Ausfüllhilfe mit Beispielen

sowie Hinweise und Hintergrundwissen zum Thema Cybersicherheit

Einleitung

Von der kontinuierlichen Entwicklung und Zunahme der Digitalisierung, welche in allen Bereichen des Lebens immer schneller voranschreitet, sind komplexe Steuerungs- und Kontrollsysteme großer Industrieanlagen genauso betroffen wie einfache elektronische Einrichtungen für Aufzugs- oder Druckanlagen. Immer häufiger werden Unternehmen oder Verwaltungen aller Größen Opfer von Angriffen, bei welchen Daten gestohlen, manipuliert oder verschlüsselt werden. Mögliche Folgen sind geschäfts-/rufschädigend, Betriebsstörungen/-ausfälle, Schadensersatz- oder Lösegeldforderungen, bis hin zu einem Personenschaden. Um die Gefahren von Personenschäden so gering wie möglich zu halten, spielt im Rechtsbereich der Betriebssicherheitsverordnung der Arbeits- und Gesundheitsschutz von Beschäftigten und dritten Personen eine entscheidende Rolle. Dabei muss der Umgang mit Arbeitsmitteln sicher sein und dem Stand der Technik entsprechen.

Die zunehmende Datenvernetzung und der steigende Automatisierungsgrad von Arbeitsmitteln führt zum Anstieg sicherheitsrelevanter Mess- Steuer- und Regeleinrichtungen (MSR), um die Arbeitsprozesse weiterhin sicher zu gestalten.

Wenn es Cyberkriminellen gelingt, die sicherheitsrelevanten MSR-Einrichtungen zu kompromittieren (dt. Fremdwort lat. Ursprungs mit den Bedeutungen [a] blamieren, bloßstellen, vorführen bzw. [b] angreifen, beeinträchtigen, manipulieren, stören – in diesem Text sei dieses Wort immer mit Bedeutung [b] zu verstehen), können Mitarbeiter des Unternehmens, aber auch weitere Nutzer oder Gäste bis hin zum Betreiber selbst in Gefahr geraten. Genau dieses gilt es zu vermeiden.

Welche Pflichten hat der Betreiber?

Zur Minderung des Risikos, welches die Cybersicherheit betrifft, hat der Gesetzgeber am 22. März 2023 im Rechtsbereich der Betriebssicherheitsverordnung (BetrSichV) die Technische Regel für Betriebssicherheit (TRBS) 1115 Teil 1 veröffentlicht. Die am 13. Mai 2024 veröffent-lichten EK ZÜS Beschlüsse B-002 (3), sowie BA-017 für den Bereich der Aufzugsanlagen, liefern ergänzende Informationen, wie die Anforderungen aus der TRBS 1115-1 durch eine ZÜS überprüft werden.

Die in der TRBS 1115-1 geforderten Vorkehrungen zur Cybersicherheit werden anhand der vom Betreiber vorgelegten Dokumentation seitdem auch auf Plausibilität, sowie zu einem späteren Zeitpunkt auf Wirksamkeit der getroffenen Maßnahmen bewertet.

Für die Einarbeitung in das Thema Cybersicherheit und die dazugehörigen Betreiberpflichten haben wir für Sie am Ende eine Auflistung kostenloser Dokumente zusammengestellt.

Betrifft diese Thematik nur Anlagen oder Anlagenteile mit einer Internetverbindung?

Nein, denn beim Thema Cybersicherheit sind alle Schnittstellen zu betrachten, über welche die Funktionsweise oder Schutzmechanismen der Anlage beeinflusst oder beeinträchtigt werden können. Denn lokale Schnittstellen oder Übergänge zu Bussystemen, Netzwerken, Mobilfunknetzen (z. B. CAN, USB, Ethernet, WiFi, Bluetooth, ...) erlauben es unter Umständen auf das Verhalten der Anlage Einfluss auszuüben.
Sei es durch Änderungen an Konfigurationsdaten oder Berechtigungen, Beeinträchtigung der Datenübertragung, Kompromittierung der eigentlichen Betriebsfunktionen (unmittelbar oder zu einem späteren Zeitpunkt), bis hin zum Außerkraftsetzen ganzer Anlagenbereiche. Gerade deshalb müssen alle Schnittstellen im Sicherheitskonzept berücksichtigt werden.

