Shodan-Lage Energie (Heizen und Strom) 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 und Gegenprobe am Abend des 02.11.2026), 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.

Kernaussage

In Deutschland, Österreich und der Schweiz sind am 02.11.2026 6.098 Dienste belastbar Heizungs- und Stromerzeugungstechnik zuzuordnen: 958 Wärme (Wärmepumpen, Solar- und Heizungsregler, Gebäudeautomation in Heizzentralen) und 5.140 Strom (PV-Wechselrichter, Datenlogger, Speicher). Bayern stellt 1.477 Dienste, also rund ein Viertel. „Über 1.600 PV-Logger ohne Herstellersupport und mehr als 500 Heizungs- und Einspeiseregler mit Webservern von 2006 bis 2014 lassen sich mit einer Abfrage je Hersteller finden. Das ist dieselbe Ausgangslage wie bei Danfoss in Frankreich, nur verteilt auf viel mehr Betreiber. Wärmepumpe, Wechselrichter und Speicher gehören hinter ein VPN, eine Portfreigabe ist keine Fernwartung“, sagt Max Gilg, OT-Cybersecurity-Experte aus Rosenheim.
Der Angriff auf Danfoss-Kühlsteuerungen in Frankreich (11./12.10.2026, laut französischer Regierung rund 700 Supermärkte) zeigt, wie aus einer offenen Weboberfläche ein physischer Schaden wird: Sollwert auf 50 °C, Ware vernichtet, laut Staatsanwaltschaft Paris auch Brände. Dieselben Merkmale (Weboberfläche direkt im Internet, alte Firmware, Geräte ohne Support) finden wir bei Heizungsreglern und PV-Loggern in DACH, und zwar in deutlich größerer Zahl als bei Danfoss: Shodan zeigte am 12.10.2026 rund 20 Danfoss-Weboberflächen in Deutschland, wir zählen 1.601 SMA Sunny WebBoxen ohne Herstellersupport, 430 Heizungsregler mit Webservern von 2006 bis 2014 und 87 Power Reducer Boxen mit Webserver von 2007.
Gesamtrisiko nach unserer Einschätzung: mittel, für einzelne Gruppen hoch (SMA Sunny WebBox ohne Herstellersupport, SMA Power Reducer Box, Heizungs- und Wärmepumpenregler mit Webservern von 2006 bis 2014). Das wahrscheinlichste Szenario mit spürbarem Schaden ist eine im Winter abgeschaltete oder verstellte Wärmepumpe bzw. Heizzentrale in einer Liegenschaft mit Frostschaden (Einschätzung).

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
Wärme belastbar	715	156	87
Strom belastbar	4.568	443	129
Summe belastbar	**5.283**	**599**	**216**
Gesamt wahrscheinlich	**5.529**	**629**	**234**
je Mio. Einwohner	63	65	24
Wärme je Mio. Einwohner	9	17	10
Strom je Mio. Einwohner	55	48	14
Region Wärme	Bayern 159	Salzburg unter 5, Tirol 28	nicht erhoben
Region Strom	Bayern 1.318	Salzburg 19, Tirol 45	nicht erhoben
SMA Sunny WebBox (ohne Support)	1.587	unter 5	11
SMA Power Reducer Box	118	0	0
Branche unklar: Modbus/TCP	1.197	123	159
Branche unklar: KNXnet/IP	1.134	858	471
Branche unklar: MQTT ohne Anmeldung	3.501	202	226
Branche unklar: VNC ohne Passwort	86	unter 5	unter 5
Branche unklar: Fernwartungsrouter	591	28	51

Hinweise zur Tabelle:

- „Wahrscheinlich“ = belastbar plus unsichere Herstellergruppen (Rohwerte, je Hersteller die größte Gruppe, u. a. iDM, Kermi, Viessmann Vitocom, Engelmann, Skytron): Deutschland 5.283 + 246, Österreich 599 + 30, Schweiz 216 + 18. Nicht enthalten sind Webtitel mit Branchenwort, Fernwartungsrouter, VNC und RDP (Branche unklar). Unsichere Werte sind nicht am Gerät geprüft.
- Einwohner gerundet: Deutschland 83,6 Mio., Österreich 9,2 Mio., Schweiz 9,0 Mio. Werte je Mio. Einwohner gerundet.
- Österreich liegt je Einwohner bei Wärme rund doppelt so hoch wie Deutschland, vor allem durch Ochsner (58) und Sauter (60).
- Bei Strom liegt Deutschland je Einwohner vorne, vor allem wegen der SMA Sunny WebBox, die fast nur in Deutschland vorkommt.
- Fernwartungsrouter = Phoenix TC Router, Phoenix mGuard, WAGO Web-Based Management, mbCONNECT24, Teltonika (Rohwerte).

1. Was dahinter steht: Anlagen und Geräte

Wärme: Wärmepumpenregler mit Weboberfläche (Ochsner Web2Com, Stiebel Eltron ISG, KEBA KeEnergy), Solar- und Heizungsregler (Resol DL2/DL3, Technische Alternative C.M.I., Solvis SolvisRemote), Biomasse (HDG Bavaria) und Automationsstationen der Gebäudeautomation in Heizzentralen (Sauter moduWeb). Betreiber sind Einfamilienhäuser, Gewerbe, Wohnungswirtschaft und kommunale Liegenschaften. Große Kessel- und Biomassehersteller (Viessmann ViCare, Buderus, Vaillant, Wolf, ETA, Fröling, Hargassner, KWB, Windhager, Ökofen) binden über Cloud-Portale an und sind auf Shodan kaum sichtbar.

