TÜV VERBAND

Berlin
November 2025

TÜV-Verband-Leitfaden zur

Cybersicherheit in der Prozessindustrie – Umsetzung und Prüfung

Bild: istock

TÜV-Verband-Leitfaden zur

Cybersicherheit in der Prozessindustrie – Umsetzung und Prüfung

Inhalt

Vorwort

Dieser Leitfaden beschreibt in allgemeiner Form die Darstellung einer rechtskonformen Umsetzung der Cybersicherheit mit dem Ziel Menschen und Umwelt zu schützen. Der Fokus liegt damit auf der Störfallverordnung sowie der Betriebssicherheitsverordnung. Das Papier zeigt auf, dass Cybersicherheitsanforderungen beider Rechtsgebiete eine starke inhaltliche Überlappung haben, die bislang rechtsformal nicht synchronisiert ist. Die mehrfache Darstellung inhaltlich ähnlicher Sachverhalte erfordert regelmäßig vermeidbaren Aufwand im Rahmen von Genehmigungsverfahren und Prüfungen. Ziel des Papiers ist es, mögliche Aufwandsreduzierungen durch den von vielen Unternehmen gewählten ganzheitlichen Prozess zur Gewährleistung der Cybersicherheit darzustellen.

Um hierzu eine rechtsgebiets- und interessenübergreifende Abstimmung zu erreichen, erfolgte die Erarbeitung unter Beteiligung von Betreibern, Behörden und Prüforganisationen.

Das im Leitfaden beschriebene Vorgehen greift die Vorgehensweisen aus der ISO 27001, IEC 62443-2-1 bzw. des BSI IT-Grundschutzes auf. Eine vertiefende Betrachtung und Beschreibung möglicher konkreter Vorgehensweisen enthält das BSI IT-Grundschutz-Profil „Chemie".

Zur Unterstützung bei der Umsetzung des Themas in der Praxis dienen u. a. die einschlägigen NAMUR-Publikationen wie NA 163 und NA 169.

Weitere rechtliche Vorgaben zur Umsetzung von Cybersicherheit zum Beispiel nach der NIS-2 Richtlinie oder dem BSI-Gesetz, insbesondere der BSI-Kritisverordnung, sind nicht Gegenstand der nachfolgenden Betrachtungen. Es empfiehlt sich aber, auch diese Anforderungen in ein ganzheitliches Management der Cybersicherheit zu integrieren.

Dieser Leitfaden erscheint inhaltsgleich als „VCI-Statuspapier zur Cybersicherheit in der Prozessindustrie – Umsetzung und Prüfung".

Rechtliche Hinweise

1. Charakteristika von Prozessanlagen und Ausgangssituation

Prozessanlagen sind im Allgemeinen individuell und komplex. Des Weiteren sind sie i. d. R. genehmigungsbedürftig. Im Rahmen des Genehmigungsverfahrens werden verschiedene Rechtsvorschriften berücksichtigt (Störfallverordnung, Betriebssicherheitsverordnung, Gefahrstoffverordnung, etc.). Die Cybersicherheit mit ihren Schutzzielen ist hierbei grundsätzlich relevant, sowohl wirtschaftlich als auch zum Schutz von Menschen und Umwelt.

Konkretisierungen zur Cybersicherheit finden sich in Regelwerken wie z. B. dem Leitfaden der Kommission für Anlagensicherheit (KAS) KAS-51, der Technischen Regel für Betriebssicherheit (TRBS) 1115 Teil 1, dem ICS-Security-Kompendium des BSI oder der Normenreihe IEC 62443. Insbesondere das Zusammenspiel von Methoden der klassischen Safety (SIL etc.) mit Methoden der Cybersicherheit ist zu konkretisieren, um Rechtssicherheit sowohl für die betroffenen Betreiber als auch für die zuständigen Behörden und die Prüforganisationen zu erreichen.

Wirtschaftlich relevante Aspekte erfordern bisher bereits vielfach Cybersicherheitsmaßnahmen, welche ebenso zu dem rechtlich geregelten Schutz von Menschen und Umwelt beitragen können.

Der Umfang der erforderlichen Maßnahmen zum Erreichen der Schutzziele aus den verschiedenen Rechtsgebieten richtet sich nach der möglichen Gefährdung. Ein risikobasiertes Vorgehen unter Berücksichtigung der anlagenspezifischen Eigenschaften und Randbedingungen ist im Bereich der Safety etabliert und bewährt. Dabei werden u. a. die erforderlichen prozessleittechnischen Sicherheitsfunktionen ermittelt und die an sie zu stellenden Zuverlässigkeitsanforderungen definiert. Im Rahmen der Bewertung der Cybersicherheit ist zu klären, in welchem Umfang Cyberbedrohungen[1] die Zuverlässigkeit der prozessleittechnischen Sicherheitsfunktionen beeinträchtigen können. Hierbei wird analog zur Safety häufig ein risikobasiertes Vorgehen gewählt.

