**Beschluss des EK ZÜS** **ZÜS B-002 rev 2**

| | | |
|---|---|---|
| Abgestimmt im EK ZÜS | Schriftliche Abstimmung | 27.05.2022 |
| | 34. Sitzung, TOP 6.2 | 16.11.2022 |
| | 36. Sitzung, TOP 8.10 | 15.11.2023 |

# 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 Betreibers 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.

Hinweis: Um den sich ständig ändernden Bedrohungen fortlaufend zu begegnen, ist es für die Cybersicherheit wesentlich, dass diesbezüglich Strukturen und Prozesse eingerichtet und aufrechterhalten werden.

(2) 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 der Abwehr von wirtschaftlichen Schäden oder von Angriffen auf den Datenschutz (z. B. von personenbezogenen Daten) dienen, werden nicht berücksichtigt.

(4) Der Prüfumfang umfasst auch über sicherheitsrelevante MSR-Einrichtungen hinausgehende Teile der überwachungsbedürftigen Anlagen (z. B. Notrufeinrichtungen, Alarmierungseinrichtungen) oder andere technische Infrastrukturen, wenn für sie als Ergebnis der Gefährdungsbeurteilung ein Schutz gegen Cyberbedrohungen als erforderlich angesehen wird. Die hinsichtlich der Prüfung von CS-Maßnahmen relevanten Einrichtungen werden nachfolgend als „schutzbedürftige Einrichtungen“ (zum Begriff siehe Abschnitt 3 Absatz 7) bezeichnet.

(5) CS-Maßnahmen derjenigen IT/OT[1]-Systeme, die mit schutzbedürftigen Einrichtungen in Verbindung stehen und als Angriffswege genutzt werden können, sind Bestandteil des Prüfumfanges.

[1] OT = Operational Technology

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

(7) Die Cybersicherheit ist Gegenstand folgender Prüfungen:

- Anhang 2 Abschnitt 2 Nummern 3 und 4.1 BetrSichV Aufzugsanlagen
- Anhang 2 Abschnitt 3 Nummern 4.1 und 5.1 BetrSichV Explosionssicherheit
- nach Anhang 2 Abschnitt 4 Nummern 4 und 5 BetrSichV (Prüfung vor Inbetriebnahme von Druckanlagen und wiederkehrende Anlagenprüfungen)
- Prüfbericht zur Erlaubnis nach § 18 Absatz 3 BetrSichV

(8) Schutzbedürftige Einrichtungen, die aufgrund nicht vorhandener Datenschnittstellen (sowohl kabelgebunden als auch kabellos) nicht kompromittiert werden können, benötigen keine Maßnahmen der Cybersicherheit.

## 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) zu beurteilen und geeignete Schutzmaßnahmen zu treffen.

(2) Die TRBS 1115-1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“ konkretisiert die Betriebssicherheitsverordnung (BetrSichV) im Hinblick auf die Ermittlung, Festlegung und Prüfung erforderlicher CS-Maßnahmen für die dauerhafte Sicherstellung der Funktionsfähigkeit von sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen (MSR-Einrichtungen), die als technische Schutzmaßnahme für die sichere Verwendung von Arbeitsmitteln inklusive überwachungsbedürftigen Anlagen eingesetzt werden.

(3) Zu CS-Maßnahmen gibt es noch keine gültigen Vorgaben für die Bereitstellung von Arbeitsmitteln auf dem Markt[2] (Inverkehrbringen). Deshalb 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 November 2023

## 3 Begriffsbestimmungen im Sinne dieses Beschlusses

(1) Es gelten die Definitionen TRBS 1115-1 für:

- Cybersicherheit,
- Cyberbedrohung,
- IT/OT-Umgebung und
- CS-Maßnahmen

(2) **schutzbedürftige Einrichtungen** sind:

- sicherheitsrelevante MSR-Einrichtungen,
- 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
- für die Sicherheit relevante Einrichtungen, die keine MSR-Einrichtung sind (z. B. Notrufeinrichtungen, Notbefehlseinrichtungen), im Folgenden autarke Sicherheitseinrichtungen genannt,

soweit eine Kompromittierung durch Cyberbedrohungen möglich ist. sowie

- Teile der IT/OT-Umgebung für die CS-Maßnahmen zum Schutz von Angriffszielen erforderlich sind

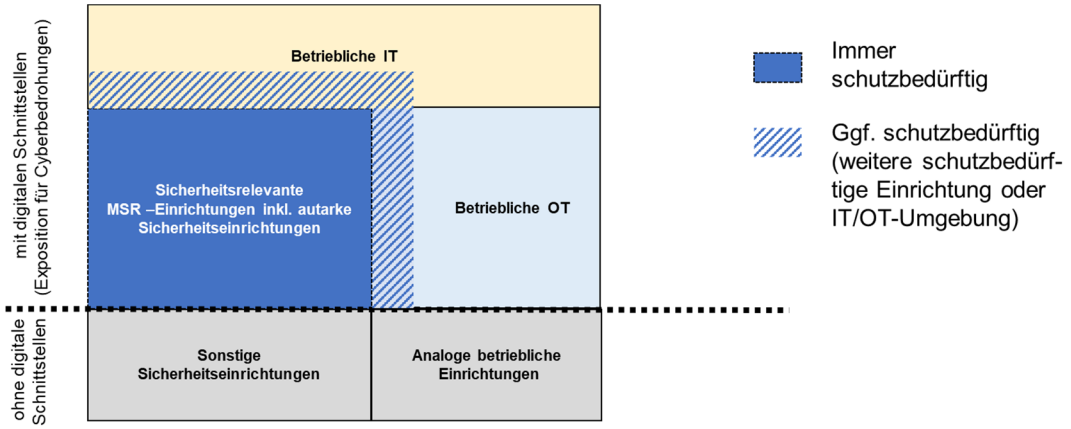


Abbildung 1: Darstellung der schutzbedürftigen Einrichtungen und der IT/OT-Umgebung

## 4 Grundsätze der Prüfung

(1) Ziel der Überprüfung ist die Bestätigung, dass die erforderliche Cybersicherheit der Einrichtungen gegeben ist.

(2) Zum Nachweis der Wirksamkeit der Schutzmaßnahmen ist sowohl eine Ordnungsprüfung als auch ein Nachweis der Funktionsfähigkeit erforderlich.

(3) Prüfinhalte, die im Rahmen eines Konformitätsbewertungsverfahrens geprüft und dokumentiert wurden, müssen nicht erneut geprüft werden (§ 14 Absatz 1 Satz 3 BetrSichV, § 15 Absatz 1 Satz 4 BetrSichV).

(4) Die zugelassene Überwachungsstelle kann sich die durch die Anwendung eines Managements der Cybersicherheit erzeugten Ergebnisse zu eigen machen. Wird kein Management der Cybersicherheit nach TRBS 1115-1 Anhang 1 angewendet, kann sich die zugelassene Überwachungsstelle die Ergebnisse der Überprüfung der Wirksamkeit der CS-Maßnahmen zu eigen machen, wenn Durchführung und Ergebnis der Überprüfung für sie plausibel und nachvollziehbar sind.

## 5 Grundanforderungen an die Cybersicherheit in überwachungsbedürftigen Anlagen

(1) Im Rahmen der Gefährdungsbeurteilung hat der Betreiber zu ermitteln, ob Cyberbedrohungen zu Gefährdungen von Beschäftigten oder Personen im Gefahrenbereich führen können.

(2) Die TRBS 1115-1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“ zeigt einen Prozess zur Ermittlung, Festlegung und Prüfung erforderlicher CS-Maßnahmen nach dem Stand der Technik. Dieser Prozess ist auf alle schutzbedürftigen Einrichtungen anwendbar und unterscheidet zwischen verwendungsfertigen Arbeitsmitteln mit bestätigtem Schutz vor Cyberbedrohungen und Arbeitsmitteln, bei denen der Betreiber die erforderlichen CS-Maßnahmen selbst ermitteln muss.