Strom: PV-Wechselrichter und Datamanager (Fronius, SMA), Datenlogger (Solar-Log, SMA Sunny WebBox), Einspeisemanagement (SMA Power Reducer Box), Speicher (sonnen, Varta, Victron) und

Eigenbau-Logger (OpenDTU für Hoymiles-Mikrowechselrichter, SolarView für Linux, Solaranzeige). BHKW, Biogas und kleine Wasserkraft binden nach Herstellerunterlagen meist über Portale und ausgehende VPN an und sind kaum sichtbar.

2. Angriffsvektor: Referenz Danfoss Frankreich

2.1 Was in Frankreich passiert ist

- 11./12.10.2026, nachts: Unbekannte verstellen aus der Ferne Kühlsteuerungen in Supermärkten. Die Kühlschränke laufen im Dauer-Abtaubetrieb mit Sollwert bis 50 °C (eine betroffene Handelsgruppe gegenüber Radio France, franceinfo 12.10.2026; Danfoss gegenüber Cooling Post).
- Umfang: Der französische Finanzminister nannte am 13.10.2026 im Parlament rund 700 betroffene von etwa 10.000 Supermärkten (AP, complexdiscovery.com). Die Staatsanwaltschaft Paris ermittelt (OFAC) und meldet Warenverluste und Entstehungsbrände (Reuters über NBC News, boursorama.com). Der Premierminister hat die ANSSI eingeschaltet (boursorama.com).
- Betroffene Geräte laut Danfoss: 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, franceinfo).
- CERT-FR, Alert CERTFR-2026-ALE-012 (12.10.2026, ergänzt 13.10. und 16.10.): zahlreiche Kompromittierungen von Fernsteuerungen für Kälteanlagen, Danfoss AK-SM und AK-SC, seit 13.10. auch Copeland xweb und Dixell xweb. Management-Oberflächen direkt im Internet widersprechen guter Praxis. Geräte ohne Sicherheitsupdates, die im Internet hängen, werden mit sehr hoher Wahrscheinlichkeit kompromittiert. Die Kampagnen laufen vermutlich weiter (cert.cyber.gouv.fr).
- Sichtbarkeit: LeMagIT fand am 12.10.2026 in Frankreich fast 3.000 erreichbare Weboberflächen, Reuters am 13.10.2026 per Shodan mindestens 4.500 Danfoss-Weboberflächen weltweit. Unsere Shodan-Abfrage vom 12.10.2026 (Titel „Danfoss“): rund 2.950 in Frankreich, 20 in Deutschland, 22 in Österreich und der Schweiz zusammen (Blog ot-cyber.de „Hacker heizen Kühlschränke“).
- Deutschland: BSI-Warnung BSI-CS 154 vom 13.10.2026 vor Nachahmern, ausdrücklich an Betreiber kleiner Anlagen, etwa Lebensmittelkühlung und Stromerzeugung. Ein Fall in Deutschland wird nicht genannt (bsi.bund.de, Pressemitteilung 13.10.2026).
- Nicht belegt: Täter, Motiv und genauer Angriffsweg. Weder Behörden noch Danfoss bringen den Angriff mit den von Claroty Team82 am 09.08.2026 veröffentlichten Lücken im AK-SM 800A (CVE-2025-41450 bis 41452) in Verbindung (SecurityWeek). Eine zweite Welle in der Nacht zum 02.11.2026 in weiteren europäischen Ländern ist berichtet, der Stand ist hier nicht geprüft.

2.2 Ablauf des Angriffs, übertragen auf Heizen und Strom

Der Ablauf in Frankreich lässt sich nach den belegten Angaben in vier Schritte fassen. Die Zuordnung zu DACH ist unsere Einschätzung.

Schritt	Danfoss Frankreich	Heizen/Strom DACH
1. Finden	Weboberfläche per Suchmaschine	6.098 Dienste per Shodan-Titel
2. Hineinkommen	offene Oberfläche, alte Firmware	Startseite 200 bei 15 von 18 Gruppen
3. Altgeräte	AK-SM 800, AK-SC 355 ohne Updates	WebBox ohne Support seit 2015
4. Eingreifen	Sollwert 50 °C, Dauer-Abtauung	Sollwerte, Betriebsart, Leistung

Erläuterung je Schritt:

- Finden: In Frankreich reichte die Suche nach der Weboberfläche (LeMagIT, Reuters). In DACH sind alle hier gezählten Gruppen über einen herstellertypischen Webtitel auffindbar, eine einzige Abfrage je Hersteller liefert die Liste.

