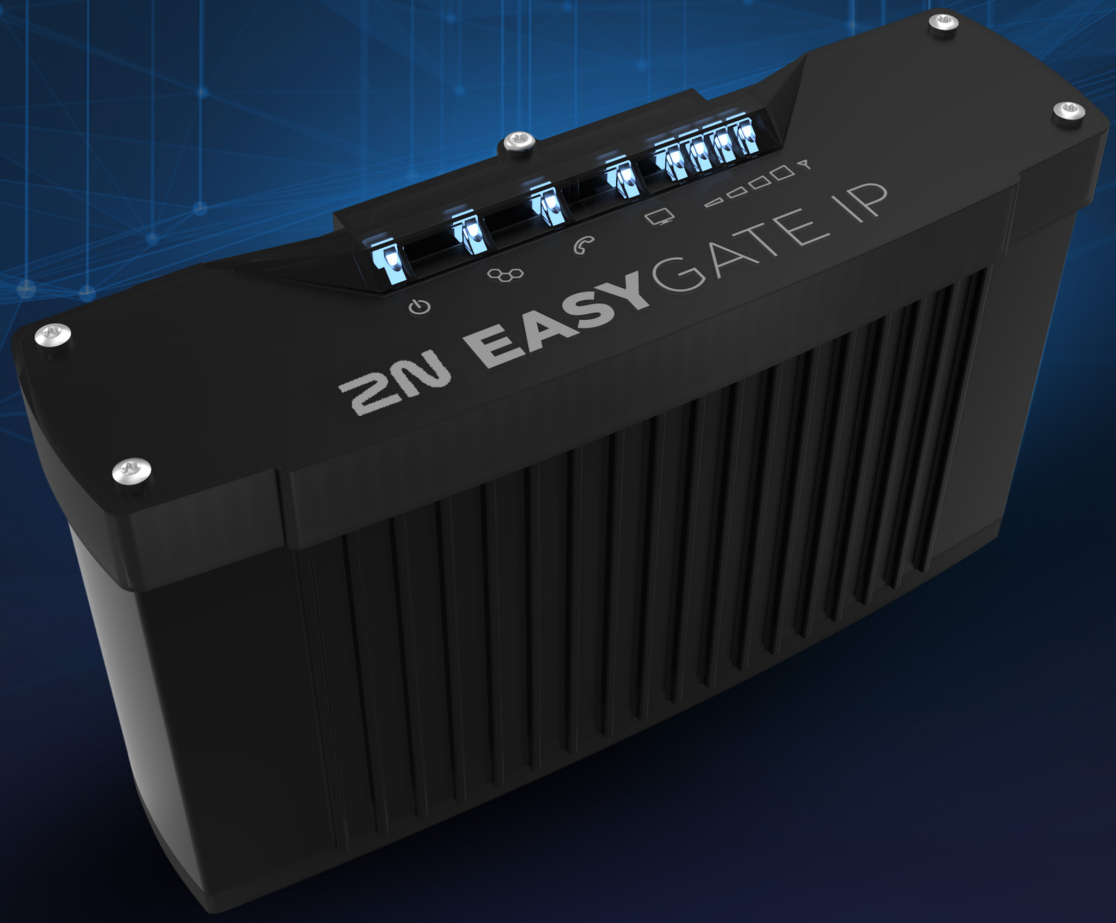


Comunicazione di emergenza dell‘ascensore

Standard di sicurezza informatica 2N

2N.com

Sicurezza informatica

Non è più un argomento limitato ai soli esperti IT che si occupano dell‘infrastruttura di rete! Una semplice carenza in un singolo prodotto può mettere a rischio l‘intero sistema. Se desiderate un edificio sicuro, dovete dedicare attenzione alla comunicazione di emergenza dell‘ascensore!

I sistemi di ascensori compromessi rappresentano una seria minaccia. I rischi di attacchi fisici sono legati all‘accesso agli edifici da parte di malintenzionati, mentre gli attacchi informatici causano una spesa di milioni in sanzioni normative, compromettono le funzioni aziendali principali e minacciano la reputazione dell‘azienda.

Quindi, cosa si può fare per assicurarsi di non mettere a rischio le operazioni quotidiane dell‘edificio e di conseguenza le persone al suo interno?

2N: il vostro partner di fiducia

Standard e certificazioni

La certificazione ISO 27001 ottenuta da 2N nel 2021 è la prova che gestiamo le informazioni sensibili in modo sistematico e sicuro. Tale certificazione è anche la risposta ideale alle esigenze dei clienti e ai requisiti legislativi come il GDPR, nonché una difesa contro le potenziali minacce alla sicurezza.

