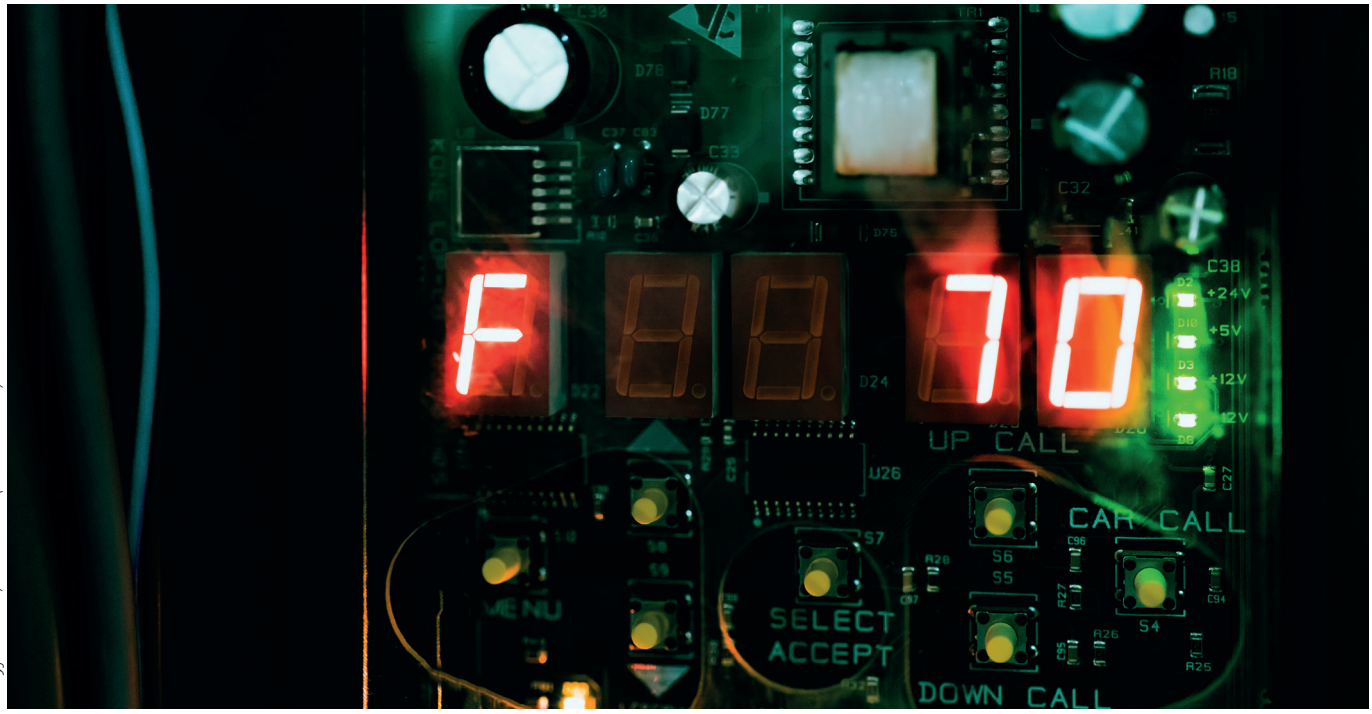
Wenn der Aufzug verrücktspielt: neue Risikoszenarien durch die Digitalisierung

Von Axel Stohlmann

Digitalisierung und Vernetzung im Internet of Things haben längst die Aufzugsbranche erreicht. Mehr noch: Aufgrund ihrer besonderen Funktion innerhalb einer Gebäudeinfrastruktur sind Aufzüge zu Treibern wichtiger technologischer Megatrends geworden. Ihre Vernetzung durch das Internet bringt aber auch neue Risikoszenarien mit sich. Der Gesetzgeber muss handeln – und die Chance bei der anstehenden Überarbeitung der Betriebssicherheitsverordnung (BetrSichV) nutzen.