- Hineinkommen: Wie die Angreifer in Frankreich angemeldet waren, ist nicht belegt. Belegt ist, dass offene Management-Oberflächen und fehlende Updates die Ursache sind (CERT-FR). Bei uns antwortet die Startseite ohne Anmeldung (HTTP 200) bei 15 von 18 Gruppen, darunter Ochsner, Sauter moduWeb, Stiebel ISG, Resol, HDG, KEBA, SMA WebBox, Power Reducer Box, Solar-Log und OpenDTU. Ob dahinter Steuerfunktionen ohne Anmeldung erreichbar sind, ist nicht geprüft. Für Ochsner Web2Com sind voreingestellte Zugangsdaten in Anwenderforen beschrieben, für Stiebel ISG laut Hersteller-Doku Modbus TCP ohne Passwort.
- Altgeräte: Die engste Parallele. Danfoss nennt Geräte ohne Updates seit 2016 bzw. 2021. Die SMA Sunny WebBox hat seit 31.12.2015 keinen Herstellersupport (VDE-2024-075), 1.601 Dienste in DACH. Bei Heizungsreglern laufen Webserver von 2006 bis 2014: Stiebel ISG lighttpd 1.4.19 (2008) 167, Sauter moduWeb Jetty 7.6.16 (2014) 134, Resol lighttpd 1.4.28 106, Ochsner Apache 2.0.58 (2006) 23, zusammen mit Power Reducer Box Apache 2.0.61 (2007) 87.
- Eingreifen: In Frankreich änderten die Angreifer Sollwert und Betriebsart. Die Weboberflächen der gezählten Heizungsregler und Wärmepumpen sind genau dafür gebaut (Sollwerte, Betriebsart, Zeitprogramme), bei PV-Loggern und Power Reducer Box für Leistungsbegrenzung und Wechselrichterparameter (Herstellerunterlagen, CVE-2019-13529 bei der WebBox).

2.3 Danfoss Frankreich gegen Heizen/Strom DACH

Merkmal	Danfoss Frankreich	Heizen/Strom DACH
Gerätetyp	Kühlsteuerung, Systemmanager	Heizungsregler, PV-Logger, Speicher
Sichtbar per Shodan	rund 2.950 (FR, 12.10.)	6.098 (DACH, 02.11.)
davon in Deutschland	rund 20 (12.10.)	5.283
Geräte ohne Support	AK-SM 800, AK-SC 355	SMA WebBox 1.601
alte Webserver	veraltete Firmware	2006 bis 2014: 517
Startseite ohne Anmeldung	nicht belegt	HTTP 200 bei 15 von 18 Gruppen
physische Wirkung	Wärme in Kühlschränken, Brände	Frost, Heizungsausfall, Leistung
Betreiber	Handelsketten, Dienstleister	Haushalte, Gewerbe, Kommunen
belegter Angriff	ja, rund 700 Märkte	in DACH nicht belegt

Erläuterung:

- „alte Webserver 517“ = Heizungsregler 430 (Stiebel ISG 167 + Sauter moduWeb 134 + Resol 106 + Ochsner 23) + Power Reducer Box 87. Gezählt sind Rohwerte mit der jeweiligen Versionsnummer laut Shodan, die Ausnutzbarkeit ist nicht geprüft.
- „HTTP 200“: Die Startseite antwortet bei 15 von 18 gezählten Gruppen. Ausnahmen: Solvis (401, Digest-Anmeldung), Technische Alternative (Anmeldebereich), sonnen (lokale API).
- Die Danfoss-Zahl zählt alle Weboberflächen mit Titel „Danfoss“, nicht nur Systemmanager. Eigene Zählung 12.10.2026, Quelle Blog ot-cyber.de.
- Unterschied: In Frankreich hingen viele Märkte an wenigen Dienstleistern und gleicher Technik. Bei Heizen und Strom in DACH sind die Betreiber stark verteilt. Ein Angriff trifft deshalb eher viele kleine Anlagen als einen großen Betreiber (Einschätzung).
- Fernwärme: Für Fernwärme-Übergaberegler (Danfoss ECL, Samson, Siemens Synco) haben wir keine belastbaren Treffer, nur 5 unsichere Danfoss-Dienste. Das Muster FrostyGoop (Lwiw 01/2024: Modbus-Befehle an Fernwärmeregler, über 600 Wohnhäuser fast zwei Tage ohne Heizung, Dragos 07/2024) ist deshalb nur über die Gruppe „Modbus/TCP, Branche unklar“ messbar: 1.479 Dienste in DACH.

3. Schadensszenarien

Alle Szenarien sind Einschätzungen. Sie beschreiben, was mit den gemessenen Zugriffsarten technisch denkbar ist. Ein Fall in DACH ist für keines belegt (Recherche 02.11.2026). Die Eintrittsschätzung bezieht sich auf die nächsten 12 Monate.

