Comunicación de emergencia en ascensores

Estándares de ciberseguridad de 2N

2N.com

Ciberseguridad

¡Este ya no es un tema exclusivo de los informáticos encargados de la infraestructura de red! Un punto débil en un producto puede poner en peligro todo el sistema. Si quiere un edificio seguro, ¡debe prestar atención a la comunicación de emergencia en su ascensor!

Los sistemas de ascensores con deficiencias plantean graves amenazas. Los ataques físicos entrañan el riesgo de que los delincuentes accedan a los edificios, y los ciberataques cuestan millones en multas reglamentarias, perjudican las funciones empresariales básicas y amenazan la reputación de las empresas.

Entonces, ¿qué puede hacer para asegurarse de no poner en peligro el funcionamiento diario del edificio y, por ende, a las personas que se encuentran en su interior?

2N: su socio de confianza

Normas y certificaciones

La certificación ISO 27001 2N recibida en 2021 es la prueba de que gestionamos la información sensible de forma sistemática y segura. Esta certificación es también la respuesta ideal a las necesidades de los clientes y a los requisitos legislativos, como el RGPD, y una defensa contra posibles amenazas a la seguridad.

La calidad de nuestros productos es crucial para nosotros y nuestros clientes, por lo que los diseñamos, desarrollamos y probamos de acuerdo con:

- Normas de seguridad de redes y sistemas **IEC 62443-4-1 y 62443-4-2**
- **Normas técnicas de seguridad operativa TRBS 1115**
- Principios seleccionados de la especificación **'Secure by Design'**
- **Marco de seguridad ASDM** de nuestra empresa matriz Axis
- Nuestros procesos y conocimientos internos

Principios de seguridad aplicados a los distintos grupos de productos

Disponemos de soluciones para tecnologías analógicas, digitales e IP. Además, hemos implementado una serie de principios para garantizar la seguridad de todos estos productos, tanto física como cibernética.

1. Productos basados en Linux

Productos de 2N diseñados para la comunicación de emergencia en ascensores basada en IP

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

- Arranque seguro basado en Quectel OS
- Claves seguras SSL: la longitud es de 256 bits como mínimo, tal y como se utiliza en HTTPS y otros protocolos protegidos
- Nuestro protocolo patentado „Tribble Tunnel“ garantiza una comunicación HTTPS segura entre los productos 2N Lift y el 2N® Elevator Center. Todo el canal está encriptado mediante TLS y se basa en certificados emitidos por la nube
- Control y protección contra la falsificación no autorizada de firmware mediante paquetes de actualización de firmware encriptados y con firma digital
- Previene ataques de diccionario gracias a nuestro sistema de contraseñas inteligente. Obliga al administrador a cambiar la contraseña por defecto por una contraseña segura tras el primer inicio de sesión.
- Previene que los piratas informáticos obtengan datos de inicio de sesión de la copia de seguridad de la configuración guardando contraseñas encriptadas que se ocultan en la configuración web.
- Posibilidad de establecer derechos de usuario: usuario invitado opcional con acceso de solo lectura
- El protocolo SIPS encripta el contenido de los mensajes SIP, previniendo el mal uso de los datos (ataque intermediario, etc.) y el robo de identidad.

2. Sistemas propietarios

Productos 2N diseñados para las comunicaciones de emergencia analógicas y digitales tradicionales

2N® Lift1 **2N® Lift8**

- Los productos tienen nuestro propio sistema patentado (firmware) que no puede piratearse ni utilizarse indebidamente con facilidad
- Actualizaciones seguras protegidas por un algoritmo de suma de comprobación especial: no se puede falsificar ningún firmware malicioso
- Diseño propietario que garantiza la seguridad física

3. Aplicaciones

- Nuestras aplicaciones basadas en Windows y Android permiten la configuración del sistema de forma local y remota, la actualización y la supervisión de las alarmas y el monitoreo de las llamadas.
- Estos incluyen 2N Call Center Communicator and Server, 2N Control Panel, 2N Lift1 y Lift8 Service Tools.
- Los instaladores de todas las aplicaciones están protegidos por algoritmos seguros basados en claves 2N y mecanismos de seguridad integrados en Windows 10 (y versiones superiores).

4. 2N® Elevator Center

Alojamiento web

Esta plataforma en la nube está alojada en Amazon Web Services (AWS). Para ofrecer a nuestros clientes la máxima seguridad posible, nuestro sistema de gestión de la seguridad de la información sigue las mejores prácticas en materia de seguridad de AWS.

Seguridad

2N® Elevator Center es una moderna solución en la nube que ofrece numerosas ventajas de seguridad:

- Supervisión de intrusiones y rendimiento 24/7
- Instalación instantánea de las últimas actualizaciones de seguridad tanto en AWS como en 2N
- Nuestro propio protocolo para mantener conexiones permanentes y seguras entre My2N Cloud y los productos 2N Lift (protocolo moderno y seguro basado en TLS)

Comunicación encriptada

La plataforma en la nube proporciona servicios que requieren múltiples interfaces de comunicación entre los componentes en la nube de 2N® Elevator Center y los dispositivos Lift. Todas estas interfaces proporcionan una comunicación segura HTTPS/TLS:

- Sincronización en la nube: todos los datos en la nube se almacenan de forma segura en unidades encriptadas y se transfieren a través de un protocolo propio basado en TLS.
- Configuración remota: el usuario puede acceder de forma segura y remota a cada interfaz web del dispositivo Lift mediante una ruta corta creada bajo petición.
- Provisión/renovación de certificados: los certificados del dispositivo se emiten con una validez de 3 meses, una renovación automática 1 mes antes de la fecha de expiración y soporte para revocación manual en caso de necesidad.
- Servidor de actualización: el dispositivo puede actualizarse de forma segura a nuevas versiones de FW firmadas digitalmente desde nuestro servidor de actualización 2N.
- Códigos de seguridad y verificación previa: los dispositivos solo pueden conectarse a la nube mediante el proceso de código de seguridad/verificación previa.

Al aplicar estos y otros muchos principios en el proceso de desarrollo, los **productos 2N para comunicaciones de emergencia en ascensores cumplen los criterios de seguridad más exigentes** en materia de protección de datos personales, seguridad de los productos y seguridad de las infraestructuras de red.

Pasos básicos que puede dar hoy mismo para mejorar la seguridad de su sistema

Cumplir con los requisitos establecidos por algún marco de control de seguridad probado (ISO 27001, IEC 62443-4-1, IEC 62443-4-2, TRBS 1115)

Asegurarse de que el sistema de comunicación de emergencia en el ascensor incluye el **uso de comunicación encriptada** (protocolos como HTTPS, SIPS, TLS deben estar activados por defecto)

Crear diferentes cuentas con diferentes privilegios (garantizando que los usuarios solo puedan realizar cambios relacionados con sus tareas específicas)

Actualizar periódicamente el software para mitigar los riesgos en materia de ciberseguridad.

Formar a los empleados para evitar las amenazas de ingeniería social. El error humano es la parte más vulnerable de cualquier sistema.

2N TELEKOMUNIKACE a.s.
Praga, República Checa | +420 261 301 500 | sales@2n.com

2N.com