Aufzugsnotfall-kommunikation

Cybersicherheitsstandards bei 2N

2N.com

Cybersicherheit

Ein Thema, das nicht mehr nur IT-Spezialisten vorbehalten ist, die für die Netzwerkinfrastruktur zuständig sind! Eine Schwachstelle in einem einzigen Produkt kann Ihr gesamtes System gefährden. Wenn Sie ein sicheres Gebäude wollen, müssen Sie auf Ihre Aufzugsnotfallkommunikation achten!

Gefährdete Aufzugssysteme stellen eine ernsthafte Bedrohung dar. Bei physischen Angriffen besteht die Gefahr, dass sich Kriminelle Zugang zu Gebäuden verschaffen, und Cyberangriffe kosten Millionen an Strafen, stören zentrale Geschäftsfunktionen und bedrohen den Ruf des Unternehmens.

Was können Sie also tun, um sicherzustellen, dass Sie den täglichen Betrieb des Gebäudes – und damit die Menschen darin – nicht gefährden?

2N: Ihr zuverlässiger Partner

Standards und Zertifizierungen

Die ISO 27001-Zertifizierung, die 2N im Jahr 2021 erhalten hat, ist der Beweis dafür, dass wir sensible Informationen systematisch und sicher verwalten. Diese Zertifizierung ist auch die ideale Antwort auf die Bedürfnisse der Kunden und auf gesetzliche Anforderungen wie die DSGVO sowie eine Verteidigung gegen potenzielle Sicherheitsbedrohungen.

Die Qualität unserer Produkte ist für uns und unsere Kunden von entscheidender Bedeutung. Deshalb entwerfen, entwickeln und testen wir sie gemäß den:

- Netzwerk- und Systemsicherheitsstandards **IEC 62443-4-1 und 62443-4-2**
- **Technischen Regeln für Betriebssicherheit TRBS 1115**
- Ausgewählten Prinzipien von **Secure by Design**
- **ASDM-Sicherheitsrahmen** unserer Konzerngesellschaft Axis
- Unseren internen Prozessen und Kenntnissen

Implementierten Sicherheitsgrundsätzen für einzelne Produktgruppen

Wir haben Lösungen für analoge, digitale und IP-Technologien. Außerdem haben wir eine Reihe von Prinzipien eingeführt, um die Sicherheit all dieser Produkte zu gewährleisten – sowohl physisch als auch im Internet.

1. Linux-basierte Produkte

Produkte von 2N für die IP-basierte Notfallkommunikation in Aufzügen

2N® LiftGate | 2N® EasyGate IP | 2N® LiftIP 2.0

- Sicheres Booten basierend auf Quectel OS
- Sichere SSL-Schlüssel: Die Länge beträgt mindestens 256 Bit, wie sie von HTTPS und anderen sicheren Protokollen verwendet werden
- Unser eigenes Protokoll „Tribble Tunnel“ gewährleistet eine sichere HTTPS-Kommunikation zwischen 2N-Aufzugsprodukten und dem 2N® Elevator Center. Der gesamte Kanal ist mit TLS verschlüsselt und basiert auf Zertifikaten, die von der Cloud ausgestellt wurden
- Bieten Sie mit digital signierten und verschlüsselten Firmware-Upgrade-Paketen Kontrolle und Schutz vor Spoofing durch nicht autorisierte Firmware
- Verhindern Sie dank unseres intelligenten Passwortsystems Wörterbuchangriffe. Es zwingt den Administrator dazu, das Standardpasswort nach der ersten Anmeldung in ein sicheres Passwort zu ändern.
- Verhindern Sie, dass Hacker Anmeldedaten aus dem Konfigurations-Backup erhalten, indem Sie verschlüsselte Passwörter speichern: Sie sind in der Webkonfiguration versteckt.
- Die Möglichkeit, Benutzerrechte festzulegen – optionaler Gastbenutzer mit Nur-Lese-Zugriff
- Das SIPS-Protokoll verschlüsselt den Inhalt von SIP-Nachrichten und verhindert so den Missbrauch von Daten (Man-in-the-Middle-Angriff usw.) und Identitätsdiebstahl.