Szenario	Einstieg	Folge	betroffene Dienste	Eintritt (Einschätzung)
S1 Wärmepumpe im Winter aus	Weboberfläche, Modbus	Frostschaden, Wasserschaden	958 Wärme	mittel
S2 Heizzentrale verstellt	Gebäudeautomation Web	Wohnanlage kalt oder überhitzt	Sauter 212, Modbus 1.479	niedrig bis mittel
S3 Fernwärmeregler (FrostyGoop)	Modbus/TCP	Heizungsausfall vieler Wohnungen	belastbar 0, Modbus 1.479	niedrig
S4 PV-Leistung auf null	Logger, WebBox	Ertragsausfall, Direktvermarktung	5.140 Strom	mittel
S5 Einspeisemanagement manipuliert	Power Reducer Box	Vorgaben Netzbetreiber umgangen	118	niedrig bis mittel
S6 viele Anlagen gleichzeitig	Herstellercloud, Massenskript	Netzschwankung	nicht messbar	niedrig
S7 Speicher falsch gesteuert	Web, lokale API	Kosten, Notstrom fehlt	322	niedrig

Erläuterung je Szenario:

- S1 Wärmepumpe im Winter aus: Einstieg über die Weboberfläche von Ochsner Web2Com (228, voreingestellte Zugangsdaten in Foren beschrieben), Stiebel ISG (192, laut Doku Modbus ohne Passwort) oder KEBA KeEnergy (10). Der Angreifer schaltet auf Sommer- bzw. Standby-Betrieb oder setzt Sollwerte herunter, nachts bei Frost, so wie in Frankreich nachts bei geschlossenen Märkten. Folge: Gebäude kühlt aus, in leerstehenden Liegenschaften, Ferienwohnungen oder Kommunalgebäuden bemerkt das niemand sofort, Leitungen frieren ein, Wasserschaden. Bei Heizungsregler-Gruppen mit HTTP 200 und alten Webservern ist der Weg am kürzesten. Beleg für den Mechanismus: Danfoss Frankreich (Sollwert und Betriebsart).
- S2 Heizzentrale einer Wohnanlage verstellt: Einstieg über Sauter moduWeb (212, Jetty von 2014, Anmeldung nicht geprüft), Solvis (172, Digest-Anmeldung über HTTP) oder Resol (103). Der Angreifer ändert Vorlauftemperaturen, Zeitprogramme oder schaltet Pumpen ab. Folge: Mieter ohne Heizung oder Warmwasser, bei zu niedrigen Warmwassertemperaturen Legionellenrisiko, Kosten für Notdienst. Bei Gebäudeautomation in Schulen, Altenheimen oder Kliniken betrifft das schutzbedürftige Menschen (Einschätzung, Betreiber nicht erhoben).
- S3 Fernwärme-Übergabestationen per Modbus: Muster FrostyGoop (Lwiw 01/2024, Dragos). Der Angreifer sendet Modbus-Befehle an Regler und bringt sie zu falschen Messwerten oder Ausfall. In DACH fanden wir keine belastbaren Fernwärmeregler. 1.479 Modbus-Dienste ohne Branchenzuordnung (DE 1.197, AT 123, CH 159) und 569 ausgeschlossene Honeypots zeigen, dass das Protokoll offen erreichbar ist. Welcher Anteil Wärme ist, ist mit Shodan nicht bestimmbar.
- S4 PV-Leistung massenhaft auf null: Einstieg über SMA Sunny WebBox (1.601, ohne Support, CSRF CVE-2019-13529 mit CVSS 9,6), Solar-Log (1.003, CVE-2024-40116/40117 bei alter Firmware, Version nicht geprüft), Fronius (1.527, 37 alte Datalogger) oder OpenDTU (599, Eigenbau). Der Angreifer setzt Leistungsgrenzen auf null oder ändert Wechselrichterparameter. Folge: Ertragsausfall bis zur Entdeckung, bei Solar-Log mit Direktvermarktung auch Ausgleichsenergie und Vertragsstrafen (Einschätzung). Beleg für Missbrauch solcher Logger: Japan 05/2024, rund 800 SolarView Compact übernommen.
- S5 Einspeisemanagement manipuliert: SMA Power Reducer Box (118, nur Deutschland, 22 in Bayern, Apache von 2007). Sie setzt Vorgaben des Netzbetreibers an die Wechselrichter um. Der Angreifer kann Reduzierungsbefehle ignorieren lassen oder Dauerdrosselung erzeugen. Folge: Netzbetreiber

verliert die Steuerbarkeit der Anlage, Betreiber verliert Ertrag. Die Einzelwirkung aufs Netz ist gering, die Box sitzt aber an Anlagen, die der Netzbetreiber steuern muss (Einschätzung).

- S6 Aggregationsrisiko: Forescout (SUN:DOWN, 27.03.2025) beschreibt die Gefahr, über Herstellerclouds viele Wechselrichter gleichzeitig zu steuern. Litauen hat am 12.11.2024 deshalb Fernzugriff aus Hochrisiko-Staaten auf Anlagen über 100 kW untersagt (LRT). Über Shodan ist dieser Weg nicht messbar. Die 5.140 offenen Stromdienste in DACH reichen nach unserer Einschätzung für eine spürbare Netzwirkung nicht aus, ihre Leistung ist nicht erhoben.
- S7 Speicher falsch gesteuert: Varta (142, nginx 1.18.0 und 1.10.3, vuln bei 70), sonnen (116, lokale API), Victron (64). Der Angreifer entlädt den Speicher, sperrt die Ladung oder ändert die Notstromreserve. Folge: höhere Stromkosten, bei Netzausfall kein Notstrom. Funktion ohne Anmeldung nicht geprüft.
- BHKW in Gewerbe: Hersteller binden laut Unterlagen über Portale und ausgehende VPN an, Shodan zeigt nur 9 Webtitel „BHKW“ (unsicher). Ein Szenario lässt sich mit unseren Daten nicht quantifizieren, wir führen es deshalb nicht als eigenes Szenario.

