Beschluss des EK ZÜS **ZÜS B-002 rev 1**

Abgestimmt im EK ZÜS	Schriftliche Abstimmung	27.05.2022
	34. Sitzung, TOP 6.2	16.11.2022

Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen von überwachungsbedürftigen Anlagen

1 Anwendungsbereich

(1) Dieser Beschluss legt für die ZÜS Mindestanforderungen für ihre Prüfung der Maßnahmen des Arbeitgebers gegen Cyberbedrohungen (Maßnahmen der Cybersicherheit, kurz CS-Maßnahmen) im Rahmen der Prüfungen gemäß §§ 15 oder § 16 BetrSichV der überwachungsbedürftigen Anlagen sowie, falls zutreffend, der Prüfung gemäß § 18 BetrSichV fest.

(2) Für Arbeitgeber oder Betreiber überwachungsbedürftiger Anlagen kann dieser Beschluss (insbesondere Kapitel 5) als Hilfestellung für geeignete Vorgehensweisen zur Festlegung erforderlicher CS-Maßnahmen dienen. In diesem Beschluss wird der Begriff „Betreiber“ verwendet.

(3) Dieser Beschluss bezieht sich ausschließlich auf Prüfungen, die der Bestätigung der Einhaltung der Vorgaben der BetrSichV dienen. Aspekte, die dem Datenschutz oder der Wirtschaftlichkeit dienen, wurden nicht berücksichtigt.

(4) Der Prüfumfang umfasst im Wesentlichen sicherheitsrelevante MSR-Einrichtungen von überwachungsbedürftigen Anlagen. Er kann sich aber um nicht sicherheitsrelevante MSR-Einrichtungen und für die Sicherheit relevante Einrichtungen, die keine MSR-Einrichtung sind, erweitern, wenn als Ergebnis der Gefährdungsbeurteilung der überwachungsbedürftigen Anlage festgestellt wurde, dass durch die Kompromittierung dieser Einrichtungen mittelbar oder unmittelbar eine Gefährdung von Beschäftigten oder anderen Personen im Gefahrenbereich verursacht werden kann. Die hinsichtlich der Prüfung von CS-Maßnahmen relevanten Einrichtungen werden nachfolgend als „schutzbedürftige OT[1]-Einrichtungen“ (zum Begriff siehe Abschnitt 3 Absatz 7) bezeichnet.

(5) Wurden CS-Maßnahmen an IT/OT-Systemen, die mit schutzbedürftiger OT-Einrichtungen datentechnisch in Verbindung stehen (Umgebung gemäß EmpfBS 1115), als notwendig identifiziert, um diese Systeme zu schützen („defence in depth“) (siehe auch hierzu Kapitel 5.2), sind diese bei der Prüfung der zugehörigen schutzbedürftigen OT-Einrichtung ebenfalls zu berücksichtigen.

(6) Die Berücksichtigung von Cyberbedrohungen setzt grundsätzlich auf einen lebenszyklusbegleitenden Prozess zur Cybersicherheit auf.

[1] OT = Operational Technology

(7) Die Cybersicherheit wird bei den folgenden nach der BetrSichV erforderlichen Prüfungen geprüft:

- Bei Aufzugsanlagen im Rahmen der Prüfung nach Anhang 2 Abschnitt 2 Nummern 3 und 4.1 BetrSichV
- Bei Anlagen in explosionsgefährdeten Bereichen im Rahmen der Prüfung nach Anhang 2 Abschnitt 3 Nummern 4.1 und 5.1 BetrSichV
- Bei Druckanlagen im Rahmen der Prüfung nach Anhang 2 Abschnitt 4 Nummern 4 und 5 BetrSichV (Prüfung vor Inbetriebnahme von Druckanlagen und wiederkehrende Anlagenprüfungen)
- Im Prüfbericht zur Erlaubnis nach § 18 Absatz 3 BetrSichV

2 Rechtliche Rahmenbedingungen

(1) Der Betreiber hat gemäß §§ 15 und 16 BetrSichV sicherzustellen, dass überwachungsbedürftige Anlagen vor Inbetriebnahme, vor Wiederinbetriebnahme nach einer prüfpflichtigen Änderung und wiederkehrend geprüft werden. Der Betreiber ist gemäß § 3 BetrSichV verpflichtet, Gefährdungen (auch die durch Cyberbedrohungen), die durch Arbeitsmittel auftreten können, zu beurteilen und geeignete Schutzmaßnahmen zu treffen.