[1] Cyberbedrohung bezeichnet gem. Verordnung (EU) 2019/881 einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte. In den Dokumenten des BSI wird in diesem Zusammenhang von Gefährdungen gesprochen.

2. Anforderungen verschiedener Rechtsgebiete

Hinsichtlich des Schutzes von Menschen und Umwelt fallen Prozessanlagen insbesondere unter die nachfolgend genannten Rechtsvorschriften, die spezifische Pflichten für Betreiber beinhalten.

2.1 Bundes-Immissionsschutzgesetz (BImSchG)

Weder das BImSchG noch die unterlagerte Störfallverordnung (12. BImSchV, StörfallV) benennen den Begriff Cybersicherheit direkt. Der Bezug ergibt sich durch die Anforderung in der StörfallV, Maßnahmen gegen Eingriffe Unbefugter zu treffen (§§ 3 und 4, 12. BImSchV).

Konkretisierend behandelt der Leitfaden KAS-51 „Maßnahmen gegen Eingriffe Unbefugter" u. a. das Thema Cybersicherheit als eine Variante des Eingriffes Unbefugter. KAS-55 „Mindestangaben im Sicherheitsbericht" verweist zum Thema Cybersicherheit auf KAS-51.

Im Rahmen der StörfallV ist der KAS-51 damit eine zentrale Erkenntnisquelle für:

- Vollzugsbehörden, z. B. in Genehmigungsverfahren oder Vor-Ort-Inspektionen,
- Sachverständige im Rahmen von Prüfungen und
- Betreiber zur Erfüllung regulatorischer Anforderungen.

Für Prüfungen nach § 29a BImSchG wurde durch die Ergänzung des Fachgebietes 10.2 „Prozessleittechnik – Cyber-Security" in der Bekanntgabeverordnung (41. BImSchV) mit der Nennung entsprechender Sachverständiger für dieses Thema seit dem 1. Juli 2025 die Möglichkeit geschaffen, dass Behörden eine Prüfung durch speziell für dieses Fachgebiet bekannt gegebene Sachverständige anordnen können. Grundlage für diese Verordnung ist § 29b BImSchG, weshalb diese Sachverständige umgangssprachlich auch „§ 29b-Sachverständige" genannt werden.

Die Erfahrungen von Sachverständigen aller Fachgebiete nach der 41. BImSchV werden in einem Prozess gemäß dem Leitfaden KAS-36, „Jährliche Erfahrungsberichte der nach § 29b Bundes-Immissionsschutz-gesetz (BImSchG) bekannt gegebenen Sachverständigen" gesammelt und ausgewertet. Diese Erfahrungen beinhalten auch die „Prozessleittechnik – Cyber-Security", die in den Berichten unter IT/OT-Sicherheit enthalten sind.

2.2 Gesetz über überwachungsbedürftige Anlagen (ÜAnlG)

Auch das ÜAnlG und die unterlagerte Betriebssicherheitsverordnung (BetrSichV) benennen den Begriff Cybersicherheit nicht direkt. Der Bezug ergibt sich über die in der BetrSichV genannten sicherheits-relevanten MSR-Einrichtungen als Teil von überwachungsbedürftigen Anlagen und Arbeitsmitteln. Die konkretisierenden Technischen Regeln zur Betriebssicherheit TRBS 1115 „Sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen" und die TRBS 1115 Teil 1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen" orientieren sich dabei an Anforderungen nationaler sowie internationaler

Regelwerke und Normen über den gesamten Lebenszyklus dieser Einrichtungen. Sie enthalten Anhänge mit Beispielen.

TRBS 1115 Teil 1 ist damit die konkretisierende Grundlage für alle Unternehmen, die mindestens der BetrSichV unterliegen, aber auch für diejenigen Unternehmen, die zusätzlich überwachungsbedürftige Anlagen betreiben und damit von unabhängigen Prüforganisationen (Zugelassenen Überwachungsstellen – ZÜS) geprüft werden.

Im Rahmen der BetrSichV ist die TRBS 1115 Teil 1 damit bezüglich Cybersicherheit eine zentrale Erkenntnisquelle für:

- Aufsichtsbehörden, z. B. in Erlaubnisverfahren,
- ZÜS und zur Prüfung befähigte Personen im Rahmen von Prüfungen und
- Arbeitgeber/Betreiber zur Erfüllung regulatorischer Anforderungen.