Ein Angriff kann beispielsweise über folgende Schnittstellen erfolgen:
- kabelgebundene Schnittstelle (z.B. USB)
- kabellose Schnittstelle (z.B. WLAN, GSM)
- Benutzerschnittstelle (z.B. Eingabefeld)
- Fernzugriff / Fernwartung / Internetzugriff

Übrigens: Ein Hacker braucht nicht zwingend einen direkten Zugriff auf sein Ziel, um dort Schaden anzurichten. Eine häufige Form der Attacke erfolgt indirekt durch sogenannte Malware (engl. malicious = böswillig). Dabei führt das Opfer den Angriff durch ein vorher kompromittiertes System selbst aus.

Inzwischen ist die Cybersicherheit Bestandteil der ZÜS-Prüfung, doch was wird hier eigentlich geprüft?

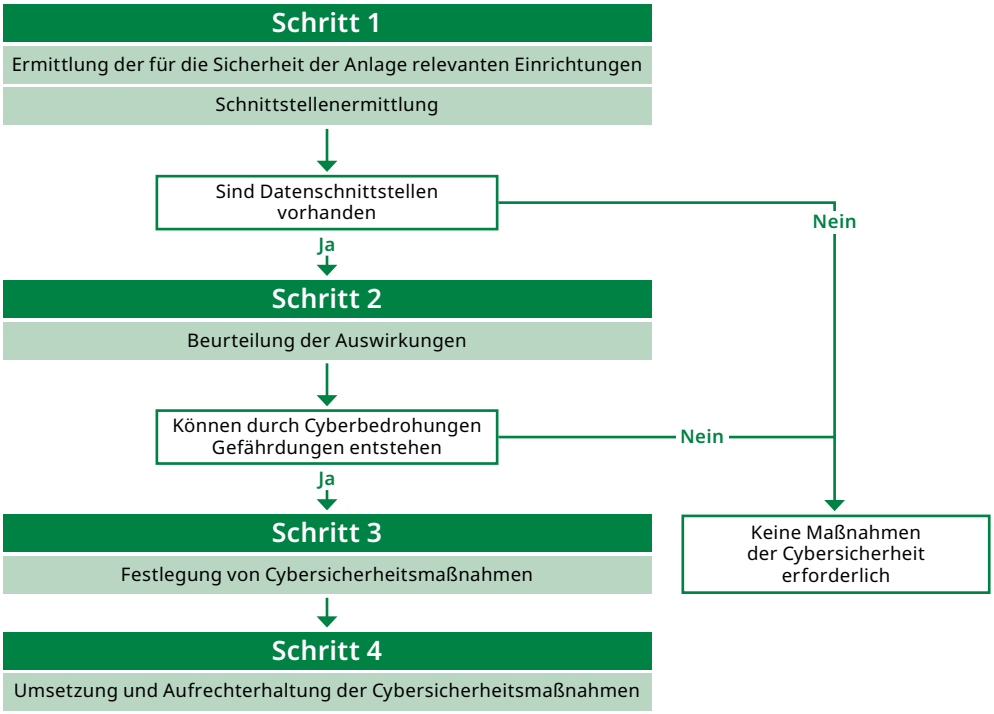
Seit 01.04.2024 hat sich der Prüfumfang für die ZÜS erhöht. Die Sachverständigen prüfen daher ab jetzt die erforderlichen Dokumente auch inhaltlich auf Vollständigkeit und Plausibilität. Der Prüfumfang und die betrachteten Kriterien sind in der aktuellen Fassung des EK ZÜS Beschluss B-002 beschrieben. Dieser gilt sowohl für die Inbetriebnahme (erstmalig oder nach prüfpflichtigen Änderungsmaßnahmen), wie auch für wiederkehrende Prüfungen. Speziell für Aufzugsanlagen dient der Beschluss BA-017 als eine zusätzliche Hilfestellung für die Inhalte des Beschlusses B-002.

Es handelt sich bei der Betrachtung zur Cybersicherheit um einen weiteren Teil der Gefährdungsbeurteilung. Analog zur Gefährdungsbeurteilung wird spezifisches Fachwissen benötigt, damit die betrachteten Gefährdungen vollumfänglich erkannt und wirksame Maßnahmen festgelegt werden. Fehlt dem Betreiber entsprechende Fachkenntnis, kann er nach eigenem Ermessen auch geeignete Dritte hinzuziehen. Hier hat der Betreiber selbst für die Qualität des Dokumentationsmaterials und dessen Umfang Sorge zu tragen.

