# Shodan-Lage Wasser und Abwasser DACH, Stand 02.11.2026

Stand: 02.11.2026. Öffentliche Fassung. Nur aggregierte Zahlen, keine Adressen oder Betreiber. Rückfragen und Interviews: Max Gilg, OT-Cyber.de. Erstellt von OT-Cyber.de, Rosenheim. Datenbasis: Shodan-API (host/count mit Facetten, Detaillauf 18:04 bis 18:50 Uhr, Gegenprobe ab 19 Uhr), keine eigenen Scans, keine Logins, keine Abfragen einzelner Hosts. Nur aggregierte Zahlen. Zählweise „Dienste“: ein von Shodan erfasster Port eines Hosts, ein Gerät kann mehrere Dienste haben. Danfoss-Angaben stammen aus unserem Vorfall-Lagebild (Stände 12.10. bis 26.10.2026) und den dort verlinkten Quellen.

## Kernaussage

Die Wasserwirtschaft in DACH ist im Internet weniger sichtbar als Gebäude- oder Energietechnik, aber sie ist erreichbar. „Die Schwachstelle der Branche sind die vielen Außenstationen. Jede Station mit Mobilfunkrouter ist ein möglicher Zugang, und viele wurden seit den 2010er-Jahren kaum angefasst. Fernwirkgeräte gehören hinter VPN oder ein privates APN, nie direkt ins Internet“, sagt Max Gilg, OT-Cybersecurity-Experte aus Rosenheim. Belastbar zuordnen lassen sich am 02.11.2026 77 Dienste, alle aus Fernwirk- und Leittechnik eines Fernwirk-Nischenherstellers aus Bayern (im Folgenden Hersteller A): 48 in Österreich, 29 in Deutschland, 19 davon in Bayern. Dazu kommen Spuren der übrigen Branchentechnik: FlowChief-Leitsysteme (15, unsicher), einzelne Leitsysteme von Rittmeyer und Siemens, Dosiertechnik von ProMinent (42, unsicher) und 73 Webseiten mit Branchenwörtern wie Wasserwerk, Brunnen, Kläranlage oder Zweckverband (DE 62, AT unter 5, CH 9). Einige dieser Webtitel sitzen auf Routern, deren Titel den Namen der Anlage nennt. Das zeigt den typischen Weg in der Branche: Die Außenstation hängt über einen Router im Netz, und der ist von außen ansprechbar.

Der größte Teil liegt in der Kategorie „Branche unklar“: rund 670 Fernwartungsrouter (Phoenix TC Router, mGuard, WAGO, mbCONNECT24, Teltonika), 1.479 Modbus- und 278 S7-Dienste ohne Anmeldung, 92 VNC-Zugänge ohne Passwort. Genau diese Gerätearten stehen in Pumpwerken, Hochbehältern und Kläranlagen (Einschätzung, gestützt auf Herstellerangaben und die Advisories in Abschnitt 6). Wie viele davon Wasseranlagen sind, lässt sich mit Shodan nicht bestimmen.

Der Angriff auf Danfoss-Kühlsteuerungen in Frankreich (11./12.10.2026, rund 700 Supermärkte laut französischer Regierung) zeigt, was mit dieser Art Erreichbarkeit passiert: Angreifer haben aus dem Internet erreichbare Steuerungen mit veralteter Firmware massenhaft angesprochen und Sollwerte verstellt. Dasselbe Muster ist bei Wasseranlagen in den USA, Polen und Norwegen schon belegt. Für DACH ist ein Eingriff in eine Wasser- oder Abwassersteuerung öffentlich nicht belegt (Recherche 02.11.2026).

Gesamtrisiko nach unserer Einschätzung: mittel, mit steigender Tendenz durch die Danfoss-Wellen (zweite Welle laut Medien am 02.11.2026 in sieben europäischen Ländern). Hoch für einzelne Leitsystemserver von Hersteller A mit offenem RDP auf demselben Host und für VNC ohne Passwort mit sichtbarem Anlagenbild (8, Branche unklar).

Einordnung nach Belastbarkeit:

- Belastbar: Hersteller A 77 Dienste (Zertifikat, Gegenprobe), darunter einzelne Leitsystemserver mit offenem RDP.
- Unsicher: FlowChief 15, ProMinent 42, Webtitel mit Branchenwort 73, dazu Einzeltreffer weiterer Leit- und Messtechnik (Rittmeyer, Siemens WinCC OA, Stebatec, IDS, Endress+Hauser). Sielaff (134) steht formal bei unsicher, gehört aber wahrscheinlich nicht zur Wasserwirtschaft (Rücknahmeautomaten, siehe Abschnitt 5).

- Branche unklar: Fernwartungsrouter, Modbus, S7, IEC 104, DNP3, VNC, OPC UA (Rohwerte, gelten identisch im Report „Heizen und Strom“).
- Ohne Treffer oder Fremdtreffer: Lacroix Sofrel, Ovarro TBox, Siemens SINAUT (Text), Siemens TeleControl Server Basic, COPA-DATA zenon, UFT, Piciorgros (Abschnitt 13).

### Gesamtzahlen im Ländervergleich

Gleiche Kennzahlen für alle drei Länder. Belastbar = nach Gegenprobe und Abzug von Hostern, Herstellerfirma und Honeypots. „Branche unklar“ = Rohwerte ohne Abzug, nicht in den Summen.

| Kennzahl | Deutschland | Österreich | Schweiz |
|---|---|---|---|
| Wasser/Abwasser belastbar (Hersteller A) | 29 | 48 | 0 |
| Wasser/Abwasser wahrscheinlich | 56 | 75 | 5 |
| je Mio. Einwohner | 0,3 | 5,2 | 0 |
| davon Leitsystem mit RDP | einzelne | 0 | 0 |
| Region | Bayern 19 | Salzburg unter 5, Tirol 0 | nicht erhoben |
| unsicher: Leit-, Fernwirk-, Dosiertechnik | 27 | 27 | 5 |
| unsicher: Webtitel mit Branchenwort | 62 | unter 5 | 9 |
| unsicher: Sielaff (wohl branchenfremd) | 109 | 25 | 0 |
| Branche unklar: Modbus/TCP | 1.197 | 123 | 159 |
| Branche unklar: Siemens S7 | 206 | 69 | unter 5 |
| Branche unklar: IEC 60870-5-104 | 21 | 0 | unter 5 |
| Branche unklar: DNP3 | 23 | unter 5 | 11 |
| Branche unklar: VNC ohne Passwort | 86 | unter 5 | unter 5 |
| Branche unklar: Fernwartungsrouter | 591 | 28 | 51 |