Zugelassene Überwachungsstellen müssen Erkenntnisse, die sie bei ihren Tätigkeiten gewonnen haben, sammeln und auswerten und diese Erkenntnisse regelmäßig austauschen (§ 13, ÜAnlG). Dieser Austausch erfolgt im Erfahrungskreis der Zugelassenen Überwachungsstellen (EK ZÜS) mit dem Ziel, einheitliche Prüfstandards und -verfahren zu erarbeiten und so konsistente Prüfungen und vergleichbare Ergebnisse zu gewährleisten. Die dazu verabschiedeten Beschlüsse sind für alle ZÜS verbindlich. Grundlage für Prüfungen der Cybersicherheit ist der öffentlich zugängliche Beschluss EK ZÜS B-002 „Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen von überwachungsbedürftigen Anlagen“.

2.3 Überlappungen / Abweichungen zwischen BImSchG und ÜAnlG

Bezüglich der Zielsetzung, Schutz der sicherheitsrelevanten MSR-Einrichtungen und der sicherheitsrelevanten Anlagenteile vor Cyberbedrohungen, sowie der erforderlichen Anforderungen an Prozesse zur Gewährleistung der Cybersicherheit, unterscheiden sich die konkretisierenden Regelungen in KAS-51 und TRBS 1115 Teil 1 nur unwesentlich.

Beispiel:
KAS-51 sieht Basismaßnahmen vor, um den Kreis der möglichen Innentäter klein zu halten, durch die ein Eingriff Unbefugter erfolgen kann. TRBS 1115 Teil 1 nutzt den Begriff „Innentäter“ nicht explizit, weist aber bei der Bewertung von Cyberbedrohungen darauf hin, dass auch Cyberbedrohungen durch kriminelle Handlungen zutritts-/zugangsberechtigter Personen berücksichtigt werden können (Anhang 2, Abschnitt A2.1, Absatz 5).

Abweichend von TRBS 1115 Teil 1 wird in KAS-51 dargestellt, dass dieser auch der Erfüllung von Anforderungen der Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) dient.

Darüber hinaus ist zu beachten, dass die überwachungsbedürftigen Anlagen und die sicherheitsrelevanten Anlagenteile im Sinne der StörfallV nicht zwangsläufig deckungsgleich sind. Eine Übernahme von Prüfergebnissen zur Reduzierung des Prüfaufwandes ist damit nur nach vorherigem Abgleich auf Übereinstimmung möglich.

2.4 Verhältnis der rechtsgebietsspezifischen Prozesse Gefährdungs-/ Risikobeurteilung

Abhängig vom jeweiligen Rechtsgebiet dienen Gefährdungsbeurteilungen (BetrSichV) oder Risikobeurteilungen (StörfallV) der Vermeidung schädlicher Auswirkungen auf Menschen oder Umwelt. Die dazu verwendeten Grundsätze und Abläufe sind inhaltlich so ähnlich, dass im Folgenden der Begriff Risikobeurteilung verwendet wird. Ergebnisse inhaltlich gleicher Schritte können damit in rechtsformalen Prozessen wie Genehmigungen oder Prüfungen wechselseitig übernommen werden, sofern im Ergebnis alle relevanten Gefahrenquellen und Schutzobjekte betrachtet wurden.

Eine Risikobeurteilung ist sowohl für die Bewertung klassischer Risiken, z. B. nach IVSS Arbeitshilfe „Risikobeurteilung in der Anlagensicherheit", basierend auf ISO 31000, als auch für IT-Risikobeurteilungen basierend auf ISO 27005/IEC 62443-3-2, ein Prozess, der aus mindestens folgenden schriftlich dokumentierten Schritten besteht:

- Identifikation von Risiken (Risk Identification)
- Analyse von Risiken (Risk Analysis)
- Evaluation oder Bewertung von Risiken (Risk Evaluation).

Die Begrifflichkeit IT-Risikobeurteilung wird in verschiedenen Erkenntnisquellen im Bereich Automatisierungstechnik und IT-Sicherheit (z. B. IEC 61511, VDI/VDE 2182, NA-163, KAS-51) verwendet. Im Rahmen des Leitfadens umfasst die IT-Risikobeurteilung auch Aspekte der "Operational Technology" (OT).

Das Risiko im Kontext Anlagensicherheit sowie IT/OT-Sicherheit ergibt sich im Rahmen der Risikobewertung (Risk Evaluation) in der Regel als Produkt von Auswirkung und Eintrittswahrscheinlichkeit oder den Bedingungen für das Eintreten eines Ereignisses (vgl. zum Beispiel Anhang II Abschnitt IV 12. BImSchV, BSI-Standard 200-3[2], VDI/VDE 2182, NA-163).

[2] Im BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz" wird Risikoanalyse synonym zum Wort Risikobeurteilung verwendet und meint den oben beschriebenen Gesamtprozess (s. BSI-Standard 200-3 S. 6 ff).

Klassische (Safety-)Risikobeurteilungen führen über die Schritte

- Erfassung möglicher Gefährdungen für Menschen und Umwelt, über die
- Identifikation der Schwere möglicher Schäden und deren Eintrittswahrscheinlichkeit hin zur
- Bewertung der erforderlichen Risikoreduktion durch geeignete organisatorische und technische Maßnahmen, i. d. R. ausgedrückt durch Safety Integrity Level (SIL).

