weyer gruppe

komplett. durchdacht.

CYBER SECURITY

Mit den vielen Vorteilen, die die Digitalisierung mit sich bringt, werden jedoch auch die negativen Aspekte immer sichtbarer: Hackerangriffe auf vernetzte Systeme nehmen zu und stellen eine zunehmende Bedrohung dar. Infolgedessen hat der Gesetzgeber reagiert und Cyber Security zunehmend in Gesetze aufgenommen, die für Betreiber und Hersteller von entscheidender Relevanz sind. Diese rechtlichen Vorgaben sollen dazu beitragen, die Sicherheit in einer zunehmend digitalisierten und vernetzten Welt zu gewährleisten.

Die zunehmende Integration von IT (Information Technology), OT (Operational Technology) und die Vernetzung verschiedenster Systeme untereinander – das Internet of Things (IoT) – sind zentrale Themen unserer Zeit. Diese Entwicklungen sind nicht nur aus der Sicht von Entwicklern von großer Bedeutung, sondern rücken auch die Sicherheit dieser Systeme – insbesondere die IT- und OT-Sicherheit sowie die allgemeine Cyber Security von Produktionsanlagen – in den Fokus.

Überblick über die rechtlichen Grundlagen der Analyse

Die Analyse der Cyber Security in Produktionsanlagen, Maschinen und Produktionsstandorten erfordert eine fundierte Kenntnis der rechtlichen Rahmenbedingungen. Dabei spielen eine Vielzahl von Richtlinien, Normen und Empfehlungen auf nationaler und internationaler Ebene eine zentrale Rolle. Diese rechtlichen Grundlagen bieten nicht nur Orientierung, sondern schaffen auch verbindliche Standards, die den Schutz sensibler Infrastrukturen sicherstellen sollen.

In der Praxis stützen wir uns bei unseren Analysen auf verschiedene rechtliche Ansätze, die auf die spezifischen Anforderungen der jeweiligen Branche und Technologieumgebung zugeschnitten sind. Dazu gehören sowohl verbindliche Vorgaben als auch Best-Practice-Empfehlungen, die von Industrieverbänden, Normungsorganisationen und staatlichen Stellen entwickelt wurden.

Unsere Analyse-Ansätze

Störfallverordnung / 12. BImSchV

IT-Sicherheitsgesetz / KRITIS-Verordnung

KAS-51

TRBS 1115-1

VDI/VDE 2180

NA 163

IEC 62443

DIN ISO/IEC 27001

Im Folgenden präsentieren wir Ihnen eine Auswahl der wesentlichen gesetzlichen Vorschriften, Standards und Leitlinien, die wir regelmäßig bei unserer Arbeit heranziehen. Diese Ansätze bieten eine solide Grundlage für die Durchführung von Sicherheitsbewertungen und die Implementierung geeigneter Maßnahmen zur Risikominimierung in Ihrem Unternehmen.

Störfallverordnung / 12. BImSchV

Für Betriebsbereiche, die unter die Störfallverordnung fallen, fordert § 3 (Allgemeine Betreiberpflichten) der 12. BImSchV vom Betreiber, geeignete Maßnahmen zur Vermeidung von Störfällen zu treffen. Diese Maßnahmen umfassen auch den Schutz vor unbefugten Eingriffen, zu denen Cyberangriffe zählen können. Besonders betroffen sind hierbei PLT- und MSR-Einrichtungen, da diese durch IT/OT-Sicherheitslücken gefährdet sein könnten. Die Verantwortung für die Umsetzung der erforderlichen Maßnahmen liegt beim Betreiber selbst. Die Behörden der einzelnen Bundesländer sind für die Genehmigung und Überwachung der Einhaltung dieser Vorgaben zuständig.

Für NRW hat das LANUV die Anforderungen zur Darstellung der IT-Sicherheit im Sicherheitsbericht und in den Genehmigungsunterlagen zur Anlagensicherheit in einem

Orientierungspapier konkretisiert. Es ist davon auszugehen, dass Behörden in NRW das Orientierungspapier ab sofort als Vorlage bei der Beurteilung von Sicherheitsberichten und Genehmigungsunterlagen heranziehen werden. Das Orientierungpapier nennt explizit die folgenden Themen, die im Sicherheitsbericht dargestellt werden müssen:

- Netzwerkarchitektur und Zonenmodelle
- Assetlisten
- IT-Risikoanalyse / IT-Risikobeurteilung

IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz (IT-SIG) wurde 2015 in Deutschland eingeführt, um die Cybersicherheit von kritischen Infrastrukturen (KRITIS) zu stärken. KRITIS umfasst Bereiche wie Energieversorgung, Wasserwirtschaft, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheitswesen, Ernährungswirtschaft, Finanz- und Versicherungswesen sowie Medien und Kultur. Betreiber dieser Infrastrukturen müssen IT-Sicherheitsmaßnahmen umsetzen und Vorfälle dem Bundesamt für Sicherheit in der Informationstechnik (BSI) melden.