Übrigens: Als Bestandteil der Gefährdungsbeurteilung muss auch dieses Dokument regelmäßig überprüft und ggf. aktualisiert werden (BetrSichV §3 (7)). Dies kann beispielsweise nach einer Modernisierung notwendig werden. Selbst wenn die Überprüfung der Gefährdungsbeurteilung ergibt, dass keine Aktualisierung erforderlich ist, hat der Betreiber dies unter Angabe des Datums der Überprüfung in der Dokumentation zu vermerken.

Grundsätzliches Vorgehen bei der Betrachtung von sicherheitsrelevanten Einrichtungen

Zum besseren Verständnis und als Hilfestellung bei der Ermittlung von Cybersicherheitsmaßnahmen kann auf das Flussdiagramm im Anhang des Beschlusses B-002 zurückgegriffen werden. Es ist in 4 Schritte aufgeteilt.



In Anlehnung an den Beschluss B-002 bietet DEKRA ein analog strukturiertes Formular für den Betreiber zum Ausfüllen an. Das Flussdiagramm und das DEKRA Formular funktionieren wie eine Art „Filter“: Zu Beginn werden alle sicherheitsrelevanten Einrichtungen mit den dazugehörigen Schnittstellen erfasst, bei denen man eine Relevanz beim Thema Cybersicherheit vermutet. Im weiteren Verlauf der weiteren Schritte werden diese Einrichtungen dann immer detaillierter betrachtet, so dass am Ende der Betrachtung die tatsächlich betroffenen Einrichtungen übrigbleiben und die hierfür notwendigen Maßnahmen feststehen.

Die Grundidee der vier Schritte basiert auf einem aus der Risikoanalyse bekannten Vorgehen. Zu Beginn (im Schritt 1) werden möglicherweise sicherheitsrelevante Einrichtungen und deren Schnittstellen erfasst. Bei fehlenden Schnittstellen wird dies dokumentiert und die Betrachtung ist damit beendet.

Wenn eine Einrichtung über Schnittstellen verfügt, führt dies nicht zu einer pauschalen Festlegung, dass diese Einrichtung auch ein tatsächliches Cyberrisiko darstellt. Denn eine kompromittierte Einrichtung ist (aus Sicht der Betriebssicherheitsverordnung und der TRBS 1115-1) nur dann gefährlich, wenn auch eine tatsächliche Gefahr für Betreiber oder Nutzer besteht.

Genau diese Betrachtung findet im zweiten Schritt statt, in dem für jede Einrichtung geprüft wird, ob bei einer Kompromittierung eine Gefährdung vorliegt. Hat eine kompromittierte Einrichtung keine Auswirkung auf den sicheren Betrieb, kann auch für diese Einrichtung die Betrachtung beendet werden. Die wirtschaftliche Seite (z. B. Anlagenstillstand) wird in der TRBS 1115-1 übrigens nicht berücksichtigt, auch wenn dieser Aspekt unter betriebswirtschaftlichen Gründen sicherlich nicht ignoriert werden sollte.

Erfüllt eine Einrichtung keine der beiden Ausschlusskriterien, durchläuft diese Einrichtung die Schritte drei und vier. Im dritten Schritt werden notwendige Maßnahmen definiert, die erfüllt sein müssen, damit die Gefährdung durch Cyberangriffe auf ein akzeptables Maß reduziert werden.

Doch die beste Maßnahme bringt nichts, wenn sie nicht angewendet wird. Daher wird im vierten Schritt festgelegt, wie die Maßnahmen aus Schritt drei umgesetzt und deren Anwendung auch langfristig sichergestellt werden. Denn das Thema Cybersicherheit ist durch den technologischen Fortschritt so kurzlebig, dass die Maßnahmen vom letzten Jahr vielleicht schon keinen ausreichenden Schutz mehr bieten und überarbeitet werden müssen.

DEKRA Formular, allgemeine Informationen zur Ausfüllhilfe

Wir haben für die Betreiber ein dreiseitiges Formular vorbereitet, welches wir kostenfrei zur Verfügung stellen. Auf den folgenden Seiten möchten wir Ihnen theoretisch und am praktischen Beispiel einer Musteranlage zeigen, wie die zuvor beschriebenen Schritte 1-4 konkret umgesetzt werden können.