Aufzüge befördern täglich weltweit über eine Milliarde Fahrgäste, das entspricht etwa 15 Prozent der Erdbevölkerung. Mit dem fortschreitenden Prozess der weltweiten Urbanisierung wird ihre Bedeutung noch zunehmen. Die OECD geht davon aus, dass im Jahr 2100 etwa 85 Prozent der Menschen weltweit in Städten leben und bereits im Jahr 2030 die Zahl der Megastädte voraussichtlich auf 41 gestiegen sein wird. Im Jahr 1950 entsprachen lediglich New York und Tokyo solchen Ballungsräumen mit mehr als 10 Millionen Einwohnern. [1]

Angesichts dieses Wachstums verwundert es nicht, dass auch Digitalisierung und Vernetzung zu festen Bestandteilen moderner Aufzugstechnik geworden sind. Digitale Aufzugstechnologien gehören bei Neuanlagen mittlerweile zum Standard – während gleichzeitig der Anlagenbestand nachgerüstet wird. Sogenannte „Retrofit"-Lösungen, die eine vorhandene Anlage oder einen Maschinenpark mit digitalen Komponenten Industrie-4.0-fähig machen, werden auch für Aufzüge angeboten. Die Vorteile liegen auf der Hand: höherer Komfort, mehr Effizienz im Betrieb, ein schonenderer Umgang mit den Res-



Szenario	Wirkung	Gefahr
Aufzugssystem während der Fahrt abschalten	Fahrkorb bleibt zwischen zwei Stockwerken stehen, gegebenenfalls zusätzlich Ausfall der Beleuchtung.	• Wenn keine Personen eingeschlossen sind: Aufzug ist nicht verfügbar, wirtschaftlicher Schaden. • Sind Personen eingeschlossen: Auswirkung auf die physische und psychische Gesundheit der Betroffenen. Durch die Möglichkeit, personenbezogene Daten und Nutzerprofile auszuspionieren, lassen sich Personen auch gezielt angreifen.
Veränderung bzw. Deaktivierung von Sicherheitsmerkmalen, z. B. durch • Angriffe von außen • Software-Updates	Bestimmte Stockwerke lassen sich nicht mehr anfahren. Hacker beeinflusst unbestimmte und willkürliche Fahrten des Fahrkorbs. Fahrkörbe halten nicht mehr bündig, Veränderungen des Anfahrts- und Bremsverhaltens, Veränderung der Nenngeschwindigkeit, Türen öffnen und schließen willkürlich.	Physische und psychische Belastung der Benutzer. Stolperfallen und unüberwindbare Hindernisse.
Angriff auf Infrastrukturen	Stilllegung einer gesamten kritischen Infrastruktur (KRITIS), z. B. ein Krankenhaus, oder Stilllegung einer hohen Zahl von Aufzügen gleicher Bauart.	Großschadensereignis, gezielte Hilfe ist für betroffene Personen nicht mehr möglich. Einfallstor für weitere nicht mehr kalkulierbare Gefährdungen.

Mögliche kritische Ereignisse bei einem Hackerangriff auf die Aufzugssteuerung

sourcen und bessere Verfügbarkeit durch gezielte und flexible Wartungskonzepte. Doch wie steht es um die Sicherheit?

Das auf Sicherheitssoftware spezialisierte Unternehmen Kaspersky hat in einer Studie ermittelt, dass das Risiko, Opfer einer Cyberattacke zu werden, bei Systemen in „Smart Buildings“ höher ist als bei Industrieanlagen, wobei ein Drittel der Angriffe direkt über das Internet erfolgt. [2] Es zeigt sich, dass die fortschreitende Digitalisierung auch das Risikopotenzial verändert. In den Fokus rücken dabei zwei Begriffe, die bislang getrennt betrachtet wurden: „Safety“ und „Security“.

Safety und Security zusammen betrachten

Unter „Safety“ wird gemeinhin die klassische funktionale oder Betriebssicherheit verstanden. Vereinfacht ausgedrückt, bezeichnet Safety den Schutz des Menschen vor (möglichen) Gefahren, die von einer Maschine oder Anlage ausgehen. „Security“ hingegen zielt auf den Schutz der Maschine oder Anlage vor Angriffen, was unter den Bedingungen des Internets eine völlig neue Relevanz bekommen hat. Für einen Angriff ist keine physische Anwesenheit mehr notwendig, die Entfernung zu einem beliebigen Punkt auf der Erde beträgt nur wenige Millisekunden. Safety und Security sind daher künftig zwingend zusammen zu betrachten – in ihrer Konvergenz, Abhängigkeit und Wechselwirkung untereinander.