4. Herstellerlandkarte mit Nischenherstellern

Hersteller	System	Einsatz
Ochsner (AT)	Web2Com	Wärmepumpen
Stiebel Eltron	ISG web	Wärmepumpen
Sauter (CH)	moduWeb, modu525	Heizzentralen, GLT
Solvis	SolvisRemote	Heizung, Solar
Resol	DL2, DL3, KM2	Solar- und Heizungsregler
Technische Alternative (AT)	C.M.I., UVR16x2	Heizungs- und Solarregler
HDG Bavaria	WebControl	Biomassekessel
KEBA KeEnergy	Wärmepumpenregelung	Wärmepumpen (M-TEC, Neura)
Viessmann	Vitogate 300, Vitocom, ViCare	Kessel, Wärmepumpen, GLT
Siemens, Kieback&Peter, Samson, Danfoss	Synco OZW, DDC4000, TROVIS, ECL	Heizzentrale, Fernwärme
SMA	Sunny WebBox, Power Reducer Box, Data Manager	PV
Fronius (AT)	Datamanager	PV
Solar-Log	Datenlogger	PV, Direktvermarktung
OpenDTU, SolarView Linux, Solaranzeige	Eigenbau	PV
sonnen, Varta, Victron	Speicher, Venus GX	Speicher
INNIO, MWM, 2G, ComAp, DEIF, SenerTec, Sokratherm	Motorsteuerung	BHKW, Biogas

Anbindung und Quelle je Hersteller:

- Ochsner: lokaler Webserver mit Digest-Anmeldung, voreingestellte Zugangsdaten (Anwenderforen, PyPI ochsner-web2com).
- Stiebel Eltron: Weboberfläche, laut Doku Modbus TCP 502 ohne Passwort (ISG-Connect-Doku).
- Sauter: Web und BACnet/IP (Shodan-Titel, Herstellerdoku nicht geprüft).
- Solvis: Web mit Digest-Anmeldung (Shodan-Anmeldebereich, Herstellerdoku nicht geprüft).
- Resol: Webserver, VBus TCP 7053, Portal VBus.net (Anwenderdoku).
- Technische Alternative: Webserver mit Anmeldung, Portal (Datenblatt).
- HDG Bavaria und KEBA KeEnergy: Web (Shodan-Titel).

- Viessmann: BACnet, Modbus, Cloud (Viessmann, CISA).
- Siemens, Kieback&Peter, Samson, Danfoss: Web, BACnet, Modbus (CISA, Hersteller).
- SMA: Web, Modbus, Portal (CERT@VDE, CISA).
- Fronius: Web, Solar.web (SEC Consult).
- Solar-Log: Web, Modbus 502 mit VPN zum Direktvermarkter (Datenblatt solar-log.com).
- OpenDTU, SolarView, Solaranzeige: Web, MQTT (Projektseiten).
- sonnen, Varta, Victron: Web, lokale API, Cloud (Hersteller).
- BHKW-Hersteller: Portal, VPN (Herstellerseiten).

5. Detailergebnis je Hersteller

Länderwerte nach Abzug, Regionen ohne Abzug. Zugriffsart aus Shodan-Facetten. vuln = Shodan-CVE aus Versionsnummer, Ausnutzbarkeit nicht geprüft.

5.1 Wärme

Hersteller	DE	AT	CH	Bayern	Salzburg	Tirol
Ochsner Web2Com	158	58	12	30	unter 5	unter 5
Sauter moduWeb	117	60	35	20	unter 5	15
Stiebel Eltron ISG	143	18	31	33	0	unter 5
Solvis	171	0	unter 5	45	0	0
Resol	94	unter 5	6	12	0	unter 5
Technische Alternative C.M.I.	13	10	unter 5	10	0	unter 5
HDG Bavaria	15	unter 5	0	8	0	0
KEBA KeEnergy	unter 5	6	0	unter 5	0	unter 5
Summe Wärme	**715**	**156**	**87**	**159**	**unter 5**	**28**

Zugriffsart, alte Versionen, vuln:

- Ochsner Web2Com: alle ohne TLS, Startseite antwortet (200). Apache 2.0.58 (2006) bei 17 DE und 6 AT. vuln bei 72 DE, 23 AT, 3 CH.
- Sauter moduWeb: alle ohne TLS, alle 200. Jetty 7.6.16 (2014) bei 134 Diensten, vuln CVE-2017-7656/7657 bei 139.
- Stiebel Eltron ISG: alle ohne TLS, alle 200. lighttpd 1.4.19 (2008) bei 167 Diensten, vuln bei allen 211.
- Solvis: alle ohne TLS, alle 401 (Digest-Anmeldung).
- Resol: ohne TLS, 200 bei 117. lighttpd 1.4.28 bei 106, vuln CVE-2011-4362.
- Technische Alternative C.M.I.: Anmeldebereich, ohne TLS.
- HDG Bavaria: alle 200. lighttpd 1.4.35 und 1.4.39, vuln bei 8.
- KEBA KeEnergy: alle 200, vuln (jQuery) bei 3 AT.