(2) Die Prüfung von Aspekten der Cybersicherheit ist bei den gesetzlich geforderten Prüfungen von überwachungsbedürftigen Anlagen ein bisher in den Technischen Regeln Betriebssicherheit (TRBS) nicht behandeltes Thema. Fehlt es an entsprechenden TRBS, bedeutet dies jedoch nicht, dass der Betreiber in diesen Bereichen von der Einhaltung des Standes der Technik befreit wäre.

(3) Gemäß § 5 Absatz 3 BetrSichV muss der Betreiber sicherstellen, dass die Arbeitsmittel neben den Vorschriften der BetrSichV den für sie zum Zeitpunkt der Bereitstellung auf dem Markt geltenden Rechtsvorschriften über Sicherheit und Gesundheitsschutz entsprechen. Da es zu CS-Maßnahmen noch keine konkretisierenden Vorgaben für die Bereitstellung des Arbeitsmittels auf dem Markt gibt[2] (Inverkehrbringen), sind die erforderlichen CS-Maßnahmen in der Gefährdungsbeurteilung unter Beachtung der Anforderungen der Betriebssicherheitsverordnung, insbesondere §§ 4, 5, 6, 8 und 9 sowie Anhang 1 BetrSichV, zu ermitteln.

(4) Gemäß § 3 Absatz 2 Satz 2 Nr. 4 BetrSichV muss der Betreiber bei seiner Gefährdungsbeurteilung auch vorhersehbare Betriebsstörungen berücksichtigen.

In TRBS 1111 Abschnitt 4.5 sind vorhersehbare Betriebsstörungen, wie z. B. „Ereignisse, die den Arbeitsablauf behindern oder zur Einstellung der Arbeiten führen oder bei denen die für den Normalbetrieb des Arbeitsmittels getroffenen Schutzmaßnahmen teilweise oder ganz außer Kraft gesetzt sein können“, benannt. Eine solche Betriebsstörung kann auch der plötzliche Ausfall von Sicherheitsfunktionen eines Arbeitsmittels durch Fremdeinwirkung sein. Die möglichen Auswirkungen einer Kompromittierung von schutzbedürftigen OT-Einrichtungen sind daher in der Gefährdungsbeurteilung zu bewerten.

Hinweis: Ergibt sich aus der Gefährdungsbeurteilung, dass ein auf dem Markt bereit gestelltes Arbeitsmittel unter Berücksichtigung der innerbetrieblichen Einsatzbedingungen und der auszuführenden Arbeiten nicht ohne zusätzliche Schutzmaßnahmen sicher verwendet werden kann, hat der Betreiber gemäß § 5 Absatz 1 BetrSichV diese geeigneten Schutzmaßnahmen festzulegen.

[2] Redaktionsschluss April 2022

3 Begriffsbestimmungen im Sinne dieses Beschlusses

(1) **Cybersicherheit** ist das Vorhandensein des erforderlichen Schutzes von schutzbedürftigen OT-Einrichtungen vor Cyberbedrohungen, soweit deren Informationstechnik durch Cyberbedrohungen kompromittiert werden kann und sie dem Schutz von Beschäftigten und anderen Personen im Gefahrenbereich dienen.

(2) **Cyberbedrohung** ist die intendierte Bedrohung der datentechnischen Integrität von überwachungsbedürftigen Anlagen einschließlich der Verfügbarkeit ihrer sicherheitsrelevanten MSR-Einrichtungen mit Methoden und Werkzeugen der Informationstechnik.

