Beschluss des EK ZÜS **ZÜS BA-017**

Abgestimmt im EK ZÜS **37. Sitzung, TOP 5.8** **17.04.2024**

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

1 Anwendungsbereich

Im Sinne der TRBS 1115 Teil 1 ist der Betreiber verpflichtet, seine überwachungsbedürftige Anlage hinsichtlich Gefährdungen durch Cyberbedrohungen zu bewerten. Betroffene Komponenten der Aufzugsanlage sind dabei alle Komponenten, die für den sicheren Betrieb und die Aufrechterhaltung von Sicherheitsfunktionen erforderlich sind. Dies ergibt sich aus der TRBS 1115 Teil 1 Abschnitt 1 Satz (1) Absatz 3: "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."

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.

2 Umsetzung der Stufe 2 gemäß EK ZÜS-Beschluss B-002

Mit Umsetzung der Stufe 2 erfolgt eine Ordnungsprüfung der vorgelegten Dokumentation vom Betreiber zur Cybersicherheit der Aufzugsanlage auf Plausibilität.

Die Dokumentation muss der zu prüfenden Anlage eindeutig zuordenbar sein. Die Plausibilitätsprüfung bezieht sich darauf, ob der Prozess gem. TRBS 1115 Teil 1 Abschnitt 4.4.3 durchgeführt wurde und ob die dabei ermittelten Ergebnisse nachvollziehbar und vollständig sind (Stichprobenprüfung der zugehörigen Dokumentation). Wird der Prozess vollständig und richtig durchgeführt, ist von einer Eignung der resultierenden Maßnahmen auszugehen. Eine Wirksamkeitsprüfung erfolgt in dieser Stufe nicht.

Der Prozess des Betreibers zur Bewertung der Cybersicherheit der Aufzugsanlage kann analog der im Anhang des EK-ZÜS B-002 in der aktuellen Fassung dargestellten Schritte 1 bis 4 erfolgen.

Dieser Prozess wird von der ZÜS auf Vollständigkeit und Plausibilität bewertet, z. B.:

– festgestellte funktional relevanten Systeme und grundsätzliche Cybersicherheitsrelevanz
– Auswirkungsanalyse des Betreibers bzgl. Cyberbedrohungen
– die vom Betreiber festgelegten Cybersicherheitsmaßnahmen inklusive der Prozesse zur Aufrechterhaltung des Schutzniveaus.

Zertifikate einzelner Komponenten sind als Nachweis für eine vollständige Anlagendokumentation im Sinne der Anforderungen der TRBS 1115 Teil 1 nicht ausreichend. Diese können jedoch in die Dokumentation des Betreibers einfließen. Bei der Bewertung berücksichtigte Herstellervorgaben sind zu dokumentieren.

Vollständige Systemzertifizierungen der gesamten Aufzugsanlage durch den Hersteller, Integrator oder Inverkehrbringer müssen nachvollziehbar, plausibel und anlagenbezogen sein. Diese können z. B. in Anlehnung an ISO 8102-20 bestätigt werden. Der Betreiber muss die Vorgaben des Herstellers umsetzen.

Beispiele betroffener Komponenten

– Sicherheitsrelevante MSR-Einrichtungen
– Zwei Wege-Kommunikationssysteme („Notrufsystem“)
– Schutzbedürftige IT/OT-Umgebung
– Weitere Bauteile gem. ISO 8102-20, sofern digital und cyberrelevant/schutzbedürftig
– PESSRAL-Komponenten
– Frequenzumrichter (FU) mit sicherheitsrelevanter Funktion

Bewertung durch den Sachverständigen gemäß EK ZÜS-Beschluss B-002

Ist die Dokumentation nicht vorhanden oder nicht plausibel, führt dies in Stufe 2 in der Regel zu einem geringfügigen Mangel.

Anhang (informativ)

Beispielhafte zusammenfassende Dokumentation des Prozesses zur Planung und Realisierung der Cybersicherheitsmaßnahmen nach EK ZÜS-Beschluss B-002 in der aktuellen Fassung:

Schritt 1	
Ermittlung der für die Sicherheit der Anlage relevanten Einrichtungen	**Schnittstellenermittlung**
Benennung der jeweiligen sicherheitsrelevanten MSR-Einrichtung [...]	**Benennung der an der Einrichtung vorhandenen Daten-Schnittstellen**
Steuerung	z. B. RS232, RJ45, Bluetooth, ...
Zwei-Wege-Kommunikationssystem (Notruf)	z. B. Internetverbindung über Router oder SIM-Karte, ...
...	