5.2 Strom

Hersteller	DE	AT	CH	Bayern	Salzburg	Tirol
SMA Sunny WebBox	1.587	unter 5	11	386	0	0
Fronius	1.149	335	43	355	15	24
Solar-Log	924	28	51	355	unter 5	18
OpenDTU	538	55	6	90	unter 5	unter 5
Varta	131	unter 5	10	42	unter 5	0
sonnenBatterie	106	unter 5	7	42	0	0
SolarView Linux	81	unter 5	0	38	0	unter 5
Victron	46	17	unter 5	9	unter 5	0
Solaranzeige	6	0	0	unter 5	0	0
Summe Strom	**4.568**	**443**	**129**	**1.318**	**19**	**45**
SMA Power Reducer Box (nicht in Summe)	118	0	0	22	0	0

Zugriffsart, alte Versionen, vuln:

- SMA Sunny WebBox: ohne TLS, 200. Ohne Herstellersupport seit 31.12.2015, vuln bei 64.
- SMA Power Reducer Box: ohne TLS, 200. Apache 2.0.61 (2007) bei 87, vuln bei 119.
- Fronius: 200. thttpd von 2003 bei 37 (alter Datalogger), nginx 1.24.0 bei 17 AT. Die TLS-Facette ist bei Fronius nicht schlüssig: Sie zeigt fast alle ohne TLS, die Vorarbeit fand 65 % auf Port 443 (nicht geprüft).
- Solar-Log: ohne TLS, 200.
- OpenDTU: ohne TLS, 200. Eigenbau, Pflegezustand unbekannt.
- Varta: 200. nginx 1.18.0 und 1.10.3, vuln bei 70.
- sonnenBatterie: lokale API, Funktion nicht geprüft, kein zweites Merkmal.
- SolarView Linux: 200, teils IIS und Apache.
- Victron: 200. nginx 1.24.0, vuln bei 72.
- Solaranzeige: 200.

6. Branche unklar: Fernzugänge und generische Protokolle

Rohwerte, gelten identisch im Report „Wasser und Abwasser“, 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
KNXnet/IP 3671	1.134	858	471	Branche unklar
MQTT 1883 ohne Anmeldung	3.501	202	226	Branche unklar
Siemens S7 102	206	69	unter 5	Branche unklar
Niagara Fox	152	27	7	Branche unklar
BACnet 47808	56	32	35	Branche unklar
CODESYS 2455	55	5	27	Branche unklar
OPC UA 4840	42	5	unter 5	Branche unklar
DNP3 20000	23	unter 5	11	Branche unklar
IEC 60870-5-104 2404	21	0	unter 5	Branche unklar

Hinweise:

- Ewon (Text, 726 DACH) ist Fremdtreffer: 95 % Hoster oder Honeypot.
- 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.
- MQTT: Fremdanteil 75 %, die Zahl ist deshalb nur ein Hinweis.
- Webtitel ohne Hersteller (DACH, unsicher): Wechselrichter 90, Photovoltaik 102, Fernsteuerung 52, Inverter Webinterface 36, BHKW 9 (Text 27), Biogas 22, Kraftwerk 17, Wehr 10.
- Einschätzung: Ein Teil der Modbus-Dienste ist PV, Speicher und BHKW, ein Teil der KNX- und BACnet-Dienste Gebäude- und Heizungstechnik. Der Anteil ist mit Shodan nicht bestimmbar.

7. Risikomatrix

Gemessen an Angriffsvektor (Abschnitt 2) und Schadensszenario (Abschnitt 3). Risiko ist unsere Einschätzung.

Gruppe	DACH	Nähe zu Danfoss	Szenario	Risiko
SMA Sunny WebBox	1.601	eng: ohne Support	S4	hoch
SMA Power Reducer Box	118	eng: Webserver 2007	S5	hoch
Stiebel Eltron ISG	192	eng: Webserver 2008	S1	hoch
Ochsner Web2Com	228	eng: Werkspasswort, 2006	S1	mittel bis hoch
Sauter moduWeb	212	mittel: Webserver 2014	S2	mittel bis hoch
Resol	103	mittel: Webserver alt	S2	mittel
Solvis	172	gering: Anmeldung	S2	mittel
Fronius	1.527	gering bis mittel	S4	mittel
Solar-Log	1.003	mittel: alte Firmware möglich	S4	mittel
OpenDTU	599	mittel: Eigenbau	S4	mittel
Technische Alternative, HDG, KEBA	51	gering bis mittel	S1, S2	niedrig bis mittel
Varta, sonnen, Victron	322	gering	S7	niedrig bis mittel
Modbus/TCP (Branche unklar)	1.479	Muster FrostyGoop	S3	nicht bewertbar
Herstellercloud	nicht messbar	anderer Weg	S6	hoch, nicht messbar

Begründung:

- Stiebel Eltron ISG hoch: Webserver von 2008 bei 167 Diensten, Startseite antwortet bei allen, laut Doku Modbus ohne Passwort, und die Folge im Winter ist ein Sachschaden am Gebäude. Das entspricht dem Danfoss-Muster am genauesten.
- SMA Sunny WebBox und Power Reducer Box: Altgeräte ohne Support bzw. mit Webserver von 2007. Auswirkung auf Ertrag und Steuerbarkeit, nicht auf Menschen.
- Ochsner: voreingestellte Zugangsdaten in Foren beschrieben, Apache von 2006 bei 23.
- Fronius, Solar-Log, OpenDTU: viele Dienste, aber ohne belegte offene Altgeräte in großer Zahl. Firmwarestand nicht geprüft.
- Herstellercloud: Sun:Down 2025 und Growatt 2025 zeigen, dass dieser Weg viele Anlagen gleichzeitig erreicht. Über Shodan nicht messbar.
- Einschätzung gesamt: Je Heizung oder Dachanlage ist der Schaden begrenzt. In Summe sind über 500 Heizungs- und Einspeiseregler mit Webservern von 2006 bis 2014 und über 1.600 nicht mehr gepflegte PV-Logger mit einer Abfrage je Hersteller auffindbar. Das ist dieselbe Ausgangslage wie bei Danfoss in Frankreich, nur verteilt auf viel mehr Betreiber.

8. Belegte Vorfälle und Advisories

Datum	Ort	Vorfall
11./12.10.2026	Frankreich	Danfoss-Kühlsteuerungen, rund 700 Märkte
01/2024	Lwiw (Ukraine)	FrostyGoop, Fernwärme
05/2024	Japan	SolarView Compact missbraucht
27.03.2025	global	SUN:DOWN, 46 Lücken
15.04.2025	global	Growatt Cloud
2024	global	Solarman/Deye-Plattform
12.11.2024	Litauen	Verbot von Fernzugriff

Was passiert ist und Quelle:

- Danfoss Frankreich (11./12.10.2026): Kühlsteuerungen per Fernzugriff auf Dauer-Abtauung mit Sollwert bis 50 °C, rund 700 Supermärkte (französischer Finanzminister, 13.10.2026), Warenverluste und Entstehungsbrände (Staatsanwaltschaft Paris), CERTFR-2026-ALE-012 mit Copeland und Dixell xweb, BSI-CS 154 vom 13.10.2026. Details in Abschnitt 2.1.
- FrostyGoop (01/2024): Modbus-Befehle an Fernwärmeregler, über 600 Wohnhäuser fast zwei Tage ohne Heizung (Dragos, 07/2024; MITRE S1165).
- Japan (05/2024): rund 800 Contec SolarView Compact übernommen und für Bankdiebstahl missbraucht, vermutlich CVE-2022-29303 (CSO Online 2024; ScanNetSecurity 14.05.2024).
- SUN:DOWN (27.03.2025): Forescout meldet 46 Lücken bei Sungrow, Growatt und SMA. Bei SMA nur Sunny Portal, CVE-2025-0731, behoben 19.12.2024 (forescout.com).
- Growatt (15.04.2025): ICSA-25-105-04, u. a. Ein- und Ausschaltbefehle über die Cloud (CISA).
- Solarman/Deye (2024): Plattform mit rund 195 GW angebundener Leistung, Lücken im Sommer 2024 gepatcht (SecurityWeek, Bitdefender).
- Litauen (12.11.2024): Fernzugriff von Herstellern aus Hochrisiko-Staaten auf PV, Wind und Speicher über 100 kW untersagt (LRT).
- DACH: Angriffe auf Heizungen, Wärmepumpen, BHKW oder PV-Anlagen mit Eingriff in die Steuerung sind öffentlich nicht belegt (Recherche 02.11.2026).

Advisories:

- SMA Sunny WebBox: ICSA-19-281-01 (CVE-2019-13529, CVSS 9,6) und VDE-2024-075 (01/2025, Support endete 31.12.2015).
- Fronius Datamanager: CVE-2019-19228 und CVE-2019-19229 (SEC Consult, 03.12.2019).
- Solar-Log: CVE-2024-40116 und CVE-2024-40117 (26.07.2024).
- Viessmann Vitogate 300: CVE-2025-9494/9495 (ICSA-25-266-04), behoben mit Firmware 3.1.0.1.
- Siemens Synco OZW672/772: CVE-2025-26389/26390 (ICSA-25-135-10, 15.05.2025), behoben in V8.0.
- Kieback&Peter DDC4000: ICSA-24-291-05, behoben in Firmware 1.21.0.
- Alpha Innotec/Novelan Luxtronik: CVE-2024-22894.
- Elvaco CMe3100: ICSA-24-291-01.
- Enphase IQ Gateway: ICSA-23-171-01 und CVE-2024-21876 bis 21881.
- Zu Stiebel Eltron ISG, Ochsner Web2Com, Resol und Technische Alternative wurde keine CVE gefunden (Suche 02.11.2026). Zu Sauter moduWeb, Solvis, HDG und KEBA KeEnergy ist die Advisory-Lage nicht geprüft.