2. Eigene Systeme

Produkte von 2N sind sowohl für die traditionelle analoge als auch für die digitale Notfallkommunikation konzipiert

2N® Lift1 **2N® Lift8**

- Die Produkte verfügen über ein eigenes, geschütztes System (Firmware), das nicht einfach gehackt oder missbraucht werden kann
- Sichere Upgrades, die durch einen speziellen Prüfsummenalgorithmus geschützt sind – kann bösartige Firmware nicht fälschen
- Eigenes Design für physische Sicherheit

3. Anwendungen

- Unsere Windows- und Android-basierten Apps ermöglichen die lokale Einrichtung, die Fernkonfiguration des Systems, Upgrades und die Überwachung von Alarm- und Kontrollanrufen.
- Dazu gehören der 2N Call Center Communicator und Server, das 2N Control Panel sowie die 2N Lift1 und Lift8 Service Tools.
- Die Installationsprogramme aller Apps sind durch sichere Algorithmen geschützt, die auf 2N-Schlüsseln und eingebetteten Sicherheitsmechanismen von Windows 10 (und höher) basieren.

4. 2N® Elevator Center

Hosting

Diese Cloud-Plattform wird bei Amazon Web Services (AWS) gehostet.
Um unseren Kunden die größtmögliche Sicherheit zu bieten, folgt unser Informationssicherheitsmanagementsystem den Best Practices der AWS-Sicherheit.

Sicherheit

2N® Elevator Center ist eine moderne Cloud-Lösung, die viele Sicherheitsvorteile bietet:

- Überwachung von Eindringlingen und Leistungsfähigkeit rund um die Uhr
- Sofortige Bereitstellung der neuesten Sicherheitsupdates sowohl auf AWS- als auch auf 2N-Seite
- Unser eigenes Protokoll zur Aufrechterhaltung permanenter und sicherer Verbindungen zwischen My2N Cloud und den 2N-Aufzugsprodukten (modernes und sicheres TLS-basiertes Protokoll)

Verschlüsselte Kommunikation

Die Cloud-Plattform bietet Services, die mehrere Kommunikationsschnittstellen zwischen den Cloud-Komponenten von 2N® Elevator Center und den Aufzugsgeräten erfordern. Alle diese Schnittstellen bieten eine sichere HTTPS/TLS-Kommunikation:

- Cloud-Synchronisierung – alle Cloud-Daten werden sicher auf verschlüsselten Laufwerken gespeichert und über ein proprietäres, TLS-basiertes Protokoll übertragen.
- Fernkonfiguration – der Benutzer kann über eine bei Bedarf erstellte, kurzlebige Route sicher auf die Webschnittstelle jedes Aufzuggeräts zugreifen.
- Bereitstellung/Erneuerung von Zertifikaten – Gerätezertifikate werden mit einer Gültigkeit von 3 Monaten ausgestellt, mit automatischer Erneuerung 1 Monat vor Ablauf und Unterstützung für manuellen Widerruf, falls erforderlich.
- Update-Server – das Gerät kann sicher auf neue, digital signierte FW-Versionen von unserem 2N-Update-Server aktualisiert werden.
- Sicherheitscodes und Vorabüberprüfung – die Verbindung von Geräten mit der Cloud ist nur über den Sicherheitscode/Vorabüberprüfungsprozess möglich.

Durch die Anwendung dieser und vieler anderer Prinzipien im Entwicklungsprozess **erfüllen 2N-Produkte für die Aufzugsnotfallkommunikation die allerhöchsten Sicherheitskriterien für den** Schutz personenbezogener Daten, die Produktsicherheit und die Sicherheit der Netzwerkinfrastruktur.

Grundlegende Schritte, die Sie heute unternehmen können, um Ihr System sicherer zu machen

Einhaltung eines bewährten Sicherheitskontrollrahmens (ISO 27001, IEC 62443-4-1, IEC 62443-4-2, TRBS 1115)

Sicherstellen, dass das System für die Aufzugsnotfallkommunikation die **Verwendung einer verschlüsselten Kommunikation** beinhaltet (Protokolle wie HTTPS, SIPS, TLS sollten standardmäßig aktiviert sein)

Erstellung verschiedener Konten mit unterschiedlichen Berechtigungen (um sicherzustellen, dass die Benutzer nur Änderungen vornehmen können, die sich auf ihre spezifischen Aufgaben beziehen)

Aktualisieren Sie die Software regelmäßig, um Cybersicherheitsrisiken zu minimieren.

Schulen Sie Ihre Mitarbeiter, um Social-Engineering-Bedrohungen zu vermeiden. Menschliches Versagen ist der anfälligste Teil eines jeden Systems.

2N TELEKOMUNIKACE a.s.
Tschechische Republik | +420 261 301 500 | sales@2n.com

2N.com