DEKRA Formular, Seite 1:
Zunächst werden die Basisinformationen zu Betreiber und der betrachteten Anlage auf der ersten Seite hinterlegt. Entsprechend dem EK ZÜS Beschluss B-017 muss die Dokumentation der Aufzugsanlage eindeutig zugeordnet werden können – die hierzu notwendigen Informationen für die Punkte 1 und 2 finden Sie z. B. auf Ihrer letzten Prüfbescheinigung.

1. Verwender (Betreiber):

Mustermann GmbH
Name

Handwerkstr. 1, 55555 Musterstadt
Adresse

2. Technische Daten der überwachungsbedürftigen Anlage:

☒ Aufzugsanlage ☐ Druckanlage ☐ Druckgeräte ☐ Ex-Anlage

Fabrikhalle, Handwerkstr. 9, 55555 Musterstadt
Betriebsort

2017	Personenaufzug Treppenhaus B
Baujahr	Interne Bezeichnung (nur wenn vorhanden)
PE5486	Aufzugsbau Nord-Süd GmbH
Fabrik-, Herstell- oder Seriennummer (nur wenn vorhanden)	Hersteller (nur wenn zutreffend)

In Punkt 3 teilt der Betreiber der ZÜS mit, ob Cybersicherheitsmaßnahmen an der betrachteten Anlage erforderlich sind. Dies trifft auf den größten Teil der am Markt befindlichen Aufzugsanlagen zu, da bereits ein verbautes konfigurierbares Notrufgerät durch seine Schnittstellen eine Gefährdung darstellen kann und daher in der Regel betrachtet werden muss.

Um die Plausibilität dieser Festlegung prüfen zu können, kann man sich dem Beiblatt „Stufe 2“ bedienen, welches man als Folgeseiten des Formulars findet, oder alternativ eigene Unterlagen bei der Prüfung bereitstellen.

In der aktuellen Fassung des Formulars neu hinzugekommen ist der Punkt 4. Hier kann auf generell gültige Dokumente verwiesen werden, die mehrere Anlagen oder Anlagenteile betreffen. Dies kann z. B. der Nachweis eines vorhandenen Cybersicherheitsmanagementsystems (CSMS) sein. Auch wird die Dokumentation für vorhandene Industrial Information Technology bzw. Operational Technology/Information Technology (IIT/OT/IT) meist nicht für die einzelne Anlage, sondern als eigener (Teil-)Bereich bescheinigt. Dies trifft besonders auf große Unternehmen zu, da hier beispielsweise eigene Netzwerke für Notrufsysteme vorhanden sein können und für diesen Anlagenverbund im Rahmen des internen Cybersichersheitsmanagements bereits Maßnahmen zur Cyberabwehr festgelegt und umgesetzt wurden.

Durch die Vorlage solcher Dokumente können Doppelprüfungen im Sinne der Betriebssicherheitsverordnung vermieden werden.

3. Bewertung der schutzbedürftigen Einrichtungen

Hinweis: Für die Plausibilitätsprüfung durch die ZÜS muss eine Auflistung der betrachteten Anlagenteile vorliegen. Hierfür kann z. B. eine eigene Vorlage, die Musterdokumentation des EK ZÜS Beschlusses B002 oder das bereitgestellte Beiblatt "Stufe 2" verwendet werden.

Die Bewertung der schutzbedürftigen Einrichtungen hat ergeben, dass:

☐ keine weiteren Maßnahmen zur Cybersicherheit notwendig sind.

☒ weitere Maßnahmen notwendig sind, die in den beigefügten Unterlagen / der Gefährdungsbeurteilung dokumentiert wurden.

4. Auflistung zentral verwalteter Dokumente, die für mehr als eine Anlage gültig sind:

Hinweis: Bitte erfassen Sie die Dokumente und deren Anwendungsbereich im Freitextfeld. Dieser Punkt ist beispielsweise bei IT/OT Netzwerken zur Steuerung/Fernüberwachung oder eigenen Notrufzentralen wichtig, da hier meist nicht für jede einzelne überwachungsbedürftige Anlage eine eigenständige Betrachtung durchgeführt wurde.

