



ConnectedCooking HMP

Inhaltsverzeichnis

1 Informationen zur Datensicherheit	4
2 Informationen zur Datenübertragung	6
3 Verwendung eines Proxy-Servers.....	8
4 Zugriff durch ConnectedCooking-Benutzer	9
5 Verbindung von ConnectedCooking Hygiene-Management Pro Sensoren	10
6 ConnectedCooking Support	11
7 Netzwerkvoraussetzungen - ConnectedCooking Hygiene Management Pro	12

1 Informationen zur Datensicherheit

Zur Datensicherheit zählen technische und organisatorische Maßnahmen, die dem Schutz der Daten vor unbefugtem Zugriff und somit auch einer Kenntnisnahme, Manipulation oder Entfernung der Daten dienen. Dabei stehen Vertraulichkeit, Integrität und Verfügbarkeit im Fokus.

Vertraulichkeit bedeutet, dass der Zugriff auf die Daten nur von befugten Personen vorgenommen werden kann. Wichtig für die Datensicherheit ist auch die Integrität, die für die Unversehrtheit der Daten, sowohl vor Manipulation als auch vor technischen Defekten steht.

Die Vertraulichkeit und Integrität der Daten wird durch Kontrollmechanismen sichergestellt, die einen unbefugten Zugriff und somit auch eine Kenntnisnahme, Manipulation oder Entfernung der Daten verhindern:

a. Zutrittskontrollen

- Physischer Zutritt zum Rechenzentrum beschränkt
- Serverräume nur für befugtes Personal zugänglich
- Zutritt zu Räumen beschränkt, in denen Datenmaterial verwahrt wird

b. Zugriffskontrollen

- Trennung von Aufgaben / Rollen / Verantwortlichkeiten
- Zugriff auf interne Dienste für Server-Administratoren nur über dedizierte VPN möglich
- Konzept für Zugriffsberechtigungen mit unterschiedlichen Zugriffsrechten zu Daten und Funktionalitäten

c. Zugangskontrollen

- Benutzerauthentifizierung erfolgt über Username und Passwort
- Richtlinien für die Gestaltung von Passwörtern
- Gehärtete Serversysteme
- Regelmäßige Installation aktueller Sicherheitsupdates
- Regelmäßige Penetration Tests

d. Weitergabekontrollen

- Umfangreiche Verschlüsselung
Daten werden in der Datenbank verschlüsselt hinterlegt
Alle Passwörter werden über eine Hashfunktion verschlüsselt gespeichert
Sämtliche Datenübertragungen erfolgen verschlüsselt
- Regelmäßige Wartung und Prüfung der Systeme

e. Eingabekontrollen

- Der Zugriff auf die Anwendung wird immer protokolliert

f. Verfügbarkeitskontrollen

- Daten gegen unbeabsichtigte Löschung oder Vernichtung für 6 Monate abgesichert durch regelmäßige Sicherungskopien
- g. Trennung von Daten unterschiedlicher Zwecke
- Schichtenarchitektur getrennt in Darstellung, Geschäftsabwicklung und Speicherung
 - Datenbankserver sind logisch und physikalisch getrennt und nicht Teil der DMZ
 - Verbindungen zwischen verschiedenen Systemen wie Web- (Internet), Anwendungs- und Datenbankservern werden durch Firewalls mit einer Stateful Firewall geschützt.

Schließlich bedeutet Verfügbarkeit, dass vorhandene Daten im Bedarfsfall auch verwendet werden können. Hohe Verfügbarkeit wird sichergestellt durch den redundanten Aufbau aller Netzwerk- und Serversysteme mit Lastverteilung.

2 Informationen zur Datenübertragung

RATIONAL-Kochsysteme werden mittels Netzwerkkabel oder dem WLAN mit dem Internet verbunden, siehe Konnektivitätsoptionen in Abbildung 1 unten. Die so mit dem Internet verbundenen Kochsysteme stellen anschließend über das Internet eine Verbindung mit den ConnectedCooking-Servern her. Die für die jeweiligen Geräte relevanten Ports sind in der Tabelle zu den Kommunikationsports dargelegt.

Wenn möglich, stellen Sie ein separates Netzwerk für den Küchenbereich zur Verfügung, das physisch oder logisch vom sonstigen Firmennetzwerk getrennt ist, z. B. durch ein VLAN.

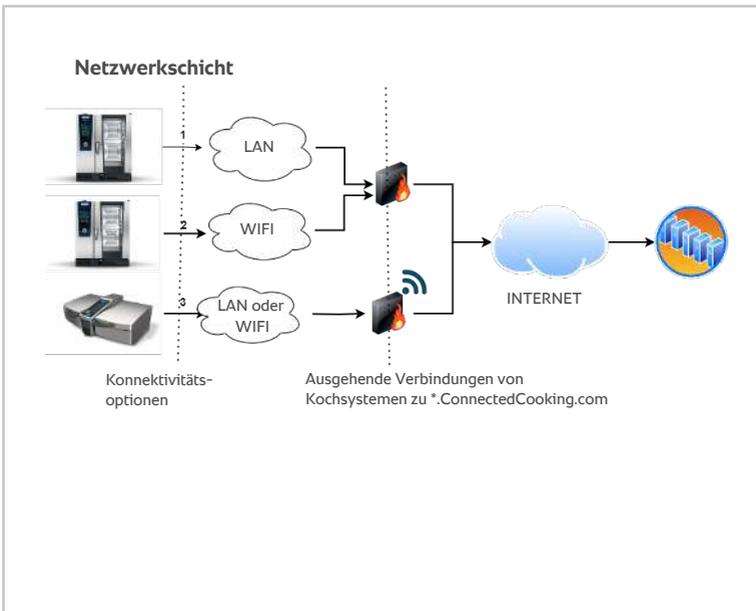


Abb. 1: Netzwerkschicht

Alle Verbindungen sind mittels TLS 1.2 verschlüsselt, sodass die übertragenen Daten nicht von Dritten gelesen werden können.

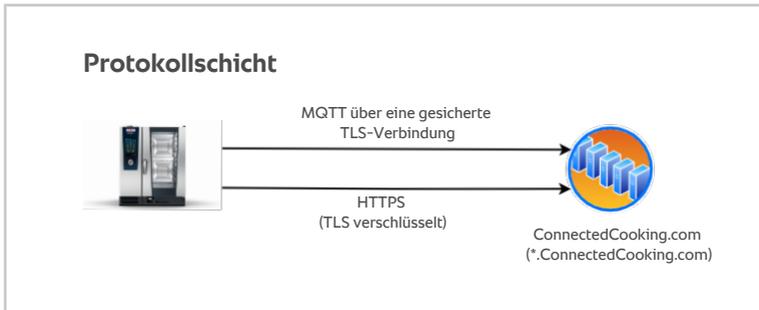


Abb. 2: Protokollschicht

Das Pairing der Geräte, sowie die anschließende Kommunikation erfolgen ausschließlich verschlüsselt.

3 Verwendung eines Proxy-Servers

RATIONAL-Kochsysteme können eine Verbindung über einen Proxy-Server herstellen. Bitte beachten Sie dabei, dass wir das Login via Standardmechanismen am Proxy-Server ermöglichen. Die Kommunikation darf dabei nicht gelesen werden (TLS-Inspektion).

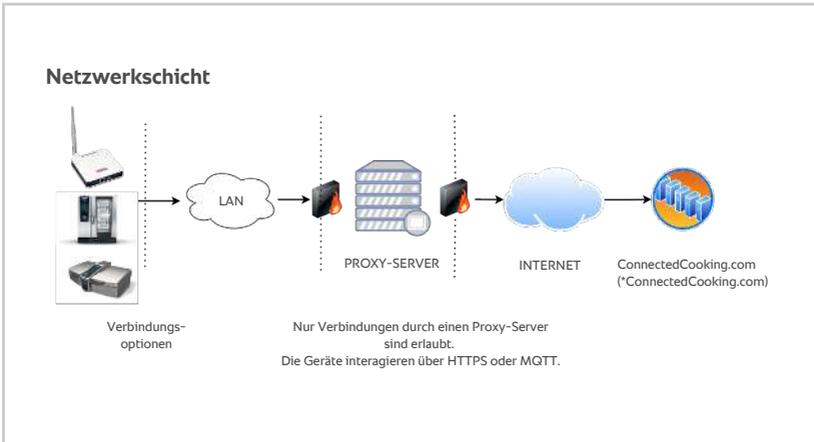


Abb. 3: Verwendung eines Proxy-Servers

- Eine Ausnahmeregel für eine MQTT-Verbindungen erforderlich, um die Verbindung durch den Proxy Server zu ermöglichen, siehe Tabelle 1: Kommunikations-Ports.
- RATIONAL nutzt ein selbstsigniertes TLS-Zertifikat, um die Verbindungen zu verschlüsseln.
- Das Gerät kann keine Verbindung herstellen, wenn eine TLS- oder SSL-Inspektion zwischen dem ConnectedCooking-Server und dem Gerät erfolgt.

4 Zugriff durch ConnectedCooking-Benutzer

ConnectedCooking-Benutzer greifen mit einem Desktopcomputer über den installierten Browser oder mit einem Smartphone oder Tablet via App über das Internet auf ConnectedCooking zu.

Der Client (App oder Browser) baut dazu ausgehende HTTPS-Verbindungen mit den ConnectedCooking-Servern auf und verwendet *.connectedcooking.com Port 443 (HTTPS).

Alle Verbindungen sind durch TLS-Version 1.2 oder höher verschlüsselt. Die ConnectedCooking-Server unterstützen ausschließlich Verbindungen mit TLS 1.2 oder höher. Unsichere Cipher Suites sind deaktiviert.

5 Verbindung von ConnectedCooking Hygiene-Management Pro Sensoren

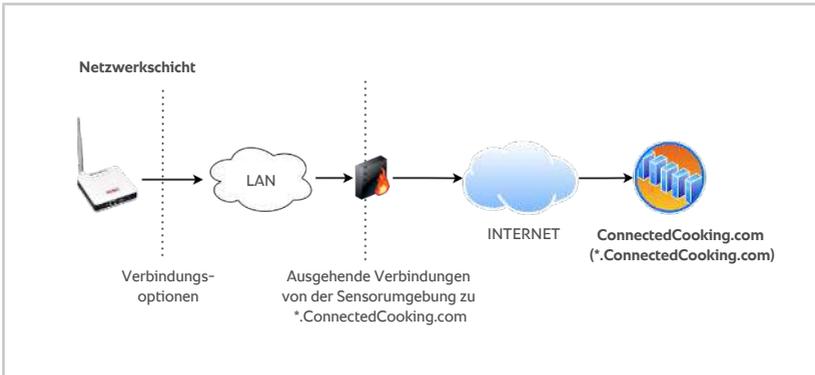


Abb. 4: Vernetzung von Sensoren für ConnectedCooking Hygiene-Management Pro

Bei der Nutzung des ConnectedCooking Hygiene-Management Pro Sensornetzwerks wird ein LoRa WAN Gateway mit dem Internet verbunden.

Die Datenübertragung zwischen den Sensoren und dem LoRaWAN Gateway erfolgt über das ISM-Band, 868 MHz (ITU-Region 1) oder 915 MHz (ITU-Region 2), wie in Tabelle 3: LoRa-Frequenzen dargestellt.

Das LoRaWAN Gateway bezieht eine IP-Adresse aus dem lokalen Netzwerk über DHCP.

Das LoRaWAN Gateway baut eine verschlüsselte Verbindung zu den Servern des ConnectedCooking-Systems auf und übermittelt regelmäßig die Sensordaten an diese, siehe Tabelle Kommunikationsports. Alle Verbindungen werden ausschließlich von innen nach außen ("outbound") aufgebaut.

Stellen Sie sicher, dass Ihre Firewall richtig konfiguriert ist, um die Übertragung der Sensordaten zur Cloud zu ermöglichen. Alle Verbindungen werden mit TLS verschlüsselt, so dass die übertragenen Daten nicht von Dritten mitgelesen werden können.

Die von den Sensoren gesammelten Daten werden alle 20 Minuten über das LoRaWAN Gateway zu den ConnectedCooking-Servern übertragen.

6 ConnectedCooking Support

Die Kontaktinformationen für den ConnectedCooking Support sowie ausführliche Dokumentationen stehen in ConnectedCooking unter dem Menüpunkt Support zur Verfügung.

7 Netzwerkvoraussetzungen - ConnectedCooking Hygiene Management Pro

Voraussetzungen für eine erfolgreiche Einbindung des RATIONAL-Geräts in Ihr Netzwerk:

- Das Gerät ist mit einem Netzwerk-Anschluss ausgestattet oder
- Das Gerät hat eine interne Wi-Fi Schnittstelle (z.B. iCombi Pro, iVario Pro oder die zusätzliche Wi-Fi-Option für das iCombi Classic Gerät) oder
- Die Option Wi-Fi Adapter (RATIONAL 60.76.714) ist installiert.
- Das Gerät zeigt das aktuelle Datum sowie Uhrzeit an.
- Das Gerät ist mit der aktuellen Software-Version ausgestattet, siehe Tabelle 2.

Der Anschluss des Geräts an das Internet erfolgt durch:

- LAN: Netzwerkanschlussdose mit Kabel in der Nähe des Gerätes. Gegebenenfalls ist die Nachrüstung älterer Gerätemodelle mit Ethernet-Anschluss erforderlich.
- Wi-Fi (802.11b/g/n 2.4 GHz, WPA2): Guter Empfang am Aufstellort über interne oder externe Wi-Fi-Schnittstelle.

Die Vernetzung des Geräts wird wie folgt durchgeführt:

- LAN: Ein RJ45-Kabel verbindet das RATIONAL Gerät mit einem nahegelegenen Netzwerkanschluss.
- Wi-Fi: Eine eingebaute oder externe Wi-Fi Schnittstelle (z.B. Artikel Nr. 60.76.714, Artikel Nr. 60.76.603), die die Verbindung zu einem WiFi 802.11b/g/n (2.4 GHz) Access Point herstellen.
- Alle Netzkomponenten müssen entsprechend den Umgebungsbedingungen spritz- und strahlwassergeschützt installiert werden.

ConnectedCooking Anwendung:

Um auf ConnectedCooking zuzugreifen, ist nur ein Internet-Browser notwendig (Chrome, Firefox, MS Edge in der aktuellen Version) sowie Zugriff auf *connectedcooking.com über Port 443 erforderlich. ConnectedCooking installiert keine Programme auf Ihrem Computer.

Gerät	Ziel	Proto- koll	Port	Richtung	Beschrei- bung
SelfCoo- kingCenter, VarioCoo- kingCenter iCombi Pro, iVario Pro	*.connectedcoo- king.com	TCP	443	Out- bound	HACCP Da- ta; Device Da- ta, wenn Proxy-Ser- ver
SelfCoo- kingCenter, VarioCoo- kingCenter iCombi Pro, iVario Pro	*.connectedcoo- king.com	TCP	8883	Out- bound	Device Da- ta
SelfCoo- kingCenter, VarioCoo- kingCenter iCombi Pro, iVario Pro	Customer DNS-Server	TCP/ UDP	53	Out- bound	DNS-Ser- vice
SelfCoo- kingCenter, VarioCoo- kingCenter iCombi Pro, iVario Pro	Customer DHCP-Server	UDP	68	Broad- cast	DHCP-Ser- vice
iCombiC- lassic	*.connectedcoo- king.com	TCP	8443	Out- bound	HACCP Da- ta, Device Da- ta, wenn Proxy-Ser- ver
iCombiC- lassic	*.connectedcoo- king.com	TCP	8884	Out- bound	Device Da- ta
iCombiC- lassic	Customer DNS-Server	TCP/ UDP	53	Out- bound	DNS Ser- vice
WGT-11	*.connectedcoo- king.com	TCP	8883	Out- bound	MQTT
WGT-10	*.connectedcoo- king.com	UDP	1800/18 01/1802	Out- bound	Semtech UDP
WGT-10 WGT-11	0.pool.ubuntu.com	UDP/ TCP	123	Out- bound	Zeit server
WGT-10 WGT-11	1.1.1.1	ICMP	Ping	Out- bound	Internet Check

Gerät	Ziel	Protokoll	Port	Richtung	Beschreibung
WGT-10 WGT-11	*.connectedcooking.com	TCP	443	Out-bound	ConnectedCooking
SenseAnywhere	8.8.8.8	TCP/ UDP	53	Out-bound	DNS-Service
SenseAnywhere	a.sa1.nl	TCP	80	Out-bound	Device Data

Tab. 1: Kommunikations-Ports

Gerät	Min. erforderliche Version	Verfügbarkeit
SelfCookingCenter	SCC_07-00-10-6.34 oder höher	Juni 2022
VarioCookingCenter	VCC-01-02-04.7 oder höher	Juni 2022
iCombi Pro	LM100-16.2.25 oder höher	Juni 2022
iCombi Classic	LM200-8.0.0 oder höher	Juni 2022
iVario Pro	LMX-2.10.0 oder höher	Juni 2022

Tab. 2: Software-Versionen

Region	Frequenz (MHz)
EU	863-870
US	902-928
AU	915-928
CN	779-787, 470-510

Tab. 3: LoRa-Frequenzen