Die IT-Risikobeurteilung

- erfasst Cyberbedrohungen für alle relevanten Anlagen/Systeme.
- identifiziert die möglichen Auswirkungen der Cyberbedrohungen auf die Integrität und Verfügbarkeit der sicherheitstechnischen Funktionen (nach DIN EN 61511) (Auswirkungsanalyse) und
- bewertet diese anhand der Wahrscheinlichkeit einer erfolgreichen Kompromittierung und leitet den erforderlichen Cyberschutzbedarf ab.

Sowohl die klassische (Safety-)Risikobeurteilung als auch die IT-Risikobeurteilung erfolgen ohne Berücksichtigung bereits vorhandener risikomindernder Maßnahmen.

Die zuvor erwähnten Erkenntnisquellen sehen vor, dass das Risiko anhand von quantitativen wie auch qualitativen Kriterien bewertet werden kann. Bei Letzterem sind objektive Kriterien zu wählen, die eine Reproduzierbarkeit und Nachvollziehbarkeit der Risikobewertung durch andere Personen gewährleistet, z. B. die für unterschiedliche Musterarchitekturen nach NA 163 kleinere oder größere Angriffsflächen für Cyberbedrohungen.

Gegebenenfalls sind neben den prozessleittechnischen Sicherheitsfunktionen / sicherheitsrelevanten MSR-Einrichtungen weitere Systeme zu berücksichtigen, soweit eine Gefährdung von Menschen oder Umwelt durch Cyberbedrohungen möglich ist. Zusammenfassend wird im Folgenden der Begriff „**Schutzbedürftige Einrichtungen**“ verwendet. Diese umfassen gemäß TRBS 1115 Teil 1, Anhang A2.1, Absatz 3:

- sicherheitsrelevante MSR-Einrichtungen,
- sicherheitsrelevante Einrichtungen, die keine MSR-Einrichtung sind (z. B. Notrufeinrichtungen, Notbefehlseinrichtungen),
- Die IT/OT-Umgebung (z. B. Service-/Programmiergeräte, Gateways) der vorgenannten Systeme, die Einfluss auf die Cybersicherheit der vorgenannten Systeme haben,
- nicht sicherheitsrelevante MSR-Einrichtungen (z. B. PLT-Betriebseinrichtungen), bei denen durch die Kompromittierung ihrer Funktion auch unter Berücksichtigung von Wechselwirkungen mit anderen Anlagenteilen eine relevante Gefährdung von Beschäftigten und anderen Personen im Gefahrenbereich verursacht werden kann.

Eine abdeckende Prüfung ist nur auf Basis eines integralen Cybersicherheitsprozesses möglich. Daher nachfolgend die Beschreibung eines entsprechenden Prozesses.

3. Schutzbedarfsfeststellung auf Basis der klassischen (Safety-) Risikobeurteilung und Festlegung von Cybersicherheitsmaßnahmen

Das Vorgehen zur Cybersicherheit erfolgt in zwei Schritten.

1. Festlegung des Cyberschutzbedarfs für schutzbedürftige Einrichtungen unter Berücksichtigung der Ergebnisse der klassischen (Safety-)Risikobewertung als zentrales Kriterium.
2. Festlegung und Umsetzung der erforderlichen Cybersicherheitsmaßnahmen für den ermittelten Cyberschutzbedarf.

