

FAQ - Sicherheitsbedenken EntryTower

Besteht die Gefahr, dass Unbefugte den EntryTower öffnen oder beschädigen?

Die robuste Aluminiumsäule bietet von Grund auf einen hohen Schutz vor äußeren Einwirkungen. Zusätzlich verhindert die abschließbare Stecktür, dass Unbefugte Zugang zum Innenraum erhalten.

Ist der EntryTower ausreichend gegen Witterungseinflüsse geschützt?

Ja, alle Komponenten des EntryTower sind für den Außeneinsatz entwickelt und besitzen passende Schutzarten für unterschiedliche Umweltbedingungen:

- Aluminiumsäule Schutzart IP54
- EntryScreen Schutzart IP65
- EntryCam Schutzart IP67
- Bluetooth-Token Schutzart IP67
- QR-Code Leser Schutzart IP54

Was passiert bei einem Internet- oder Stromausfall – bleibt der EntryTower funktionsfähig?

Der EntryTower ist so ausgelegt, dass die Zugangsdaten auch in Ausnahmesituationen zuverlässig verfügbar bleiben. Die Whitelist wird lokal gespeichert und wird im Falle eines Internetausfalls weiterhin genutzt. Selbst bei einem Stromausfall bleibt die Whitelist erhalten, sodass keine Daten verloren gehen.

Wie stellt der EntryTower den Datenschutz gemäß DSGVO sicher?

Die Verarbeitung personenbezogener Daten erfolgt vollständig DSGVO-konform. Die Daten werden ausschließlich auf Servern innerhalb der EU gespeichert – konkret in Deutschland und Finnland.

Der Zugriff auf das Profil lässt sich über klar definierte Rollen steuern – Admin, Techniker und Betreiber – sodass nur berechtigte Personen auf die für sie vorgesehenen Bereiche zugreifen können.

Daten werden maximal 30 Tage nach Ablauf ihrer Gültigkeit gespeichert und anschließend automatisch gelöscht. Die EntryCam überträgt lediglich das erkannte Kennzeichen, speichert jedoch keine Bilder. Die Whitelist prüft ausschließlich das Kennzeichen gegen die Kameradaten. Zudem kann der Aufnahmebereich der Kamera exakt definiert werden, um nur den erforderlichen Bildausschnitt zu erfassen.

Aktuell werden keine Vorgänge geloggt und ungültige Kennzeichen werden nicht an die Cloud übertragen. Die einzige regelmäßige Cloud-Kommunikation ist die Aktualisierung der Whitelist, die im Datensparmodus alle 10 Minuten und ohne aktiven Datensparmodus alle 60 Sekunden stattfindet.

Wie ist der EntryTower gegen IT-Sicherheitsbedrohungen und unbefugten Zugriff geschützt?

Für den Zugriff auf das System steht optional eine Zwei-Faktor-Authentifizierung über YubiKey zur Verfügung, sodass nur eindeutig verifizierte Nutzer Zugriff erhalten.

Zusätzlich wurde die gesamte Systemarchitektur durch unabhängige Sicherheitsexperten geprüft. Wir haben unser System auditieren lassen und von der Firma SSYS aus Tübingen gezielt auf Schwachstellen testen lassen.

Wie wird die Sicherheit der Kommunikation zwischen EntryTower und Server gewährleistet?

Alle Daten werden ausschließlich über gesicherte Verbindungen übertragen. Der EntryTower nutzt HTTPS, MQTT und TLS-Verschlüsselung, um die Kommunikation zuverlässig vor unbefugtem Zugriff zu schützen.

Wie wird eine Fehlbedienung oder Fehlkonfiguration des EntryTower verhindert?

Der EntryTower ist so aufgebaut, dass Fehlfunktionen durch falsche Einstellungen oder Bedienfehler weitgehend ausgeschlossen sind. Unterschiedliche Rollen mit abgestuften Rechten sorgen dafür, dass nur befugte Personen Konfigurationen vornehmen können. Die Einfahrt kann über verschiedene, leicht handhabbare Methoden wie Kennzeichen, QR-Code oder App gesteuert werden, und die Nutzeroberfläche ist bewusst intuitiv gestaltet. Zusätzlich bieten wir Schulungen an, um den sicheren Umgang mit dem System zu unterstützen.

Wie funktioniert die Wartung des EntryTower – und haben Servicetechniker einen eigenen Zugang?

Ja, Servicetechniker erhalten ein eigenes Login, das speziell für Wartungs- und Serviceaufgaben vorgesehen ist. Zudem sorgt ein einsehbares Wartungsprotokoll für volle Transparenz über alle durchgeführten Arbeiten und Systemzustände.