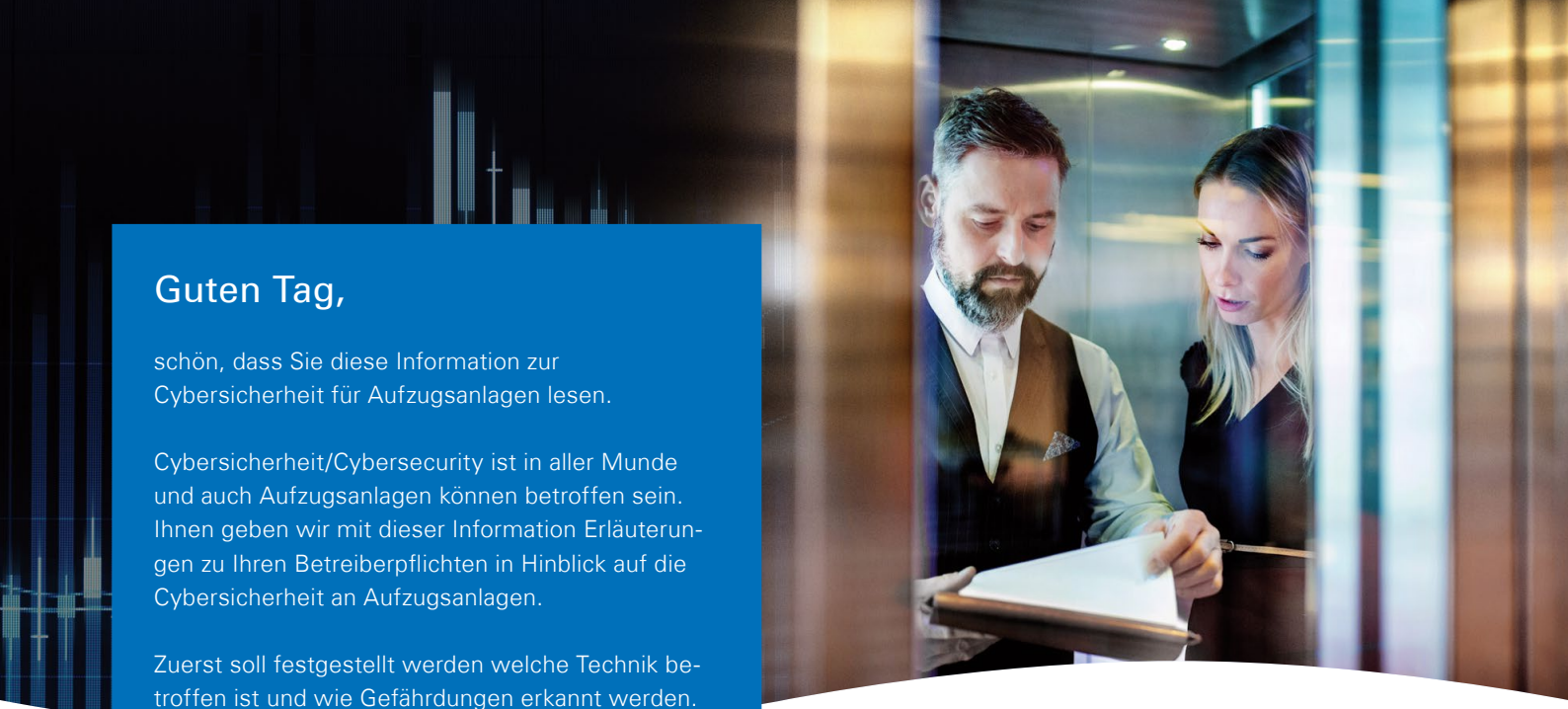

Guten Tag,

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 zu Ihren Betreiberpflichten in Hinblick auf die Cybersicherheit 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 eine Aufzugsanlage kann betroffen sein.