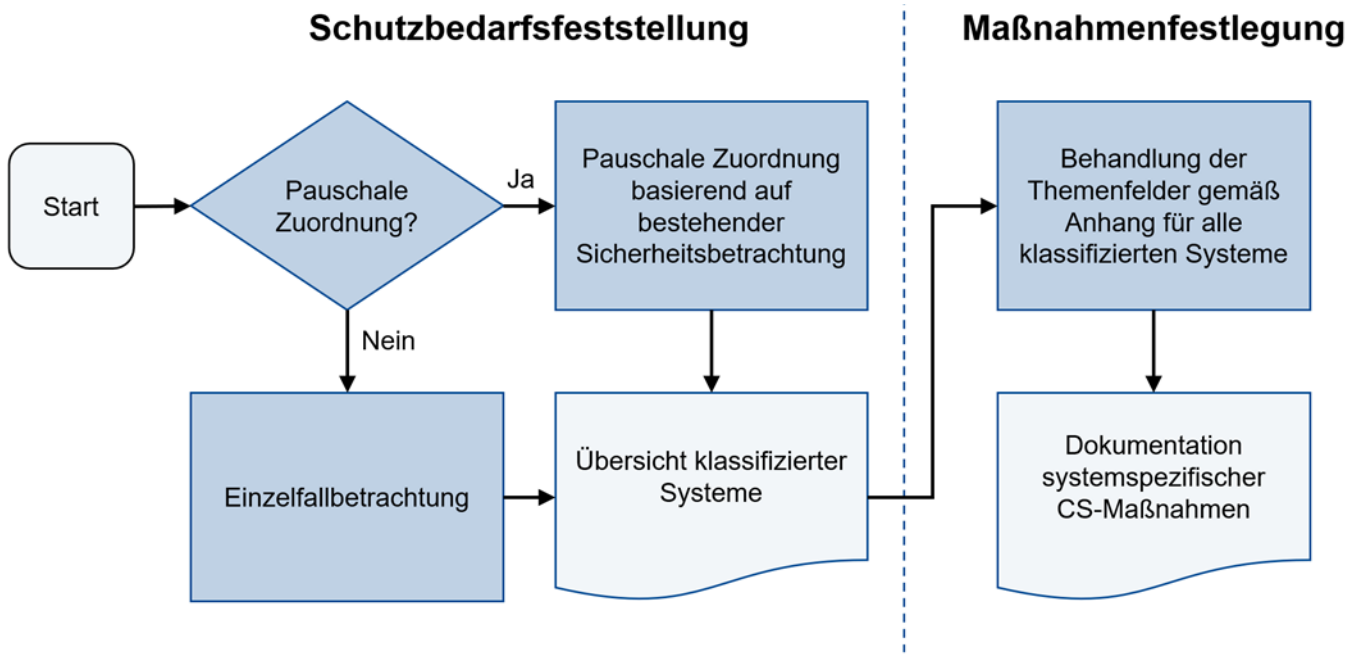

Abbildung 1 Vorgehen zur Cybersicherheit

Hilfestellung für die Festlegung geeigneter Cybersicherheitsmaßnahmen für sicherheitstechnisch „einfache" IT/OT-Architekturen bietet Anhang 2 der TRBS 1115 Teil 1.

3.1 Feststellung des Cyberschutzbedarfes

Der Schutzbedarf wird in diesem Dokument in Anlehnung an den IT-Grundschutz des BSI definiert als das benötigte Maß an Schutz für das schutzbedürftige System, und orientiert sich an den potenziellen sicherheitsrelevanten Auswirkungen von Cyberbedrohungen auf Menschen und Umwelt. Er sagt nichts aus über das Risiko eines erfolgreichen Angriffs oder über den Umfang tatsächlich erforderlicher Cybersicherheitsmaßnahmen.

Klassische (Safety-) Risikobeurteilungen bewerten das Risiko im Sinne der Eintrittswahrscheinlichkeit von Ereignissen und deren Auswirkungen. Da die Eintrittswahrscheinlichkeit einer Cyberbedrohung von verschiedenen Faktoren abhängt, die nicht ausreichend quantifizierbar sind, ist lediglich eine qualitative Abschätzung möglich.

Der Cyberschutzbedarf schutzbedürftiger Einrichtungen ergibt sich damit im Wesentlichen aus den möglichen sicherheitsrelevanten Auswirkungen der Kompromittierung verfahrenstechnischer Funktionen.

Für die bereits in der (Safety-)Risikobeurteilung bewerteten Auswirkungen einzelner verfahrenstechnischer Fehlfunktionen, z. B. Regelungen, Dosierungen ist es unerheblich, ob diese Fehlfunktionen durch eine Kompromittierung oder eine fehlerhafte Komponente verursacht werden. Der Cyberschutzbedarf steht deshalb im Zusammenhang mit den Ergebnissen der (Safety-)Risikobeurteilung. Die Höhe des Cyberschutzbedarfs kann sich damit am maximalen Safety-Schutzbedarf der Funktionen des jeweiligen Betrachtungsumfanges orientieren.

Im Folgenden wird durch eine Verknüpfung des Cyberschutzbedarfes mit dem Safety-Schutzbedarf ein vereinfachtes Vorgehen bei der Festlegung der erforderlichen Cybersicherheitsmaßnahmen beschrieben („Pauschale Zuordnung“ gemäß Abbildung 1).

Alternativ können der Cyberschutzbedarf und die erforderlichen Cybersicherheitsmaßnahmen auch im Rahmen von individuellen Detailbetrachtungen ermittelt werden. Der dabei erforderliche hohe Aufwand individueller Analysen ist bei der Wahl der Methoden zu berücksichtigen.

Alle schutzbedürftigen Einrichtungen (Angriffsziel) einschließlich der datentechnischen Systeme, die mit diesen Einrichtungen temporär oder dauerhaft verbunden sind (Angriffsweg), sind gemäß des festgelegten Cyberschutzbedarfs zu beurteilen und ggf. zu schützen.

Dies schließt ein, dass durch Cyberbedrohungen und deren Einfluss auf das Prozessleitsystem bzw. betriebliche Einrichtungen Anlagenzustände ausgelöst werden können, die durch die Ergebnisse der klassischen (Safety-)Risikobeurteilung nicht abgedeckt werden.