(3) **Maßnahmen** der **Cybersicherheit (CS-Maßnahmen)** sind Maßnahmen zum Schutz vor Cyberbedrohungen.

(4) **Sicherheitseinrichtungen** sind gemäß TRBS 1201 Einrichtungen zur Verhinderung von unzulässigen oder instabilen Betriebszuständen von Arbeitsmitteln. Dazu können auch MSR-Einrichtungen zählen.

(5) **MSR-Einrichtungen** sind Einrichtungen, die dem Messen physikalischer Größen und dem auf dieser Grundlage erfolgenden Regeln oder Steuern von Arbeitsmitteln dienen. MSR-Einrichtungen können betrieblichen und/oder sicherheitstechnischen Zwecken dienen.

Hinweis: In anderen Regelwerken werden MSR-Einrichtungen auch als PLT- oder PLS-Einrichtungen bezeichnet.

(6) **Sicherheitsrelevante MSR-Einrichtungen** sind gemäß TRBS 1201 Mess-, Steuer- und Regeleinrichtungen an Arbeitsmitteln inkl. überwachungsbedürftigen Anlagen, die deren sicherer Verwendung dienen. Sie bestehen aus Sensor-, Aktor- und Logikeinheiten sowie zugehörigen Verbindungseinrichtungen und unterliegen üblicherweise auch Anforderungen an ihre funktionale Sicherheit.

(7) **schutzbedürftige OT-Einrichtungen** ist der Sammelbegriff für

- sicherheitsrelevante MSR-Einrichtungen von überwachungsbedürftigen Anlagen (Zone A gemäß EmpfBS 1115),
- 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 (innerhalb oder außerhalb der Zone B gemäß EmpfBS 1115)
- für die Sicherheit relevante Einrichtungen, die keine MSR-Einrichtung sind (z. B. Notrufeinrichtungen, Notbefehlseinrichtungen), im Folgenden autarke Sicherheitseinrichtungen genannt,

die durch Cyberbedrohungen kompromittiert und in ihrer Funktion beeinträchtigt werden können (Angriffsziele).

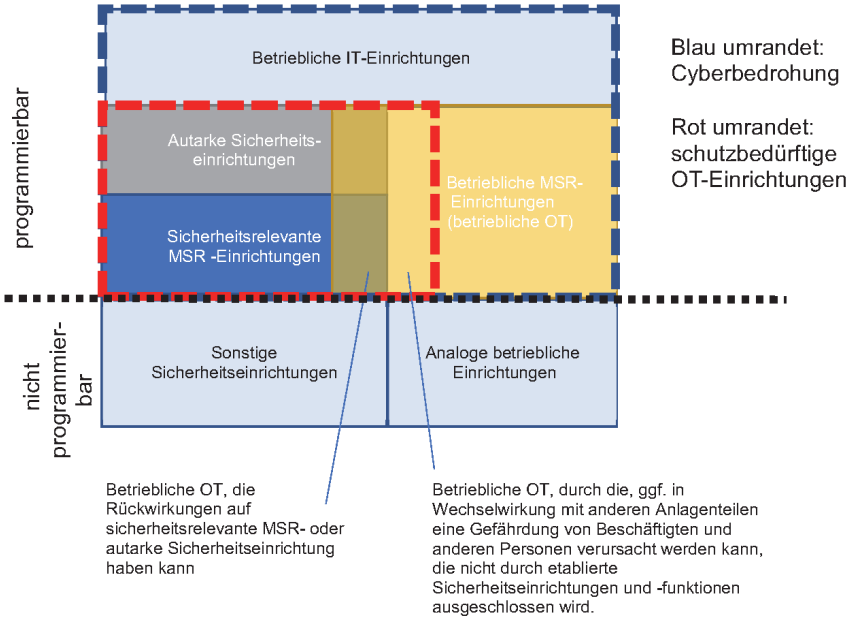

Abbildung 1: Darstellung der schutzbedürftigen OT-Einrichtungen und ihrer Abgrenzungen

Hinweis: Schutzbedürftige OT-Einrichtungen werden in diesem Beschluss nur für überwachungsbedürftige Anlagen und nur bezüglich der zugehörigen gefahrenfeldbezogenen Gefährdungen behandelt. Dessen ungeachtet kann dieser Beschluss auch für andere Anlagen und Gefährdungen angewendet werden.

(8) **Kompromittierung** ist der unberechtigte datentechnische Zugriff auf eine schutzbedürftige OT-Einrichtung mit dem Ziel der Manipulation der Funktion.

(9) Die **Umgebung** sind IT/OT-Komponenten und Systeme, die weder direkt noch indirekt der schutzbedürftigen OT-Einrichtung zuzuordnen sind, aber mit dieser in Verbindung stehen (z. B. Betriebsdateninformationssystem, Visualisierung des Sicherheitsfunktion-Zustands, Service-IT für z. B. Patchmanagement, Domain Control und Virenschutz, Internet) und daher als Angriffswege dienen können.

(10) Als **schutzbedürftige Systeme** werden die schutzbedürftige OT-Einrichtung und der Teil ihrer Umgebung bezeichnet, für die CS-Maßnahmen erforderlich sind.

4 Grundsätze der Prüfung

(1) Um eine durch die Kompromittierung ausgelöste unmittelbare oder mittelbare Gefährdung von Personen durch die Anlage zu vermeiden, müssen die schutzbedürftigen OT-Einrichtungen einer überwachungsbedürftigen Anlage gegen durch Kompromittierung ausgelöste Störungen gesichert sein.

(2) Die sicherheitsrelevanten MSR-Einrichtungen und autarken Sicherheitseinrichtungen von überwachungsbedürftigen Anlagen und ihre Folgefunktionen müssen auch unter Beachtung der jeweils vom Betreiber festgelegten CS-Maßnahmen geeignet und funktionsfähig sein.

(3) Der Betreiber hat gem. § 3 Absatz 7 BetrSichV seine festgelegten CS-Maßnahmen regelmäßig und anlassbezogen in Abhängigkeit der allgemeinen Cyberbedrohungslage oder nach Cybersicherheits-Vorfällen zu überprüfen, ggf. anzupassen und zu dokumentieren.

(4) Die Prüfaussage richtet sich nach den zum Zeitpunkt der jeweiligen Prüfung geltenden Anforderungen aus der Prüfungsgrundlage (BetrSichV) und den zugehörigen technischen Regeln (TRBS). Empfehlungen zur Betriebssicherheit (EmpfBS) werden in geeigneter Form berücksichtigt.

5 Grundanforderungen an die Cyber-Sicherheit in überwachungsbedürftigen Anlagen (abgeleitet aus EmpfBS 1115 zur BetrSichV)

5.1 Allgemeines

(1) Im Rahmen der Gefährdungsbeurteilung hat der Betreiber zu ermitteln, ob sicherheitsrelevante MSR-Einrichtungen, nicht sicherheitsrelevante MSR-Einrichtungen und autarke Sicherheitseinrichtungen durch Kompromittierung derart verändert werden können,

- dass sicherheitsrelevante MSR-Einrichtungen und autarke Sicherheitseinrichtungen ihre Funktion nicht mehr hinreichend zuverlässig erfüllen und/oder
- dass durch nicht sicherheitsrelevante MSR-Einrichtungen Gefährdungen von Beschäftigten oder anderen Personen ausgelöst werden können.

Hinweis: Ist dies der Fall, ist für diese schutzbedürftige OT-Einrichtungen unter Berücksichtigung ihrer Umgebung zu ermitteln, welche Maßnahmen erforderlich sind, um die individuellen Cyberbedrohungen nach dem Stand der Technik und den Maßgaben der technischen Vernunft abzuwehren.