Die zunehmende Digitalisierung und Vernetzung von Aufzugsanlagen führt dazu, dass die Wahrscheinlichkeit, Opfer eines Cyberangriffs zu werden, stetig zunimmt. So können durch nicht berechtigte 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 Sie als Betreiber von Aufzugsanlagen ihre Gefährdungsbeurteilungen anpassen und die sich daraus ergebenen Schutzmaßnahmen umsetzen.

Die getroffenen Cybersicherheitsmaßnahmen müssen geeignet, funktionsfähig und dokumentiert sein.

Gerne beantworten wir erste Fragen!

www.tuv.com/aufzug

TÜVRheinland®
Genau. Richtig.

01 WELCHE RECHTLICHEN GRUNDLAGEN GIBT ES?

Der Gesetzgeber hat diese Gefährdungen erkannt und Maßnahmen für Betreiber festgelegt. Seit November 2022 ist die TRBS 1115 Teil 1 in Kraft und konkretisiert im Rahmen ihres Anwendungsbereichs die Anforderungen der Betriebssicherheitsverordnung hinsichtlich der Cybersicherheit.

02 IST MEINE ANLAGE BEZÜGLICH CYBERSICHERHEIT GEFÄHRDET?

Wenn es etwa Schnittstellen zum Internet gibt, besteht grundsätzlich die Möglichkeit eines Angriffs auf Ihre Anlage. Das kann bereits durch das Zweiwegekommunikationssystem und Motorsteuerungen wie Frequenzumrichter erfolgen oder aber durch Einrichtungen, die z.B. einen Fernzugriff auf die Anlage ermöglichen. Nicht selten gibt es online Zugriffsmöglichkeiten auf Anlagen oder es sind Schnittstellen zu anderen Systemen vorhanden. Die Möglichkeiten für potenzielle Angreifer sind vielfältig.

03 WIE MUSS ICH MICH ALS BETREIBER NUN VERHALTEN?

Für Sie von primärer Bedeutung ist es nun festzustellen, ob ihre Anlagen betroffen sind und wie eine erste Bewertung der Gefährdungen durch Cybersicherheit erfolgen könnte. Dies geschieht i.d.R. durch die Anpassung Ihrer Gefährdungsbeurteilung um die neu zu betrachteten Gefahren.

04 WELCHE ROLLE SPIELEN DIE TÜV-ORGANISATIONEN?

Die zugelassene Überwachungsstellen der TÜV-Organisationen sind aufgefordert, im Rahmen der regelmäßigen Prüfungen festzustellen, ob potenzielle Gefährdungen identifiziert, betrachtet und Maßnahmen zu deren Abwehr festgelegt wurden. Sollte dies nicht nachvollziehbar sein, so muss eine entsprechende Einstufung als Mangel erfolgen.

05 WIE WERDEN POTENZIELLE GEFÄHRDUNGEN DER CYBERSICHERHEIT BEWERTET?

Wurden die potenziellen Gefährdungen identifiziert, betrachtet und Maßnahmen zu deren Abwehr festgelegt? Wenn ja, sind die wichtigsten Schritte bereits getan. Das kann beispielsweise mit Hilfe von Nachweisen Ihrer Lieferanten oder durch die Kontrolle der bestimmungsgemäßen Verwendung erfolgen. Wurde beispielsweise das Standard-Passwort einer WLAN-Schnittstelle entsprechend den Herstellervorgaben 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?

Gerne unterstützen wir Sie mit einer anlagenspezifischen Vorlage zur Erstellung einer Gefährdungsbeurteilung, welche sich auf die Sicherheitsanalyse zum Stand der Technik inkl. den Anforderungen der neuen TRBS 1115 Teil 1 bezieht. Unsere Expertinnen und Experten für Cybersicherheit unterstützen Sie gerne ergänzend bei weiteren Fragen zum Thema und zertifizieren Ihre Anlagen und Systeme in Bezug zur Cybersecurity/Cybersicherheit.

TÜV Rheinland Industrie Service GmbH
Am Grauen Stein
51105 Köln
industrie@de.tuv.com

www.tuv.com/aufzug

TÜVRheinland®
Genau. Richtig.