Weitergehende Informationen bzgl. der Kategorisierung des Cyberschutzbedarfs können dem BSI-Standard 200-2 IT-Grundschutz-Methodik entnommen werden. Die nachfolgende Terminologie der Klassifizierung der Schutzbedarfe orientiert sich an dem vorgenannten Dokument[3].

Die Ergebnisse der Cyberschutzbedarfsfeststellung für die betrachteten Systeme sind in einer Übersicht zu dokumentieren.

[3] https://www.docsetminder.de/it-grundschutz-bsi-200-2-und-200-3

3.2 Sehr hoher Schutzbedarf

Für Sicherheitsfunktionen ≥ SIL 1 ist ein sehr hoher Cyberschutzbedarf erforderlich. Dies schließt zusätzlich ein, dass das für die betriebliche Steuerung eingesetzte PLS mindestens den Anforderungen eines hohen Schutzbedarfes genügt. Weitere Konkretisierungen zum Umgang mit Einrichtungen, die einem sehr hohem Schutzbedarf unterliegen, sind z. B. in NA 163 enthalten.

3.3 Hoher Schutzbedarf

Ein hoher Cyberschutzbedarf für Sicherheitsfunktionen < SIL 1 (z. B. PLT-BS) ist für Einrichtungen erforderlich, die im betrieblichen PLS umgesetzt sind, da durch diese Einrichtungen eine geringere Risikoreduzierung als durch SIL-klassifizierte Einrichtungen gewährleistet wird.

Erfolgt für das Prozessleitsystem bzw. betriebliche Einrichtungen keine Detailbetrachtung, so ist aus vorgenannten Gründen auch für diese Systeme von einem hohen Cyberschutzbedarf auszugehen.

Cyberschutzbedarfe die aus Gründen der Wirtschaftlichkeit (Verfügbarkeit der Anlagen und Produktqualität) festgelegt wurden, können bei der Festlegung des Cyberschutzbedarfes der vorgenannten Sicherheitsfunktionen und Prozessleitsysteme bzw. betrieblichen Einrichtungen berücksichtigt werden.

3.4 Normaler Schutzbedarf

Der normale Cyberschutzbedarf ist für sicherheitsrelevante Aspekte nicht geeignet.

4. Festlegung, Umsetzung und Aufrechterhaltung anlagenspezifischer Cybersicherheitsmaßnahmen

Cybersicherheit erfordert eine Vielzahl unterschiedlicher Maßnahmen. Ziel ist es hierbei immer, ein ausreichendes Cybersicherheitsniveau für die schutzbedürftigen Einrichtungen zu gewährleisten. Dies kann durch eine geeignete Kombination von technischen und organisatorischen Cybersicherheitsmaßnahmen erreicht werden, die auf Basis der IT-Risikobeurteilung ausgewählt werden.

Den spezifisch festzulegenden Cybersicherheitsmaßnahmen übergeordnet gibt es grundsätzliche Themenfelder, die in diesem Zusammenhang bearbeitet werden müssen. Der Themenkatalog im Anhang beschreibt, zu welchen Themenfeldern geeignete Maßnahmen festzulegen und umzusetzen sind. Im Einzelnen sind dies:

- Informationssicherheitsmanagement mit Einbeziehung der OT
- Gefährdungsanalyse und Risikomanagement
- Netzwerkarchitektur & Netzwerksicherheit
- Systemhärtung / Funktionsreduktion
- Zugangs und Zugriffsschutz
- Verhindern bzw. Erkennung von nicht autorisierter Änderung
- Fernzugriff
- Sichere Installation und Modifikation
- Training / Sensibilisierung betroffener Personen

Des Weiteren enthält der Themenkatalog Fragen für eine strukturierte Vorgehensweise zur Festlegung der Cybersicherheitsmaßnahmen.

Eine direkte Festlegung der erforderlichen Cybersicherheitsmaßnahmen für Prozessanlagen in einer statischen, dauerhaften und abschließenden Checkliste anstelle des Themenkataloges ist wegen der Charakteristika dieser Anlagen dagegen nicht zielführend. Dies ergibt sich aus den vielfältigen Netzwerkstrukturen und Assets, sowie deren unterschiedlichem Cyberschutzbedarf, der zudem einer dynamischen, zeitlichen Entwicklung unterliegt. Letztlich sind auch bei den Maßnahmen vielfältige Kombinationen bzw. Konzepte zur Abdeckung des Cyberschutzbedarfs möglich.

Für die schutzbedürftigen Einrichtungen erfolgt die Festlegung der Cybersicherheitsmaßnahmen unter Berücksichtigung des Cyberschutzbedarfs und der relevanten Cyberbedrohungen. Zur Ermittlung der Cyberbedrohungen kann der BSI IT-Grundschutz als Hilfestellung dienen.