(2) In der Gefährdungsbeurteilung sind auch alle aus der Integration (Zusammenführung von Teilsystemen zu einem vollständigen System) stammenden erforderlichen CS-Maßnahmen zu berücksichtigen. Gegebenenfalls vorhandene Vorgaben von Herstellern sind dabei

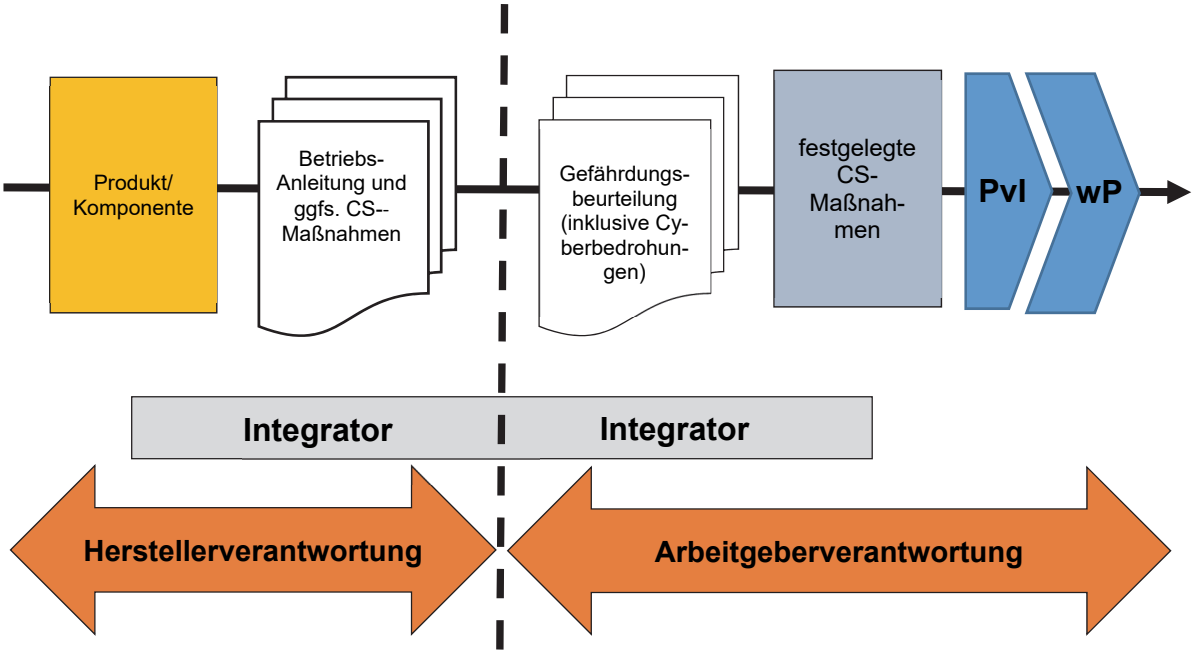

Abbildung 2: Verantwortlichkeit bei der Auswahl und dem Betrieb von schutzbedürftiger OT-Einrichtungen innerhalb der überwachungsbedürftigen Anlage. Der Integrator kann sowohl auf der Hersteller- als auch auf der Betreiberseite tätig sein.

ebenfalls zu berücksichtigen.

(3) Damit die schutzbedürftigen OT-Einrichtungen wirksam geschützt werden können, müssen sowohl die Hard- und Softwarekomponenten einschließlich ihrer nutzbaren Schnittstellen, der zugehörigen Daten als auch die Prozesse, Organisationen und Personen, die die schutzbedürftigen OT-Einrichtungen beeinflussen können, gegen mögliche Cyberbedrohungen gerüstet sein.

5.2 Prozessdarstellung (Vorgehensweise) zur Beurteilung von Cyberbedrohungen

(1) Der Prozess der Beurteilung und Behandlung von CS-Bedrohungen muss durch den Betreiber in einer durch eine ZÜS nachvollziehbaren Form durchgeführt werden, um eine Prüfung der CS-Maßnahmen durch eine ZÜS zu ermöglichen. Dazu sind in der Regel die folgenden Schritte einer Gefährdungsbeurteilung erforderlich.

