CTOUCH® The power to engage **SOFTWARE SECURITY**

Sicherheit ist die Grundlage der CTOUCH-Softwareentwicklung

Wir tun alles, um Ihre Daten zu schützen. Branchenübliche Best Practices und Frameworks bilden die Grundlage für unsere Sicherheitsrichtlinien. Diese Grundlage wurde von Grant Thornton entwickelt und wird regelmäßig aktualisiert. Unsere Mitarbeiter werden geschult, um sicherzustellen, dass unsere Hardware- und Softwareprodukte den Sicherheitsstandards entsprechen.

Allgemeine Software-Sicherheitsgrundsätze von CTOUCH

Das Sicherheitskonzept von CTOUCH basiert auf dem Prinzip der tiefgreifenden Absicherung: Sicherung Ihrer Daten auf jeder Ebene unter Verwendung mehrerer spezifischer Grundsätze und Kontrollen. Zu diesen Grundsätzen gehören:

- Sicherheit durch Design
- „Secure by default" – sicherste Standard-Einstellungen für die gesamte CTOUCH-Software
- "Zero Trust"- und "Least Privilege"-Prinzipien
- Regelmäßige Audits (durch Dritte)
- App-Vetting-Prozess unter Verwendung von MobSF für die Drittanbieter-Konformität unserer Sicherheitsstandards

CTOUCH Konformitätszertifizierungen & Vorschriften

CTOUCH ist ein Vorreiter in unserer Branche in Bezug auf die Sicherheit unserer Bildschirme und Software. Wir verwenden allgemein anerkannte Sicherheitsstandards und überprüfen regelmäßig unsere Einhaltung dieser Standards.

CTOUCH Zertifizierungen und Bescheinigungen

Einhaltung der GDPR-Standards

Verifiziert durch Grant Thornton

ISO IEC 27001 zertifiziert

Ab Sommer 2023

Einhaltung des deutschen Datenschutzgesetzes

Konformität mit Auth0-Protokollen

CTOUCH Sphere – Geräteverwaltung

CTOUCH Sphere ist die Webanwendung für die Geräteverwaltung, mit der Sie alle Ihre CTOUCH-Touchscreens aus der Ferne verwalten können. Auf diese Weise können Sie Ihre CTOUCH-Touchscreens immer auf dem neuesten Stand und sicher halten. Wir verwenden in Sphere eine robuste Reihe spezifischer Sicherheits- und Datenschutzprinzipien, die sicherstellen, dass Sie unsere Produkte unbesorgt nutzen und verwalten können.

Identitäts- und Zugriffsmanagement

Die Geräteverwaltung in Sphere beginnt mit der Identitätskontrolle. Wir verwenden das Sicherheitsprinzip des geringsten Privilegs, um einen Benutzertyp zuzuweisen. Standardmäßig erhalten alle Benutzer ein Kundenbenutzerprofil. Ein Händler kann dann eine Aktualisierung des Benutzerprofils beantragen, die von CTOUCH überprüft und genehmigt wird. Damit der Händler oder CTOUCH aus der Ferne auf die Hardware-Einstellungen des Touchscreens des Kunden zugreifen kann, muss der Kunde den Zugriff in Sphere ausdrücklich genehmigen. So hat der Benutzer die Kontrolle über die Einstellungen, die er freigibt.

IDENTITÄTS- & ZUGANGSKONTROLLEN

- Dauer der Sitzung
- JIT-Privileged-Access-Management
- Passwortkontrolle mit Auth0
- Single Sign-On und Zwei-Faktor-Autorisierung

Datenschutz

Standardmäßig verschlüsselt CTOUCH die Daten im Ruhezustand und bei der Übertragung als Teil unserer grundlegenden Sicherheitskontrollen. Wir verwenden Hashing- und Salting-Verschlüsselung, um sicherzustellen, dass Ihre Passwörter nur Ihnen bekannt sind. Wir stellen auch sicher, dass keine Daten aus Sphere exportiert werden können. Alle Sphere-Daten werden in Deutschland gespeichert und verwenden die höchsten Sicherheitsstandards in Europa.

DATENSCHUTZMASSNAHMEN

- HTTPS- und WSS-Protokolle
- Entschlüsselung im Sicherheitsschlüssel-Tresor auf dem Azure-Server
- Aktive Schwachstellenerkennung und -verwaltung
- Automatisierte Sicherheitstests mit Azure-Diensten

Datenprotokollierung und -speicherung

CTOUCH speichert keine personenbezogenen Daten in Sphere oder auf unseren Touchscreens. Aufgezeichnete Daten von Ihren Bildschirmen, die in Sphere sichtbar sind, sind für CTOUCH-Mitarbeiter nicht zugänglich, es

sei denn, CTOUCH verwaltet Ihr Konto - dies muss vom Kunden in den Sphere-Einstellungen ausdrücklich bestätigt werden. Die aufgezeichneten Daten werden niemals an Dritte weitergegeben.

AUFGEZEICHNETE DATEN

- Die letzten Bildschirmeinstellungen werden aufgezeichnet
- Täglicher Energieverbrauch pro Bildschirm wird protokolliert
- Nur die E-Mail-Adresse und der Firmenname werden für das Sphere-Konto verwendet
- Es werden keine benutzerbezogenen Statistiken aufgezeichnet
- Dritte haben keinen Zugriff auf Sphere- und Bildschirmdaten