Hinweise zur Tabelle:

- „Wahrscheinlich“ = belastbar plus unsicher (Leit-, Fernwirk- und Dosiertechnik): Deutschland 29 + 27, Österreich 48 + 27, Schweiz 0 + 5. Nicht enthalten sind die Webtitel mit Branchenwort und Sielaff (wohl branchenfremd). Unsichere Werte sind nicht am Gerät geprüft.
- Einwohner gerundet: Deutschland 83,6 Mio., Österreich 9,2 Mio., Schweiz 9,0 Mio.
- Leit-, Fernwirk-, Dosiertechnik unsicher: ProMinent (DE 11, AT 26, CH 5), FlowChief (DE 15), dazu Einzeltreffer weiterer Hersteller.
- Webtitel je Land nach Abzug der Hoster. Deutschland: Wasserwerk 11, Brunnen 11, Wasserversorgung 10, Zweckverband 10, Kläranlage 9, übrige Begriffe zusammen 11. Österreich: Einzeltreffer. Schweiz: Wasserversorgung 6, übrige Einzeltreffer. Überschneidungen möglich, Branche je Seite nicht geprüft. Ein Teil sind normale Webseiten von Verbänden, nicht Anlagen.
- Fernwartungsrouter = Phoenix TC Router, Phoenix mGuard, WAGO Web-Based Management, mbCONNECT24, Teltonika (Rohwerte).
- Österreich hat je Einwohner rund 15 Mal so viele belastbare Wasser-Dienste wie Deutschland, fast alles Fernwirkgeräte von Hersteller A im Mobilfunk.

## 1. Was dahinter steht: Anlagen, Betreiber, Außenstation

Betreiber sind vor allem Gemeinden, Zweckverbände, Wasser- und Abwasserverbände und Stadtwerke. In Deutschland liegen nur große Versorger über der KRITIS-Schwelle (22 Mio. m³ pro Jahr, BSI-KritisV). Die Masse sind kleine Betreiber mit vielen Außenstationen, wenig eigenem Personal und einem Integrator, der per Fernwartung betreut (Einschätzung aus Branchenpraxis).

Typische Außenstation (Brunnen, Hochbehälter, Pumpwerk, Regenüberlaufbecken):

- SPS (häufig Siemens S7, WAGO, Phoenix Contact, Schneider) steuert Pumpen, Schieber und Füllstände.
- Fernwirkstation (Hersteller A, Rittmeyer, Sofrel, Ovarro TBox, Siemens SINAUT/TeleControl, UFT, Piciorgros) meldet über Mobilfunk, DSL oder Funk an die Leitstelle. Protokolle: IEC 60870-5-104, Modbus TCP, DNP3, OPC UA (Herstellerangaben, siehe Abschnitt 4).
- Industrierouter für die Fernwartung des Integrators (Ewon, mbCONNECT24, Teltonika, Phoenix TC Router und mGuard, INSYS, Welotec, LANCOM).
- Vor Ort häufig ein Bedienpanel (HMI), teils mit Web- oder VNC-Server.

Kläranlage und Wasserwerk:

- Leitsystem (Hersteller A, RITOP, FlowChief, zenon, WinCC OA) auf einem Windows-Server, Bedienung oft per RDP.
- Mess- und Dosiertechnik (ProMinent, Endress+Hauser, Hach): Chlor, Flockungsmittel, pH, Sauerstoff im Belebungsbecken.
- Alarmierung per SMS, SIP oder App an die Rufbereitschaft (z. B. FCPhone bei FlowChief, Tixi-Modems im Altbestand).

Die Schwachstelle der Branche ist nach unserer Einschätzung nicht das einzelne Produkt, sondern die Summe der Außenstationen: Jede Station mit Mobilfunkrouter ist ein möglicher Zugang, und viele wurden in den 2010er-Jahren eingerichtet und seither selten angefasst.

# 2. Angriffsvektor: von Danfoss Frankreich zur Wasserwirtschaft

## 2.1 Was in Frankreich passiert ist (belegt)

- Nacht vom 11. auf den 12.10.2026: Angreifer haben per Fernzugriff Kühlsteuerungen in Supermärkten verstellt, die Abtauung dauerhaft ausgelöst und Sollwerte auf bis zu 50 °C gesetzt. Zwei französische Handelsgruppen haben den Angriff bestätigt, eine davon ordnet ihn dem Zulieferer Danfoss zu (franceinfo, 12.10.2026).
- Umfang: Die französische Regierung nannte am 13.10. rund 700 betroffene Supermärkte von etwa 10.000 (AP, complexdiscovery). Die Märkte mussten Ware entsorgen, laut Staatsanwaltschaft Paris kam es teils zu Bränden.
- Geräte: Danfoss nennt vor allem Altgeräte ohne Sicherheitsupdates, AK-SM 800 (End-of-Life seit 2021) und AK-SC 355 (abgekündigt 2016), dazu AK-SM 800A mit veralteter Firmware (Cooling Post; Reuters über The Hacker News, 13.10.2026).
- CERT-FR (ANSSI), Alert CERTFR-2026-ALE-012 vom 12.10.2026, ergänzt am 13.10. (Copeland xweb, Dixell xweb) und am 16.10. (Empfehlungen): „zahlreiche Kompromittierungen“ von Fernsteuerungen für Kälteanlagen. Eine Management-Oberfläche offen ins Internet zu stellen, widerspricht laut CERT-FR bewährter Praxis. CERT-FR hält die Kampagne für vermutlich noch aktiv.
- Sichtbarkeit: Reuters fand am 13.10. per Shodan mindestens 4.500 öffentlich sichtbare Danfoss-Weboberflächen. LeMagIT fand am 12.10. in Frankreich fast 3.000 erreichbare Weboberflächen, viele zuletzt zwischen 2021 und 2024 geändert. Forescout zählte fast 6.000 offene Kühlsteuerungen in 99 Ländern (Borns IT-Blog, 26.10.2026).
- Schwachstellen: Claroty Team82 hat am 09.08.2026 drei Lücken im AK-SM 800A veröffentlicht (CVE-2025-41450 Umgehung der Authentifizierung, CVE-2025-41451, CVE-2025-41452), behoben ab Firmware R4.3.1. Ob sie beim Angriff genutzt wurden, ist nicht belegt.
- Deutschland: BSI-Warnung BSI-CS 154 vom 13.10.2026 an Betreiber kleiner Anlagen (Kühlung, Energieerzeugung), Warnung vor Nachahmern. Ein bestätigter Fall in Deutschland wird nicht genannt.

- Zweite Welle: In der Nacht zum 02.11.2026 wurden laut Medienberichten (u. a. ERR) in mehr als 115 Supermärkten und Fachgeschäften in sieben Ländern (Belgien, Schweden, Luxemburg, Niederlande, Irland, Estland, Finnland) Kühlschränke aus der Ferne in den Abtaumodus geschaltet. Behördlich nicht bestätigt (Nachtrag Vorfall-Lagebild, Stand 02.11.2026).
- Offen: Täter, Motiv und genauer Angriffsweg sind offiziell nicht geklärt (Stand 26.10.2026).

## 2.2 Ablauf des Angriffs (aus den Belegen abgeleitet)

- Schritt 1, Finden: Die Weboberflächen waren über Internet-Suchmaschinen sichtbar (Reuters per Shodan, 13.10.). Dass die Angreifer selbst so gesucht haben, ist nicht belegt, aber naheliegend (Einschätzung).
- Schritt 2, Zugang: Direkt erreichbare Management-Oberflächen (CERT-FR), Altgeräte ohne Updates und AK-SM 800A mit veralteter Firmware (Danfoss). Laut Lagebild wurden die Steuerungen einzeln und massenhaft angesprochen, nicht über eine zentrale Plattform oder einen Dienstleister.
- Schritt 3, Eingriff: Sollwert der Kühlstellen bis 50 °C, Dauer-Abtauung.
- Schritt 4, Wirkung: Ware verdorben, teils Brände, Schaden bei hunderten Betreibern gleichzeitig. Claroty hatte schon im August gezeigt, dass ein kompromittierter Controller normale Temperaturen anzeigen kann, während die Kühlung aus ist.

## 2.3 Derselbe Weg in Wasser und Abwasser

Schritt für Schritt, Einschätzung mit Belegen aus der Branche:

- Schritt 1, Finden: Wer nach Leitsystemnamen, FlowChief, WinCC OA, Phoenix TC Router oder nach Titeln wie „Wasserwerk“ sucht, findet in DACH dieselbe Art Liste wie bei Danfoss. Unsere Zählung: 77 belastbare Wasser-Dienste, 73 Webtitel mit Branchenwort, rund 670 Fernwartungsrouter (Branche unklar).
- Schritt 2, Zugang Fernwirkstation oder HMI im Mobilfunk: 48 Geräte von Hersteller A in Österreich sind direkt erreichbar, geschützt nur durch die Web-Anmeldung (HTTP 401). Bei schwachen oder Standardpasswörtern ist das der Danfoss-Weg.
- Schritt 3, Zugang Weboberfläche oder VNC am HMI: 86 VNC-Dienste ohne Passwort in Deutschland, davon 8 mit sichtbarem Anlagenbild. Genau dieser Weg ist bei Wasseranlagen belegt: CISA, NSA und FBI beschreiben im Fact Sheet vom 01.05.2024 den Einstieg pro-russischer Hacktivisten über VNC und HMIs mit Standardpasswort; das gemeinsame Advisory vom 09.12.2025 (CARR, Z-Pentest, NoName057(16), Sector16) nennt VNC als Einstieg.
- Schritt 4, Zugang Leitsystem per RDP: Einzelne Leitsystemserver von Hersteller A haben RDP auf demselben Host offen. Wer hier per Credential Stuffing oder schwachem Passwort hineinkommt, bedient die ganze Kläranlage oder das Kanalnetz.
- Schritt 5, Zugang über den Fernwartungsrouter: Phoenix TC Router (DE 186), mGuard (DE 79), mbCONNECT24 (DE 75), Teltonika (davon 29 RUT955 mit Telnet). Für mehrere gibt es Advisories (Abschnitt 6). Hinter dem Router liegt meist ein flaches Anlagennetz.
- Schritt 6, Eingriff per Protokoll: Modbus/TCP (1.479 DACH) und S7 (278 DACH) kennen keine Anmeldung. Ein Schreibbefehl ändert Sollwerte, Pumpen-Freigaben oder Grenzwerte. In Aliquippa (11/2023) wurde eine Unitronics-SPS mit Standardpasswort übernommen, in Polen (2025) laut ABW fünf Wasseraufbereitungsanlagen über offene Weboberflächen mit schwachen Passwörtern.

- Schritt 7, Wirkung: wie bei Danfoss viele kleine Betreiber gleichzeitig, aber mit anderer Folge: kein Warenverlust, sondern Versorgungsunterbrechung oder Gewässerschaden (Abschnitt 3).

| Merkmal | Danfoss Frankreich | Wasser DACH |
|---|---|---|
| Zielgeräte | Kühlsteuerungen AK-SM, AK-SC | Fernwirkstationen, HMI, Leitsystem |
| Sichtbar im Internet | mind. 4.500 (Reuters) | 77 belastbar, rund 670 Router unklar |
| Firmware | Altgeräte ohne Updates | nicht geprüft, Router teils alt |
| Anmeldung | Weboberfläche, teils umgehbar | Web 401, RDP, VNC teils ohne |
| Eingriff | Sollwert 50 °C, Abtauung | Pumpe, Füllstand, Dosierung |
| Betreiber | Hunderte Märkte, ein Hersteller | Hunderte Kommunen, viele Hersteller |
| Schaden | Ware, Brände | Versorgung, Gewässer, Gesundheit |
| Belegter Fall DACH | keiner bestätigt (BSI) | keiner öffentlich belegt |

Erläuterungen:

- Unterschied 1: Danfoss ist ein Hersteller mit einer gleichartigen Gerätefamilie. In der Wasserwirtschaft verteilt sich die Technik auf viele Hersteller. Eine einzige Welle über alle Anlagen ist deshalb unwahrscheinlicher (Einschätzung). Bei Hersteller A in Österreich (48 gleichartige Geräte) wäre eine Welle in kleinem Maßstab aber technisch denkbar.
- Unterschied 2: Wasseranlagen haben meist Sicherheitsabschaltungen, Schwimmerschalter und Handbetrieb. Das begrenzt den Schaden, wenn jemand rechtzeitig vor Ort ist. In Muleshoe lief ein Tank trotzdem 30 bis 45 Minuten über.
- Gemeinsam: Erreichbare Oberflächen, alte Firmware, kleine Betreiber ohne eigenes OT-Team, Integrator mit Fernzugang.
- Die Wasserwerte in der Tabelle sind Shodan-Zählungen vom 02.11.2026, die Danfoss-Werte stammen aus den genannten Quellen.

# 3. Schadensszenarien

Alle Szenarien sind Einschätzungen von OT-Cyber. Belege aus realen Fällen sind genannt, wo es sie gibt.

| Szenario | Einstieg | Folge | Eintritt (Einschätzung) |
|---|---|---|---|
| S1 Pumpwerk aus, Hochbehälter leer | Fernwirkgerät, HMI, Router | Druckabfall, Versorgung weg | möglich |
| S2 Hochbehälter läuft über | VNC/HMI, Modbus | Wasserverlust, Schäden vor Ort | möglich, belegt in USA |
| S3 Dosierung Chlor verstellt | Dosiertechnik, Leitsystem | Gesundheitsgefahr, Abkochgebot | selten, hohe Wirkung |
| S4 Kläranlage Belüftung aus | Leitsystem per RDP | Fischsterben, Grenzwerte überschritten | möglich |
| S5 Regenüberlaufbecken bei Starkregen | Fernwirk Kanalnetz | Abwasser ins Gewässer | selten, wetterabhängig |
| S6 Leitsystem verschlüsselt | RDP, IT-Netz | Blindflug, Handbetrieb Wochen | am wahrscheinlichsten |

Erläuterungen je Szenario:

- S1 Pumpwerk aus: Angreifer schaltet über Fernwirkstation oder HMI Förderpumpen ab oder setzt den Einschaltpegel herunter. Der Hochbehälter leert sich über Stunden, danach fällt der Druck im Ortsnetz. Folge: Ausfall der Versorgung für eine Gemeinde, Feuerwehr ohne Löschwasser, Verkeimungsrisiko beim Wiederbefüllen. Bis Handbetrieb: wenige Stunden, wenn Rufbereitschaft den

Alarm sieht. Gruppe: Hersteller A (77), Fernwartungsrouter, Modbus/S7. Beleg: Arkansas City (09/2024) musste auf Handbetrieb.

- S2 Hochbehälter läuft über: Ausschaltpegel verstellt oder Alarm unterdrückt. Folge: Wasserverlust, Ausspülungen, Schaden an der Anlage. Bis Handbetrieb: 30 bis 60 Minuten bis zur Entdeckung. Gruppe: VNC ohne Passwort (92), Modbus. Beleg: Muleshoe (01/2024), Tank lief 30 bis 45 Minuten über.
- S3 Dosierung: Sollwert für Chlor, Flockungsmittel oder pH verstellt. Folge: Gesundheitsgefahr oder Abkochgebot, Vertrauensverlust, Meldung an Gesundheitsamt. Messgeräte und Grenzwertalarme fangen das oft ab, deshalb eher selten, aber die Wirkung ist hoch. Gruppe: ProMinent (42, unsicher), Leitsysteme. Beleg: kein öffentlich belegter Fall, weder in DACH noch in den ausgewerteten Quellen.
- S4 Kläranlage Belüftung aus: Über das Leitsystem werden Gebläse im Belebungsbecken abgeschaltet. Nach einigen Stunden kippt die Biologie, ungeklärtes Abwasser geht in den Vorfluter. Folge: Fischsterben, Grenzwertüberschreitung, Ermittlungen gegen den Betreiber, Wochen bis die Biologie wieder stabil ist. Gruppe: Leitsystemserver von Hersteller A mit RDP (einzelne), FlowChief (15). Beleg: kein öffentlicher Fall in DACH.
- S5 Regenüberlaufbecken: Schieber oder Pumpen im Kanalnetz bei Starkregen verstellt. Folge: Abwasser fließt ungedrosselt in Bäche und Seen, gerade im Voralpenland mit Badeseen relevant. Gruppe: Fernwirktechnik von Hersteller A in Kanalnetzen, Fernwartungsrouter. Beleg: keiner, Einschätzung.
- S6 Leitsystem verschlüsselt: Ransomware über RDP oder aus dem IT-Netz legt den Leitsystemserver lahm. Die Anlage läuft lokal weiter, aber ohne Überblick. Folge: Handbetrieb mit Personal vor Ort, oft Wochen bis zur Wiederherstellung, Kosten für Incident Response. Nach unserer Einschätzung das wahrscheinlichste Szenario, weil es keine OT-Kenntnisse braucht. Gruppe: Leitsysteme mit RDP. Beleg: Bekannte Fälle bei deutschen Stadtwerken betrafen die IT (ZfK).

Zum Vergleich mit Danfoss: In Frankreich war der Schaden ein Warenverlust bei vielen Betreibern zur gleichen Zeit. In der Wasserwirtschaft würde dieselbe Methode (viele erreichbare Geräte nachts gleichzeitig verstellen) S1 und S2 in mehreren Gemeinden auslösen. Mit wenigen Rufbereitschaften pro Region wäre der Handbetrieb dann der Engpass (Einschätzung).

## 4. Herstellerlandkarte der Branche

| Hersteller | System | Einsatz |
|---|---|---|
| Hersteller A (Bayern) | dessen Leitsystem | Kläranlagen, Kanalnetze, Wasserversorgung |
| Rittmeyer (CH) | RITOP | Wasserversorgung in Gemeinden |
| Stebatec (CH) | ARAbella, AQUAbella | Kläranlagen, Wasserversorgung |
| FlowChief | Leitsystem, FCPhone | Wasserversorger |
| COPA-DATA (Salzburg) | zenon | Wasserversorgung |
| Lacroix Sofrel | SOFREL | Wasser, Abwasser |
| Ovarro | TBox | Fernwirk |
| UFT | Fernwirktechnik | Regenbecken, Pumpwerke |
| Piciorgros | Funk-Fernwirktechnik | Wasser, Gas, Fernwärme |
| Siemens | SINAUT, WinCC OA, TeleControl | Fernwirk Wasser/Abwasser |
| ProMinent | Dosier- und Messtechnik | Wasseraufbereitung |
| Tixi.Com | Alarm-Modems | Pumpwerke (Altbestand) |
| Fernzugang | Industrierouter | Fernwartung |

Anbindung und Quelle je Hersteller:

- Hersteller A: Modbus TCP, M-Bus, IEC 60870-5-104, OPC UA über DSL, Mobilfunk, LTE-M (Herstellerunterlagen, Fachpresse).

- Rittmeyer: Leitwarte und Fernwirk (Gemeindebeschlüsse 07/2024 und 11/2024).
- Stebatec: Anbindung nicht geprüft (aqua suisse).
- FlowChief: Web-Client, Alarmierung per SIP (flowchief.de).
- COPA-DATA zenon: Leitsystem, Referenzen bei österreichischen Wasserversorgern (Herstellerangaben).
- Lacroix Sofrel: Mobilfunk, IP (Broschüre DE 07/2025).
- Ovarro TBox: IP, OpenVPN (CISA ICSA-21-054-04, ICSA-23-180-03).
- UFT: Anbindung nicht geprüft (uft.eu). Piciorgros: Funk, IP (openPR).
- Siemens: IEC 104, DNP3, Mobilfunk (Siemens Anwenderbericht).
- ProMinent: Web, nicht geprüft (Herstellerangaben). Tixi.Com: Modbus, GSM (modbus.org).
- Fernzugang: Ewon, mbCONNECT24, Teltonika, Phoenix mGuard und TC Router, INSYS, Welotec, Tosibox, LANCOM.

## 5. Detailergebnis je Hersteller

Nicht 100 % sicher: Shodan erkennt Hersteller nur an Banner, Seitentitel oder Zertifikat. Die erste Spalte zeigt, wie sicher die Zuordnung ist. Belastbar heißt: ein zweites Merkmal bestätigt den Treffer. Unsicher heißt: nur ein Merkmal, Zuordnung nicht geprüft. Fremdtreffer heißt: überwiegend Hoster, Firmen-IT, Honeypots oder Namensgleiche, nicht gezählt. Belastbare Werte nach Abzug, alle anderen Rohwerte. Regionen immer ohne Abzug.

| Sicherheit | Hersteller | DE | AT | CH | Bayern | Salzburg | Tirol |
|---|---|---|---|---|---|---|---|
| belastbar | Hersteller A (Zertifikat) | 29 | 48 | 0 | 19 | unter 5 | 0 |
| unsicher | FlowChief | 15 | 0 | 0 | 6 | 0 | 0 |
| unsicher | ProMinent | 11 | 26 | 5 | 7 | 0 | 0 |
| unsicher | Stebatec ARAbella | unter 5 | 5 | 0 | unter 5 | 0 | 0 |
| unsicher | Webtitel mit Branchenwort | 62 | unter 5 | 9 | 14 | 0 | 0 |
| unsicher | Sielaff (wohl fremd) | 109 | 25 | 0 | 31 | 0 | 15 |

- Geprüft, aber nicht gezählt (überwiegend Hoster, Firmen-IT, Honeypots oder Namensgleiche): Inductive Automation Ignition, Ovarro TBox, KSB, ABB AC500, Wilo, Siemens SINAUT (Text), Tixi.Com, Kisters (KISTERS, WISKI), Krohne, Grundfos, NIVUS, Rittmeyer (Text).
- Geprüft, ohne erkennbaren Treffer auf Shodan: Lacroix Sofrel, COPA-DATA zenon, Siemens TeleControl Server, Rittmeyer RIFLEX, Dr. Riedel, UFT, Piciorgros, SEBA Hydrometrie, Unitronics (Produkt), Xylem/Flygt, Hach Claros.

Zugriffsart und Befund:

- Hersteller A Österreich: 46 mit 401 (Anmeldung), Apache.
- Hersteller A Deutschland: 50 roh, 29 nach Abzug. 44 ohne TLS, 30 mit 200, darunter Mail- und Webserver; ein Teil ist Firmen-IT (nicht geprüft).
- Leitsystemserver von Hersteller A: einzelne mit RDP auf demselben Host. Teilmenge der Zeile Hersteller A.
- Einzeltreffer (je unter 5 Dienste, unsicher): Rittmeyer RITOP (Anmeldung auf Nicht-Standardport), Siemens WinCC OA (BACnet ohne Anmeldung), IDS, Endress+Hauser.
- FlowChief: 16 roh, 15 gezählt. Web-Logon über IIS (teils alte Version 7.5), FCPhone (SIP) bei 7.
- ProMinent: 31 roh in DE, davon 20 bei Hostern, gezählt 11. Teils Zope httpd, 401 bei 9 Diensten.
- Stebatec ARAbella: Fremdanteil 56 %, Zuordnung nicht geprüft.
- Webtitel mit Branchenwort (Wasserversorgung 25, Brunnen 19, Zweckverband 18, Wasserwerk 13, Kläranlage 10, Abwasser 7, Wasserverband 5, übrige zusammen 6; DACH roh, Überschneidungen

möglich): fast alle ohne TLS und mit HTTP 200, einige auf Routern. Die Titel „Klärwerk“, „Regenbecken“ und „Trinkwasser“ sind Fremdtreffer.

- Sielaff: nur SSH (OpenSSH 7.2p2 bei 96, 8.9p1 bei 12). Laut Vorrecherche (02.11.2026) baut Sielaff Verkaufs- und Rücknahmeautomaten, das Banner „Sielaff RVM“ passt dazu. Wahrscheinlich nicht Wasserwirtschaft.
- Fremdtreffer: Ignition 100 % bei Hostern, KSB Fremdanteil 59 %, bei den übrigen überwiegend Namensgleiche oder Firmen-IT.
- Kein Treffer heißt nur: kein erkennbares Merkmal auf Shodan. Die Geräte können trotzdem hinter Routern oder im Mobilfunk erreichbar sein.
- Weitere Hersteller ohne eigene Abfragegruppe im Detaillauf (VEGA, Jung Pumpen, Huber, HIMA, INSYS, Welotec, SCALANCE M) hatten im Nischenlauf vom 02.11.2026 keine oder nur unsichere Treffer.
- VNC auf Hosts von Hersteller A: 0.

## 6. Branche unklar: Fernzugänge und generische Protokolle

Rohwerte, gelten identisch im Report „Heizen und Strom“, nicht in den Summen.

| Gruppe | DE | AT | CH | Bewertung |
|---|---|---|---|---|
| Phoenix Contact TC ROUTER | 186 | 11 | 10 | Produkt belastbar |
| WAGO Web-Based Management | 176 | 16 | 24 | Produkt belastbar |
| Phoenix Contact mGuard | 79 | 0 | 5 | Produkt belastbar |
| mbCONNECT24 | 75 | 0 | 0 | unsicher |
| Teltonika | 75 | unter 5 | 12 | unsicher |
| VNC ohne Passwort | 86 | unter 5 | unter 5 | unsicher |
| RDP mit ICS-Bild | unter 5 | unter 5 | 0 | unsicher |
| Modbus/TCP 502 | 1.197 | 123 | 159 | Branche unklar |
| Siemens S7 102 | 206 | 69 | unter 5 | Branche unklar |
| IEC 60870-5-104 2404 | 21 | 0 | unter 5 | Branche unklar |
| DNP3 20000 | 23 | unter 5 | 11 | Branche unklar |
| OPC UA 4840 | 42 | 5 | unter 5 | Branche unklar |
| CODESYS 2455 | 55 | 5 | 27 | Branche unklar |

Hinweise:

- Ewon (Text, 726 DACH) ist Fremdtreffer: 95 % Hoster oder Honeypot.
- Phoenix TC ROUTER: 49 in Bayern. mbCONNECT24: 15 in Bayern. mGuard: Fnord httpd 1.6 bei 39 Diensten.
- Teltonika: davon RUT955 mit Telnet 29 (DACH). VNC ohne Passwort: davon 8 mit ICS-Bild, alle in Deutschland.
- Modbus: zusätzlich 569 Dienste mit Honeypot-Markierung (DE 383, CH 185), ausgeschlossen. IEC 104: Fremdanteil 50 %.
- IEC 104 und DNP3 sind die klassischen Fernwirkprotokolle von Wasser- und Energieversorgern. Mit 22 bzw. 36 Diensten in DACH sind sie selten offen, was für VPN-Anbindung spricht (Einschätzung).
- Advisories mit Bezug: Siemens TeleControl Server Basic SQL Injection, CVSS 9,8, behoben ab V3.1.2.2 (SSA-443402, ICSA-25-112-01). Ovarro TBox ICSA-21-054-04, ICSA-23-180-03. Phoenix TC ROUTER Code Injection (WID-SEC-2026-0067, 01/2026). Phoenix mGuard VDE-2024-039, VDE-2024-052. mbNET VDE-2024-056, VDE-2024-068, VDE-2026-054. COPA-DATA zenon CD_SVA_2025_01.

- Zu Hersteller A, FlowChief, Rittmeyer und Stebatec wurde keine CVE gefunden (Suche 02.11.2026). Das heißt nicht, dass es keine Schwachstellen gibt.

## 7. Risikomatrix (gemessen an Angriffsvektor und Schadensszenario)

| Gruppe | DACH | Vektor | Szenario | Risiko (Einschätzung) |
|---|---|---|---|---|
| Leitsystem Hersteller A mit RDP | einzelne | RDP-Anmeldung | S4, S6 | hoch |
| VNC ohne Passwort mit ICS-Bild | 8 | keine Anmeldung | S1, S2 | hoch, Branche unklar |
| Modbus/S7 ohne Anmeldung | 1.479 / 278 | Schreibbefehl | S1, S2, S3 | hoch, Branche unklar |
| Fernwirkgeräte Hersteller A, AT | 48 | Web-Anmeldung (401) | S1, S5 | mittel |
| Hersteller A, DE | 29 | Web, teils ohne TLS | S1, S5 | mittel |
| FlowChief und weitere Leitsysteme | 17 | Web bzw. BACnet | S1, S6 | mittel |
| Fernwartungsrouter | rund 670 | Login, 29 Telnet | alle | mittel, Branche unklar |
| Webtitel Branchenwort | 73 | Web ohne TLS | S1 | niedrig bis mittel |
| ProMinent | 42 | Web, teils 401 | S3 | niedrig bis mittel |
| Sielaff | 134 | nur SSH | keins | niedrig |

Begründung:

- Hoch heißt: Danfoss-Muster direkt anwendbar (erreichbar, schwache oder keine Anmeldung, Eingriff in Sollwerte möglich) und Szenario mit Versorgungs- oder Umweltfolge.
- Mittel heißt: erreichbar, aber mit Anmeldung, Firmwarestand nicht geprüft. Bei schwachem Passwort wird daraus hoch.
- Die Leitsystemserver von Hersteller A sind die einzige belastbar der Wasserwirtschaft zugeordnete Gruppe mit hohem Risiko.

## 8. Belegte Vorfälle

| Datum | Ort | Vorfall |
|---|---|---|
| 25.11.2023 | Aliquippa (USA) | Unitronics-SPS übernommen |
| 01/2024 | Muleshoe (Texas) | Wassertank übergelaufen |
| 01.05.2024 | USA/global | Fact Sheet zu VNC und HMIs |
| 22.09.2024 | Arkansas City (Kansas) | Handbetrieb |
| 07.04.2025 | Bremanger (Norwegen) | Dammventil geöffnet |
| 2025 | Polen | 5 Wasseraufbereitungsanlagen |
| 09.12.2025 | global | Gemeinsames Advisory Hacktivisten |
| 2026 | USA | AA26-097A, Minnesota |
| 11./12.10.2026 | Frankreich | Danfoss-Kühlsteuerungen, rund 700 Märkte |
| 02.11.2026 | 7 EU-Länder | Zweite Kühlwelle (Medien) |

Was passiert ist und Quelle:

- Aliquippa: Unitronics-SPS einer Druckerhöhungsstation mit Standardpasswort übernommen, Handbetrieb (CBS News; CISA AA23-335A).
- Muleshoe: Wassertank lief 30 bis 45 Minuten über, Bekennung pro-russischer Hacktivisten (Texas Tribune, 19.04.2024).

- Fact Sheet 01.05.2024: Einstieg über VNC und HMIs mit Standardpasswort (CISA, NSA, FBI).
- Arkansas City: Wasseraufbereitung auf Handbetrieb, Ursache nicht bestätigt (SecurityWeek).
- Bremanger: Auslassventil eines Damms rund 4 Stunden offen (BleepingComputer; Security Affairs, PST 08/2025).
- Polen: Eingriff in 5 Wasseraufbereitungsanlagen über offene Weboberflächen mit schwachen Passwörtern (ABW-Bericht, veröffentlicht 06.05.2026, nur Presse gelesen).
- Advisory 09.12.2025: CARR, Z-Pentest, NoName057(16), Sector16, VNC als Einstieg (cyber.gov.au, CISA). Laut Bloomberg-Recherche (Nachtrag Vorfall-Lagebild, 10/2026) greifen CARR und Z-Pentest offen erreichbare Steuerungen in rund 20 NATO-Staaten an.
- AA26-097A: Angriffe auf SPS seit 03/2026, Ende 07/2026 über 30 Wassersysteme in Minnesota betroffen (Tenable Blog).
- Danfoss Frankreich und zweite Welle: siehe Abschnitt 2.1.
- DACH: Ein Eingriff in die Steuerung einer Wasser- oder Abwasseranlage ist öffentlich nicht belegt (Recherche 02.11.2026). Bekannte Fälle bei deutschen Stadtwerken betrafen die IT (ZfK).

# 9. Regionallage Bayern, Salzburg, Tirol

| Region | belastbar | unsicher | Branche unklar (Auswahl) |
|---|---|---|---|
| Bayern | 19 | 28 ohne Sielaff | TC Router 49, mbCONNECT24 15, mGuard 10 |
| Salzburg | unter 5 | unter 5 | TC Router 0, VNC 0 |
| Tirol | 0 | 15 Sielaff | TC Router und VNC je unter 5 |

- Bayern: 19 Dienste von Hersteller A, darunter einzelne Leitsystemserver mit RDP. Unsicher: 6 FlowChief, 7 ProMinent, 14 Webtitel mit Branchenwort (davon 8 „Brunnen“), dazu 31 Sielaff und Einzeltreffer. Ein Teil der Treffer kann Firmen-IT des Herstellers sein (nicht geprüft).
- Salzburg: einzelne Dienste von Hersteller A und ein unsicherer Einzeltreffer.
- Tirol: 0 belastbar, 15 Sielaff-Dienste (vermutlich Automaten). Herstellerreferenzen beschreiben IEC 104 bei Abwasserverbänden in der Region, auf Shodan ist das nicht erkennbar.
- Österreich gesamt: 48 Fernwirkgeräte von Hersteller A, überwiegend im Mobilfunk. Mobilfunkadressen landen oft am Sitz des Netzbetreibers, die echte Lage ist nicht geprüft.
- Einschätzung für die Grenzregion: Viele kleine Wasser- und Abwasserverbände, Fernwartung durch wenige regionale Integratoren. Ein kompromittierter Integrator-Zugang würde mehrere Gemeinden zugleich betreffen.

# 10. Empfehlungen nach SANS Five ICS Critical Controls

- CC1 ICS Incident Response: Handbetrieb für Pumpwerke, Hochbehälter und Kläranlagen festlegen und üben, mit Rufbereitschaft des Integrators. Szenario „viele Stationen gleichzeitig nachts“ (Danfoss-Muster) durchspielen: Wer fährt wohin, in welcher Reihenfolge? Aliquippa und Arkansas City zeigen, dass schnelles Umschalten auf Hand die Versorgung sichert.
- CC2 Defensible Architecture: Keine Leitsystemserver, SPS, HMIs oder Fernwirkgeräte direkt im Internet. Das ist die Kernlehre aus Frankreich: CERT-FR nennt offen erreichbare Management-Oberflächen als Verstoß gegen bewährte Praxis, Danfoss setzt mit Kunden auf das Ende der direkten Internetanbindung und besseren Netzwerkschutz. Fernwirkgeräte nur über VPN oder privates APN zur Leitstelle, Leitsystem- und IT-Netz trennen.
- CC3 ICS Network Visibility & Monitoring: RDP-Anmeldungen an Leitsystemservern, neue Verbindungen zur Leitstelle, schreibende Modbus-Befehle und Sollwertänderungen außerhalb der Dienstzeit überwachen. Claroty hat gezeigt, dass ein kompromittierter Controller Normalwerte anzeigen kann, deshalb unabhängige Messung (Schwimmerschalter, separater Druckmelder) beibehalten. Für KRITIS-Betreiber ist Angriffserkennung (SzA) Pflicht.

- CC4 Secure Remote Access: RDP an Leitsystemservern nur über VPN mit Mehrfaktor-Anmeldung. Standardpasswörter an Fernwirkgeräten und HMIs ändern (Danfoss, Aliquippa, Polen). Telnet an Teltonika-Routern abschalten, VNC nie ohne Passwort. Fernzugänge der Integratoren inventarisieren.
- CC5 Risk-Based Vulnerability Management: Zuerst erreichbare Systeme mit Advisory: TeleControl Server Basic ab V3.1.2.2, TC ROUTER nach WID-SEC-2026-0067, mGuard und mbNET nach den VDE-Advisories, alte IIS-Versionen ersetzen. Altgeräte ohne Updates wie bei Danfoss (AK-SM 800, AK-SC 355) gibt es auch in der Wasserwirtschaft (Tixi-Modems, alte Fernwirkstationen): ersetzen oder vom Internet trennen. Danfoss rät zu Firmware-Updates, wo es sie gibt.
- BSI-CS 154 (13.10.2026) richtet sich an Betreiber kleiner Anlagen und passt auch für kleine Wasserversorger. Die Empfehlungen des CERT-FR vom 16.10.2026 haben wir im Wortlaut nicht ausgewertet (nicht geprüft).

## 11. Regulatorischer Bezug

- NIS2 Deutschland: NIS2UmsuCG in Kraft seit 06.12.2025, Registrierung beim BSI bis 06.03.2026 (usd.de, secjur.com). Wasser und Abwasser sind erfasste Sektoren.
- KRITIS-Schwelle Wasser: 22 Mio. m³ pro Jahr, rund 500.000 versorgte Einwohner (BSI-KritisV, Anhang 2). Branchenstandard B3S Wasser/Abwasser (DWA-M 1060, DVGW W 1060, Edition 2023).
- Österreich: NISG 2026 kundgemacht am 23.12.2025 (BGBl. I 94/2025), in Kraft seit 01.10.2026 (WKO).
- Schweiz: Meldepflicht für Cyberangriffe auf kritische Infrastrukturen seit 01.04.2025, Meldung an das BACS innerhalb von 24 Stunden (Merkblatt BACS).
- CRA: Für Hersteller von Fernwirk- und Leittechnik gilt der Cyber Resilience Act (VO (EU) 2024/2847) für Produkte mit digitalen Elementen. Der Danfoss-Fall zeigt das Problem abgekündigter Geräte ohne Updates. Eine Einstufung einzelner Produkte haben wir nicht geprüft.

## 12. Methodik und Grenzen

- Nur Shodan-API host/count mit Facetten. Keine Logins, keine Seitenabrufe, keine Einzelhost-Abfragen, keine Kontaktaufnahme.
- Gegenprobe je Gruppe über ein zweites Merkmal (Favicon-Hash, Zertifikatsaussteller, Produkt). Rechenweg im internen Zählprotokoll dokumentiert.
- Bewertung: belastbar = zweites Merkmal bestätigt oder starkes Merkmal (Zertifikat, Produkt, Anmeldebereich) bzw. herstellerspezifischer Titel mit Fremdanteil unter 20 %; Fremdtreffer = mindestens 60 % Hoster, Herstellerfirma oder Honeypot; sonst unsicher. Je Hersteller zählt nur die stärkste Gruppe: Hersteller A 98 Treffer minus 21 bei Hostern = 77.
- Abzug je Land: Hoster, eigene Firmen-IT des Herstellers, Honeypots. Regionswerte (Bayern, Salzburg, Tirol) ohne Abzug.
- „Ohne TLS“ stammt aus der Shodan-Facette und ist je Dienst gezählt. Die Anmeldepflicht hinter HTTP 200 ist nicht geprüft.
- CVE-Angaben von Shodan beruhen auf Versionsnummern, Ausnutzbarkeit nicht geprüft.
- Schadensszenarien und Risikostufen sind Einschätzungen von OT-Cyber, keine Messung.
- Danfoss-Angaben aus unserem Vorfall-Lagebild (Stände 12.10., 24 h, 72 h, 14 Tage) mit den dort verlinkten Quellen. Die zweite Welle (02.11.) ist nur über Medien belegt.
- Viele Anlagen hängen hinter VPN oder privatem Mobilfunk und sind auf Shodan unsichtbar. Eine kleine Zahl heißt nicht, dass es keine Fernzugänge gibt.
- Organisationen, Seitentitel und Zertifikatsinhalte wurden ausgewertet, aber bewusst nicht aufgeführt. Gruppen unter 5 Diensten in einer Region nennen wir nur als „unter 5“ oder „einzelne“.

- Betreiber erkennbar (vorläufig): Bei einem Teil der Dienste ließe sich der Betreiber direkt benennen (Wasser 15,4 %, Energie 8,9 %, Gebäudeautomation 9,1 %, allein über die von Shodan gemeldete Organisation). Wir veröffentlichen keine Betreiber.

## 13. Hersteller ohne belastbare Treffer

- Fremdtreffer (aussortiert): Siemens SINAUT (Text), KSB, Wilo, Grundfos, Kisters (KISTERS, WISKI), Krohne, NIVUS, Ovarro TBox, ABB AC500, Inductive Automation Ignition, Tixi.Com, Rittmeyer (Text), Ewon, Tosibox, Webtitel „Klärwerk“, „Regenbecken“, „Trinkwasser“.
- Ohne Treffer oder nicht erkennbar (Nischenlauf 02.11.2026): Lacroix Sofrel, UFT, Piciorgros, Seba, VEGA, Xylem, Jung Pumpen, Huber, Hach, HIMA, COPA-DATA zenon, Siemens TeleControl Server, Unitronics (Banner), INSYS, Welotec (Einzeltreffer, unsicher), SCALANCE M, Webtitel „Hochbehälter“, „Pumpwerk“, „Kanalnetz“, „Regenüberlaufbecken“.