(2) Erfassung der

a) schutzbedürftigen OT-Einrichtungen (einschl. der in Abschnitt 5.1 Absatz 3 aufgeführten Elemente) und ihrer Aufgaben als Schutzmaßnahmen sowie

b) Umgebung der schutzbedürftigen OT-Einrichtungen (bei Bedarf)

(3) Beurteilung der möglichen Auswirkung von Cyberbedrohungen auf die erfassten schutzbedürftigen OT- Einrichtungen. Der Schutzbedarf der einzelnen schutzbedürftigen OT-Einrichtung richtet sich nach der möglichen Gefährdung durch die überwachungsbedürftige Anlage.

(4) Nachvollziehbares Festlegen von CS-Maßnahmen für schutzbedürftige Systeme, um den Cyberbedrohungen in geeigneter Weise zu begegnen und die Auswirkungen im erforderlichen Umfang zu begrenzen.

a) Bisher gibt es noch keine einheitliche Vorgehensweise, um den Schutzbedarf der jeweiligen Systeme zu klassifizieren. Eine geeignete Vorgehensweise ist beispielsweise in EmpfBS 1115 oder DIN EN 62443 vorhanden.

b) Durch die CS-Maßnahmen dürfen keine Rückwirkungen auf die schutzbedürftigen OT-Einrichtungen entstehen, die zu Gefährdungen führen.

Hinweis: Auch der Einsatz von nicht-digitalen Systemen kann ein Weg sein, Cyberbedrohungen zu begegnen.

(5) Umsetzung der festgelegten CS-Maßnahmen

a) Implementierung geeigneter CS-Maßnahmen für die schutzbedürftigen Systeme,

b) Festlegung geeigneter organisatorischer Regelungen.

(6) Überprüfung der Wirksamkeit, ob

a) die umgesetzten CS-Maßnahmen (weiterhin) vorhanden und in Funktion sind bzw. ob organisatorische Regelungen eingehalten werden und

b) mit dem fortschreitenden Stand der Technik bestehende CS-Maßnahmen unter Berücksichtigung einer sich verändernden Bedrohungslage weiterhin als wirksam angesehen werden können oder sie durch neue CS-Maßnahmen zu ersetzen bzw. durch weitere zu ergänzen sind und

c) das TOP-Prinzip eingehalten wurde.

(7) Überprüfung zum Ausschluss von unzulässigen Rückwirkungen der CS-Maßnahmen auf sicherheitsrelevante MSR-Einrichtungen und autarke Sicherheitseinrichtungen

(8) Festlegung eines Zeitschemas für die Implementierung der CS-Maßnahmen und der zugehörigen Prüfungen.

6 Prüfung der CS- Maßnahmen

Vorbemerkung:

Die folgenden Prüfschritte durch eine ZÜS richten sich nach den zum Zeitpunkt der jeweiligen Prüfung geltenden Anforderungen aus der Prüfungsgrundlage (BetrSichV) und den zugehörigen technischen Regeln (TRBS 1201 und ihrer Teile 1 bis 4) bei der Prüfung einer überwachungsbedürftigen Anlage durch eine zugelassene Überwachungsstelle. Die EmpfBS 1115 wurde hierbei zugrunde gelegt. Die Einführung der einzelnen Prüfschritte nach diesem Abschnitt erfolgt zeitlich gestaffelt in einem stufenweisen Prozess.

Bei Prüfungen der ZÜS wird die Prüfung der CS-Maßnahmen im Zuge der Prüfung gemäß Abschnitt 1 Absatz 7 der sicherheitsrelevanten MSR-Einrichtungen sowie der autarken Sicherheitseinrichtungen durchgeführt. Die gemäß Kapitel 5 festgelegten CS-Maßnahmen bei betrieblichen MSR-Einrichtungen, die als schutzbedürftige OT-Einrichtungen identifiziert wurden, sowie der Umgebung sind hierbei zusätzlich zu berücksichtigen.

