
KONE
Cybersecurity
Referierende: Ramona Ruci, Burghard Meyer, Andreas Backer
Im Chat: Benjamin Schwan
Dedicated to
People Flow™

Mit mir haben Sie es heute zu tun

Ramona Ruci

- Vor KONE: IT-Technikerin
- Programmierung Notrufsysteme
- Teamlead - Programmierung Notrufsysteme
- Technical Helpdesk Manager Österreich
- Technical Helpdesk Manager Digital Solutions DACH

- Leitung von vier Teams in D und CH für digitale Lösungen, die eine Schnittstellenfunktion zwischen Global/ Frontline, sowie Zentrale und Regionen darstellen und sich mit nicht lösbaren Fällen bzw. Projektausarbeitungen, Customer Onboarding, Analysen befassen

07.07.2023

Mit mir haben Sie es heute zu tun

Burghard Meyer

- Vor KONE: Systemberater IBM Mittelstands- und Systemcenter
- Start bei KONE: September 1992
- PC und Netzwerkkordinator
- Teamleiter Netzwerkkoordination
- IT Country Coordinator Germany
- IT Service Delivery Manager Germany
- Digital Service Specialist DACH

07.07.2023

Mit mir haben Sie es heute zu tun

Andreas Backer

- Seit September 2022 bei KONE
- Produktmanagement Digital Solutions
- Einführung und Betreuung digitaler Lösungen
- Vorher:
  - Softwareentwicklung in der Automobilindustrie (Dienstleister im Bereich Produktion)
  - IT-Administration & Beauftragter für Informationssicherheit

07.07.2023

Unsere heutigen Themen

1. Warum Cybersecurity & Was hat es mit einem Haus auf sich?
2. Do's & Don‘ts – Worauf sollte man achten?
3. Was hat Cybersecurity mit einer Zwiebel zu tun?
4. Aufzüge und Cybersecurity
5. Betreiberpflichten – Neue Regelungen zu Cybersecurity
6. Wie kann ich Cybersecurity bewerten?

Cybersecurity betrifft jede/n und beginnt mit dem Mindset!

WAS BEDEUTET EIGENTLICH CYBERSECURITY?

- MAßNAHME GEGEN BÖSWILLIGE ANGRIFFE DURCH EINE PERSON ODER ORGANISATION, DIE VERSUCHT, SICH ZUGANG ZU EINEM NETZWERK ZU VERSCHAFFEN, DATEN ZU BESCHÄDIGEN ODER VERTRAULICHE INFORMATIONEN ZU STEHLEN

DAS IOT (INTERNET OF THINGS) ERÖFFNET GROßE CHANCEN FÜR EINE VERBESSERTE KUNDENERFAHRUNG UND INNOVATION.

GLEICHZEITIG BEDEUTET ES, DASS CYBER-KRIMINELLE MEHR MÖGLICHKEITEN HABEN, UNSERE LÖSUNGEN ZU STÖREN

Was hat Cybersecurity mit diesem Haus zu tun?

DIE TECHNOLOGIE BREITET SICH RASANT AUS.
GEBÄUDE UND GERÄTE WERDEN IMMER SMARTER!

Sehen wir uns das Haus von Innen an

POTENTIELLE ANGRIFFSOBJEKTE LAUERN ÜBERALL:

- KÜHLSCHRANK
- MIKROWELLE
- LED-BELEUCHTUNG
- SAUGROBOTER
- JALOUSIEN
- AUFZUG

Neue Features bringen neue Vorteile, jedoch auch Gefahren mit sich!

Neue Features bringen neue Vorteile, jedoch auch Gefahren mit sich!

SMARTE-Produkte

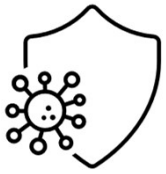
- Vernetzung von physischen Objekten
- Geräte, Sensoren und Cloud-Dienste, die miteinander kommunizieren, Informationen austauschen und aus der Ferne gesteuert werden können

Cybersicherheit beginnt bei der Produktentwicklung. Es müssen potenzielle Sicherheitsbedrohungen identifiziert und analysiert werden, damit man sie frühzeitig erkennen und darauf reagieren kann

Kein Unternehmen ist vor Cyberangriffen und Datenschutzverletzungen ungefährdet!

Einige Cyberangriffe können sogar Computersysteme zerstören

Da Cyberbedrohungen immer raffinierter werden, müssen Unternehmen Sicherheitsvorkehrungen treffen und die Cybersicherheitsrisiken analysieren, um die Daten zu schützen.



Arten von Cyberattacken

KONE

Malware

Phishing

Spear Phishing

DDos

Was sind die wichtigsten und häufigsten Sicherheitsbedrohungen?

- Malware
- Phishing
- Spear Phishing
- Distributed Denial of Service (DDoS)

Malware

KONE

Spyware

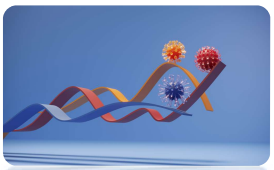
Ransomware

Backdoor

Würmer

Trojaner

Computervirus



07.07.2023

11

Malware

- häufigste Cyberattacke
- bösartige Software
- dazu gehören Spyware, Ransomware, Backdoors, Trojaner, Viren und Würmer

- **Spyware:** Software, die es Angreifern ermöglicht, Informationen über Ihre Computeraktivitäten zu erhalten, indem sie heimlich Daten von Ihrer Festplatte überträgt
- **Ransomware:** verschlüsselt Dateien auf einem Gerät und so alle Dateien (und die Systeme, die auf ihnen basieren) unbrauchbar macht. Häufig verlangen Hacker ein Lösegeld für die Entschlüsselung
- **Backdoor:** umgeht Authentifizierungsverfahren, um auf ein System zuzugreifen. So erhält der Angreifer Fernzugriff auf Datenbanken und Dateiserver. Dies ermöglicht es Hackern, Systembefehle zu erteilen und Malware aus der Ferne zu aktualisieren
- **Würmer:** Schadsoftware, die sich automatisch über das Netzwerk verbreitet. Würmer vervielfältigt sich selber, sobald die Software einmal

aufgeführt worden ist. Ziel ist es, sich so weit wie möglich zu verbreiten um großen Schaden anzurichten

- **Trojaner:** Malware oder Code, die sich als Anwendung oder Datei ausgeben, bei denen der Benutzer verleitet wird, die Malware auf Ihrem Gerät zu laden und auszuführen. Ziel ist es, Daten eines Unternehmens zu beschädigen, zu stehlen oder dem Netzwerk Schaden zuzufügen
- **Computervirus:** bösartiger Computercode, der sich von Gerät zu Gerät verbreitet. Ziel ist es, einen Computer zu beschädigen oder Daten zu stehlen

Phishing Spear-Phishing

Phishing: Angriff in Form von E-Mails, die scheinbar von vertrauenswürdigen Absendern wie Banken, Versicherungen, Providern, Freunden oder Arbeitskollegen stammen

Dadurch sollen Benutzer gebracht werden, auf Links in den E-Mails zu klicken, auf denen man auf betrügerische Websites gelangt, die persönliche Daten abfragen oder Malware auf Geräte installieren

Weiters kann das Öffnen von Anhängen, ebenfalls Malware installieren oder es Hackern ermöglichen, Geräte fernzusteuern

Spear-Phishing: Hacker nehmen gezielt Benutzer wie Führungskräfte und IT-Systemadministratoren ins Visier.

Sie verwenden meistens Details aus Social-Media-Konten einer Person, um die Zielperson glauben zu lassen, dass man die Person ist für die man sich ausgibt

KONE

Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS)

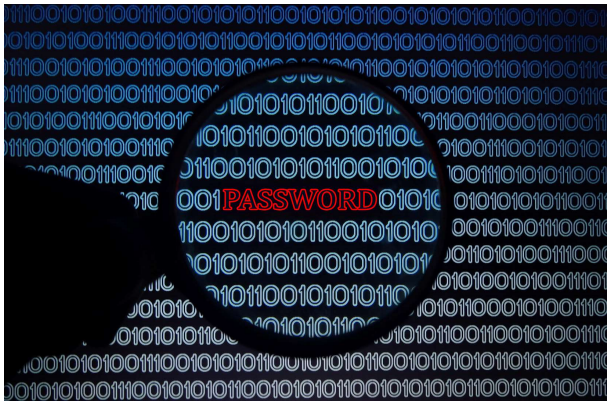
Ziel: Website eines Unternehmens lahm zu legen, indem Server mit Anfragen überhäuft werden

- vergleichbar mit einem permanenten Anruf, bei dem Anrufer nur ein Besetztzeichen erhalten und nie durchkommen
- Hierbei kommen Anfragen von Hunderten oder Tausenden von IP-Adressen, deren Nutzer dazu verleitet wurden, die Website eines Unternehmens ständig anzufordern
- kann Server überlasten und erheblich verlangsamen oder vorübergehend vom Netz nehmen
- kein Websitezugriff möglich

Am häufigsten verwendete Passwörter?

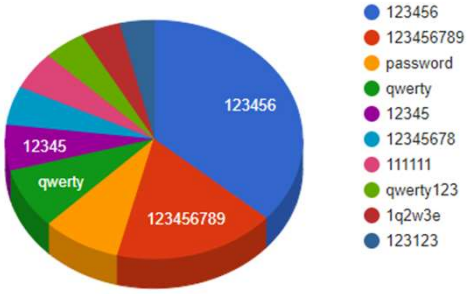
Top 10 der deutschen Passwörter in 2021

1. 123456
2. passwort
3. 12345
4. hallo
5. 123456789
6. qwertz
7. schatz
8. basteln
9. Berlin
10. 12345678



Im Jahr 2022 am häufigsten geleakte Klartextkennwörter

Verteilung der 10 häufigsten Kennwörter



Quelle: https://sec.hpi.de/ilc/statistics

1. 123456
2. 123456789
3. Password
4. Qwerty
5. 12345
6. 12345678
7. 111111
8. qwerty123
9. 1q2w3e
10. 123123

Passwörter Do´s & Dont´s

59 % verwenden denselben Benutzernamen und dasselbe Passwort für alle ihre Konten. Wird eines der Konten kompromittiert, haben Hacker freien Zugriff auch auf alle andern Konten.

LastPass, Psychology of Passwords report 2018

Zu vermeiden

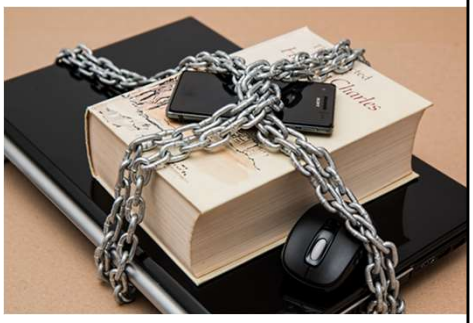
- Namen, Geburtsdaten, etc.
- Einfache oder bekannte Wiederholungs- bzw. Tastaturmuster wie “qwert1234”
- Ziffern oder Sonderzeichen an den Anfang oder ans Endeeines einfachen Passwortes
- Dasselbe Passwort bei mehr als einem Account

Generell gilt

- Ein individuelles Passwort pro Account!
- Eine Mehr-Faktor-Authentisierung ist empfehlenswert.
- Alle verfügbaren Zeichen nutzen inclusive Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (?!%+, Leerzeichen)
- Das vollständige Passwort sollte nicht im Wörterbuch vorkommen

Empfehlungen für ein sicheres Passwort

- Lange Passwörter (> 15 Zeichen)
- Alle Zeichenklassen verwenden (Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen)
- Keine Wörter aus dem Wörterbuch
- Keine Wiederverwendung von gleichen oder ähnlichen Passwörtern bei unterschiedlichen Diensten
- Verwendung von Passwortmanagern
- Passwortwechsel bei Sicherheitsvorfällen und bei Passwörtern, die die obigen Regeln nicht erfüllen
- Zwei-Faktor-Authentifizierung aktivieren, wenn möglich



Beispiel sicheres Passwort

My1RaftingAdventure!
(nicht als Passwort verwenden)

[My] + [1] + [Rafting] + [Adventure] + [!]
= 5 Teile

My1RaftingAdventure!
= 20 Zeichen

Kleingeschrieben [y], Großschrift [M], Zahlen [1] und Symbole [!]
= 4 verschiedene Charaktertypen

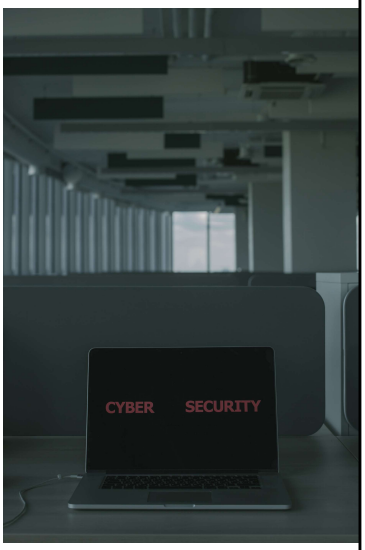
& zusätzliche Absicherung über MFA wann immer möglich

(MFA) Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (MFA) ist ein Verfahren, um einen Identitätsnachweis in Anmelde- oder Freigabeprozessen auf seine Authentizität zu überprüfen. Die MFA prüft die Identität des Benutzers durch mindestens zwei voneinander unabhängige Faktoren, wie etwas, das der Benutzer weiß (Passwort), das er hat (Sicherheitstoken) und das ihn auszeichnet (biometrisches Merkmal). Während des Anmeldevorgangs wird der Benutzer aufgefordert, ein weiteres Identifizierungsverfahren durchzuführen, z. B. per Eingabe eines Codes auf dem Smartphone oder per Fingerabdruckscan.

Grundsätzliche Tipps zur IT-Sicherheit

1. Browser anpassen und aktuell halten
2. Betriebssystem und Software aktuell halten
3. Virenschutz und eine Firewall nutzen
4. Unterschiedliche Benutzerkonten anlegen
5. Sichere Passwörter für Online- und Benutzerkonten
6. Vorsicht walten lassen bei E-Mails und deren Anhängen
7. Seien Sie vorsichtig bei Downloads
8. Zurückhaltung bei der Weitergabe persönlicher Daten
9. Datenschutz durch Verschlüsselung
10. Regelmäßig Sicherheitskopien erstellen



Ein bewährtest Prinzip, um IT-Systeme sicher zu machen, ist das „Zwiebelprinzip“
D.h. man setzt beim Schutz gegen Cyberangriffe nicht nur auf einen Schutzmechanismus, sondern baut das System von Grund auf aus Komponenten und Schichten auf.
Die Schichten haben alle für sich einen eigenen Schutzmechanismus.
Wenn ein Angreifer nun eine Schicht durchdringt, hat er alle weiteren Schichten noch vor sich und hat nicht gleich das ganze System kompromittiert.
Eine der Schichten stellt hier auch die Awareness der Anwender dar (siehe vorherige Folien).

Dieses Prinzip wird auch „Defense in Depth“ (Also Verteidigung in der Tiefe) genannt.

Aufzugsanlagen werden digitaler Warum eigentlich?

07.07.2023

21

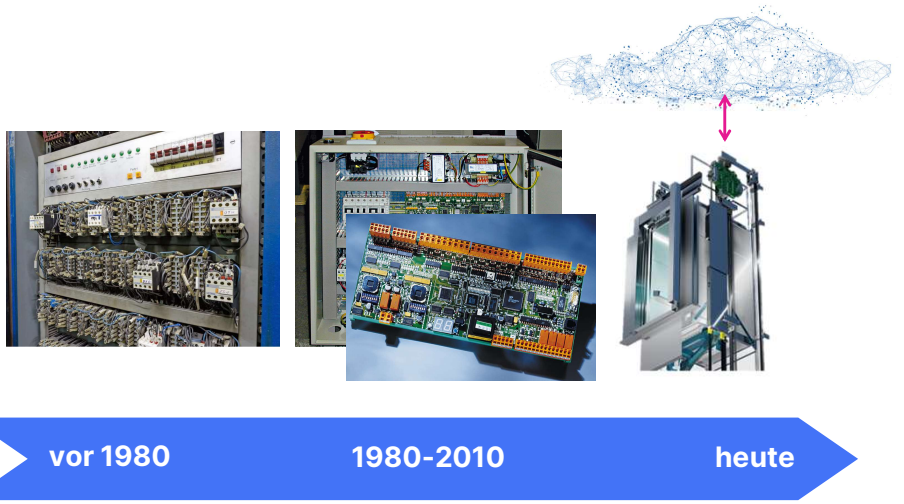
Aufzugsanlagen werden digitaler.
Damit können wir Mehrwert für die Anwender erzeugen.
Mit einem einfachen Aufzug kann ich nur hoch und runter fahren. Wenn ich ihn mit Drittsystemen koppele, entstehen Anwendungsfälle, die so vorher nicht möglich waren.

Hier einige Beispiele:

- Prädiktive Wartung
  - Betriebsdaten der Aufzüge werden gesammelt und auf Unregelmäßigkeiten analysiert
  - Dadurch kann frühzeitig der Ausfall eines Bauteils prognostiziert werden und ein Austausch vorgenommen werden, ohne dass eine Störung auftritt
- Smartphone App zur Aufzugssteuerung
  - Aufzug schon in der Wohnung oder im Büro rufen und keine Zeit beim Warten verlieren
- Sprachsteuerung
  - Aufzüge per Sprachbefehl rufen, komplett berührungslos
- Indoor Navigationsapps
  - Navigation innerhalb von Gebäuden mit Integration der Aufzüge
  - Z.B. interessant für blinde Menschen

- Anbindung Smarthome Systeme
  - Sammlung und Auswertung von Betriebsdaten des Aufzugs
  - Anwendungsfall Gästesteuerung (Aufzug vorprogrammiert nach unten senden, um einen Gast abzuholen)
- Serviceroboter
  - Serviceroboter, die sich in mehrstöckigen Gebäuden bewegen sollen, müssen dafür Aufzug fahren
  - Dafür benötigen sie eine Schnittstelle zum Aufzug, um die entsprechenden Befehle senden zu können
  - Interessant z.B. für
    - Zimmerservice in Hotels
    - Lieferroboter
    - Reinigungsroboter

Aufzugsanlagen werden digitaler



Bei der Digitalisierung und bei der Frage nach der Cybersicherheit spiel die Steuerung eine besondere Rolle.
Wie haben sich die Steuerungen über die Jahre entwickelt?
Vor 1980:

- Überwiegend Relaissteuerungen
- Man hat den Strom, der dort fließt regelrecht gehört
- Daher auch nicht ganz ungefährlich
- Cybersecurity war noch kein Thema. Die Steuerungen waren nicht vernetzt und es gab ja auch noch gar kein Internet

Nach 1980:

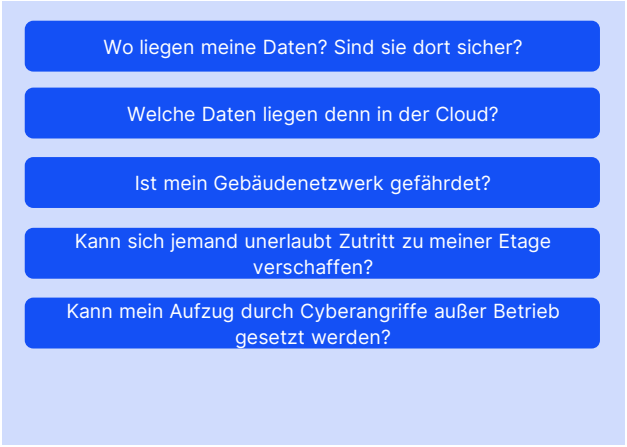
- Steuerungen wurden zunehmend in form von Controllerboards gebaut
- Anfangs auch noch mit fest eingebrannter Software
- Steuerungen wurden dadurch kleiner und sicherer (keine offenen Relais mehr)
- Cybersecurity war immer noch kein Thema, da die Anlagen keine Schnittstellen nach außen hatten
- Der physische Schutz musste damals wie heute gewährleistet werden, da mit direktem Zugriff auf die Anlagenbauteile auch Manipulationen möglich gewesen wären.
  Das war früher so und gilt heute noch genauso

Heute:

- Die Steuerungen sind heute mehr oder weniger kleine Computer und haben Schnittstellen zu externen Systemen (z.B. Cloud)
- Das ermöglicht die gerade vorgestellten Anwendungsfälle und die Erzeugung von Mehrwert
- Hier müssen wir uns dann auch mit dem Thema Cybersicherheit beschäftigen

Cybersecurity für Aufzugsanlagen

Typische Fragestellungen



07.07.2023 23

Einige typische Fragestellungen, die zum Thema Cloudanbindung und Cybersecurity häufig aufkommen:

Wo liegen meine Daten und sind sie dort sicher?

- Das ist einer der ersten Gedanken, die die meisten Leute beim Thema Clouddienste haben
- Man hat grundsätzlich 2 Möglichkeiten:
  - Selbst eine Infrastruktur aufbauen, um die nötigen Dienste anzubieten
    - Man muss sich selbst um die Sicherheit der Systeme kümmern
    - Updates müssen selbst eingespielt werden
    - Man muss dafür ggf. Personal vorhalten, das entsprechend geschult ist
  - Sich auf etablierte Clouddienstleister verlassen
    - Dort gibt es Sicherheitsspezialisten, die den ganzen Tag nichts anderes machen
    - Sicherheit, Updates und Verfügbarkeit werden durch den Dienstleister gewährleistet
    - Redundante Standorte, die vor Ausfällen schützen
- Bei etablierten Clouddienstleistern hat man in der Regel die Möglichkeit auszuwählen, in welchen Ländern die genutzten Server stehen sollen (z.B. in der EU)

- Das ist wichtig für die Einhaltung von Datenschutzanforderungen
- Die Sicherheit der Daten wird gewährleistet durch
  - Einsatz von Systemen und Schutzmechanismen nach aktuellem Stand der Technik
  - Verschlüsselung der Daten durch den Aufzugshersteller vor dem Hochladen in die Cloud

Welche Daten liegen denn in der Cloud?

- Es handelt sich hier weitestgehend um Betriebsdaten des Aufzugs, z.B.:
  - Wann ist der Aufzug in welche Etage gefahren
  - Historische Wartungsdaten
  - Daten zu Störungen
  - Kommunikationsdaten mit Drittsystemen
- Keine persönlichen Daten
- Ein Smartphone sammelt da weitaus mehr persönliche Daten und sendet sie in die Cloud

Ist mein Gebäudenetzwerk gefährdet?

- Zwei Möglichkeiten:
  - In den meisten Fällen ist der Aufzug gar nicht mit dem Gebäude verbunden und hat seine eigene Cloudanbindung z.B. über eine Mobilfunkverbindung
  - In größeren Gebäuden kann es erforderlich sein, den Aufzug mit dem Gebäudenetz zu verbinden, z.B. zur Interaktion mit Gebäudemanagement- / Zugangskontroll- / Besuchermanagementsystemen
    - In diesem Fall sorgt man durch die Trennung der Netzwerke für Sicherheit
      - Z.B. durch Einsatz von Routern und Firewalls
- Andererseits muss natürlich auch das Aufzugsnetzwerk vor Zugriffen aus dem Gebäudenetzwerk geschützt werden

Kann sich jemand unerlaubt Zutritt zu meiner Etage verschaffen?

- Anwendungsfall: Kartenleser/Schlüsselschalter vor oder im Aufzug, Freier Zugang zu Etagen gesperrt
- Aufzugssysteme (zumindest bei KONE) sind durch verschiedene Sicherheitsmechanismen geschützt und nach dem „Defense in Depth“ Prinzip entwickelt
- Schutzmechanismen werden nach aktuellem Stand der Technik eingesetzt
- Zu beachten:
  - Ein Aufzug sollte nie die letzte Sicherheitsinstanz beim Zugang zu sensiblen Bereichen (z.B. einer Penthouse-Wohnung) sein
  - Es können Situationen auftreten, in denen eine Person im Aufzug in eine gesperrte Etage gebracht wird (z.B. Referenzfahrt nach Stromausfall)
  - Auch ein Wartungstechniker auf dem Fahrkorbdach hat Zugang zu allen Etagen

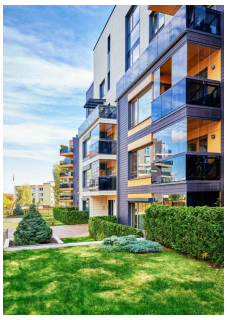
Kann mein Aufzug durch Cyberangriffe außer Betrieb gesetzt werden?

- Gleiche Argumentation wie beim letzten Punkt:
  - Aufzugssysteme (zumindest bei KONE) sind durch verschiedene Sicherheitsmechanismen geschützt und nach dem „Defense in Depth“ Prinzip entwickelt
  - Schutzmechanismen werden nach aktuellem Stand der Technik eingesetzt
- Die Gefahr ist relativ gering

Bei diesen Fragestellungen(Risikoabschätzung) ist auch das Umfeld, in dem der Aufzug betrieben wird zu betrachten.

Cybersecurity für Aufzugsanlagen

Es kommt auch auf das Umfeld an



Kleine Wohngebäude

vs

Banken / Krankenhäuser

Das Umfeld des Aufzugs spielt eine Rolle bei der Betrachtung der Cybersicherheit

Ein Aufzug in einem einfachen/mittleren Wohngebäude wird kein lohnendes Ziel für einen Hacker sein.
Wenn ein Aufzug hier durch einen Angriff ausfallen würde, würde das erstmal keinen massiven Schaden verursachen.

Anders sieht es hingegen z.B. bei Krankenhäusern aus.
Wenn hier ein Aufzug vom Heli-Pad zum Operationsaal ausfällt stehen ggf. Menschenleben auf dem Spiel.
Hier muss das Risiko ganz anders betrachtet werden, als in Wohngebäuden.

Solch ein hohes Risiko besteht aber nur beim kleinsten Teil aller Aufzugsanlagen.

Daher: Immer das tatsächliche Risiko mitbetrachten bei der Bewertung von Cybersecurity-Anforderungen und –Maßnahmen.

Cybersecurity für Aufzugsanlagen

Typische Fragestellungen

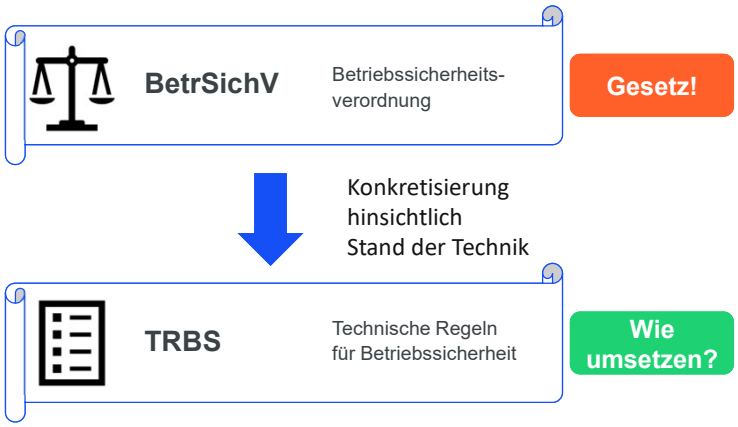
- Wo liegen meine Daten? Sind sie dort sicher?
- Welche Daten liegen denn in der Cloud?
- Ist mein Gebäudenetzwerk gefährdet?
- Kann sich jemand unerlaubt Zutritt zu meiner Etage verschaffen?
- Kann mein Aufzug durch Cyberangriffe außer Betrieb gesetzt werden?
- **Können Personen gefährdet werden?**

Ganz häufig stellt sich bei Aufzügen die Frage nach der Sicherheit.

Aus einschlägigen Filmen kennt man Szenen, in denen immer wieder Aufzüge abstürzen.
Kurz: Das kann nicht passieren. Es gibt mehrere redundante, elektrische und auch mechanische Sicherheitseinrichtungen, die einen Absturz unmöglich machen.
Daran ändern auch Cyberangriffe nichts.

Nichts desto trotz ist das Thema Sicherheit so wichtig, dass sich auch der Gesetzgeber dazu Gedanken gemacht hat.

Betreiber sind verantwortlich für ihre Aufzüge



07.07.2023

26

Die Betriebssicherheitsverordnung (deutsches Gesetz) regelt in die Bereitstellung und Benutzung von Arbeitsmitteln sowie Errichtung und Betrieb von überwachungsbedürftigen Anlagen im Sinne des Arbeitsschutzes.
Quasi alle Aufzüge gelten nach der BetrSichV als Arbeitsmittel.
Daher sind Sie als Betreiber grundsätzlich einem Arbeitgeber gleichgestellt und unterliegen den Pflichten der BetrSichV.

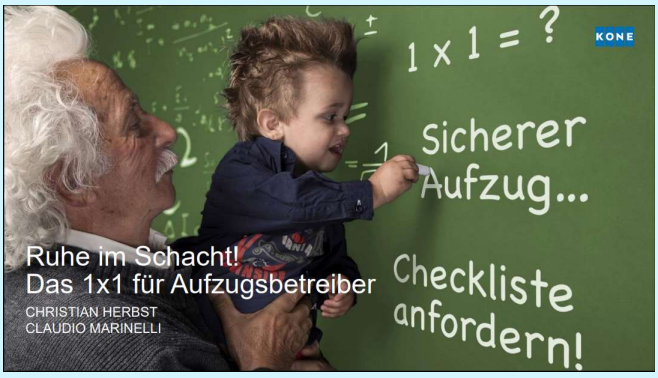
Betreiber ist, wer die wirtschaftliche Macht über den Aufzug hat und entscheidet, was mit dem Aufzug passiert.
Betreiber ist für die Aufzugssicherheit verantwortlich und steht in der Haftung.

TRBS konkretisieren die BetrSichV hinsichtlich des Standes der Technik und beschreibt, wie ein Betreiber die Anforderungen aus der BetrSichV erfüllen kann.
TRBS sind nicht spezifisch für Aufzugssysteme, sondern gelten vor allem auch für große Industrieanlagen.

Ein Betreiber ist nach der BetrSichV verpflichtet eine Gefährdungsbeurteilung für seinen Aufzug zu erstellen.

Betreiber sind verantwortlich für ihre Aufzüge

Handout vergangenes Webinar



Wer die wirtschaftliche Macht über den Aufzug hat, betreibt ihn

Betreiber sind für die Aufzugssicherheit verantwortlich und stehen in der Haftung

07.07.2023

27

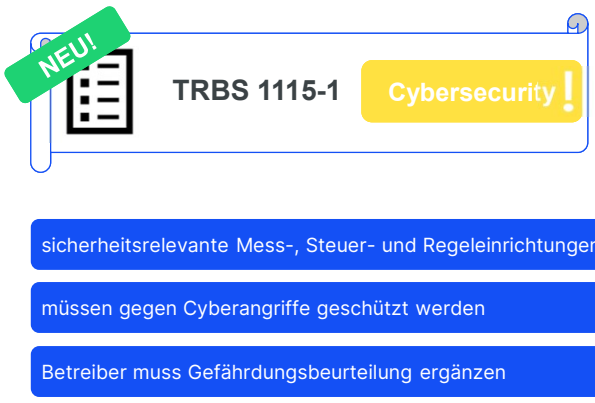
Das Handout finden Sie hier

Hinweis auf Handout zu vergangenem Webinar „Ruhe im Schacht! Das 1x1 für Aufzugsbetreiber

Hier wird u.a. detailliert erklärt:
- Wer ist Betreiber?
- Betreiberpflichten, Verantwortlichkeiten eines Betreibers
- Gefährdungsbeurteilungen und Stand der Technik

Link zum Handout: https://www.kone.de/Images/KONE_Live-Onlinetraining_Ruhe-im-Schacht_Handout_tcm26-115165.pdf

Es gibt eine neue TRBS!



07.07.2023 28

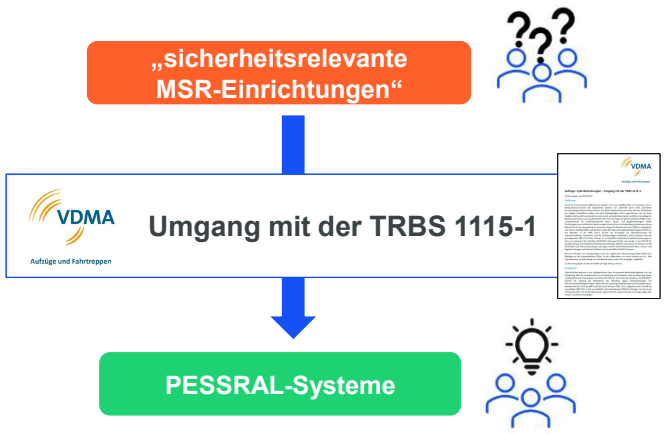
Stand der Technik umfasst mittlerweile auch Digitalisierung/Digitale Schnittstellen und Anbindung an Cloud

Neue TRBS 1115-1 bezieht sich explizit auf das Thema Cybersecurity.

Gefordert wird:
Sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen (MSR-Einrichtungen) müssen gegen Cyberangriffe geschützt werden. Der Betreiber muss seine Gefährdungsbeurteilung dahingehend ergänzen.

Die ZÜSen prüfen aktuell nach der neuen TRBS und weisen in den Prüfberichten auf fehlende Dokumentationen zum Thema Cybersecurity hin.

Was sind sicherheitsrelevante MSR-Einrichtungen?



Was sind sichherheitsrelevante MSR-Einrichtungen

VDMA (Verein deutscher Maschinen- und Anlagenbauer) Positionspapier: sicherheitsrelevante MSR-Einrichtungen sind ausschließlich PESSRAL Systeme.

Was sind nun PESSRAL-Systeme?

Sicherheitseinrichtungen eines Aufzugs

Mechanische Sicherheitseinrichtungen	Beispiel: Fangvorrichtung
Elektrische Sicherheitseinrichtungen	Sicherheitskreis
Elektronische/ programmierbare Sicherheitseinrichtungen	PESSRAL (programmierbares elektronisches System in sicherheitsrelevanten Anwendungen)

07.07.2023

30

Sicherheitseinrichtungen an Aufzügen:

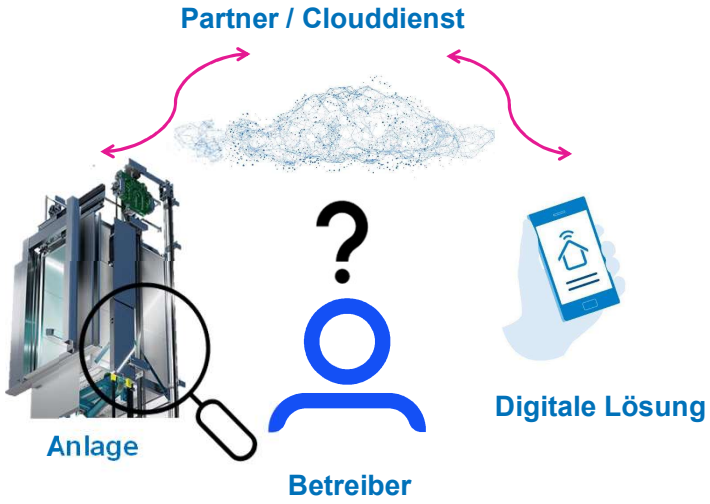
- Mechanische Sicherheitseinrichtungen
  - Rein mechanische, unabhängige Sicherheitseinrichtungen. Z.B. Fangvorrichtung

- elektrische Sicherheitseinrichtungen
  - Elektrische Sicherheitssysteme, die in Reihe geschaltet sind. Wenn eines Auslöst wird der Stromkreis unterbrochen und die Bremsen aktiviert

- Elektronische/Programmierbare Sicherheitseinrichtungen
  - Das sind die so genannten PESSRAL-Systeme (Programmable Electronic System in Safety-Related Applications for Lifts)
  - Separate, von der Steuerung unabhängige Sicherheitsplatinen
  - Sind besonders vor Veränderungen geschützt (z.B. per Siegel, das bei Wiederkehrenden Prüfungen auf Beschädigungen geprüft warden muss)
  - Software auf diesen Platinen kann nicht verändert werden (es muss die ganze Platine getauscht werden)
  - PESSRAL Systeme sind geschlossene Komponenten und haben eine

eigene Baumusterprüfbescheiningung
- PESSRAL Systeme kommen in neueren Aufzugsgenerationen zum Einsatz

Wie kann ich prüfen, ob mein Aufzug "cybersicher" ist?



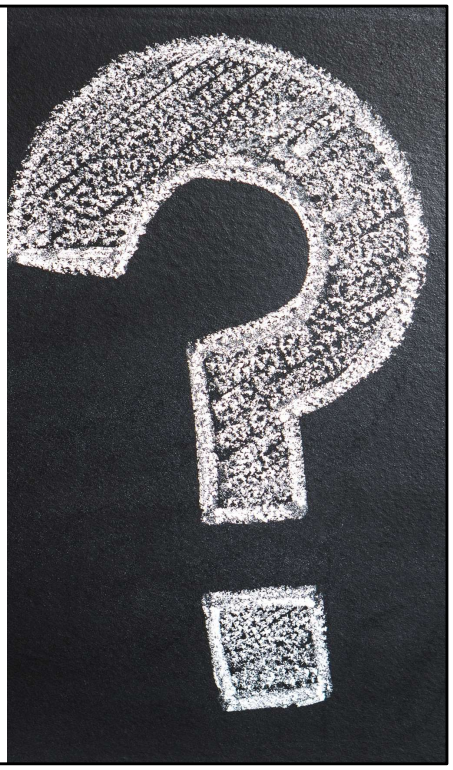
Wie kann ich als Betreiber nun die Cybersicherheit meines Aufzugs bewerten?

Ich kann ja nicht in die Systeme reingucken und selbst bewerten, ob sie sicher sind.

Wie kann ich prüfen, ob mein Aufzug "cybersicher" ist?

- Selbst kann ich meist nur ein grobes Gefühl entwickeln...
  - Ist mein Aufzug überhaupt mit dem Internet verbunden?
  - Ist er in mein Gebäudenetzwerk eingebunden?
  - Welche Angaben macht der Anbieter zur Cybersecurity?
  - Wo stehen die Server des Anbieters?
- **Normen und Zertifikate geben Sicherheit!**

07.07.2023



Betreiber können ein eigenes Gefühl entwickeln bzgl. der Cybersicherheit.

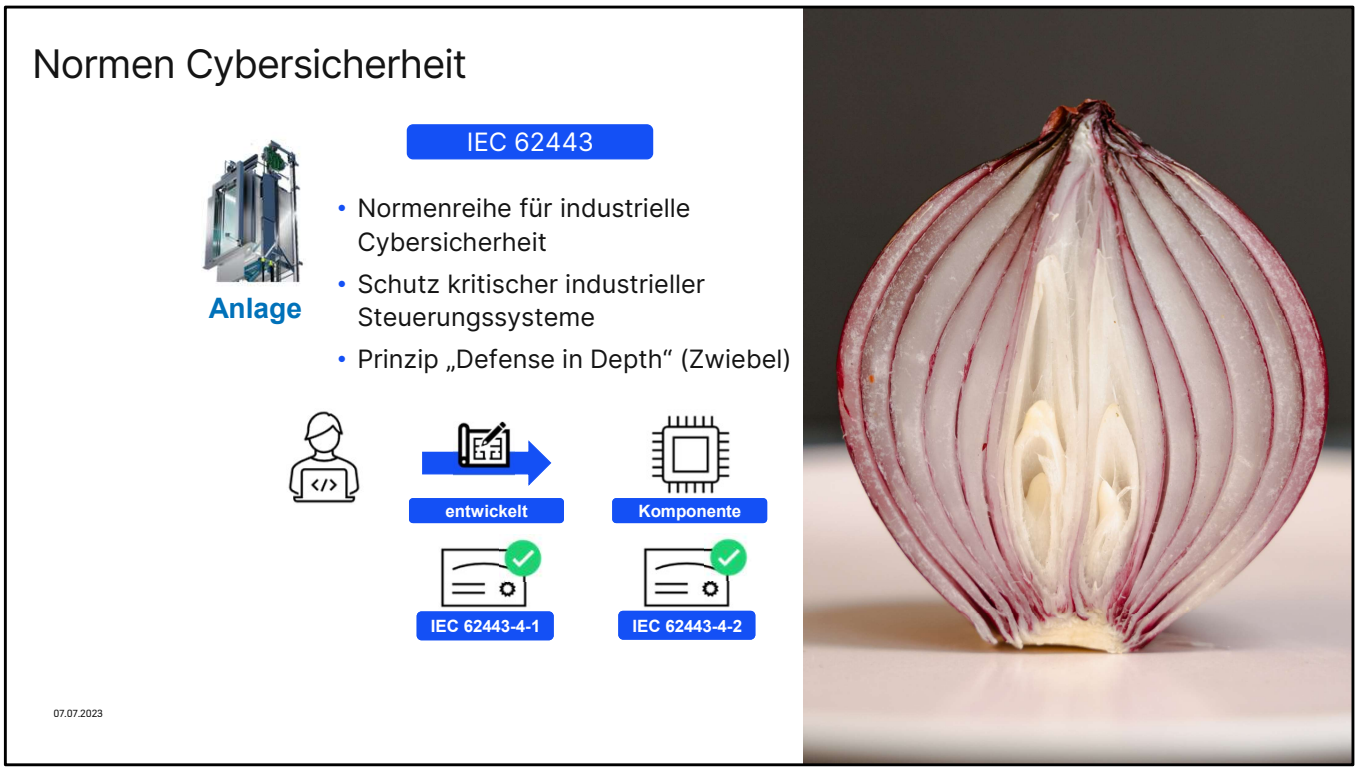
- Ist mein Aufzug mit dem Internet verbunden?
  - Wenn nicht, besteht über diesen Weg kein Risiko eines Cyberangriffs
- Ist mein Aufzug mit einem Gebäudenetzwerk verbunden?
  - Wenn nicht, besteht auch hier kein Risiko eines Cyberangriffs
- Welche Angaben macht mein Anbieter zum Thema Cybersecurity?
  - Geht er transparent mit dem Thema um? Finde ich auf seinen Webseiten Infos, wie er mit der Cybersecurity bei seinen Produkten umgeht?
- Wo stehen die Server des Anbieters (wenn er Clouddienste einsetzt?)
  - Macht er Angaben wo die Server der Clouddienste stehen? Ist damit meinen Datenschutzanforderungen genüge getan?

Als Betreiber kann ich nur auf die Angaben eines Herstellers vertrauen...

... oder ich verschaffe mir Gewissheit durch Zertifizierungen gegen einschlägige Normen durch unabhängige Prüforganisationen.

Normen Cybersicherheit

Zur Bewertung der Anlage selbst ist die IEC 62443 gut geeignet.



Die IEC 62443 ist eine Normenreihe für industrielle Cybersicherheit und zum Schutz kritischer industrieller Steuerungssysteme.
Sie funktioniert nach dem Anfangs vorgestellten Zwiebelprinzip (Defense in Depth).

Im Grunde handelt es sich um eine sehr detaillierte Anleitung, nach welchen Kriterien und Methoden sichere industrielle Steuerungssysteme und Komponenten entwickelt werden sollten.

Die IEC 62443-4-1 behandelt die Cybersicherheit im Entwicklungsprozess einer Komponente und ermöglicht eine entsprechende Zertifizierung.

Anhand der IEC 62443-4-2 kann anhand verschiedenster konkreter Anforderungen die Cybersicherheit einer entwickelten Komponente (z.B. eines Steuerungsmoduls) bewertet und zertifiziert werden.

Normen Cybersicherheit

ISO 8102-20: Cybersicherheit bei Aufzugsanlagen

Normen Cybersicherheit

Anlage

ISO 8102-20

- Internationale Norm zu Cybersicherheit für Aufzüge
- Basiert maßgeblich auf der IEC 62443 und referenziert diese
- Aktuell noch nicht in der EU harmonisiert

In der EU noch nicht gültig!

07.07.2023

Die ISO 8102-20 ist eine internationale Norm zur Cybersicherheit für Aufzüge.
Sie referenziert an vielen Stellen direkt auf die IEC 62443 und basiert daher auch auf dem Defense in Depth Prinzip.

Im Gegensatz zur IEC 62443 ist sie keine allgemeine industrielle Norm, sondern behandelt speziell Aufzüge.

Gilt aktuell noch nicht in der EU, da noch nicht harmonisiert. Kommt aber.

Normen Cybersicherheit

ISO 27001 zur Bewertung von Partnerfirmen und Dienstleistern

Normen Cybersicherheit

Partner / Clouddienst

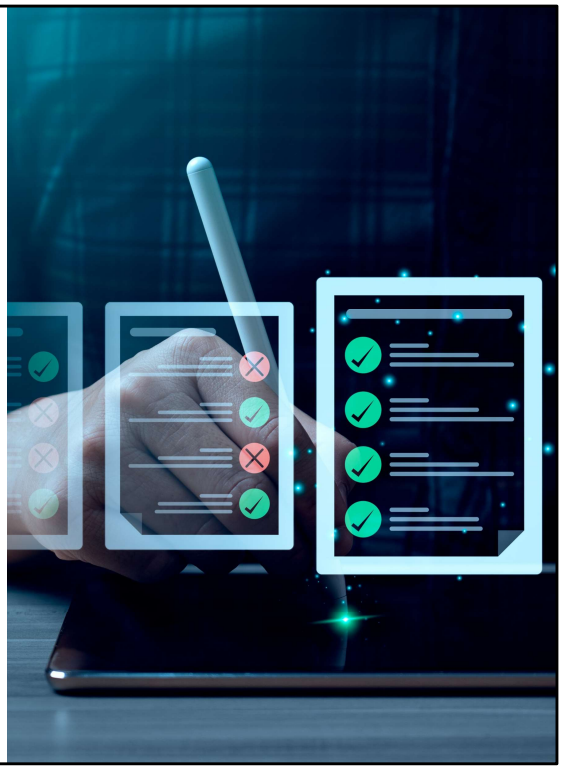
ISO 27001

- Internationale Norm zur Informationssicherheit
- Zertifizierung von Informationssicherheits-Managementsystemen und Prozessen

Kunden

Partner

07.07.2023



Die ISO 27001 ist eine internationale Norm zur Informationssicherheit. Sie wird verwendet zur Zertifizierung von Informationssicherheitsmanagementsystemen und -prozessen in Unternehmen.

Kunden können anhand Zertifizierungen nach dieser Norm die Informationssicherheit eines Unternehmens beurteilen. Unternehmen können die Norm verwenden, um geeignete Partner auszuwählen.

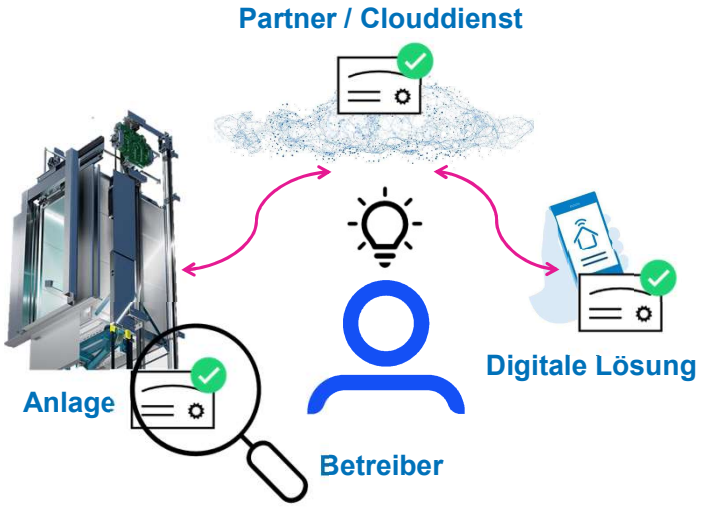
Normen Cybersicherheit

Das sind die 3 Normen zum Thema Cybersecurity bei Aufzügen.

Für die Anlage die IEC 62443 und zukünftig die ISO 8102-20.

Zur Bewertung der Sicherheit von Cloudanbietern und Partnern, die ISO 27001.

So kann ich prüfen, ob mein Aufzug "cybersicher" ist!



Ein Betreiber kann anhand von Zertifikaten nach den vorgestellten Normen die Cybersicherheit seiner Aufzugsanlage bewerten und seine Gefährdungsbeurteilung entsprechend ergänzen.

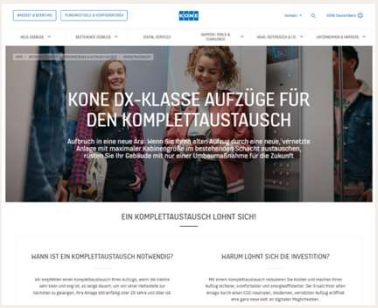
Das haben wir heute gelernt

1. Arten von Cyberbedrohungen
2. Do’s & Don’ts
3. Aufzüge werden digitaler
4. Cybersecurity spielt daher eine größere Rolle
5. Betreiber sind für ihre Anlagen verantwortlich
6. Normen und Zertifikate helfen!

Der Aufzug ist das sicherste Verkehrsmittel und bleibt es auch!

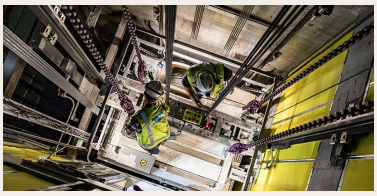
Weitere Informationen

AUF UNSEREN WEBSITES



www.kone.at
www.kone.ch/de
www.kone.ch/fr
www.kone.de

IM NÄCHSTEN LIVE-ONLINETRAINING



Donnerstag, 3. August 2023, 15 - 16 Uhr

„Die Aufzugsmontage – von der Vorbereitung bis zur Inbetriebnahme“

Jetzt anmelden »

Sagen Sie uns die Meinung

Im Anschluss an dieses Webinar erhalten Sie per E-Mail

- Einen Link zu unserem Feedbackbogen
- Die Präsentation als PDF zum Download

Vielen Dank. Wie lauten Ihre Fragen?

Ramona Ruci
Technical Helpdesk Manager Digital Solutions DACH
E-Mail: ramona.ruci@kone.com
Telefon: +43 664 853 59 80

Burghard Meyer
Digital Services Specialist DACH
E-Mail: burghard.meyer@kone.com
Telefon: +49 172 815 78 24

Andreas Backer
Produktmanager Digital Solutions DACH
E-Mail: andreas.backer@kone.com
Telefon: +49 151 113 793 53

Dedicated to People Flow™