



Guten Tag,

schön, dass Sie diese Information zur Cybersicherheit für Aufzugsanlagen lesen.

Cybersicherheit/Cybersecurity ist in aller Munde und auch Aufzugsanlagen können betroffen sein. Ihnen geben wir mit dieser Information Erläuterungen zur Betrachtung der Cybersicherheit und für die Auswahl von Maßnahmen an Aufzugsanlagen. Zuerst soll festgestellt werden welche Technik betroffen ist und wie Gefährdungen erkannt werden.

Ihr Christian Thielmann  
Leiter des Kompetenzzentrums  
Aufzüge & Fördertechnik, TÜV Rheinland

## Aktuelle Information zur Cybersicherheit von Aufzugsanlagen – TRBS 1115 Teil 1

Nahezu kein Tag vergeht, an dem nicht in den Medien über Cyberangriffe und deren Folgen berichtet wird. Ob im privaten oder beruflichen Umfeld, wir erleben täglich, wie Cybersicherheit einen immer größeren Stellenwert einnimmt. Auch Aufzugsanlagen können betroffen sein.

Die zunehmende Digitalisierung und Vernetzung von Aufzugsanlagen führt dazu, dass die Wahrscheinlichkeit, Opfer eines Cyberangriffs zu werden, stetig zunimmt. So können durch unberechtigte Zugriffe Gefährdungen dadurch entstehen, dass z. B.:

- Personen eingeschlossen werden,
- Notrufsysteme nicht funktionieren,
- Steuerungen manipuliert werden,
- Aufzüge ausfallen.

In Hinblick auf Cyberbedrohungen ist es wichtig, dass die Betreiber von Aufzugsanlagen ihre Gefährdungsbeurteilungen anpassen und die sich daraus ergebenden Schutzmaßnahmen umsetzen.

Die getroffenen Cybersicherheitsmaßnahmen müssen geeignet, funktionsfähig und dokumentiert sein.

Nachfolgend beantworten wir erste Fragen!

### 01 WOHER WEISS ICH, WELCHE AUFZUGSANLAGE BETROFFEN IST?

Jeder Aufzug, der softwarebasierte Komponenten hat oder eine Schnittstelle nach außen wie z. B. bei einem Fernnotrufsystem besitzt, muss durch geeignete Maßnahmen gegen Cyberangriffe geschützt werden.

### 02 WELCHE RECHTLICHEN GRUNDLAGEN GIBT ES?

Das Gesetz über überwachungsbedürftige Anlagen (ÜAnlG), die Betriebssicherheitsverordnung (BetrSichV) und zur Konkretisierung die Technische Regel für Betriebssicherheit Ändern zu TRBS 1115 Teil 1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“.

### 03 WER FÜHRT DIE PRÜFUNGEN DURCH?

Die Prüfung der Maßnahmen wird von ZÜS-Sachverständigen durchgeführt und bescheinigt.

Für Sie von primärer Bedeutung ist festzustellen, ob ihre Anlagen betroffen sind und wie eine erste Bewertung der Gefährdungen durch Cybersicherheit erfolgen könnte.

### 04 IST MEINE ANLAGE BEZÜGLICH CYBERSICHERHEIT GEFÄHRDET?

Wenn es Schnittstellen zum Internet gibt, besteht grundsätzlich die Möglichkeit eines Angriffs auf Ihre Anlage. Das kann beispielsweise auch bereits durch das Zweiwegekommunikationssystem / durch den Notruf oder beispielsweise auch durch Motorsteuerungen wie Umrichter erfolgen.

Oft gibt es online Zugriffsmöglichkeiten auf Anlagen oder es sind Schnittstellen zu anderen Systemen vorhanden.

Dies können Tore für potentielle Angreifer sein.

### 05 WIE WERDEN POTENTIELLE GEFÄHRDUNGEN DER CYBERSICHERHEIT BEWERTET?

Wurden die potentiellen Gefährdungen identifiziert, betrachtet und Maßnahmen zu deren Abwehr festgelegt? Wenn ja, sind die wichtigsten Schritte bereits getan.

Das kann beispielsweise durch Informationen aus der technischen Dokumentation von Komponenten und durch die Kontrolle der bestimmungsgemäßen Verwendung erfolgen. Wurde beispielsweise das Standard-Passwort des Repeaters entsprechend den Vorgaben geändert?

### 06 MUSS DIESE BEWERTUNG NACHVOLLZIEHBAR SEIN?

Eventuell erforderliche Maßnahmen sind in der technischen Dokumentation festzuhalten. Dem Betreiber einer Anlage sind die erforderlichen Informationen zur Verfügung zu stellen.

### 07 WO KÖNNEN SIE HILFE BEKOMMEN?

Eine erste Bewertung kann durch unsere ZÜS Sachverständige des TÜV Rheinland für Aufzugsanlagen erfolgen.

Unsere Expert\*innen zur Cybersicherheit unterstützen Sie gerne bei der Bewertung der Sicherheit oder zertifizieren auch Ihre Systeme in Bezug zur Cybersecurity/ Cybersicherheit.

