Communication d‘urgence pour ascenseurs

Normes de cybersécurité 2N

2N.com

Cybersécurité

Ce n‘est plus un sujet réservé uniquement aux informaticiens en charge de l‘infrastructure réseau ! Une faiblesse dans un seul produit peut mettre en danger l‘ensemble de votre système. Si vous voulez un bâtiment sécurisé, vous devez aussi faire attention à la communication d‘urgence de votre ascenseur !

Un système d‘ascenseur compromis est une menace sérieuse. Les attaques physiques risquent que les criminels accèdent aux bâtiments, et les cyberattaques coûtent des millions en pénalités réglementaires, perturbent les fonctions commerciales essentielles et menacent la réputation des entreprises.

Alors, que faire pour s‘assurer que les opérations quotidiennes du bâtiment ne soient pas mises en danger - de même que les personnes à l‘intérieur ?

2N : votre partenaire de confiance

Normes et certifications

La certification ISO 27001 que 2N a reçue en 2021 est la preuve que nous gérons les informations sensibles de manière systématique et sécurisée. Cette certification est également la réponse idéale aux besoins des clients et aux exigences législatives telles que le RGPD, et une défense contre les menaces potentielles pour la sécurité.

La qualité de nos produits est cruciale pour nous et nos clients, c'est pourquoi nous les concevons, les développons et les testons selon :

- Les normes de sécurité du réseau et du système **CEI 62443-4-1 et 62443-4-2**
- **Les règles techniques de sécurité opérationnelle TRBS 1115**
- Les principes sélectionnés de la spécification **« Secure by Design »**
- Le **cadre de sécurité ASDM** de notre société mère Axis
- Nos processus internes et nos connaissances

Mise en place de principes de sécurité pour chaque groupe de produits

Nous avons des solutions pour les technologies analogiques, numériques et IP. De plus, nous avons mis en place un certain nombre de principes pour assurer la sécurité de tous ces produits, tant physiques que numériques.

1. Produits basés sur Linux

Produits 2N conçus pour la communication d'urgence basée sur la technologie IP dans les ascenseurs

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

- Démarrage sécurisé basé sur Quectel OS
- Clés sécurisées SSL : la longueur est d'au moins 256 bits telle qu'utilisée par HTTPS et d'autres protocoles sécurisés
- Notre protocole propriétaire « Tribble Tunnel » assure une communication HTTPS sécurisée entre les produits d'ascenseur 2N et le 2N® Elevator Center. L'ensemble du canal est crypté à l'aide de TLS et sur la base de certificats émis par le cloud
- Fournir un contrôle et une protection contre l'usurpation de micrologiciels non autorisés avec des forfaits de mise à niveau de micrologiciels signés numériquement et cryptés
- Empêcher les attaques de dictionnaire grâce à notre système de mot de passe intelligent. Cela oblige l'administrateur à changer le mot de passe par défaut en un mot de passe fort après la première connexion.
- Empêcher les pirates d'obtenir des données de connexion à partir de la sauvegarde de la configuration avec des mots de passe cryptés : ils sont cachés dans la configuration Internet.
- La possibilité de définir des droits d'utilisateur - utilisateur invité facultatif avec accès en lecture seule
- Le protocole SIPS crypte le contenu des messages SIP, empêchant l'utilisation abusive des données (MITM ou l'attaque de l'homme du milieu, etc.) et le vol d'identité.

2. Systèmes propriétaires

Produits 2N conçus pour la communication d‘urgence analogique et numérique traditionnelle

2N® Lift1 **2N® Lift8**

- Les produits sont équipés de notre propre système propriétaire (logiciel) qui ne peut pas être facilement piraté ou utilisé à mauvais escient.
- Mises à niveau sécurisées protégées par un algorithme de somme de contrôle spécial - ne peut pas usurper un micrologiciel malveillant
- Conception exclusive pour une sécurité physique

3. Applications

- Nos applications Windows et Android permettent la configuration locale, la configuration à distance du système, la mise à niveau et la surveillance des appels d‘alarme et cycliques.
- Il s‘agit notamment du 2N Call Center Communicator and Server, du 2N Control Panel, du 2N Lift1 and desLift8 Service Tools.
- Les installateurs de toutes les applications sont protégés par des algorithmes sécurisés basés sur des clés 2N et des mécanismes de sécurité intégrés Windows 10 (et supérieurs).

4. 2N® Elevator Center

Hébergement

Cette plateforme cloud est hébergée sur Amazon Web Services (AWS). Afin de fournir à nos clients la plus grande sécurité possible, notre système de gestion de la sécurité de l'information suit les meilleures pratiques de sécurité AWS.

La sécurité

Le 2N® Elevator Center est une solution cloud moderne qui offre de nombreux avantages en matière de sécurité :

- Surveillance des intrusions et des performances 24h/24 et 7j
- Déploiement instantané des dernières mises à jour de sécurité du côté de l'AWS et du côté de 2N
- Notre propre protocole pour maintenir des connexions permanentes et sécurisées entre le cloud My2N et les produits 2N Lift (protocole moderne et sécurisé basé sur TLS)

Communication cryptée

La plateforme cloud fournit des services qui nécessitent plusieurs interfaces de communication entre les composants cloud 2N® Elevator Center et les appareils Lift. Toutes ces interfaces assurent une communication sécurisée HTTPS/TLS :

- Synchronisation du cloud - Toutes les données du cloud sont stockées en toute sécurité sur des disques cryptés et transportées via un protocole propriétaire basé sur TLS.
- Configuration à distance - L'utilisateur peut accéder en toute sécurité à chaque interface Internet de l'appareil Lift à distance en utilisant un itinéraire de courte durée créé sur demande.
- Obtention/renouvellement des certificats – Les certificats de l'appareil sont délivrés avec une validité de 3 mois, avec renouvellement automatique 1 mois avant l'expiration et prise en charge de la révocation manuelle si nécessaire.
- Serveur de mise à jour – L'appareil peut être mis à jour en toute sécurité vers de nouvelles versions FW signées numériquement à partir de notre serveur de mise à jour 2N.
- Codes de sécurité et prévérification - Connecter les appareils au cloud uniquement possible en utilisant le processus de code de sécurité/prévérificateur.

En appliquant ces principes et de nombreux autres dans le processus de développement, les **produits 2N pour la communication d'urgence d'ascenseur répondent aux critères de sécurité les plus élevés** en matière de protection des données personnelles, de sécurité des produits et de sécurité de l'infrastructure réseau.

Étapes de base que vous pouvez suivre dès aujourd‘hui pour rendre votre système plus sûr

Poursuivre la conformité avec un cadre de contrôle de sécurité éprouvé (ISO 27001, IEC 62443-4-1, IEC 62443-4-2, TRBS 1115)

Assurez-vous que le système de communication d‘urgence de l‘ascenseur comprend **l‘utilisation d‘une communication cryptée** (les protocoles tels que HTTPS, SIPS, TLS doivent être activés par défaut)

Créer différents comptes avec différents privilèges (en veillant à ce que les utilisateurs ne puissent apporter que des modifications liées à leurs tâches spécifiques)

Mettre à jour le logiciel régulièrement pour atténuer les risques de cybersécurité.

Former vos employés pour éviter les menaces d‘ingénierie sociale. L‘erreur humaine est la composante la plus vulnérable de tout système.

2N TELEKOMUNIKACE a.s.
Prague , République tchèque | +420 261 301 500 | sales@2n.com

2N.com