La qualità dei nostri prodotti è fondamentale sia per noi che per i nostri clienti, ed è per questo che li progettiamo, li sviluppiamo e li testiamo in base alle norme vigenti:

- Standard di sicurezza di rete e di sistema **IEC 62443-4-1 e 62443-4-2**
- **Regole tecniche per la sicurezza di funzionamento TRBS 1115**
- Principi selezionati della specifica **„Secure by Design“**
- **Modulo di sicurezza ASDM** della nostra azienda madre Axis
- I nostri processi e la nostra conoscenza interni

Implementazione dei principi di sicurezza per i singoli gruppi di prodotti

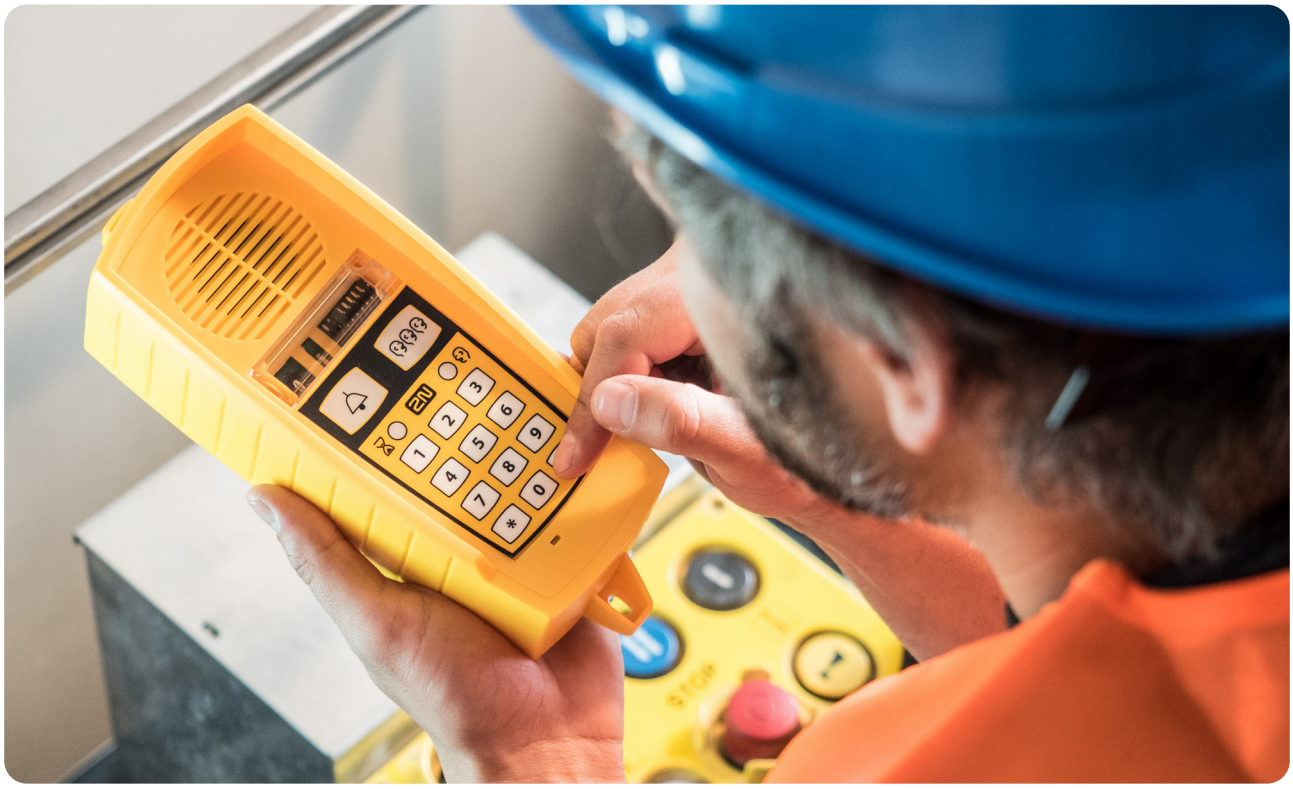
Disponiamo di soluzioni per le tecnologie analogiche, digitali e IP. Inoltre, abbiamo implementato una serie di principi per garantire la sicurezza di tutti questi prodotti, sia fisica che informatica.