Die BSI-KritisV (BSI-Kritische-Infrastrukturen-Verordnung), die seit dem 3. Mai 2016 in Kraft ist, konkretisiert die Anforderungen des IT-SIG für Betreiber kritischer Infrastrukturen. Sie definiert, welche Sektoren und Einrichtungen als KRITIS gelten und legt spezifische Sicherheitsanforderungen fest.

Die Verordnung präzisiert insbesondere, welche Schutzmaßnahmen umgesetzt werden müssen und wie Sicherheitsvorfälle zu melden sind.

Mit dem IT-Sicherheitsgesetz 2.0 von 1. Mai 2021 wurde der Geltungsbereich auf „Unternehmen im besonderen öffentlichen Interesse“ erweitert, darunter Rüstungshersteller und große Chemieunternehmen. Zudem wurden die Befugnisse des BSI ausgebaut, um proaktive Sicherheitsprüfungen durchzuführen und Sicherheitslücken direkt zu adressieren.

Die Novellierung vom 1. Januar 2024 verschärft diese Anforderungen weiter, so zählen z.B. Unternehmen der Abfall- und Recyclingwirtschaft, Anlagen zur Entsorgung von Siedlungsabfällen (Müllverbrennung) ab einer bestimmten Größe oder sensible Bereiche von Wirtschaft und Verwaltung wie Register- und Meldewesen zu den kritischen Infrastrukturen und müssen besondere Anforderungen an die IT/OT-Sicherheit erfüllen. Das Ziel des IT-SIG ist es, das Funktionieren dieser lebenswichtigen Systeme zu gewährleisten und die Bevölkerung vor den Folgen von Cyberangriffen zu schützen.

KAS-51

Die Kommission für Anlagensicherheit (KAS) ist ein unabhängiges Gremium zur Beratung der deutschen Bundesregierung bzw. des zuständigen Bundesministeriums in Fragen der Sicherheit von Anlagen im Sinne des Bundes-Immissionsschutzgesetzes (BImSchG).

weyer gruppe

komplett. durchdacht.

Ihr Nutzen

Kompetente Unterstützung im Bereich Cyber Security

Individuelle Betreuung Ihrer Fragestellungen

Prävention von Hackerangriffen

Sicherstellung der Einhaltung rechtlicher Vorgaben

Der Leitfaden KAS 51 „Maßnahmen gegen Eingriffe Unbefugter" der Kommission für Anlagensicherheit konkretisiert die Anforderungen der Störfallverordnung, Vorkehrungen gegen Störfälle zu treffen. Darunter fallen beispielsweise die Festlegung von Verantwortlichkeiten sowie das Zugangsmanagement und die Zutrittsüberwachung. Die Sicherheitsanalyse, die der Leitfaden KAS-51 fordert, besteht aus der Bedrohungsanalyse, der Gefahrenanalyse und der IT-Risikobeurteilung. Letztere kann u. a. nach IEC 62443, DIN ISO/IEC 27001 oder NA 163 durchgeführt werden.