Können keine nachvollziehbaren und ausreichend aktuellen Nachweise der Eignung und Funktionsfähigkeit von CS-Maßnahmen vorgelegt werden, sind vertiefende Prüfungen durch die ZÜS (nach entsprechender Beauftragung) erforderlich.

6.1 Prüfung im Erlaubnisverfahren

Es ist zu prüfen, ob der Antragsteller CS-Maßnahmen in den für das Erlaubnisverfahren zu prüfenden Unterlagen angemessen berücksichtigt hat.

6.2 Prüfung vor Inbetriebnahme oder vor Wiederinbetriebnahme nach einer prüfpflichtigen Änderung

(1) Für eine festzulegende Übergangszeit ist zu prüfen, ob Cyberbedrohungen im Rahmen der Gefährdungsbeurteilung dokumentiert behandelt werden.

(2) Nach Abschluss der Übergangszeit nach Absatz 1 ist zu prüfen, ob Cyberbedrohungen im Rahmen der Gefährdungsbeurteilung geeignet behandelt werden, u. a. sind hierbei die in den folgenden Absätzen dargestellten Punkte zu prüfen.

(3) Sind die schutzbedürftigen Systeme gemäß Abschnitt 5.2 Absatz 2 sowie ihre Aufgaben erfasst und dokumentiert?

(4) Sind die schutzbedürftigen OT-Einrichtungen hinsichtlich der Möglichkeit eines Integritätsverlusts und der Auswirkungen durch Cyberbedrohungen bewertet?

a) Liegt eine Bewertung vor, ob die schutzbedürftigen OT-Einrichtungen ihre Funktionen im Falle einer Kompromittierung noch hinreichend zuverlässig erfüllen können?

b) Wurde bewertet welche Auswirkung das unerwünschte Funktionsverhalten der jeweiligen schutzbedürftigen OT-Einrichtungen in der überwachungsbedürftigen Anlage hat?

c) Wurde bewertet welche Auswirkung es hat, wenn gleichzeitig mehrere schutzbedürftigen OT-Einrichtungen kompromittiert werden?

(5) Sind Festlegungen von CS-Maßnahmen für die schutzbedürftigen Systeme getroffen worden, um den Cyberbedrohungen in geeigneter Weise zu begegnen und die Auswirkungen zu begrenzen? Dazu zählen gem. EmpfBS 1115 (sinngemäß auch in DIN EN IEC 62443 enthalten) z. B.:

a) Reduktion der schutzbedürftigen OT-Einrichtungen auf das dem Einsatzzweck entsprechende Mindestmaß (z. B. Entfernen von Softwarekomponenten und Funktionen,

die zur Erfüllung der vorgesehenen Aufgabe nicht zwingend notwendig sind, Abschalten oder Unterdrücken von nicht autorisierten Kommunikationsverbindungen, Diensten oder Funktionen (z. B. durch Whitelisting))

b) Hard- und Softwarelösungen (z. B. Rückwirkungsfreiheit, d.h. keine unzulässige Beeinflussung von schutzbedürftigen OT-Einrichtungen durch deren Umgebung)

c) Organisatorische Maßnahmen (z. B. Zugangs- und Zugriffskontrolle, Schulung, Sicherstellung der Integrität von Daten der schutzbedürftigen OT-Einrichtungen (z. B. durch elektronische Signatur und Verschlüsselung zentraler Spezifikationsdokumente))

(6) Sind die vom Betreiber festgelegten CS-Maßnahmen für die schutzbedürftigen Systeme geeignet und in geeigneter Weise umgesetzt?

(7) Beeinträchtigen die festgelegten CS-Maßnahmen und deren Umsetzung die Wirksamkeit der sicherheitsrelevanten MSR-Einrichtungen und autarken Sicherheitseinrichtungen?

