Auszug aus der Gefährdungsbeurteilung nach § 3 der BetrSichV zur Behandlung von Cyberbedrohungen nach TRBS 1115-1

Dieses Formblatt kann vom Betreiber dazu genutzt werden, die von Ihm festgelegten Maßnahmen zur Cybersicherheit der ZÜS in einer einheitlichen und nachvollziehbaren Form mitzuteilen. Die Nutzung des Formblattes ist nicht verpflichtend – die Dokumentation kann selbstverständlich auch in einer anderen Form vorgelegt werden.

Bitte beachten Sie die neuen Vorgaben aus den EK ZÜS Beschlüssen B002 und BA017 (speziell für Aufzugsanlagen) zur Dokumentation des Prozesses zur Planung und Realisierung von Cybersicherheitsmaßnahmen. Wenn Sie keine eigenen Vorlagen erstellen möchten, können Sie hierfür auch das Beiblatt „Stufe 2“ auf der nächsten Seite verwenden. Aktuelle Informationen zur weiteren Vorgehensweise und Prüfumfängen der ZÜS sowie das Beiblatt „Stufe 2“ finden Sie auch auf **www.dekra.de/cybersicherheit**

1. Verwender (Betreiber):

Name

Adresse

2. Technische Daten der überwachungsbedürftigen Anlage:

☐ Aufzugsanlage ☐ Druckanlage ☐ Druckgeräte ☐ Ex-Anlage

Betriebsort

Baujahr

Interne Bezeichnung (nur wenn vorhanden)

Fabrik-, Herstell- oder Seriennummer (nur wenn vorhanden)

Hersteller (nur wenn zutreffend)

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.

Bei der durchgeführten Betrachtung von möglichen Cyberbedrohungen und festgelegten Maßnahmen zur Cybersicherheit wurde die TRBS 1115-1 berücksichtigt.

Ort Datum Unterschrift

08/2024

Beiblatt "Stufe 2" zur Einsicht bei der ZÜS Prüfung

DEKRA

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. festverdrahtete 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

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

Fabrik-, Herstell- oder Seriennummer:

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

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

Fabrik-, Herstell- oder Seriennummer: