Ausgabe: März 2019
GMBl 2019 S. 289 [Nr. 13–16]

Empfehlungen zur Betriebssicherheit	Umgang mit Risiken durch Angriffe auf die Cyber-Sicherheit von sicherheitsrelevanten MSR-Einrichtungen	EmpfBS 1115

Die Empfehlungen zur Betriebssicherheit (EmpfBS) werden gemäß § 21 Absatz 5 Nummer 1 der Betriebssicherheitsverordnung (BetrSichV) vom **Ausschuss für Betriebssicherheit (ABS)** ausgesprochen und geben den Stand der Technik, Arbeitsmedizin und Arbeitshygiene sowie sonstige gesicherte arbeitswissenschaftliche Erkenntnisse für die Verwendung von Arbeitsmitteln wieder.

Die EmpfBS lösen im Gegensatz zu den Technischen Regeln für Betriebssicherheit (TRBS) nicht die Vermutungswirkung im Sinne von § 4 Absatz 3 Satz 2 BetrSichV aus.

Inhalt

1 Anwendungsbereich

(1) Diese Empfehlung richtet sich an Arbeitgeber, die im Rahmen der Betriebssicherheitsverordnung (BetrSichV) eine Gefährdungsbeurteilung im Hinblick auf die sichere Verwendung von Arbeitsmitteln durchzuführen und daraus geeignete Schutzmaßnahmen abzuleiten haben.

(2) Sie beschreibt in allgemeiner Form Wege zur Ermittlung von Risiken durch Angriffe auf die Cyber-Sicherheit von sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen (MSR-Einrichtungen) sowie Maßnahmen zur wirksamen Reduzierung der ermittelten Risiken.

2 Begriffsbestimmungen

Cyber-Sicherheit	Cyber-Sicherheit im Sinne dieser Empfehlung umfasst die Aspekte der Sicherheit von MSR-Einrichtungen, soweit deren Informationstechnik durch Cyber-Bedrohungen kompromittiert werden kann.
Cyber-Bedrohung	Bedrohung der Integrität, Verfügbarkeit und Vertraulichkeit der MSR-Einrichtung mit Methoden und Werkzeugen der IT
Prozessleitsystem	Automatisierungssystem, mit dem eine Anlage/ein technischer Prozess automatisch gesteuert, geregelt und visualisiert wird.
Sicherheitsrelevante MSR-Einrichtungen	Sicherheitsrelevante MSR-Einrichtungen sind Mess-, Steuer- und Regeleinrichtungen an Arbeitsmitteln, die deren sicherer Verwendung dienen. Sie bestehen aus Sensor-, Aktor- und Logikeinheiten sowie zugehörigen Verbindungseinrichtungen.

3 Ermittlung von Gefährdungen durch Angriffe auf die Cyber-Sicherheit

3.1 Allgemeine Anforderungen

(1) Der Arbeitgeber hat nach § 3 BetrSichV die auftretenden Gefährdungen zu beurteilen und daraus notwendige Maßnahmen für das sichere Verwenden von Arbeitsmitteln abzuleiten. Nach § 5 Absatz 1 BetrSichV dürfen nur Arbeitsmittel zur Verfügung gestellt werden, die unter Berücksichtigung der am Arbeitsplatz gegebenen Bedingungen geeignet sind und gemäß § 6 Absatz 1 BetrSichV sicher verwendet werden können.

(2) Durch den Einsatz von IT-basierten Technologien und steigendem Vernetzungsgrad von Automatisierungssystemen können sicherheitsrelevante MSR-Einrichtungen zum Ziel von Manipulationen werden.

(3) Cyber-Sicherheitsaspekte sind während der gesamten Verwendungsdauer (Lebenszyklus), d. h. in der Planung, der Beschaffung, der Bereitstellung, im Betrieb, bei Änderungen und bei der Außerbetriebnahme, zu berücksichtigen. Betroffen sind die folgenden Komponenten einer sicherheitsrelevanten MSR-Einrichtung:

- Hardware,
- Software,
- Daten,
- Netzwerk(-verbindungen) sowie die mit ihrer Verwendung verbundenen
- Prozesse,
- Organisationen sowie
- Personen.