Alle Notrufgeräte auf dem Firmengelände in der Handwerkstr. 9 sind an ein eigenes, separates Netzwerk angeschlossen. Das Netzwerk verfügt über keine Schnittstellen zu öffentlichen Netzwerken. Der Leitrechner und das Netzwerk unterliegen dem akkreditierten Cybersicherheitsmangement der Firma Mustermann GmbH.
Nachweise: Cybersicherheitsmanagement Dokument 5.3 - Netzwerk für Notruf;
Nachweise: Prüfprotokoll CSM 05.03.2023 zur Wirksamkeit des Cybersicherheitsmanagement

DEKRA Formular, Seite 2, Schritt 1:
Im ersten Schritt werden die für die Cybersicherheit relevanten Einrichtungen und deren Schnittstellen erfasst. Anhaltspunkte für die zu betrachtenden Einrichtungen liefert z.B. das Prüfbuch oder die Bedienanleitung. Eine umfangreiche Liste mit möglichen Bauteilen findet sich als Hilfestellung auch auf **www.dekra.de/cybersicherheit** in den FAQs.

Zur Erfassung der Einrichtungen kann eine der mitgelieferten Vorlagen im DropDown gewählt oder ein freier Text eingegeben werden. Im Idealfall wird die Einrichtung über die Felder „Ermittlung … der sicherheitsrelevanten Einrichtung" und „Hersteller – Typ / Bezeichnung" eindeutig beschrieben.

Die letzte Spalte des ersten Schrittes dient dazu, die an der betrachteten sicherheitsrelevanten Einrichtung vorhandenen Schnittstellen zu erfassen. Hat eine Einrichtung keine Schnittstellen, ist die Betrachtung für diese Einrichtung bereits nach dem ersten Schritt beendet und der Fokus kann auf die übrigen Einrichtungen gelegt werden. Die Einrichtung braucht somit auch nicht mehr im zweiten Schritt „weitergeführt" werden, die im ersten Schritt vergebene laufende Nummer (lfd. Nr.) wird somit nicht mehr weitergeführt.

Sind mehr als 4 Einrichtungen notwendig, speichert man eine weitere Version des Formulars und zählt das „Laufende Nummer“ Feld weiter hoch.

Zur Veranschaulichung wurden an der Musteranlage 4 sicherheitsrelevante Einrichtungen identifiziert, die bei der Betrachtung zur Cybersicherheit berücksichtigt wurden. Die Einrichtungen wurden in den Zeilen 1-4 vollständig mit Hersteller und Bezeichnung erfasst und kategorisiert. Anschließend wurden die vorhandenen Schnittstellen ausgewählt.

Falls die betrachtete Einrichtung über keine Schnittstellen verfügt, oder man über die vorhandenen Schnittstellen keine Veränderungen der Anlagenkonfiguration herbeiführen kann, braucht man keine weiteren Maßnahmen zur Cybersicherheit in Betracht zu ziehen. Dies betrifft im aufgeführten Beispiel die Einrichtung mit der laufenden Nummer 4. Da diese Einrichtung nicht angreifbar ist, muss auch nicht näher darauf eingegangen werden. In allen anderen Fällen geht es mit Schritt 2 weiter.

Schritt 1 - Ermittlung der relevanten Einrichtungen

lfd. Nr.	Ermittlung der für die Sicherheit der Anlage relevanten Einrichtungen	Hersteller - Typ / Bezeichnung	Schnittstellen der Einrichtung(en): 1. keine / nicht programmierbar (z.B. festverdrahtet, Schütz-steuerung, EPROM)	2. kabelgebundene Schnittstelle (z.B. USB)	3. kabellose Schnittstelle (z.B. WLAN, GSM)	4. Benutzerschnittstelle (z.B. Eingabefeld)	5. Fernzugriff / Fernwartung / Internetzugriff
1	Steuerung mit UCM Erkennung	Kotina - FTL Pessral 2.8		X	X	X	X
2	Notruf	Teloris - LSV 2 XXL			X	X	
3	Frequenzumrichter ohne PESSRAL	Zahl-Obick - Gamma 3W		X			
4	Sicherheitsschaltung	Thoissen - SRT 2	X				

DEKRA Formular, Seite 2, Schritt 2:
Der zweite Schritt dient dazu, ein besseres Verständnis für die Auswirkungen von Cyberbedrohungen, auf die im ersten Schritt identifizierte, Einrichtung zu bekommen. Hierzu wird im ersten Feld die eigentliche Schutzfunktion / das Schutzziel der Einrichtung erfasst. Denn nur wenn klar ist, welches Schutzziel durch die Einrichtung sichergestellt werden soll, kann auch die spätere Gefährdung bei einer Kompromittierung richtig eingeschätzt werden.