1. Prodotti con sistema operativo Linux

Prodotti 2N progettati per la comunicazione di emergenza basata su IP negli ascensori

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

- Avvio sicuro basato sul sistema operativo Quectel
- Chiavi di protezione SSL: la lunghezza minima è di 256 bit, come quella utilizzata da HTTPS e da altri protocolli sicuri
- Il nostro protocollo brevettato „Tribble Tunnel“ garantisce una comunicazione HTTPS sicura tra i prodotti per ascensori 2N e il 2N® Elevator Center. L‘intero canale è crittografato con TLS e fondato su certificati emessi dal cloud
- Controllo e protezione contro lo spoofing di firmware non autorizzato con pacchetti di aggiornamento del firmware firmati digitalmente e crittografati
- Prevenzione degli attacchi a dizionario grazie al nostro sistema intelligente di password. Impone all‘amministratore di cambiare la password predefinita con una forte dopo il primo accesso.
- Impedisce agli hacker di ottenere i dati di accesso dal backup della configurazione con il salvataggio delle password crittografate: sono nascoste nella configurazione web.
- Possibilità di impostare i diritti dell‘utente - utente ospite opzionale con accesso di sola lettura
- Il protocollo SIPS cripta il contenuto dei messaggi SIP, impedendo l‘uso improprio dei dati (attacchi „man in the middle“, ecc.) e il furto di identità.



2. Sistemi brevettati

Prodotti 2N progettati per la comunicazione di emergenza sia analogica che digitale

2N® Lift1 2N® Lift8

- I prodotti dispongono di un sistema brevettato (firmware) che non può essere facilmente violato o utilizzato in modo improprio
- Aggiornamenti sicuri, protetti da uno speciale algoritmo di checksum: non è possibile eseguire spoofing di firmware dannosi
- Design brevettato per la sicurezza fisica

3. Applicazioni

- Le nostre applicazioni per Windows e Android consentono l'impostazione locale, la configurazione remota del sistema, l'aggiornamento e il monitoraggio delle chiamate di allarme e verifica.
- Queste includono il 2N Call Center Communicator e Server, il 2N Control Panel, i 2N Lift1 e Lift8 Service Tools.
- Gli installatori di tutte le applicazioni sono protetti da algoritmi sicuri con chiavi 2N e meccanismi di sicurezza integrati in Windows 10 (e versioni successive).

4. 2N® Elevator Center

Hosting

Questa piattaforma cloud è in hosting su Amazon Web Services (AWS). Per fornire ai nostri clienti la massima sicurezza possibile, il nostro sistema di gestione della sicurezza delle informazioni segue le migliori pratiche di sicurezza AWS.

Sicurezza

2N® Elevator Center è una moderna soluzione cloud che offre numerosi vantaggi in termini di sicurezza:

- Monitoraggio di intrusioni e prestazioni 24 ore su 24, 7 giorni su 7
- Distribuzione immediata degli ultimi aggiornamenti di sicurezza sia a livello AWS che 2N
- Il nostro protocollo per mantenere connessioni permanenti e sicure tra il cloud My2N e i prodotti 2N Lift (protocollo moderno e sicuro di tipo TLS)

Comunicazione crittografata

La piattaforma cloud fornisce servizi che richiedono molteplici interfacce di comunicazione tra i componenti cloud di 2N® Elevator Center e i dispositivi Lift. Tutte queste interfacce forniscono una comunicazione sicura HTTPS/TLS:

- Sincronizzazione cloud: tutti i dati del cloud vengono archiviati in modo sicuro su unità crittografate e trasportati tramite un protocollo brevettato di tipo TLS.
- Configurazione remota: l'utente può accedere in modo sicuro all'interfaccia web di ciascun dispositivo Lift da remoto, utilizzando un percorso di breve durata creato su richiesta.
- Fornitura/rinnovo dei certificati: i certificati dei dispositivi vengono emessi con una validità di 3 mesi, con rinnovo automatico un mese prima della scadenza e supporto per la revoca manuale, se necessario.
- Server di aggiornamento: il dispositivo può essere aggiornato in modo sicuro a nuove versioni firmware firmate digitalmente dal nostro server di aggiornamento 2N.
- Codici di sicurezza e verifica preliminare: il collegamento dei dispositivi al cloud è possibile solo utilizzando il processo di verifica preliminare e codici di sicurezza.

Applicando questi e molti altri principi nel processo di sviluppo, i **prodotti 2N per la comunicazione di emergenza dell'ascensore soddisfano i più elevati criteri di sicurezza** per la protezione dei dati personali, la sicurezza del prodotto e la sicurezza dell'infrastruttura di rete.

Misure di base che potete adottare oggi stesso per rendere il vostro sistema più sicuro

Ottenere la conformità con un quadro di controllo della sicurezza comprovato (ISO 27001, IEC 62443-4-1, IEC 62443-4-2, TRBS 1115)

Assicurarsi che il sistema di comunicazione di emergenza dell'ascensore preveda **l'uso di comunicazioni criptate** (protocolli come HTTPS, SIPS, TLS dovrebbero essere abilitati di default)

Creare diversi account con livelli di privilegio differenti (per garantire che gli utenti possano apportare modifiche solo in relazione ai loro compiti specifici)

Aggiornare regolarmente il software per ridurre i rischi di sicurezza informatica.

Formare i dipendenti per evitare le minacce di ingegneria sociale. L'errore umano è la parte più vulnerabile di qualsiasi sistema.

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