Bewertung der Cybersicherheit an Aufzugsanlagen im Sinne der TRBS 1115 Teil 1

Cybersicherheit ist ein wichtiger Bestandteil der Anlagensicherheit. Im März 2023 wurde die Technische Regel Betriebssicherheit (TRBS) 1115-1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“ auf der Internetseite der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) veröffentlicht und ist somit für Betreiber verbindlich.
Liegt dem Sachverständigen der Zugelassenen Überwachungsstelle (ZÜS) bei der Prüfung der Aufzugsanlage kein Nachweis vor, dass das Thema Cyberbedrohungen in der Risikobewertung behandelt wurde, notiert er einen entsprechenden Mangel in der Prüfbescheinigung.

Der TÜV Thüringen e.V. versucht die Sachverhalte an dieser Stelle so verständlich wie möglich darzustellen. Sollten Sie weiterführend Hilfe benötigen, diese Bewertung selbstständig durchzuführen, wenden Sie sich bitte an den Hersteller der Komponenten. Der TÜV Thüringen e.V. unterstützt Sie gerne bei der Bewertung im Rahmen einer Gefahrenanalyse. Als Hilfestellung haben wir Ihnen ein Musterschreiben an den Hersteller beigefügt (z.B. Versand an: Hersteller des Notrufsystem und Hersteller der Sicherheitseinrichtungen).

Textbaustein für das Anschreiben der Hersteller

> *Sehr geehrte Damen und Herren,*
>
> *wir bearbeiten derzeit die Gefährdungsbeurteilung unserer Aufzugsanlage hinsichtlich einer Ergänzung zur Cybersicherheit. Hierzu bitten wir um Informationen zu den Komponenten Zweiwege-Kommunikationssystem (Notrufsystem) und/oder relevanten Sicherheitseinrichtungen mit Schnittstellen (sowohl internetbasiert als auch physikalisch) und den umzusetzenden Schutzmaßnahmen.*

Ablauf einer Risikobewertung

- Identifizieren und Auflisten der Schnittstellen der Komponenten des Aufzugs, die kompromittiert werden können
- Bewerten, ob die Komponente durch einen Cyberangriff so beeinflusst werden kann, dass ein kritischer Zustand der Anlage entstehen kann
- Hierbei ist zu berücksichtigen, dass Komponenten, insbesondere Sicherheitseinrichtungen, bewusst außer Kraft gesetzt, ausgelöst oder deren Parameter verändert werden können
- Maßnahmen festlegen und dokumentieren

Die Umsetzung der Maßnahmen erfolgt im Anschluss an die Risikobewertung durch den Betreiber.

Wo finden Sie als Betreiber Informationen zu den gefährdeten Komponenten und mögliche Maßnahmen?

- Technische Anlagendokumentation der Aufzugsanlage
- Herstellerinformationen, z.B. aus der Betriebsanleitung
- Zertifikate hinsichtlich Cybersicherheit der verwendeten Komponenten / unterstützenden Dienstleister

Im Zweifelsfall wenden Sie sich an den Hersteller zur Umsetzung der Anforderungen bzgl. Cybersicherheit und sich daraus zu ergebenden möglichen Maßnahmen.

Bewertung der Cybersicherheit an Aufzugsanlagen im Sinne der TRBS 1115 Teil 1

Beispiele für zu betrachtende Sicherheitseinrichtungen

- Zwei-Wege-Kommunikationssystem bzw. Notrufsystem
  - Die Deaktivierung stellt bereits einen kritischen Betriebszustand dar, da eineeingeschlossene Person sich nicht mehr bemerkbar machen kann.
  - Ein möglicher Fernzugriff über die im Notrufsystem nach außen führende Schnittstelle ist besonders zu betrachten
- PESSRAL-Komponenten (softwaregesteuerte Sicherheitseinrichtungen, z.B. Schachtkopierung)
- Frequenzumrichter (FU) mit sicherheitsrelevanter Funktion (z.B. Safe Torque Off STO-Funktion)

Mögliche Maßnahmen nach TRBS 1115-1

- Reduzierung aller Schnittstellen zur Außenwelt durch Verzicht, Deaktivierung oder Sperrung nicht benötigter Hardwareschnittstellen mechanische Zugangsbeschränkungen für Bedienerschnittstellen und drahtgebundene Schnittstellen
  - mechanische Barrieren (Triebwerksräume, Schaltschränke verschlossen halten etc.)
  - zugewiesene Berechtigungsebenen in der Steuerung für z.B. Betrieb, Wartung und Instandhaltung
- notwendige Schnittstellen mit Fernzugriff (z.B. Notrufsystem/Fernwartung) können durch Firewalls und Passwörter geschützt werden
- W-LAN / Bluetooth Schnittstellen für Wartung und Instandhaltung nur für den Zeitraum aktivieren, wenn sie erforderlich sind

Beispiele für Steuerungsbauarten, gefährdete Schnittstellen und mögliche Maßnahmen:

<table>
<tr><th colspan="2">Aufzugssteuerung Bauart</th><th>Steuerung</th><th>Weitere Komponenten (z.B. PESSRAL, FU)</th><th>Mögliche Maßnahmen</th></tr>
<tr><td colspan="2">Netzwerkschnittstellen</td><td>Notrufsystem Fernzugriff auf Steuerung</td><td>---</td><td>Firewall / Passwortschutz /</td></tr>
<tr><td rowspan="6">Hardware und Benutzer-schnitt-stellen</td><td rowspan="3">Draht-gebunden</td><td>RS 232</td><td>USB</td><td rowspan="3">Schnittstelle unter Verschluss halten, im Schaltschrank oder Triebwerksraum,

Zugangsbeschränkungen...</td></tr>
<tr><td>USB</td><td>LAN</td></tr>
<tr><td>LAN, CANopen</td><td>CANopen</td></tr>
<tr><td rowspan="3">nicht draht-gebunden</td><td>W-LAN</td><td>---</td><td rowspan="3">Schnittstelle nur betreiben, wenn Wartungsarbeiten durchgeführt werden

Firewall / Passwortschutz /...</td></tr>
<tr><td>Bluetooth</td><td>---</td></tr>
<tr><td>sonstige Funkschnittstellen</td><td></td></tr>
</table>

Bewertung der Cybersicherheit an Aufzugsanlagen im Sinne der TRBS 1115 Teil 1

Arbeitgeber/Betreiber **Standort der Aufzugsanlage**

Technische Daten der Aufzugsanlage
Hersteller:
Fabrik-Nr.:
Baujahr:

Aufzugssteuerung Bauart		**Steuerung**	**Weitere Komponenten (z.B. PESSRAL, FU)**	**Mögliche Maßnahmen**
Netzwerkschnittstellen		**Notrufsystem Fernzugriff auf Steuerung**	**---**	**Firewall / Passwortschutz /**
Hardware und Benutzer-schnitt-stellen	**Draht-gebunden**			
	nicht draht-gebunden			

_____ _____
Ort, Datum Unterschrift Betreiber der Aufzugsanlage

Bitte legen Sie die ausgefüllte Dokumentation zu den Unterlagen an der Aufzugsanlage.