Dies beinhaltet auch geeignete Prozesse, um die Aufrechterhaltung des Cybersicherheitsniveaus über den gesamten Lebenszyklus der Einrichtungen zu gewährleisten.

Des Weiteren gibt es eine Vielzahl an Regelwerken/Erkenntnisquellen, welche zur Ableitung konkreter Cybersicherheitsmaßnahmen herangezogen werden können wie z. B. das ICS-Security-Kompendium des BSI, IEC 62443, NIST SP 800-82. Das BSI IT-Grundschutz-Profil “Chemie” sowie das NAMUR-Arbeitsblatt 163 bieten darüber hinaus bereits branchenspezifische Lösungsansätze.

Für das betriebliche PLS werden Cybersicherheitsmaßnahmen, welche einen hohen Schutzbedarf abdecken, üblicherweise als ausreichend angesehen. Dies liegt darin begründet, dass folgende Aspekte einen erfolgreichen Angriff zusätzlich erschweren:

- Es sind verfahrenstechnische und anlagenbezogene Spezialkenntnisse erforderlich.
- Die Manipulationen müssen an mehreren – häufig an vielen – Stellen wirksam werden und Fehlzustände auslösen.
- Betriebliche regelungstechnische Einrichtungen der Anlage wirken Fehlzuständen kontinuierlich entgegen.
- Bedienpersonal kann ggf. korrigierend in das Prozessleitsystem und die Anlage vor Ort eingreifen (z. B. unabhängiger Not-Aus) und somit Fehlzuständen ebenfalls entgegenwirken.

5. Prüfung der Cybersicherheit

Der Abschnitt „Überlappungen/Abweichungen zwischen BImSchG und ÜAnlG" im Kapitel „Anforderungen verschiedener Rechtsgebiete" verdeutlicht, dass bei Nachweisen und Prüfungen Synergien genutzt werden können. Möglich wird dieses dadurch, dass die rechtsgebietsspezifischen Prüfungen in zwei Teile aufgeteilt werden. Der erste Teil ist der Nachweis eines geeigneten Managements der Cybersicherheit, z. B. Cybersicherheitsmanagementsystem, CSMS, i. d. R. auf Unternehmensebene oder für übergeordnete Unternehmensbereiche, der zweite Teil ist die Prüfung der anforderungsgerechten Umsetzung an den zu prüfenden Anlagen.

5.1 Prüfung des Managements der Cybersicherheit

Ziel der Prüfung eines Managements der Cybersicherheit ist die Feststellung, ob der Betreiber geeignete Prozesse etabliert hat, um die erforderlichen Cybersicherheitsmaßnahmen zu ermitteln, umzusetzen und das erreichte Schutzniveau auf Dauer aufrechtzuerhalten. Hierfür ist die Anwendung der klassischen Werkzeuge eines Managementsystems auf den relevanten Bereich der OT-Systeme des Betreibers erforderlich. Die im Anhang dargestellten Fragen ermöglichen eine Einschätzung der Eignung des Managements der Cybersicherheit durchzuführen. Prüfungen oder Audits können sich an diesen Fragen orientieren.

Die Fragen enthalten u. a. Bezüge zu den Regelungen des Leitfadens KAS-51, der TRBS 1115 Teil 1 sowie dem EK ZÜS B-002, sodass diese rechtsgebietsspezifischen Anforderungen im Audit berücksichtigt werden können.

Gegenstand des Audits sind sowohl das Vorhandensein geeigneter Prozesse als auch deren systematische und dokumentierte Umsetzung.

Bei der Auditierung ist sowohl dem berechtigten Interesse der Betreiber an die vertrauliche Behandlung sensibler Informationen als auch dem Informationsbedürfnis des Auditors für seine Prüfung ausreichend Rechnung zu tragen. Dem Auditor sind für die Durchführung des Audits alle für seine Bewertung erforderlichen Informationen zugänglich zu machen. Andernfalls ist eine positive Bewertung der zu prüfenden Aspekte nicht möglich.

Der Umfang des Audits ist vorab festzulegen. Als Erkenntnisquelle für relevante Randbedingungen zur Durchführung von Audits kann die DIN EN ISO/IEC 27006-1 herangezogen werden. Da hier jedoch der gesamte Informationssicherheitsprozess von Unternehmen bis hin zur Zertifizierung betrachtet wird, sind für die Auditierung eines Managements der Cybersicherheit im Sinne dieses Dokuments deutlich geringere Auditumfänge als ausreichend anzusehen.

Bei einem positiven Abschluss der Auditierung können sich sowohl Behörden als auch Sachverständige der zugelassenen Überwachungsstellen und Sachverständige nach §29b

BImSchG die Ergebnisse des Audits zu eigen machen. Voraussetzung hierfür sind insbesondere:

- Das Audit muss die für das jeweilige Rechtsgebiet erforderlichen schutzbedürftigen Einrichtungen einschließen
- Das Audit muss explizit die Safety-relevanten Auswirkungen von Cyberbedrohungen auf schutzbedürftige Einrichtungen behandeln
- Es dürfen keine aus Cyberbedrohungen hervorgehenden Safety-Risiken akzeptiert werden, für deren Vermeidung Maßnahmen nach dem Stand der Technik möglich wären
- Für die Behebung von Abweichungen muss ein geeigneter Umsetzungsplan existieren
- Die Auditergebnisse müssen eine angemessene Aktualität besitzen
- Die Auditergebnisse sollten durch Referenzieren/Auflisten der mitgeltenden Unterlagen unabhängig nachvollziehbar sein.

5.2 Prüfung der anforderungsgerechten Umsetzung

In der Regel ist bei einem positiven Prüfergebnis des Managements der Cybersicherheit davon auszugehen, dass geeignete Prozesse zur Festlegung von Maßnahmen der Cybersicherheit vorgesehen sind. Im nächsten Schritt ist spezifisch für die zu prüfende Anlage anhand einer geeigneten Dokumentation des Betreibers festzustellen, ob basierend auf diesen Prozessen für die schutzbedürftigen Einrichtungen geeignete organisatorische und technische Cybersicherheitsmaßnahmen festgelegt wurden.

Abschließend ist die Funktionsfähigkeit der Maßnahmen der Cybersicherheit durch Prüfungen vor Ort in geeigneter Form nachzuweisen.

Je nach Art des Genehmigungs- oder Aufsichtsverfahrens können der zu berücksichtigende Betrachtungsumfang und die erwartete Prüftiefe stark divergieren. Für die Prüfung sind daher vorab geeignete Festlegungen zu Art, Umfang und Fristen zu treffen.

Liegen bereits Prüfergebnisse z. B. aus anderen Rechtsgebieten vor, die sich der Prüfer zu eigen machen kann, so ist eine erneute Prüfung gleicher Prüfinhalte nicht mehr erforderlich.

Anhang Themenkatalog

Der Themenkatalog (TÜV-Verband-Leitfaden_Cybersicherheit_Themenkatalog.xlsx) wird als eigenständige Datei zur Verfügung gestellt. Er enthält praktische Fragen für eine strukturierte Vorgehensweise zur Festlegung der Cyberschutzmaßnahmen. Die Fragen stellen keine rechtsverbindliche Prüfgrundlage für Behörden und Prüforganisationen dar. Sie sind durch dieses zwischen Betreibern, Behörden und Prüforganisationen breit abgestimmte Papier aber geeignet, Betreibern eine Hilfestellung für den Nachweis eines rechtskonformen Umgangs mit Cyberbedrohungen z. B. bei behördlichen Inspektionen oder Prüfungen durch zugelassene Überwachungsstellen zu geben.

Mitwirkende

Dr. Amrei Baasner	GAA Hildesheim
Jörg Becker	TÜV SÜD
Benedikt Bittcher	Wacker
Jens Cordt	BSI
Marcus Geiger	TÜV SÜD
Dr. Jens Hagenow	RP Darmstadt
Klaus Kleine Büning	TÜV Nord InfraChem
Hartmut Manske	Merck
Ludwig Schenk	LANUK NRW
Ralf Schmitt	TÜV Rheinland
Dr. Thomas Steffen	BASF
Christoph Thust	Evonik

Ansprechpartner:innen

Dr. Hermann Dinkler
Referent Druck- & Rohrleitungsanlagen, Brand- & Explosionsschutz, wassergefährdende Stoffe
E-Mail: hermann.dinkler@tuev-verband.de
Tel. +49 30 760095-540
www.tuev-verband.de

Claudia Tautorus
Leiterin Industrie und Anlagentechnik
E-Mail: claudia.tautorus@tuev-verband.de
Tel. +49 30 760095-420
www.tuev-verband.de

Als TÜV-Verband e.V. vertreten wir die politischen Interessen der TÜV-Prüforganisationen und fördern den fachlichen Austausch unserer Mitglieder. Wir setzen uns für die technische und digitale Sicherheit sowie die Nachhaltigkeit von Fahrzeugen, Produkten, Anlagen und Dienstleistungen ein. Grundlage dafür sind allgemeingültige Standards, unabhängige Prüfungen und qualifizierte Weiterbildung. Unser Ziel ist es, das hohe Niveau der technischen Sicherheit zu wahren, Vertrauen in die digitale Welt zu schaffen und unsere Lebensgrundlagen zu erhalten. Dafür sind wir im regelmäßigen Austausch mit Politik, Behörden, Medien, Unternehmen und Verbraucher:innen.

Herausgeber
TÜV-Verband e. V.
Friedrichstraße 136
10117 Berlin

Tel.: +49 30 760095-400
Fax: +49 30 760095-401
E-Mail: berlin@tuev-verband.de
www.tuev-verband.de