Über das Einfallstor der digitalen und mit dem Internet verbundenen Aufzugssteuerung lässt sich so direkt die Funktion einer Anlage manipulieren. Die Tabelle oben zeigt mögliche kritische Ereignisse, die durch einen Angriff auf die Aufzugssteuerung ausgelöst werden können.

Die Szenarien machen deutlich: Ein Ansatz, der sowohl Safety als auch Security berücksichtigt, ist für die Sicherheit von Aufzugsanlagen dringend geboten. Dabei muss die Aufzugsanlage als Gesamtsystem mit seinen Schnittstellen bekannt sein.

Schnittstellen sind Risikopunkte

Bei Aufzugsanlagen sind Monitoring und Bedienung zunehmend entkoppelt. Durch die Verbindung der Aufzugssteuerung mit dem Internet lässt sich die Anlage aus der Ferne genauso steuern wie durch einen physischen Zugang vor Ort. Die Aufzugssteuerung ist in Bezug auf die Sicherheit einer Anlage besonders kritisch, da hier Schnittstellen zu allen – auch sicherheitsrelevanten – Anlagenkomponenten bestehen, insbesondere der Mess-, Steuerungs- und Regeltechnik (MSR-Technik). Ein Angriff auf diese zentrale Steuerungseinheit ermöglicht schlimmstenfalls den Zugriff auf mechanische Sicherheitsvorrichtungen, etwa auf die Antriebseinheit, Geschwindigkeitsbegrenzer, Notbremssysteme oder die Kabinentür. Auch können dadurch Lüftungssysteme, Brandmeldeanlagen oder die Notrufweiterleitung manipuliert werden.

Risiken stellen auch Schnittstellen zu netzbasierten Fernwartungssystemen dar, die durch „Predictive Maintenance"-Konzepte zunehmend an Bedeutung gewinnen. Darüber hinaus lassen sich bei intelligent gesteuerten Anlagen, die etwa Zugangsberechtigungen für Mitarbeiter eines Unternehmens abfragen, personenbezogene Daten ausspionieren und illegal Nutzerprofile anlegen. Und schließlich: Durch ihre Einbindung in die Gebäudeinfrastruktur bilden Aufzugsanlagen ein Einfallstor für Angriffe auf ein gesamtes Unternehmen. Vor allem mit einem „Advanced Persistent Threat" (APT) können Hacker großen Schaden anrichten, da sich ein APT-Angreifer möglichst lange unentdeckt im Netzwerk einer Organisation bewegen kann und dabei vor allem Daten ausspioniert.

Gesetzgeber muss aktiv werden

Um diesen Herausforderungen zu begegnen, müssen vor allem Prüfungen durch unabhängige Dritte unbedingt beibehalten werden. Dazu gehört vor allem eine Anpassung der Regularien, denn bislang hat der Gesetzgeber einen integrierten Ansatz von Safety und Security zu wenig im Fokus. Damit Aufzüge auch unter digitalen Bedingungen sicher betrieben werden können, ist eine umfassende Risikoanalyse des Gesamtsystems notwendig. Prüfungen müssen nach dem Stand der Technik erfolgen, also Safety und IT-Security beinhalten. Dabei gilt es, vor allem das Zusammenspiel zwischen mechanischen Sicherheitsbauteilen und Schutzfunktionen mit der Steuerung und Software in den Fokus zu rücken. Und Software-Updates müssen gemeldet und regelmäßig überprüft werden.

Eine Chance, die neuen Prüfumfänge gesetzlich zu implementieren, ist die anstehende Überarbeitung der Betriebssicherheitsverordnung (BetrSichV), wenn das Produktsicherheitsgesetz (ProdSG) aufgrund der Änderungen im EU-Recht novelliert wurde. Mit dem Gesetz für überwachungsbedürftige Anlagen (ÜAnlG) kann nun die umfassende Grundlage für einen zukunftsfähigen Safety- und Security-Ansatz unter den Bedingungen der fortschreitenden Digitalisierung geschaffen werden.

Quellen

[1] OECD: Das Jahrhundert der Metropolen (2015), abgerufen unter https://www.oecd.org/cfe/regional-policy/Metropolitan-Century-Policy-Highlights-German.pdf

[2] https://securelist.com/smart-buildings-threats/93322/

Dipl.-Ing. Axel Stohlmann
TÜV NORD Systems GmbH & Co. KG
astohlmann@tuev-nord.de