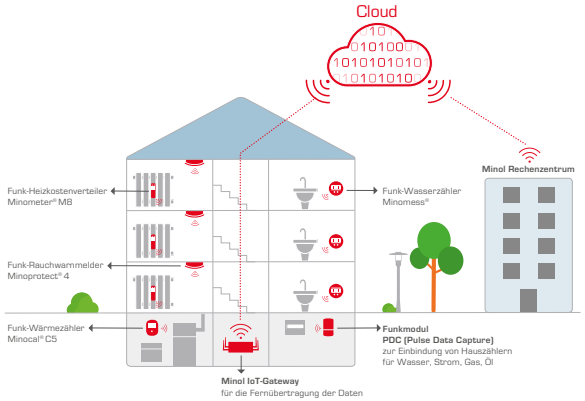
So funktioniert die Minol Cloud



Alle Datenpakete werden vom IoT-Gateway über das Mobilfunknetz an den Minol Connect Netzwerkserver weitergeleitet. Die Netzwerkserver identifizieren zulässige Geräte und entfernen zudem doppelte Datenpakete, falls diese von mehreren IoT-Gateways weitergeleitet wurden.

Vom Netzwerkserver werden die Daten dann an die Minol Cloud weitergeleitet und dort entschlüsselt. Nun stehen die Daten zur Nutzung in den unterschiedlichen Minol Anwendungen zur Verfügung. Die Abrechnungssoftware von Minol bezieht die Verbrauchsdaten beispielsweise auch aus der Minol Cloud genau wie auch das Kundenportal „Minol direct“.

Informationen im Internet

Alle Minol Informationen zum Thema Datensicherheit finden Sie über den folgenden Link oder den nebenstehenden QR-Code.

minol.de/connect-datensicherheit

Minol Messtechnik
W. Lehmann GmbH & Co. KG | Nikolaus-Otto-Str. 25 | 70771 Leinfelden-Echterdingen
Telefon 0711 94 91-0 | Telefax 0711 94 91-238 | info@minol.com | minol.de

Stand 16.02.2019

Datensicherheit bei Minol

Wissenswertes zur Cyber-Security

Datensicherheit garantiert

Rechenzentrum in Deutschland

- Hosting in einem „Tier IV“ zertifizierten Rechenzentrum in Deutschland. Dies ist die höchste Sicherheitsstufe in der Zertifizierung nach DIN EN 50600.
- Kontrollierter Zugang in Sicherheitsbereiche durch biometrische Personenvereinzelungsschleuse.
- Hohes physisches Sicherheitsniveau mit Einbruchmeldeanlage und Überwachungssystemen.

Sicherheit für Online Kundenplattform (EMT-Anwendungssicherheit)

- Sicherer Login und sichere Authentifizierungs- und Autorisierungsmechanismen (z.B. via OAuth 2.0).
- Geprüfte Sicherheit bei Benutzer- und Rechteverwaltung.
- Sichere Speicherung und Verarbeitung von Passwörtern (z.B. Verwendung von bcrypt als Hash-Algorithmus)

Datenschutz

- Einhaltung der Datenschutzanforderungen gemäß DSGVO und BDSG (Bundesdatenschutzgesetz).
- Speicherung der Daten und Hosting der Anwendungen in ausschließlich deutschen Rechenzentren.

Kommunikationssicherheit

- Verschlüsselte und authentifizierte Kommunikation gemäß den BSI (Bundesamt für Sicherheit in der Informationstechnik) Vorgaben zur Smart Metering PKI (SM-PKI).
- Schutz der von den Haushalten übermittelten Messdaten durch eine gegenseitige Authentisierung der Kommunikationspartner sowie durch verschlüsselte und integritätsgesicherte Kommunikationskanäle sichergestellt.

Zertifiziertes ISMS (Informationssicherheits-Managementsystem) der SaaS (Software-as-a-Service) Infrastruktur und des sicheren Betriebs nach ISO 27001

- Die ISO 27001 ist eine internationale Norm für Informationssicherheit und hat sich als weltweiter Standard durchgesetzt.
- Etabliertes Risikomanagementsystem zur Erkennung, Analyse, Bewertung, Überwachung, Steuerung und Kontrolle von Informationssicherheitsrisiken.
- Update- und Patchmanagement, Änderungs- und Freigabeprozesse, Datensicherungs- und Wiederherstellungsprozesse, Monitoring und Alarmierung.

Sichere Betriebsumgebung und technische Sicherheit der Betriebsumgebung

- Härtung der Systemlandschaft auf Basis von „Best-Practices“ wie beispielsweise den Center for internet security (CIS) Benchmarks.
- Trennung von Netzwerksegmenten und Umsetzung von restriktiven Firewallregelwerken.
- Einsatz von Intrusion Detection Systemen (IDS) und Monitoring der System- und Anwendungslandschaft.
- Gewährleistung von Datensicherung und Wiederherstellung.
- Regelmäßige professionelle Penetrationstests zur Überprüfung des technischen Sicherheitsniveaus.