

uwo-smart control

uwo-smart control verwendet die sogenannte Cloud-Techniken für Ihre Gerätesicherheit. Dabei setzt UWO-Water GmbH grundsätzlich nur Server aus Rechenzentren mit Standort in Deutschland und der Europäischen Union ein. Die Server sind mit DoS-Schutz, Firewall und Einbruchserkennung sowie -blockierung ausgestattet.

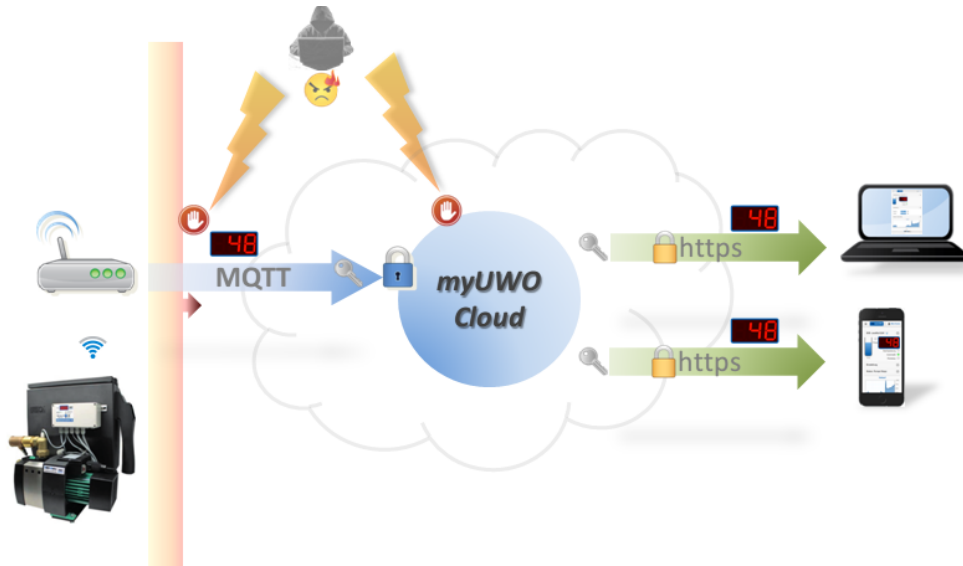


Abbildung 1: uwo-smart control

Datenverbindungen

Ihre Regenwassersteuerung mit uwo-smart control verbindet sich mit Ihrem WLAN und sendet mit Hilfe des MQTT¹-Protokolls Statusinformationen an den myUWO Cloud Server. Der myUWO Cloud Server als auch jedes andere Gerät oder Person im Internet haben keine Möglichkeit, eine Datenverbindung zu Ihrem Router und somit auch nicht zu Ihrer Regenwassersteuerung aufzubauen.

Um Ihr Heimnetz zu schützen, erfolgt der Datenverkehr immer nur aktiv von der Regenwassersteuerung ausgehend in das Internet an die myUWO Cloud. Ankommende Daten von der myUWO Cloud können so nur nach vorheriger aktiver Abfrage von Seiten der Regenwasserzentrale zur Steuerung gelangen.

Der Zugang von uwo-smart control zur myUWO Cloud erfolgt ausschließlich über eine Anmeldung am Cloud-Server mit ID und Passwort. Die ID und das Passwort ist uwo-smart control einmalig und von uwo-smart control Gerät zu uwo-smart control Gerät unterschiedlich. Die Übertragungen erfolgen mit Standardtechniken wie TCP und sind SSL-verschlüsselt. Der Kundenzugang zur myUWO Cloud mittels PC oder Smartphone kann nur über ein zuvor eingerichtetes Kundenkonto mit Zugangskennung und Passwort erfolgen. Der Zugang ist beschränkt auf die kundeneigene Regenwassersteuerung.

¹ *Message Queuing Telemetry Transport* ist ein offenes Verbindungsprotokoll zur Maschine-zu-Maschine (M2M) Kommunikation, das, trotz event. hoher Verzögerungen oder beschränkter Netzwerke, die Übertragung von Daten in Form von Nachrichten zwischen den Teilnehmern ermöglicht.

Datensicherheit

Auf den myUWO Cloud Servern verwendete Passworte werden grundsätzlich niemals im Klartext gespeichert oder zwischengespeichert. Es werden nur Passwort-Fingerabdrücke (sogenannte Hash-Werte) der Passworte gesichert. Diese lassen selbst bei Einbruch in das System keinen Rückschluss auf die ursprüngliche Anmeldedaten zu.

Uwo-Water kann Ihnen daher z. B. bei vergessenen Anmeldedaten Ihre Daten nicht nennen, Sie können sich lediglich ein neues Passwort erstellen lassen, dass die nach Erhalt umgehend ändern sollten. Die Sicherheit Ihres Kontos hängt alleine von der Komplexität ihres gewählten Passworts ab. Verwenden Sie ausreichend komplexe Passworte mit einer hohen Entropie - Uwo-Water empfiehlt dazu Passworte mit Sonderzeichen und Ziffern mit mindestens 12 Zeichen oder lange sinnfreie Sätze.

Falls Ihr Router ein Gäste-WLAN anbietet, können Sie Ihr uwo-smart control zur zusätzliche Sicherheit an diesem Gäste-WLAN anmelden. Damit ist Ihre Regenwassersteuerung vollkommen getrennt von Ihrem privaten Netzwerk.

Die Regenwassersteuerung sendet an die myUWO Cloud Statusinformationen (Füllstand, Betriebsmodi) sowie Anfragen für Befehlsanforderungen. Das erfolgt in der Regel innerhalb weniger 100stel Sekunden.

Web-App vs. Smartphone-App



Abbildung 2: Unsichere Direktverbindung einer App

Eine direkte Steuerung von uwo-smart control per App mit direkt nötigen Zugriff auf die Regenwassersteuerung würde erhebliche Einbruchs- und Manipulationsrisiken einschließen, da nicht nur die App sondern auch Unberechtigte Zugriff auf uwo-smart control und Teile ihres Netzwerks erhalten könnten.