3.2 Gefährdungen durch Cyber-Bedrohungen ermitteln und bewerten

(1) Im Rahmen der Gefährdungsbeurteilung ist zu ermitteln, welche Möglichkeiten bestehen, dass durch Manipulation eine sicherheitsrelevante MSR-Einrichtung ihre Sicherheitsfunktion nicht mehr ausüben kann und damit Gefährdungen nicht mehr verhindert bzw. sogar herbeigeführt werden können. Dazu ist erforderlich:

1. Erfassen aller Elemente gemäß Nummer 3.1 Absatz 3 des betrachteten Systems und ihrer Aufgaben,
2. Erfassen und Bewerten von Bedrohungen der Integrität der sicherheitsrelevanten MSR-Einrichtungen, die durch Manipulation dieser Elemente ausgehen.

(2) Sicherheitsrelevante MSR-Einrichtungen können in Bezug auf Cyber-Sicherheit in drei wesentliche Bereiche unterteilt werden (siehe Abbildung):

- Zone A (sicherheitsrelevante MSR-Einrichtung) umfasst sicherheitsrelevante MSR-Einrichtungen, die für die Sicherheitsfunktion zwingend erforderlich sind:
  - Logiksystem,
  - Ein- und Ausgabebaugruppen inkl. Remote-I/O sowie den Aktoren und Sensoren, Verbindungen und
  - ggf. vorhandene Netzwerkkomponenten (Switches, Router, Server etc.), die der Verbindung zwischen Geräten der Zone A dienen.
- Zone B (erweiterte sicherheitsrelevante MSR-Einrichtung) umfasst Komponenten, die für die Auslösung der Sicherheitsfunktion nicht notwendig sind, jedoch das Verhalten der sicherheitsrelevanten MSR-Einrichtung beeinflussen können. Typische Beispiele sind Bedien-/Eingabestationen und Visualisierungsstationen mit sicherheitsrelevanter Funktion, das Programmiergerät (Engineering Station) für die sicherheitsrelevante MSR-Einrichtung und das Asset Management System (AMS) bzw. Vorrichtungen zu Sensor/Aktor-Konfiguration.
- Die Umgebung umfasst Komponenten und Systeme, die weder direkt noch indirekt der sicherheitsrelevanten MSR-Einrichtung zuzuordnen sind, aber in Verbindung mit der Sicherheitsfunktion stehen können (z. B. Betriebsdateninformationssystem – BDIS, Visualisierung Sicherheitsfunktion-Zustand etc., Service-IT für z. B. Patchmanagement, Domain Control und Virenschutz, Internet).