## 6 Prüfung der CS-Maßnahmen

Vorbemerkung:

Die folgenden Prüfschritte richten sich nach den zum Zeitpunkt der jeweiligen Prüfung geltenden Anforderungen aus BetrSichV und ÜAnlG und den zugehörigen technischen Regeln, insbesondere der TRBS 1115-1. Die Einführung der einzelnen Prüfschritte erfolgt zeitlich gestaffelt.

Die Prüfung der CS-Maßnahmen erfolgt im Umfang des Abschnitt 1 Absätze 4 und 5.

Die Überprüfung der Wirksamkeit von CS-Maßnahmen gemäß TRBS 1115-1 Abschnitt 5 und der Kontrollen gemäß TRBS 1115-1 Abschnitt 8.2 sind nicht Bestandteil der Prüfung durch die ZÜS gemäß TRBS 1115-1 Abschnitt 6 und 7. Soll die Überprüfung / Kontrolle durch die ZÜS im Rahmen der Prüfung erfolgen, ist eine entsprechende Beauftragung erforderlich.

Die Prüfung der Eignung von CS-Maßnahmen setzt einen strukturierten und dokumentierten Prozess zur Festlegung der CS-Maßnahmen entsprechend den Vorgaben der TRBS 1115-1 voraus. Die Dokumentation hierzu ist zur Prüfung vorzulegen.

### 6.1 Prüfung im Erlaubnisverfahren

Es ist zu prüfen, ob der Antragsteller Aspekte der Cybersicherheit in den für das Erlaubnisverfahren zu prüfenden Unterlagen entsprechend den Anforderungen der TRBS 1115-1 angemessen berücksichtigt hat.

### 6.2 Grundlagen zur Prüfung vor Inbetriebnahme oder vor Wiederinbetriebnahme nach einer prüfpflichtigen Änderung durch eine ZÜS

(1) Aus der TRBS 1115-1 ergeben sich die folgenden Prüfinhalte:

- Eignung und Funktionsfähigkeit der CS-Maßnahme,
- Plausibilität der Dokumentation und der Festlegung der erforderlichen CS-Maßnahmen,
- Feststellung, ob ein Verfahren zur Aufrechterhaltung des Cybersicherheitsniveaus vorhanden ist.

(2) Die Prüfung der Eignung der CS-Maßnahmen erfolgt in Form einer Plausibilitätsprüfung des Prozesses gemäß TRBS 1115-1 Abschnitt 4.4.3.

## 6.3 Vorgehen bei der Prüfung vor Inbetriebnahme oder vor Wiederinbetriebnahme nach einer prüfpflichtigen Änderung

(1) Bis zum 31. März 2024 ist zu prüfen, ob Cyberbedrohungen im Rahmen der Gefährdungsbeurteilung dokumentiert behandelt werden.

(2) Ab dem 1. April 2024 wird eine Plausibilitätsprüfung der Prozesse zur Planung und Realisierung der CS-Maßnahmen durchgeführt. Insbesondere sind hierbei die in den folgenden Absätzen dargestellten Punkte zu prüfen.

(3) Sind die sicherheitsrelevanten MSR-Einrichtungen und weitere schutzbedürftige Einrichtungen erfasst und dokumentiert?

Hinweis: Im Rahmen der Prüfung durch die ZÜS sind hinsichtlich der Cybersicherheit insbesondere die sicherheitsrelevanten MSR-Einrichtungen, die für den sicheren Betrieb erforderlich sind (vgl. z.B. TRBS 1201-x, TRBS 1115, EK ZÜS Beschluss BE-006) und auch im Rahmen der klassischen Anlagen-/Anlagenteilprüfung geprüft werden, einschließlich relevanter Teile der IT-/OT-Umgebung, zu betrachten.