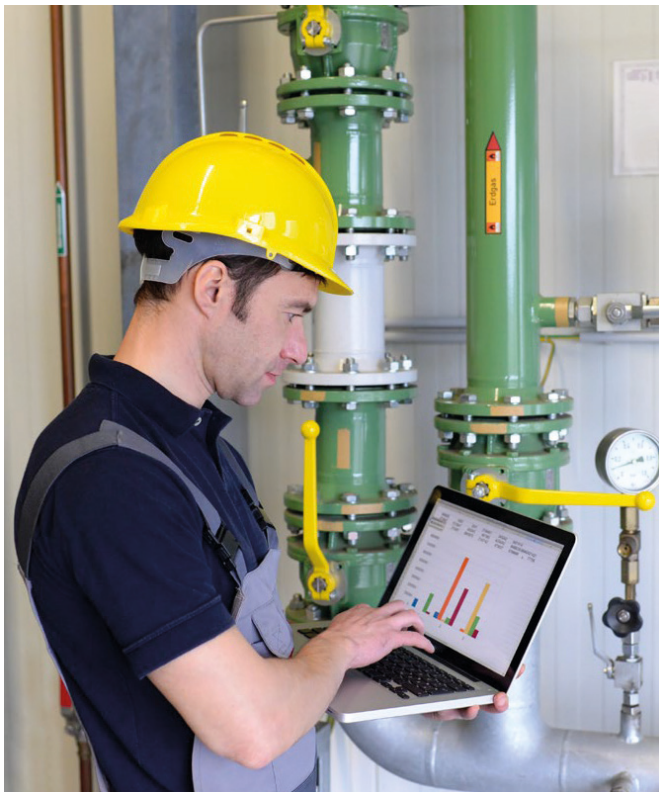
Der Anhang 2 des Leitfadens KAS-51 befasst sich mit dem Schutz vor cyberphysischen Angriffen und behandelt Themen wie die IT-Security als Führungsaufgabe und die Reaktion auf neue Schwachstellen und Bedrohungen. Alle Themen, die im Anhang 2 aufgeführt werden, werden durch Kontrollfragen implementiert. Die Überprüfung durch die Behörde fokussiert sich letztendlich auf die Sicherheitsanalyse und die Qualität der Umsetzung.

Bei Feststellung des ausreichenden Schutzes ist dabei keine separate Sicherheitsüberprüfung nach § 10a Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) erforderlich. Der Sicherheitsbericht dient dem Anlagenbetreiber als rechtssicherer Nachweis der Erfüllung seiner Betreiberpflichten.

TRBS 1115-1

Die Technische Regel für Betriebssicherheit (TRBS) 1115 Teil 1 richten sich an Betreiber und Verantwortliche, die sich mit der Cybersicherheit von sicherheitsrelevanten MSR-Einrichtungen (Mess-, Steuer- und Regelungseinrichtungen) auseinandersetzen. TRBS 1115-1 spezifiziert Maßnahmen zur Identifizierung, Bewertung und Reduzierung von Risiken durch Cyberangriffe und unbefugte Eingriffe in den Betrieb sicherheitsrelevanter Systeme. Die Regelung legt dabei besonderen Wert auf die Bedrohungsanalyse, Gefahrenbewertung und IT-Risikobeurteilung, welche nach anerkannten Standards, z.B. IEC 62443 oder DIN ISO/IEC 27001, erfolgen sollte.

Im Anwendungsbereich von TRBS 1115-1 steht die Prävention von sicherheitsrelevanten Störungen im Fokus. Zu den spezifischen Anforderungen zählen unter anderem das Zugangsmanagement, die Implementierung geeigneter Sicherheitsprotokolle und regelmäßige Sicherheitsüberprüfungen der MSR-Einrichtungen. Die Verantwortlichkeiten zur Umsetzung und Überwachung der festgelegten Maßnahmen liegen beim Betreiber. Die Umsetzung des Konzeptes zur Cyber Security wird bei den Prüfungen des Explosionsschutzes nach Betriebssicherheitsverordnung (BetrSichV) vor Inbetriebnahme und alle sechs Jahre wiederkehrend überprüft.



VDI/VDE 2180

Als Folge der Konkretisierung der Normen IEC 61508 und IEC 61511 wurde die VDI/VDE 2180, die Richtlinie für die funktionale Sicherheit in der Prozessindustrie, im April 2019 erneuert. Einen neuen Schwerpunkt bildet die Cyber Security: „Im Management der funktionalen Sicherheit müssen IT-Sicherheitsaspekte in der Planung, der Beschaffung, der Validierung, im Betrieb, bei Änderungen und bei der Außerbetriebnahme berücksichtigt werden." Weiter heißt es in der Neufassung: „Durch den Einsatz IT-basierter Technologien und die zunehmende Vernetzung von Systemen können Automatisierungssysteme inklusive der zugehörigen Programmier- und Konfigurationsgeräte zum Ziel von Cyber-Bedrohungen werden. […] Um das Gefährdungspotenzial einzuschätzen und geeignete Gegenmaßnahmen festzulegen, muss eine IT-Risikobeurteilung durchgeführt werden." (Blatt 1, S. 38 ff.)

Die IT-Sicherheitsbeurteilung für PLT-Sicherheitseinrichtungen kann dabei unabhängig oder gemeinsam mit der allgemeinen IT-Risikobeurteilung durchgeführt werden. Bestandteile, die davon betroffen sind, sind Hardware, Software, Daten, Verbindungen, Prozesse und Personen. Die VDI/VDE 2180 gibt auf den folgenden Seiten außerdem an, dass die NA 163 Methoden zur Durchführung einer IT-Risikoanalyse sowie einen Maßnahmenkatalog enthält, die gemeinsam mit der VDI/VDE 2180 zu einem geeigneten IT-Absicherungskonzept führen können.