6.3 Wiederkehrende Prüfung

(1) Die wiederkehrende Prüfung der CS-Maßnahmen erfolgt auf Basis der gemäß Abschnitt 6.2 geprüften und als geeignet bewerteten CS-Maßnahmen.

(2) Die erstmalige Prüfung der CS-Maßnahmen bei einer Anlage, die wiederkehrend gemäß § 16 BetrSichV geprüft wird, erfolgt in sinngemäßer Anwendung von Abschnitt 6.2.

(3) Im Rahmen der wiederkehrenden Prüfung sind zur Feststellung der Eignung und Anwendung der CS-Maßnahmen folgende Punkte additiv zu prüfen:

a) Sind die bisher festgelegten CS-Maßnahmen für die schutzbedürftigen Systeme weiterhin vorhanden und in Funktion bzw. werden organisatorische Regelungen eingehalten?

b) Hat der Betreiber die Belange der Cyber-Sicherheit gemäß § 4 Absatz 6 BetrSichV in seine betriebliche Organisation eingebunden (z. B. durch einen geeigneten Prozess) und überprüft entsprechend den Vorgaben des § 3 Absatz 7 BetrSichV, ob seine CS-Maßnahmen noch geeignet sind?

c) Sind die bisher festgelegten CS-Maßnahmen, auch unter Berücksichtigung des fortschreitenden Standes der Technik und der Cyberbedrohungen, weiterhin als wirksam anzusehen bzw. wurden sie, falls dieses nicht der Fall ist, durch neue CS-Maßnahmen ersetzt oder ergänzt?

7 Prüfaussagen und Mängeldefinitionen

(1) Es wird empfohlen, in der Prüfbescheinigung nach § 17 Absatz 1 BetrSichV je nach Prüfumfang die folgenden ggf. zutreffenden Aussagen, zumindest Buchstabe a), zu CS-Maßnahmen sinngemäß aufzunehmen:

a) „Eine Dokumentation zur Behandlung von Cyberbedrohungen wurde nicht vorgelegt."

b) „Die schutzbedürftigen Systeme sowie ihre Aufgaben wurden vom Betreiber nicht erfasst und dokumentiert."

c) „Die schutzbedürftigen Systeme wurden durch den Betreiber nicht hinsichtlich der Möglichkeit eines Integritätsverlusts und der Auswirkungen durch Cyberbedrohungen bewertet."

d) „Es wurden keine Festlegungen von CS-Maßnahmen durch den Betreiber getroffen, um den Cyberbedrohungen in geeigneter Weise zu begegnen und die Auswirkungen zu begrenzen."

e) „Die organisatorischen CS-Maßnahmen sind geeignet und in die betriebliche Organisation eingebunden. Die technischen CS-Maßnahmen sind geeignet und funktionsfähig."

Die unter b) – d) aufgeführten Aussagen können falls sinnvoll auch geeignet zusammengefasst werden.

(2) Abweichend von den allgemeinen Begriffsbestimmungen für die Mängeleinstufungen werden für die vollständige Prüfung der Cybersicherheit nach Abschnitt 6 die folgenden Mängeldefinitionen festgelegt:

Ohne Mangel:	Die Maßnahmen der Cybersicherheit für die schutzbedürftigen Systeme entsprechen dem Stand der Technik zum Zeitpunkt der Prüfung und sind geeignet und funktionsfähig.
Geringfügiger Mangel:	Für die Cybersicherheit erforderliche Prozesse sind nicht dokumentiert oder es gibt Mängel bei der technischen Umsetzung von Prozessen, die nicht einem erheblichen Mangel entsprechen.
Erheblicher Mangel:	Es gibt ungeschützte Verbindungen von schutzbedürftigen Systemen in unzureichend geschützte Bereiche, die zu Gefährdungen führen können oder für die Cybersicherheit erforderliche Prozesse und Verantwortlichkeiten sind nicht vorhanden.
Gefährlicher Mangel:	Eine Kompromittierung von schutzbedürftigen Systemen ist aktuell gegeben.

Inhaltsverzeichnis