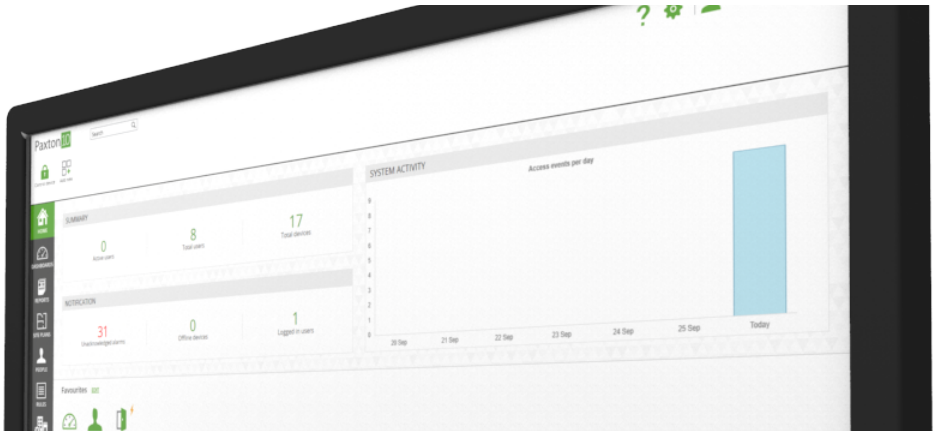

Paxton10 Sicherheit

Übersicht

Paxton10 ist ein netzwerkbasiertes Zugangskontroll- und Videomanagementsystem, das vom Paxton10-Server über seine Web-Benutzeroberfläche gesteuert und konfiguriert wird. Dieses Dokument beschreibt, wie Paxton10 sicher und widerstandsfähig gegen Sicherheitsangriffe und Datenverletzungen bleibt.

Paxton10 Server

Betriebssystem und BIOS

Auf dem Paxton10 Server läuft Microsoft Windows 10 IoT (ab Februar 2020). Einige frühere Modelle (vor 2020) laufen jedoch möglicherweise unter Windows 7 Embedded - bitte kontaktieren Sie den Support, um mehr zu erfahren.
< www.paxton.info/596 >

Remote-Desktop und Dateifreigabe werden auf dem Server aktiviert, gesichert mit einem 40-Zeichen-Betriebssystem-Passwort, das für jedes System einzigartig ist. Das Server-BIOS ist ähnlich passwortgeschützt.

Windows Updates

Server werden im Rahmen von Windows Update mit vorgewählten Sicherheitskorrekturen und Patches ausgestattet. Diese werden, wo möglich, im Hintergrund und, wo nicht möglich, parallel zu Service-Releases als Teil des vom Systemingenieur kontrollierten Upgrade-Prozesses aktualisiert. Möglicherweise muss der Server nach einem Windows-Update neu gestartet werden. Die Paxton10-Software bietet bei Bedarf die Möglichkeit, um dies zu tun. Für den Empfang von Paxton10-Software und Windows-Updates ist eine Internetverbindung erforderlich.

Virenschutz

Server mit Windows 10 IoT werden Windows Defender mit automatischen Updates enthalten. Für den Empfang von Updates ist eine Internetverbindung erforderlich.

USB-Anschlüsse

Der Paxton10 Server wird mit einem USB-Speicherstick zur Systemsicherung geliefert. Dieser Speicherstick kann in jeden Paxton10-Server eingesteckt werden, um die Systemdatenbank auf diesem Server wiederherzustellen/installieren. Die Datenbanksicherung auf USB erfolgt automatisch alle 24 Stunden. Die Sicherung auf USB kann einfach durch Entfernen des USB-Speichersticks deaktiviert werden.

APN-0053-D

Die USB-Anschlüsse sind nicht gesperrt und können als solche verwendet werden, um auf die Daten des Servers zuzugreifen oder Befehle auszuführen. Die Sicherheit der USB-Anschlüsse wird durch die Sicherung des Standortes des Servers erreicht. Nur die erforderlichen Installateure und das IT-Personal sollten Zugang zum Standort des Servers haben.

Passwörter und Client-Zugang

Die Anmeldung bei der Paxton10-Software ist auf Gruppen-/Funktionsebene erlaubt. Jeder Systembenutzer erhält nur Software-Zugriff auf die Daten und die Kontrolle darüber, ob ihm dies erlaubt ist oder nicht.

Die Anmeldung ist durch E-Mail-Adresse und Passwort geschützt. Alle Passwörter müssen mindestens 3 Typen von Zeichen enthalten: Kleinbuchstaben, Großbuchstaben, Zahlen, Interpunktion. Zusätzlich müssen alle Passwörter mindestens 6 Zeichen umfassen.