Schritt 2			
Beurteilung der Auswirkungen von Cyberbedrohungen			
Benennung der betrachteten Einrichtung	**Kurzbeschreibung der Schutzfunktion / des Schutzziels**	**Durch die Folgen einer Manipulation (z. B. [...]) können grundsätzlich Gefährdungen entstehen. (Ja/Nein) Wenn „Ja“ bitte beschreiben.**	**Es gibt folgende nicht digitale Maßnahmen, um die Folgen der Manipulation auf ein ungefährliches Maß zu reduzieren. [...]**
Steuerung	z. B. Sicherstellung und Steuerung des ordnungsgemäßen Betriebs, Überwachung des Sicherheitskreises, ...	Ja, z. B. wenn Sicherheitsfunktionen deaktiviert oder manipuliert werden, ...	Zugang zu Schnittstellen darf nicht unbefugt möglich sein, ...
Zwei-Wege-Kommunikationssystem (Notruf)	z. B. Möglichkeit zum Hilfe holen bei Personeneinschluss, ...	Ja, z. B. der Notruf wird nicht an die richtige Stelle weitergeleitet, ...	Zugang zu Schnittstellen darf nicht unbefugt möglich sein, ...
...			

Schritt 3					
Festlegung von Cybersicherheitsmaßnahmen					
Benennung der schutzbedürftigen Einrichtungen	**Elemente gemäß TRBS 1115-1 Abschnitt 3.2 sind [...] erfasst (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**	**Standardmaßnahmen der TRBS 1115-1 Abschnitt 4.5.2 Absatz 2 wurden im erforderlichen Umfang berücksichtigt (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**	**Festschreibung der erforderlichen Cybersicherheitsmaßnahmen ist erfolgt. (Ja/Nein) (Spezifikation der Cybersicherheit) (zzgl. Verweis auf Dokumentationsort)**	**Wenn Herstellervorgaben zur Cybersicherheit vorhanden sind, werden diese berücksichtigt. (Ja/Nein)**	**Verfahren zur Aufrechterhaltung des Cybersicherheitsniveaus ist festgelegt (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**
Steuerung	Ja, z. B. Dokumentation im Prüfbuch an der Anlage hinterlegt, ...	Ja, Maßnahmen z. B. nach ISO 8102-20 oder aus der Cybersicherheitsspezifikation des Herstellers, ...	Ja, z. B. übernommen in die Gefährdungsbeurteilung, hinterlegt im Prüfbuch an der Anlage, ...	Ja (wenn vorher berücksichtigt)	Ja, z. B. Verantwortlichkeit und Überprüfungszyklus ist in der Dokumentation im Prüfbuch beschrieben, ...
Zwei-Wege-Kommunikationssystem (Notruf)	Ja, z. B. Dokumentation im Prüfbuch an der Anlage hinterlegt, ...	Ja, z. B. aus der Cybersicherheitsspezifikation des Herstellers, ...	Ja, z. B. übernommen in die Gefährdungsbeurteilung, hinterlegt im Prüfbuch an der Anlage, ...	Ja (wenn vorher berücksichtigt)	Ja, z. B. Verantwortlichkeit und Überprüfungszyklus ist in der Dokumentation im Prüfbuch beschrieben, ...
...					

Schritt 4		
Umsetzung und Aufrechterhaltung der Cybersicherheitsmaßnahmen		
Benennung der schutzbedürftigen Einrichtungen	**Organisatorische Maßnahmen der Cybersicherheit sind in einer Betriebsanweisung festgeschrieben (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**	**Technische Maßnahmen der Cybersicherheit sind nachweislich funktionsfähig/wirksam (Ja/Nein) (siehe hierzu TRBS 1115-1 Abschnitt 5 und 8.2)**
Steuerung	z. B. Sicherstellen, dass Zugang nicht unbefugt möglich ist, z. B. Verhaltensanweisung bei Verlassen des Triebwerksraum in Betriebsanweisung, ...	RS232, RJ45 z. B. Zugang zu Schnittstellen darf nicht unbefugt möglich sein (Schaltschranktür, Triebwerksraumtür), ... Bluetooth z.B. wirksame Authentifizierungsverfahren (z.B. Passwörter), Nachvollziehbarkeit eingestellter Parameter, ... Aufrechterhaltung gemäß Dokumentation im Prüfbuch (Verantwortlichkeit, Überprüfungszyklus, ...)
Zwei-Wege-Kommunikationssystem (Notruf)	z. B. Sicherstellen, dass Zugriff nicht unbefugt möglich ist, z. B. den jeweiligen Tätigkeitsprofilen (Rollen) zugeordnete Rechte, ...	Internetverbindung über Sim-Karte (Netzwerk einschränken z. B. Firewall, Fernzugriff begrenzen, ...) Aufrechterhaltung gemäß Dokumentation im Prüfbuch (Verantwortlichkeit, Überprüfungszyklus, ...)
...		

Nachweisdokumente für Cybersicherheit von Komponenten können z. B. sein:

- Technische Anlagendokumentation der Aufzugsanlage
- Herstellerinformationen, z. B. aus der Betriebsanleitung
- Zertifikate hinsichtlich Cybersicherheit inkl. Maßnahmen für den Betrieb

Inhaltsverzeichnis