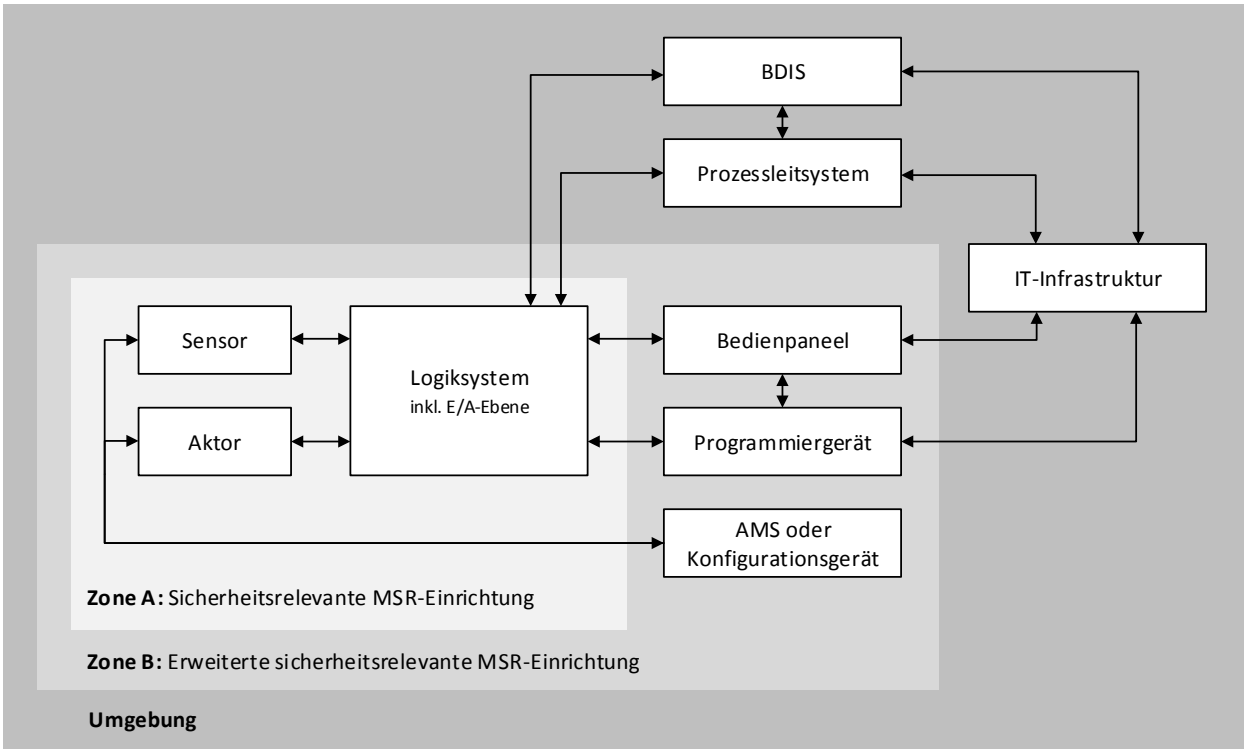

Abb. Funktionale Zonen einer sicherheitsrelevanten MSR-Einrichtung (nach NAMUR-Arbeitsblatt NA 163)

4 Schutzmaßnahmen

4.1 Allgemeine Anforderungen

(1) Ziel der Maßnahmen ist der Schutz der Komponenten und Konfigurationsdaten der sicherheitsrelevanten MSR-Einrichtung vor Verletzung der funktionalen Integrität bzw. Minderung der Auswirkungen einer verletzten funktionalen Integrität. Damit die Komponenten und Daten wirksam geschützt werden können, müssen sowohl die Hard- und Softwarekomponenten als auch die Prozesse, Personen und Organisationen, die den Lebenszyklus der sicherheitsrelevanten MSR-Einrichtung beeinflussen, gegen mögliche Cyber-Bedrohungen gerüstet sein.

(2) Um das unberechtigte Eindringen in eine sicherheitsrelevante MSR-Einrichtung zu unterbinden, ist in folgender Weise zu verfahren:

1. Festlegen von Maßnahmen, um den Bedrohungen in geeigneter Weise zu begegnen und die Auswirkungen zu begrenzen.
2. Umsetzung der festgelegten Maßnahmen und überprüfen, ob die festgelegten Maßnahmen wirksam umgesetzt sind.
3. Regelmäßige Überprüfung, dass die festgelegten Maßnahmen die Auswirkungen der Bedrohungen noch wirksam begrenzen.

(3) Die Anforderungen nach Absatz 2 können im Rahmen eines geeigneten IT-Security-Management, z. B. ISMS nach ISO 27000-Normenreihe umgesetzt werden.

4.2 Schutzmaßnahmen festlegen und umsetzen

4.2.1 Zugangs- und Zugriffskontrolle

(1) Der Schutz der Komponenten wird u. a. durch die Kontrolle des physischen und logischen Zugangs auf die Komponenten erreicht. Entsprechend sind Rollen, Rechte und wirksame Authentifizierungsverfahren (Zugangskarten, Passwörter etc.) zu betrachten und eindeutig festzulegen. Dazu gehört beispielsweise die Änderung von Standardpasswörtern vor erstmaliger Inbetriebnahme.

(2) Der Benutzerzugriff aus Zone A und B auf das Internet und umgekehrt, z. B. E-Mail-Anhänge, ist mit besonders hohen Risiken verbunden und deshalb technisch zu unterbinden. Der Zugriff aus Zone A und B durch automatisierte Dienste, z. B. Auslesen von Statusinformationen, ist in Zone A und B rückwirkungsfrei zu initiieren und geeignet abzusichern.

4.2.2 Härtung von Komponenten

Die Systemkomponenten (Software, Hardware, Daten) sind auf ein dem Einsatzzweck entsprechendes Mindestmaß zu reduzieren, ggf. ist Rücksprache mit dem Hersteller zu halten. Reduzierung umfasst 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).

4.2.3 Umgang mit Daten

(1) Statische Daten, wie z. B. die Parameter eines Sensors oder das Applikationsprogramm des Logik-Systems, bestimmen die Integrität der sicherheitsrelevanten MSR-Einrichtung. Andere statische Daten stehen in einem mittelbaren Zusammenhang mit der Integrität der sicherheitsrelevanten MSR-Einrichtung (z. B. Material- und Anlagenspezifikationen, Betriebsanleitungen, Risiko-Analysen (z. B. HAZOP) für Prozessanlagen, Funktionspläne, Systemarchitekturdiagramme). Solche Daten entstehen über den gesamten Lebenszyklus hinweg und werden an vielen Orten erzeugt und gespeichert (bei Planern, Kontraktoren, System-Integratoren, System-Herstellern, Betreibern).

(2) Statische Daten sind von ihrem Eigentümer ihrer Relevanz entsprechend zu klassifizieren (z. B. intern, vertraulich, streng vertraulich). Entsprechend der Klassifizierung werden Maßnahmen zum Schutz vor Ausspähen und Manipulation dieser Daten veranlasst. Dabei sind alle Orte zu berücksichtigen, an denen diese Daten gespeichert sind.

(3) Je nach Auswirkung auf die Integrität der sicherheitsrelevanten MSR-Einrichtung muss bei der Anwendung im Lebenszyklus der MSR-Einrichtung die Integrität der Daten sichergestellt werden (z. B. durch elektronische Signatur und Verschlüsselung zentraler Spezifikationsdokumente).

4.2.4 Unabhängigkeit von Einrichtungen

(1) Sicherheitsrelevante MSR-Einrichtungen müssen so ausgelegt sein, dass sie durch betriebliche MSR-Einrichtungen nicht unzulässig beeinflusst werden können.

(2) In Einzelfällen können Komponenten von verschiedenen Systemen gemeinsam genutzt werden, d. h. es erfolgt eine Kombination von sicherheitsrelevanten und betrieblichen Funktionen innerhalb einer Komponente. Derartige Kombinationen liegen beispielsweise auf Sensor-/Aktor-Ebene, beim Logiksystem, beim Programmiergerät und bei der IT-Infrastruktur vor.

(3) Für die Cyber-Sicherheit der gemeinsam genutzten Komponente ist ein zusätzlicher Nachweis zu erbringen, d. h. in der Gefährdungsbeurteilung ist zu bewerten, ob sich durch die gemeinsame Nutzung erhöhte Cyber-Sicherheitsrisiken für die sicherheitsrelevante MSR-Einrichtung ergeben können.

4.3 Cyber-Schutzmaßnahmen überprüfen und anpassen

Aus § 3 Absatz 7 BetrSichV lassen sich insbesondere folgende Anlässe für eine Überprüfung der Maßnahmen zur Sicherheit des Arbeitsmittels ableiten:

- regelmäßige Wirksamkeitsprüfung in bestimmten Zeitabständen,
- bei sich ändernden Gegebenheiten, z. B. nach Änderungen am Arbeitsmittel, der Arbeitsaufgabe, des Arbeitsverfahrens, der Umgebungsbedingungen, der allgemeinen Cyber-Bedrohungslage,
- Anpassung bei neuen Erkenntnissen anstreben, z. B.
  - nach Cyber-Sicherheits-Vorfällen,
  - bei überarbeitetem Technischem Regelwerk,
  - bei Änderungen des sicherheitstechnischen Niveaus und
  - bei Änderungen des Standes der Technik beim Bereitstellen auf dem Markt.

5 Literatur

TRBS 1111 (März 2018) Gefährdungsbeurteilung

KAS-44 (November 2017) Leitsätze der Kommission für Anlagensicherheit zum Schutz vor cyberphysischen Angriffen

DIN EN ISO/IEC 27001:2013 + Cor. 1:2014 + 2:2015 Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen

DIN EN 61511-1:2005 Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie

NA 163: Ausgabe 2017-12-15 IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen

IT-Grundschutz-Kompendium – Edition 2018 (Bundesamt für Sicherheit in der Informationstechnik)

Leitfaden zur Basis-Absicherung nach IT-Grundschutz (Oktober 2017) (Bundesamt für Sicherheit in der Informationstechnik)

ICS-Security-Kompendium (November 2014) (Bundesamt für Sicherheit in der Informationstechnik)

IT-Security in der Industrie 4.0 – Handlungsfelder für Betreiber (2016)