Passwörter werden sicher in der Server-Datenbank unter Verwendung von Salted Hash gespeichert.

Netzwerkkommunikation

Client-Software-Zugriff

Beim Zugriff auf die Paxton10-Software aus dem lokalen Netzwerk (über die lokale URL des Servers) erfolgt die Kommunikation zwischen dem Client und dem Server. Die Kommunikation wird über HTTPS mit einem selbstsignierten SSL-Zertifikat von Paxton10 gesichert, zusätzlich zu allen Sicherheitsmaßnahmen des lokalen Netzwerks.

Beim Zugriff auf die Paxton10-Software von einem anderen Standort (über die Remote-Access-URL des Servers), wird die Paxton10-Software mit Microsoft Azure gehostet. Die Kommunikation zwischen Server, Client und Azure wird über HTTPS mit AES-256-Verschlüsselung gesichert. Eine Internetverbindung ist erforderlich. In Azure werden keine Benutzer- oder Gerätedaten gespeichert.

E-Mails von Paxton10

Paxton10 verwendet E-Mail zum Zurücksetzen von Passwörtern und zum Ausstellen von Smart Credentials. Die E-Mails werden von der folgenden Adresse gesendet: support@paxton10portal.com. Von Paxton10 gesendete E-Mails verwenden TLS-Verschlüsselung.

Ein zusätzlicher E-Mail-Server kann in Paxton10 für die Verwendung mit Auslösern und Aktionen konfiguriert werden. Die Sicherheit dieses E-Mail-Servers wird durch den Host bestimmt.

Controller-Kommunikation und Firmware-Updates

Die Kommunikation mit Paxton10-Controllern erfolgt über HTTPS/SSL.
Wir verwenden TLS 1.2 für standortübergreifende Anwendung, das SHA-256, also eine 256-Bit-Verschlüsselung, verwendet.

Weitere Informationen zur Netzwerksicherheit und den verwendeten Kommunikationsprotokollen finden Sie unter AN0051-D Netzwerkanforderungen, -optimierung und -sicherheit in Paxton10 < www.Paxton.Info/6391 >.

Berechtigungsnachweise und smarte Geräte

RFID-Tags und -Karten

Paxton10-Karten und -Transponder speichern ihre Seriennummer in einem passwortgeschützten Bereich, wodurch unbefugtes Lesen oder Kopieren verhindert wird. Darüber hinaus liest Paxton10 die gesamte Karte oder den Transponder, nicht nur die Kartendaten; das Identifikationsmedium wird dann mit einer Kombination der Kartendaten (Transponderdaten, Seriennummer, Herstellungsdatum usw.) erstellt, was das Klonen der Karte nahezu unmöglich macht.

Die Paxton10-Software bietet zusätzliche Merkmale und Funktionen, die so konfiguriert werden können, dass jegliches Risiko des Klonens von Karten und des Zugriffs auf gestohlene Karten weiter beseitigt werden kann, wie z. B. Anti-Passback, Verfallsdaten der Benutzer, Transpondersperre und doppelte Authentifizierung (Transponder + Code oder Transponder + PIN).

Bluetooth-Kommunikation

Smart-Identifikationsmedien (Smartphones, Tablets und Uhren) und Bluetooth-Anhänger kommunizieren mit Paxton10-Lesern über Bluetooth Low Energy (BLE). Es wird ein Rolling-Code-Algorithmus mit Verschlüsselung verwendet, um das Klonen von Identifikationsmedien und Code-Grabbing zu verhindern.

Smart-Identifikationsmedien

Smart-Identifikationsmedien (Smartphones, Tablets und Uhren) werden mit einem eindeutigen 32-Zeichen-Identifikationsmedium ausgestellt. Jedes Identifikationsmedium kann für ein einzelnes Android- oder iOS-Konto registriert werden, und einmal registrierte Identifikationsmedien können nicht erneut ausgestellt werden. Das Identifikationsmedium wird im Schlüsselbund oder im sicheren Speicher des Kontos gespeichert.

Wenn zusätzliche Sicherheit erforderlich ist, kann ein Paxton10-System alle smarten Geräte zwingen, eine Bildschirmsperre zu verwenden, die vor unbefugtem Zugriff durch verlorene oder gestohlene Geräte schützt. Weitere Sicherheit kann durch Softwarefunktionen wie Anti-Passback und Identifikationsmedium-Management erreicht werden, und es kann eine zusätzliche Authentifizierung auf dem Gerät und eine Bildschirmsperre, wie PIN oder Code an einer Tastatur, verlangt werden.