Diese Bewertung der durch eine Kompromittierung entstehenden Gefährdung erfolgt im zweiten Textfeld. Führt eine Kompromittierung zu einer möglichen Gefährdung (z. B. Ausfall der Einrichtung), sollte die Gefährdung möglichst genau beschrieben werden und es muss eine weitere Betrachtung in Schritt 3 und Schritt 4 durchgeführt werden.

Gibt es trotz Kompromittierung jedoch nachvollziehbar keine Gefährdungen (siehe hierzu auch Kapitel „Grundsätzliches Vorgehen bei der Betrachtung von sicherheitsrelevanten Einrichtungen“), kann an dieser Stelle die Betrachtung für die betroffene Einrichtung beendet werden.

Schritt 2 - Beurteilung der Auswirkungen von Cyberangriffen

lfd. Nr.	Kurzbeschreibung der Schutzfunktion / des Schutzziels	Durch die Folgen einer Manipulation können grundsätzlich Gefährdungen entstehen (Ja, Nein): bei "Ja" bitte eine kurze Beschreibung der Gefährdung Hinweis: bei "Nein" aufgrund fehlender Gefährdung keine weiteren Cybersicherheitsmaßnahmen erforderlich
1	Verhinderung unkontrollierter Fahrkorbbewegung	Ja, Quetschgefahr und Schergefahr bei Deaktivierung der UCM-Erkennung oder Veränderung der hinterlegten Werte
2	Verbindung zur Notrufzentrale bei Personeneinschluß	Ja, Personeneinschluß bliebe unerkannt, Hilfe kann nicht eingeleitet werden
3	Regelung der Fahrgeschwindigkeit	Nein, da eine Veränderung der Fahrgeschwindigkeit aufgrund weiterer verbauter Schutzeinrichtungen nicht zu einer Gefährdung führt. Mechanische Schutzeinrichtung für den aufwärtsfahrenden Fahrkorb gegen Übergeschwindigkeit (SAFÜ) und gegen Absturz verbaut.

DEKRA Formular, Seite 3, Schritt 3:
Im Schritt 3 wird auf die identifizierten Gefährdungen aus Schritt 2 Bezug genommen. Die Verknüpfung stellt man weiterhin über die laufende Nummer her (Feld lfd. Nr.).

Entsprechend des EK ZÜS Beschlusses BA-017 können Herstellerzertifikate oder Systemzertifizierungen in die Bewertung einfließen, solange diese nachvollziehbar sind und der Betreiber die dort aufgeführten Vorgaben umsetzt. In diesen Dokumenten sollten daher notwendige Maßnahmen aufgeführt sein, welche es dem Betreiber ermöglichen, die geeigneten Maßnahmen nach TRBS 1115-1 Abschnitt 4.5.2 auszuwählen und umzusetzen. Fließt ein solches Dokument in die Bewertung ein, kann dieses im ersten Auswahlfeld vermerkt werden.

Anschließend wird die konkret gewählte Maßnahmenkategorie entsprechend TRBS 1115-1 Abschnitt 4.5.2 im dazugehörigen Auswahlfeld angekreuzt (Mehrfachnennungen möglich). Eine ausführliche Erläuterung zu den einzelnen Maßnahmen finden Sie in der TRBS 1115-1 oder in den FAQs auf **www.dekra.de/cybersicherheit**. Übrigens: Auch bei fehlenden Vorgaben des Herstellers kann der Betreiber mit Hilfe dieses Prozesses die notwendigen Maßnahmen realisieren.

Im letzten Eingabefeld des dritten Schrittes wird vermerkt, wie die geeignete Maßnahme umzusetzen ist und wo die dazugehörigen Informationen beschrieben sind. Insbesondere die Kurzbeschreibung hilft dem ZÜS-Sachverständigen zielgerichtet an die relevanten Informationen zu gelangen und deren Plausibilität im Zusammenhang der gesamten Schutzmaßnahmen zu prüfen. Sinnvollerweise kann hier auch festgehalten werden, wo die besagten Unterlagen aufzufinden sind.

Für die zwei verbliebenen Einrichtungen unserer Musteranlage liegen bereits unterschiedliche Dokumente der Hersteller vor. Die dort aufgeführten Maßnahmen wurden in Schritt 3 des Formulars übernommen und die dazugehörigen Referenzdokumente vermerkt. Die Herstellervorgaben der zweiten Einrichtung hat der Betreiber zusätzlich in eine von Ihm erstelle Handlungsanweisung Cybersicherheit übernommen und entsprechend verteilt, damit der betroffene Personenkreis (z. B. Wartungs- und Prüfpersonal) über die Vorgaben informiert ist.