(4) Wurden mögliche Auswirkungen auf die Integrität und Verfügbarkeit der Einrichtungen durch Cyberbedrohungen ermittelt und bewertet?

Hinweis: Die Bewertung der möglichen Auswirkungen erfolgt ohne Berücksichtigung von bereits bestehenden oder geplanten CS-Maßnahmen.

(5) Sind nachvollziehbare Festlegungen von CS-Maßnahmen für die Einrichtungen getroffen, um die geforderte Funktionsfähigkeit sicher zu stellen, und sind sie plausibel?

- Gibt es eine dokumentierte Festlegung der erforderlichen Maßnahmen der Cybersicherheit (Ja / Nein). Wenn ja, wurden die Standardmaßnahmen der TRBS 1115-1 Abschnitt 4.5.2 Absatz 2 behandelt?
- Sind Herstellervorgaben vorhanden und wenn ja, wurden diese berücksichtigt?

(6) Gibt es Verfahren zur Aufrechterhaltung des Cybersicherheitsniveaus (z. B. Aufspielen von Software-Updates oder sicherheitsrelevanten Patches)?

(7) Wurden die Vorgaben für die organisatorischen CS-Maßnahmen in Betriebsanweisungen umgesetzt?

(8) Liegt ein Nachweis der Funktionsfähigkeit der CS-Maßnahmen vor? (je nach Art und Umfang der CS-Maßnahmen erfolgt die Prüfung auch in Form einer geeigneten Stichprobe)

(9) Wurde die mögliche Beeinträchtigung der Wirksamkeit der sicherheitsrelevanten MSR-Einrichtungen und autarken Sicherheitseinrichtungen durch die festgelegten CS-Maßnahmen und deren Umsetzung betrachtet (Rückwirkungsfreiheit)?

## 6.4 Grundlagen zur wiederkehrenden Prüfung

(1) Aus der TRBS 1115-1 ergeben sich die folgenden Prüfinhalte:

- Sind die vorgesehenen CS-Maßnahmen weiterhin geeignet und funktionsfähig?
- Werden anlassbezogene neue Erkenntnisse zu Cyberbedrohungen, z. B. nach bekanntgewordenen Sicherheitslücken oder aus dem fortschreitenden Stand der Cybersicherheitstechnik berücksichtigt,
- Wurden falls erforderlich Anpassungen an den CS-Maßnahmen vorgenommen,
- Wurden prüfpflichtige Änderungen an der überwachungsbedürftigen Anlage hinsichtlich der Auswirkungen auf die erforderlichen CS-Maßnahmen bewertet?

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

## 6.5 Vorgehen bei der wiederkehrenden Prüfung

(1) Im Rahmen der wiederkehrenden Prüfung sind die nachfolgenden Punkte zu prüfen.

a) Sind Nachweise der Kontrolle der technischen CS-Maßnahmen vorhanden?

b) Werden organisatorische CS-Maßnahmen angewendet bzw. eingehalten? (je nach Art und Umfang der CS-Maßnahmen erfolgt die Prüfung auch in Form einer geeigneten Stichprobe)

(3) Sind die CS-Maßnahmen weiterhin geeignet?

a) werden neue Erkenntnisse zu Cyberbedrohungen, soweit es diese gibt, berücksichtigt und erforderliche Anpassungen an den CS-Maßnahmen vorgenommen

b) wurden die Auswirkungen auf die CS-Maßnahmen für prüfpflichtiger Änderungen bewertet

# 7 Mängeldefinitionen

Abweichend von den allgemeinen Begriffsbestimmungen für die Mängeleinstufungen werden für die vollständige Prüfung der Cybersicherheit nach Abschnitt 6 dieses Beschlusses die folgenden Mängeldefinitionen festgelegt, die bei der Bewertung der überwachungsbedürftigen Anlage zu berücksichtigen sind:

| | |
|---|---|
| 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 geschützten Bereichen, 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