Paxton10 Security

Overzicht

Paxton10 is een netwerkgebaseerd toegangscontrole en video management systeem. De software is geïnstalleerd op de handige software controller en kan benaderd worden vanuit iedere PC of tablet met een webbrowser.

In dit document leggen we uit welke beveiliging we hebben toegepast op Paxton10.

Paxton10 Software controller

Besturingssysteem en BIOS (Basic Input Output System)

De Paxton10 Software Controller is voorzien van Microsoft Windows 10 IoT.

Remote desktop en bestandsdeling is ingeschakeld en beveiligd met een 40 karakter wachtwoord dat voor ieder systeem uniek is.

De BIOS van de software controller is op dezelfde manier beveiligd.

Windows updates

De software controllers worden geleverd met vooraf geselecteerde beveiligingsfixes en patches als onderdeel van Windows update. Deze worden op de achtergrond bijgewerkt en geïnstalleerd.
De software controller moet mogelijk opnieuw worden opgestart na een Windows update. De Paxton10 software biedt u de mogelijkheid om de software controller opnieuw op te starten na een update.

Een internetverbinding is vereist om Paxton10 software en Windows updates te ontvangen.

Virus bescherming

Software controllers met Windows 10 IoT zijn voorzien van Windows Defender met automatische updates.

Een internetverbinding is vereist om updates te ontvangen.

USB poorten

De Paxton10 Software Controller wordt geleverd met een USB stick waar de back-ups van het systeem op worden geschreven. Deze USB stick kan in elke Paxton10 Software Controller worden geplaatst om de systeemdatabase op die server te herstellen. De systeem back-up naar USB stick vindt automatisch elke 24 uur plaats. Back-up naar de USB kan eenvoudig worden uitgeschakeld door de USB stick te verwijderen.
De USB poorten zijn niet vergrendeld en kunnen worden gebruikt om toegang te krijgen tot de servergegevens of om opdrachten uit te voeren. Beveiliging van de USB poorten wordt bereikt door de locatie van de server te beveiligen. Alleen de vereiste installateurs en IT-personeel mogen toegang hebben tot de locatie van de server.

Wachtwoorden en toegang tot de software

Voor Paxton10 gebruikt u een e-mailadres en wachtwoord in te loggen.
Bij het aanmaken van een wachtwoord moet de gebruiker voldoen aan de minimale eisen voor een wachtwoord: minimaal 7 tekens en een mix van ten minste drie tekensoorten: hoofdletters, kleine letters, cijfers en leestekens.

Het systeem controleert nieuwe wachtwoorden ook tegen een grote open-sourcelijst van meer dan 100.000 veelgebruikte of eerder gelekte wachtwoorden. Staat een wachtwoord op die lijst, dan weigert Paxton10 het wachtwoord om zwakke of onveilige wachtwoorden te voorkomen. Een ingebouwde sterkte-indicator laat zien hoe veilig het wachtwoord is tijdens het typen.

Indien nodig kunnen beheerders de minimale lengte van wachtwoorden verhogen of een beleid inschakelen dat gebruikers verplicht hun wachtwoord elke 60 dagen te wijzigen. Beide opties zijn te configureren in het menu systeeminstellingen. Paxton10 staat zes mislukte inlogpogingen toe. Na de zesde foutieve poging wordt de gebruiker 15 minuten geblokkeerd voordat opnieuw kan worden geprobeerd.

Wachtwoorden worden veilig opgeslagen in de serverdatabase met behulp van salted hash.

Communicatie

Software toegang

Wanneer u in het lokale netwerk via de lokale Paxton10 URL inlogt via uw webbrowser maak u een verbinding vanuit uw browser naar de software controller. Dit is een HTTPS verbinding en maakt gebruik van een SSL certificaat.

Wanneer u remote toegang gebruikt om op afstand in te loggen in Paxton10 maakt uw webbrowser via Microsoft Azure verbinding met uw Paxton10 Software Controller. De communicatie tussen uw browser, software controller en Microsoft Azure is beveiligd door middel van een HTTPS verbinding met een AES-256 bits encryptie. Er worden geen gebruikersgegevens opgeslagen in Microsoft Azure.

E-mails vanuit Paxton10

Paxton10 maakt gebruik van e-mails voor het versturen van smart credentials en om het wachtwoord van uw account te resetten. Het e-mailadres wat hiervoor gebruikt wordt is: support@paxton10portal.com. De e-mailserver is beveiligd door middel van een TLS encryptie.

In Paxton10 kan een extra e-mail server worden geconfigureerd voor gebruik met Triggers en Acties. De beveiliging van deze e-mailserver wordt bepaald door de aanbieder van het e-mail account.

Communicatie met de Paxton10 Controllers

De communicatie tussen de Paxton10 Software Controller en Paxton10 Controller is voorzien van HTPPS met een SSL certificaat. Wanneer u gebruik maakt van Multi-site wordt de verbinding beveiligd door middel van TLS 1.2 welke een SHA-256 bits encryptie gebruikt.

Voor meer informatie over netwerken en beveiliging zie ook: AN0051-NL - Handige informatie over netwerken en beveiliging voor het gebruik met Paxton10 < www.Paxton.Info/6314 >.

Credentials en smart credentials

Secure kaarten en tags

Paxton10 Secure kaarten en tags hebben een uniek nummer wat is voorzien van een eigen wachtwoord. Tijdens het lezen wordt er een authenticatieprotocol uitgevoerd in de vorm van een wachtwoorduitwisseling tussen de tag en een Paxton10 lezer. Bovendien verifieert de Paxton10 lezer alle informatie zoals productiedatum, fabrikant informatie en serienummer van de tag en niet alleen het kaartnummer waardoor het klonen van Paxton10 tags vrijwel onmogelijk is. Verder zorgt deze verificatie ervoor dat de kaarten authentiek zijn, wat voor een extra beveiligingslaag binnen uw Paxton10 systeem zorgt.

De Paxton10 software biedt extra functies die kunnen worden geconfigureerd om het risico van kaartklonen en gestolen kaarten verder te beperken zoals anti-passback, dubbele verificatie i.c.m het Paxton10 lezerkeypad (Kaart + code of Kaart + PIN).

Bluetooth communicatie

Een rolling code-algoritme met encryptie wordt gebruikt om het klonen van de smart credential en bluetooth handsfree tag te voorkomen. Ook zijn lezers zo in te stellen dat er een extra verificatie vereist is bij het gebruik van een smart credential.

Smart credentials

Smart credentials worden uitgeven met een 32 cijferige registratie code. Iedere smart credential kan eenmalig gebruikt worden op een Android of IOS toestel, wanneer de code is gebruikt kan deze niet opnieuw gebruikt worden op een ander toestel.

Het is mogelijk om dual verificatie in te stellen op uw Paxton10 kaartlezer. Wanneer dit ingesteld is wordt er gevraagd om een biometrische verificatie op uw smartphone voordat de deur ontgrendeld wordt. Uw smartphone dient wel voorzien te zijn van een schermvergrendeling.

De Paxton10 software biedt extra functies die kunnen worden geconfigureerd om het risico van het gebruik van een gestolen smartdevice verder te beperken zoals anti-passback, dubbele verificatie i.c.m het Paxton10 lezer keypad (Kaart + code of Kaart + PIN).