Schritt 3 - Festlegung von Cybersicherheitsmaßnahmen

lfd. Nr.	Folgende individuelle Dokumente wurden bei der Festlegung von Cybersicherheitsmaßnahmen berücksichtigt Hinweis: Dropdown oder freie Eingabe möglich	Festgelegte Maßnahmen nach TRBS 1115-1 Abschnitt 4.5.2: 1. Segmentierung von Netzwerken	2. Funktionsreduzierung	3. Zugangskontrolle (Hardware)	4. Zugangskontrolle (Software)	5. Überwachung von Hardware, Software, Kommunikation	6. Notfallmanagement	Die Festlegung der konkreten organisatorischen und technischen Maßnahmen sowie ein Verfahren zur Aufrechterhaltung des Sicherheitsniveaus sind an folgender Stelle dokumentiert Hinweis: Bitte den Dokumentationsort und eine Kurzbeschreibung der Maßnahme eintragen
1	Systemzertifizierung		X	X				Betriebsanleitung Kapitel 2: Regelung des physikal. Zugang zur Anlage Kapitel 3: Bluetooth Schnittstelle deaktiviert ; kann nur durch einen Administrator und Freigabe des Herstellers wieder aktiviert werden.
2	Herstellervorgaben			X	X			Handlungsanweisung Cybersicherheit Konfigurationsänderungen nur mit PIN. Muß angefragt werden. Fernwartungsfunktionen wurden gemäß CS-Prozeßbeschreibung und interner CS-Richtlinie grundsätzlich deaktiviert ; eine spätere Aktivierung kann nur bei Änderung der Anlagenvernetzung stattfinden

DEKRA Formular, Seite 3, Schritt 4:

Im Schritt 4 dokumentiert der Betreiber, wie die in Schritt 3 festgelegten Maßnahmen tatsächlich umgesetzt werden und deren Anwendung auch langfristig über die Lebenszeit sichergestellt wird. Denn mit der Festlegung von Maßnahmen ist beim Thema Cybersicherheit noch nicht getan: Erst bei vollständiger Anwendung kann auch davon ausgegangen werden, dass der Betreiber die notwendigen Schritte umgesetzt hat. Für den ZÜS-Sachverständigen ist es daher wichtig, wo die Maßnahmen zur Umsetzung und Aufrechterhaltung dokumentiert sind. Im Feld „Belege und Nachweise“ kann daher auch direkt dokumentiert werden, welche organisatorischen oder technischen Maßnahmen bereits umgesetzt wurden und inwiefern diese zukünftig regelmäßig überprüft werden. Dies kann beispielsweise durch regelmäßige Überprüfung der Zugriffsüberwachung oder einer jährlichen Auffrischung zum Notfallkonzept realisiert sein.

An der Musteranlage wurden die notwendigen Schritte bereits umgesetzt und entsprechend nachvollziehbar dokumentiert. Die Dokumentation erfolgt idealerweise durch die zuständige Fachkraft des Betreibers.

Schritt 4 - Umsetzung und Aufrechterhaltung der Cybersicherheitsmaßnahmen

Die Anforderungen der TRBS 1115-1 Abschnitt 5 und Abschnitt 8.2. sind bekannt und wurden bei der Festlegung von Maßnahmen zur Aufrechterhaltung und zur Überprüfung der Funktion/Wirksamkeit der Cybersicherheitsmaßnahmen berücksichtigt. (z.B. Festlegung von Art und Umfang der Überprüfung und Kontrollfristen)

lfd. Nr.	Die Maßnahmen zur Aufrechterhaltung sind an folgender Stelle dokumentiert:	Belege oder Nachweise zur Funktion/Wirksamkeit der festgelegten technischen/ organisatorischen Maßnahmen und deren Aufrechterhaltung
1	Betriebsanleitung	Schlüsselausgabe für Anlagenzutritt ist protokolliert. Hausmeister wird von Tel.zentrale des Betreibers autorisiert. Deaktivierung von BT bei Inbetriebnahme der Anlage durchgeführt (Abnahmeprotokoll).
2	Handlungsanweisung Cybersicherheit	Protokoll zu allen PIN Anfragen wegen Konfigurationsänderungen vorhanden. Zeit und Name des Wartungstechnikers hinterlegt. Vierteljährlich wird neue PIN vergeben.