NA 163

Da die oben genannten Ansätze für eine IT-Risikoanalyse nach IEC 62443 oft sehr zeit- und personalintensiv sind, soll das NAMUR Arbeitsblatt 163 dabei helfen, Gesetze und Regelwerke auch dann sicher einzuhalten, wenn die Sicherheitsanalyse durch nicht IT-Fachleute (z. B. PLT-Ingenieur) durchgeführt wird. Die Zeiterfordernis soll durch das Arbeitsblatt auf maximal einen Tag pro Anlage beschränkt sein.

Im NA 163 wird empfohlen, die IT-Risikobeurteilung nach IEC 62443 zu verfassen. Die Basisparameter sind allgemeingültig: SIL 1 bis 3, eine niedrige Anforderungsrate und ein zonierter Aufbau des Netzwerks.

Die IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen nach NA 163 erfolgt letztendlich in fünf Schritten:

1. Identifikation des betrachteten Systems
2. High-Level-IT-Risikobeurteilung
3. Einteilung des betrachteten Systems in Zonen und Verbindungen
4. Detaillierte IT-Risikobeurteilung
5. Dokumentation

Unsere Leistungen

Aufnahme und Aufteilung der Betriebsbereiche / Anlagen in überschaubare Einheiten (Sektionierung) zur Analyse der notwendigen Maßnahmen

- IT/OT-Risikobeurteilung
- Ableitung und Priorisierung von Maßnahmen
- Unterstützung bei der Umsetzung von Maßnahmen
- Einarbeitung der Maßnahmen in das Gesamt-Sicherheitskonzept der Anlage
- Beratung von Equipment-Herstellern
- Ergänzung des Sicherheitsberichtes sowie vorhandener Dokumentation um die Themen der IT/OT-Sicherheit
- Penetrationstest, kurz Pentest(ing)
- Digitale Forensik bzw. IT-Forensik
- Beratung zur Umsetzung der BSI-KritisV
- KRITIS-Prüfungen und interne Audits

weyer gruppe

komplett. durchdacht.

Referenzen (Auszug):

- Bewertung nach KAS-51 (Leitfaden: Maßnahmen gegen Eingriffe Unbefugter) und Gefährdungsbeurteilung nach TRBS 1115-1 (Cybersicherheit für sicherheitsrelevante MSR-Einrichtungen) für einen Störfallbetrieb der oberen Klasse zur Herstellung von Spezialchemikalien in Nordrhein-Westfalen
- Aufnahme des IST-Zustandes der OT-Anlagen einer Müllverbrennungsanlage hinsichtlich Cybersicherheit in Vorbereitung auf die künftige Einstufung als kritische Infrastruktur gemäß KRITIS-Verordnung
- Bewertung nach KAS-51 (Leitfaden: Maßnahmen gegen Eingriffe Unbefugter) für einen Störfallbetrieb der oberen Klasse im Bereich Chemikalienkonfektionierung und -logistik in Nordrhein-Westfalen

Die weyer gruppe ist ein konzernunabhängiger Unternehmensverbund von Ingenieur- und Consulting-Unternehmen in Deutschland, Österreich, der Schweiz und Polen.

Immer ausgehend von den Erwartungen und Wünschen unserer Kunden hat die weyer gruppe seit 1976 ein breites Spektrum an Kompetenzen entwickelt.

Kontakt

Deutschland

horst weyer und partner gmbh
Schillingsstraße 329
52355 Düren
Tel.: +49 (0) 24 21 – 69 09 1 – 0
E-Mail: info@weyer-gruppe.com

weyer IngenieurPartner GmbH
Hälterstraße 2
06217 Merseburg
Tel.: +49 (0) 34 61 – 29 01 0
E-Mail: info.wip@weyer-gruppe.com

Österreich

AS-U Gamerith-Weyer GmbH
Industriestraße 19
4840 Vöcklabruck
Tel.: +43 (0) 76 72 309 310 11
E-Mail: office.asu@weyer-gruppe.com

Schweiz

Weyer und Partner (Schweiz) AG
Güterstrasse 137
4053 Basel
Tel.: +41 (0) 61 683 26 00
E-Mail: schweiz@weyer-gruppe.com

Polen

Weyer Polska Sp. z o. o.
Ul. Zielona 19
Puławy 24-100
Telefon: +48 (0) 784 58 05 56
E-Mail: weyer-polska@weyer-group.com