SICHERE KOMMUNIKATION IN WURM-ANLAGEN

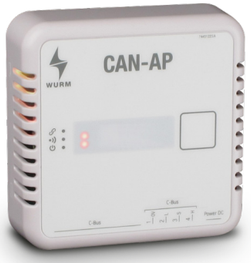
Die Kommunikation in den Wurm-Anlagen läuft über das CAN-Bus-System. Als sog. Embedded Bus ist es ein geschlossenes System, das sich durch hohe Zuverlässigkeit auszeichnet.

Die Maßnahmen für die sichere Datenübertragung über den CAN-Bus passen wir entsprechend der zunehmenden Vernetzung von Geräten und Systemen laufend an. Hier gilt unser Augenmerk besonders den Schnittstellen nach außen. Sie sind potenzielle Angriffspunkte für unbefugte Zugriffe auf die Datenkommunikation und bedürfen besonderer Sicherheitsvorkehrungen. Die Konfiguration unserer Gateways gehört hierzu, um externen Angreifern einen Riegel vorzuschieben.

Für den drahtlosen Zugriff auf Ihre Wurmanlage über die App Frida haben wir das leicht zu implementierende Modul CAN-AP entwickelt. Die drahtlosen Schnittstellen müssen besonders vor Angriffen geschützt werden. Als Funktechnik verwenden wir Bluetooth® LE. Im Gegensatz zum W-LAN liegt der Kommunikationsbereich bei nur wenigen Metern. Zugriff auf Endgeräte ist nur aus unmittelbarer Nähe zur Kälteanlage möglich. Diese räumliche Begrenzung und weitere hocheffektive Authentifizierungsmechanismen mindern die Gefahr durch potenzielle Eindringlinge ins System.

Setzt man den CAN-AP zudem bei der Konfiguration auf Default „inaktiv“, wird die (zeitlich begrenzte) Kommunikation erst durch einen manuellen Eingriff ermöglicht - was den Schutzfaktor nochmals erhöht.

Hinter den hier exemplarisch dargelegten Maßnahmen, die mit weiteren zum bestmöglichen Schutz der Kundendaten ineinandergreifen, steht ein Team erfahrener Wurm-Entwickler. Sie beobachten ständig die Entwicklungen im Bereich Cyberkriminalität und Sicherheitstechnologien. Über Jahre aufgebaute Kompetenz und kontinuierlich erweitertes technologisches Knowhow unserer Experten sorgen mit dafür, dass Ihre Daten bei Wurm bestens aufgehoben sind.



SICHERHEIT MIT SYSTEM

- Eine ausgefeilte Sicherheitsarchitektur mit diversen ineinandergreifenden Maßnahmen sorgt für bestmöglichen Schutz Ihrer Daten. Zentrale Ziele der IT-Sicherheit - Verfügbarkeit, Vertraulichkeit und Integrität - werden erfüllt.
- Die komplexe Sicherheitsstruktur wird laufend an technologische Innovationen und neue Risikofaktoren angepasst.
- Sämtliche Kunden– und Anlagendaten werden auf Wurm-eigenen redundanten Servern am Standort Remscheid gespeichert.
- Ausgefeilte Verschlüsselungsmethoden sowie mehrstufige Authentifizierungsverfahren sichern die Verbindungen zu den angeschlossenen Filialen.
- Unsere Web-Anwendungen basieren alle auf dem sicheren https-Protokoll.
- Gateways von Wurm sind so konfiguriert, dass sie plattformunabhängig den gleichen Sicherheitsstandard gewährleisten. Schnittstellen nach außen werden besonders abgesichert.

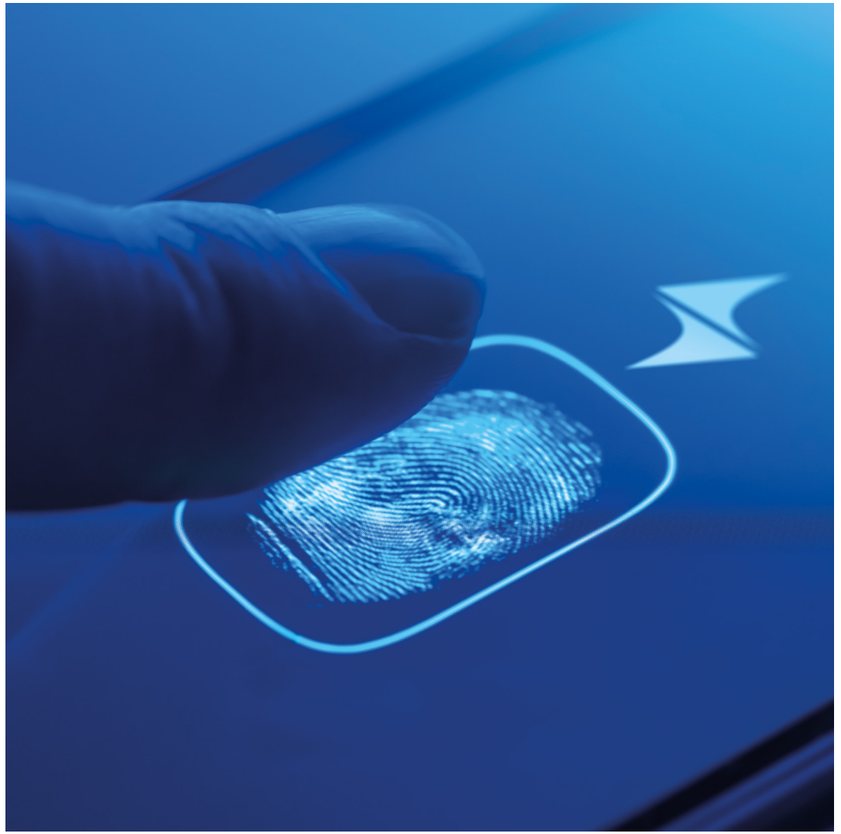
WURM SYSTEME

Wurm GmbH & Co. KG Elektronische Systeme
Morsbachtalstraße 30
D-42857 Remscheid

Tel: +49 (0) 2191 - 8847 300
Fax: +49 (0) 2191 - 8847 9300
Email: info@wurm.de

FSC
www.fsc.org
RECYCLED
Papier aus Recyclingmaterial
FSC® C010193

024A-DE



SICHERHEIT FÜR IHRE DATEN

WURM SYSTEME

IHRE SICHERHEIT HAT FÜR UNS HÖCHSTE PRIORITÄT

In Zeiten zunehmender internationaler Vernetzung und Digitalisierung sind IT-Sicherheit und Datenschutz von größter Bedeutung.

Als Unternehmen der High-Tech-Branche steht die Wurm GmbH & Co. KG in der Verantwortung, effektive Lösungen zum Schutz für Unternehmens- und Kundendaten zu entwickeln. Wir setzen alles daran, die zentralen Ziele der IT-Sicherheit wirkungsvoll umzusetzen: Verfügbarkeit, Vertraulichkeit und Integrität. Mit einer Einzelmaßnahme ist es hierbei nicht getan – vielmehr müssen ineinander greifende Sicherheitsmechanismen in firmeninternen Prozessen und in unseren Produkten implementiert werden.

Wurm hat daher schon seit vielen Jahren eine komplexe Sicherheitsstruktur etabliert, die kontinuierlich an den technologischen Fortschritt und die sich ständig verändernden Risikofaktoren angepasst wird.

Dies umfasst u.a. die Speicherung aller Kunden- und Anlagendaten auf eigenen redundanten Servern, ausgefeilte Verschlüsselungsmethoden für hochsichere Verbindungen zu den angeschlossenen Filialen und mehrstufige Authentifizierungsverfahren.

Wir möchten Ihnen hier einen Überblick geben, welche Maßnahmen unser Unternehmen für Ihre Sicherheit und die Sicherheit Ihrer Daten ergreift.

WURM DATA-CENTER: HERZSTÜCK UNSERES SERVER-KONZEPTS

Herzstück unseres Systems ist das Wurm DATA-CENTER. Von dort werden die Daten aller angeschlossenen Anlagen für das Anlagenmonitoring mit Wurm-Lösungen bereitgestellt.

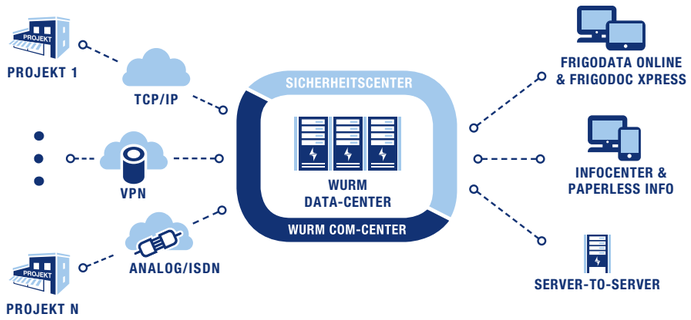
Zum Schutz Ihrer Daten haben wir ein umfangreiches Maßnahmenpaket geschnürt. Es umfasst u.a. Zugriffs- und Zugangskontrollen, ausgefeilte Berechtigungskonzepte, regelmäßige Mitarbeiter-Schulungen und intelligente Angriffs-Abwehr-Systeme.

Mit der Verwaltung der individuellen Nutzeridentitäten und der Konfiguration von Zugangsberechtigungen schafft das SICHERHEITSCENTER die unverzichtbaren Bedingungen für die Authentifizierung des Einzelnen bei der Anmeldung am Wurm-System. Gewerkespezifische Zugriffsrechte werden nur an Personen ausgegeben, die für das betreffende Projekt zugangsberechtigt sind.

Unsere Kunden haben entsprechend ihrer spezifischen Anforderungen verschiedene Optionen, sich anzumelden – etwa mit unserer App OneID, aber auch per SMS und Email.

Grundsätzlich verwenden wir für alle Web-Anwendungen das sichere https-Protokoll und weitere Sicherheitsmechanismen. Alle Wurm-Gateways sind durch entsprechende Vorkehrungen vor Passwort-Attacken (brutforce) geschützt.

Auf den Wurm-Servern sind sämtliche Daten sicher gespeichert. Die Server-Umgebung unterliegt regelmäßigen TÜV-Zertifizierungen.



SICHERE FERNÜBERTRAGUNG IHRER DATEN

Bei der Datenfernübertragung haben Gateways eine Schlüsselfunktion. Den verschiedenen Modellen in unserem Portfolio sind jeweils passende Sicherheitsmechanismen implementiert, die plattformunabhängig alle den gleichen Sicherheitsstandard garantieren.

Die Wirksamkeit unserer Schutzmaßnahmen wird regelmäßig von externen Sicherheitsexperten geprüft. Die strengen Anforderungen wurden stets von jedem Gerät erfüllt.

Alle Gateways werden pro Gewerk mit individuellem Passwort ausgeliefert, das ausschließlich die zuständige Servicefirma erhält. Bei einem Service-Partner-Wechsel ändert Wurm die Passwörter. Geschlossene Ports auf unseren Gateways und VPN-Routern sorgen zudem für möglichst wenig Angriffsfläche für Hacker.

Die Konfiguration des Email-Clients im jeweiligen Gateway ist nur für den Versand von Störmeldungen ausgelegt. Damit ist der Empfang von Schad-Emails mit Malware oder Spähsoftware vom Ansatz her ausgeschlossen.