Liste von hilfreichen Dokumenten bei der Einarbeitung in das Thema:

Wir weisen darauf hin, dass die DEKRA als zugelassene Überwachungsstelle keine Rechtsberatung und Unterstützung bei der Gefährdungsbeurteilung anbieten darf und die nachfolgende Auflistung daher nur als unvollständige und unverbindliche Empfehlung angesehen werden kann.

Betriebssicherheitsverordnung

- Die Betriebssicherheitsverordnung (BetrSichV) regelt in Deutschland die Bereitstellung von Arbeitsmitteln durch den Arbeitgeber, die Benutzung von Arbeitsmitteln durch die Beschäftigten bei der Arbeit sowie die Errichtung und den Betrieb von überwachungsbedürftigen Anlagen im Sinne des Arbeitsschutzes.

TRBS 1111 – Gefährdungsbeurteilungen

- Diese Technische Regel soll den Arbeitgeber im Hinblick auf die Vorgehensweise bei der Durchführung der Gefährdungsbeurteilung nach § 3 Betriebssicherheitsverordnung (BetrSichV) unterstützen. Ziel der Gefährdungsbeurteilung ist es, die auftretenden Gefährdungen der Beschäftigten bei der Verwendung von Arbeitsmitteln zu beurteilen und daraus notwendige und geeignete Schutzmaßnahmen abzuleiten.

TRBS 1201 – Prüfung und Kontrolle von Arbeitsmitteln und überwachungsbedürftigen Anlagen

- TRBS 1201-1 Prüfung von Anlagen in explosionsgefährdeten Bereichen
- TRBS 1201-2 Prüfung im Gefahrenfeld Druckanlagen
- TRBS 1201-3 Instandsetzung an Geräten, Schutzsystemen, Sicherheits-, Kontroll- und Regelvorrichtungen im Sinne der Richtlinie 2014/34/EU
- TRBS 1201-4 Prüfung von Aufzugsanlagen

TRBS 1115 Teil 1 – Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen

- Diese Technische Regel konkretisiert die Betriebssicherheitsverordnung (BetrSichV) im Hinblick auf die Ermittlung und Festlegung erforderlicher Cybersicherheitsmaßnahmen für die dauerhafte Sicherstellung der Funktionsfähigkeit von sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen (MSR–Einrichtungen), die als technische Schutzmaßnahme für die sichere Verwendung eines Arbeitsmittels inklusive einer überwachungsbedürftigen Anlage eingesetzt werden.
- Die in dieser TRBS dargestellte Vorgehensweise zur Festlegung, Umsetzung und Prüfung von Cybersicherheitsmaßnahmen ist auch geeignet, um über sicherheitsrelevante MSR–Einrichtungen hinausgehende Teile des Arbeitsmittels (z. B. notwendige Kommunikationsmittel) oder andere technische Infrastrukturen gegen Cyberbedrohungen zu schützen, wenn dieses als Ergebnis der Gefährdungsbeurteilung als erforderlich angesehen wird.

EK ZÜS Beschluss B-002 - Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen von überwachungsbedürftigen Anlagen

- 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.
- Für Arbeitgeber oder Betreiber überwachungsbedürftiger Anlagen kann dieser Beschluss (insbesondere Kapitel 4.3.2 zum Prüfumfang) als Hilfestellung für geeignete Vorgehensweisen zur Festlegung erforderlicher CS-Maßnahmen dienen.

EK ZÜS Beschluss BA-017 - Prüfungen zur Cybersicherheit in Stufe 2 nach EK ZÜS-Beschluss B-002 (aktuelle Fassung) bei Aufzugsanlagen

- Dieser Beschluss ergänzt den EK-ZÜS Beschluss B-002 in der aktuellen Fassung und beschreibt die Umsetzung der Plausibilitätsprüfung bei Aufzugsanlagen durch die Sachverständigen der ZÜS. Der EK ZÜS-Beschluss B-002 in der aktuellen Fassung legt für die ZÜS Mindestanforderungen für ihre Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen im Rahmen der Prüfungen gemäß §§ 15, 16 BetrSichV fest.
- Für Arbeitgeber oder Betreiber überwachungsbedürftiger Anlagen kann dieser Beschluss eine Hilfestellung zum erwarteten Dokumentationsumfang der Stufe 2 geben. Hilfreich ist hier auch der Anhang des BA-017, da hier Beispiele und möglicherweise betroffener Komponenten aufgeführt sind.