hin zu vollständig vernetzten Systemen. Der Anhang zur TRBS 1115 Teil 1 erfasst alle Konstellationen und beschreibt die dafür nötigen grundlegenden Cybersicherheitsmaßnahmen.

Eine weitere Erleichterung bringt der europäische Cyber Resilience Act (CRA). Künftig werden Betreiber auf Produkte zurückgreifen können, bei denen der Hersteller bereits ein gewisses Maß an Cybersicherheit integriert hat. Aber Boris Göppert warnt: „Einerseits gibt es dann Produkte mit gewissen Sicherheitsgarantien, andererseits sind damit nicht automatisch alle Betreiberpflichten abgedeckt." Seine Wirkung wird der CRA wegen langer Übergangsfristen allerdings erst ab Ende 2027 entfalten.

Verantwortungsvoll handeln, Effizienz ermöglichen

Cybersicherheit ist kein einmaliges Projekt, sondern ein fortlaufender Prozess. Betreiber überwachungsbedürftiger Anlagen sollten einen integrativen Ansatz verfolgen, der alle relevanten Schutzziele berücksichtigt, eine effiziente Dokumentation ermöglicht und eine kontinuierliche Weiterentwicklung zulässt. Das erfordert bewusste Entscheidungen, welche Vernetzung von welchen Anlagen wirklich notwendig ist. „Zusätzlicher Komfort durch vernetzte Systeme bedeutet immer einen zusätzlichen Aufwand für Cybersicherheit", gibt Jörg Becker hierzu zu bedenken.
Eine weitere zentrale Voraussetzung für effektive Cybersicherheit ist die Koordination zwischen den verschiedenen Aufsichtsbehörden. Eine unstrukturierte Umsetzung von Anforderungen aus unterschiedlichen Rechtsgebieten kann die Implementierung und den Nachweis von Schutzmaßnahmen erheblich erschweren. Die Prüforganisationen setzen sich auch in Zukunft für verständliche, koordinierte und zielgerichtete Regelwerke ein, die praxistauglich sind und sich wirtschaftlich umsetzen lassen. Eine zwischen den verschiedenen Rechtsakten abgestimmte Cybersicherheitsregulierung reduziert Aufwände bei Betreibern und Prüforganisationen und trägt damit maßgeblich zum Bürokratieabbau bei.