9. Regionallage Bayern, Salzburg, Tirol

Region	Wärme	Strom	Summe
Bayern	159	1.318	1.477
Salzburg	unter 5	19	22
Tirol	28	45	73

- Bayern Wärme: Solvis 45, Stiebel 33, Ochsner 30, Sauter 20, Resol 12, Technische Alternative 10, HDG 8, KEBA unter 5.
- Bayern Strom: SMA WebBox 386, Fronius 355, Solar-Log 355, OpenDTU 90, sonnen 42, Varta 42, SolarView 38, Victron 9, Solaranzeige unter 5, dazu 22 Power Reducer Boxen. Beim Solar-Log liegen 37 % der deutschen Treffer in Bayern, bei Technischer Alternative 10 von 14.
- Tirol: Sauter moduWeb 15 (ein Viertel der österreichischen Sauter-Treffer), Fronius 24, Solar-Log 18, dazu einzelne KEBA- und Stiebel-Regler.
- Salzburg: vor allem Fronius 15, dazu einzelne Heizungsregler.
- Grenzregion: Biomassekessel (ETA, Fröling, Hargassner, KWB, Windhager) sind dort verbreitet (Einschätzung), auf Shodan aber praktisch unsichtbar, weil sie über Herstellerportale angebunden sind. Das Risiko liegt dann bei Portal-Konten und Fernwartung der Heizungsbauer (nicht geprüft).
- Danfoss-Bezug: In Deutschland zeigte Shodan am 12.10.2026 rund 20 Danfoss-Weboberflächen, in Österreich und der Schweiz zusammen 22. Allein in Bayern liegen 386 SMA Sunny WebBoxen und 159 Heizungsregler (eigene Zählung 02.11.2026).

10. Empfehlungen nach SANS Five ICS Critical Controls

- CC1 ICS Incident Response: Für Heizzentralen und Wärmepumpen in Liegenschaften den Handbetrieb und eine nachts erreichbare Nummer des Heizungsbauers festlegen. Danfoss-Lehre: Der Angriff lief nachts bei geschlossenen Märkten, entdeckt wurde er erst morgens (Berichte vom 12.10.2026). Für leerstehende Gebäude im Winter eine Frostwarnung unabhängig vom Regler vorsehen. Für PV: wer schaltet ab, wer informiert Netzbetreiber und Direktvermarkter.
- CC2 Defensible Architecture: Keine Portfreigabe für Heizungsregler, Gebäudeautomation, Wechselrichter, Logger und Speicher. CERT-FR: Geräte ohne Sicherheitsupdates gehören gar nicht ins Internet (CERTFR-2026-ALE-012). Sunny WebBox und Power Reducer Box ersetzen oder vom Internet trennen.
- CC3 ICS Network Visibility & Monitoring: Stadtwerke, Contractoren, Heizungsbauer und Direktvermarkter gleichen ihre Anlagen regelmäßig mit Shodan-Daten ab. Ungewöhnliche Sollwertänderungen, Betriebsartwechsel, Abschaltungen und Leistungsgrenzen als Sicherheitsereignis behandeln.
- CC4 Secure Remote Access: Zugriff nur über VPN mit Mehrfaktor-Anmeldung, so wie CERT-FR es nach dem Danfoss-Angriff fordert. Werkspasswörter (Web2Com, ISG) ändern, HTTP abschalten. Steuerung durch Netzbetreiber über Smart-Meter-Gateway und Steuerbox nach BSI TR-03109-5.
- CC5 Risk-Based Vulnerability Management: Zuerst Geräte ohne Support (WebBox) und mit alten Webservern (Power Reducer Box, ISG, moduWeb, Web2Com, Resol). Dann Firmware von Fronius Datamanager und Solar-Log, danach Vitogate 300, OZW672, DDC4000 und Luxtronik nach den Advisories.
- Für bereits kompromittierte Geräte (CERT-FR-Maßnahmenplan, Stand 16.10.2026): vom Internet trennen, auf Werkseinstellungen zurücksetzen, patchen, neue Zugangsdaten, Konten prüfen, vollständig neu konfigurieren, danach Zugang nur per VPN. Ein Neustart oder Werksreset allein reicht nicht, die Konfiguration (bei Kühlung die Abtauzeiten, übertragen: Sollwerte, Zeitprogramme, Leistungsgrenzen) muss geprüft werden.

11. Regulatorischer Bezug

- NIS2 Deutschland: NIS2UmsuCG in Kraft seit 06.12.2025 (usd.de, secjur.com). Fernwärme und größere Stadtwerke sind erfasst, für kleine Betreiber von Wärmepumpen und PV meist nicht einschlägig (Einschätzung).
- KRITIS-Schwellen: Fernwärme 2.300 GWh pro Jahr, Stromerzeugung 104 MW (BSI-KritisV). Die Änderung vom 15.05.2026 und der Entwurf einer neuen KritisV sind nicht geprüft.
- Österreich: NISG 2026 in Kraft seit 01.10.2026 (WKO). Schweiz: Meldepflicht an das BACS seit 01.04.2025.
- CRA (VO (EU) 2024/2847): Wärmepumpenregler, Wechselrichter, Logger und Speicher mit Netzanbindung sind Produkte mit digitalen Elementen. Hersteller müssen Updates über die Lebensdauer liefern und Schwachstellen melden. Eine Einstufung in Anhang III ist nicht geprüft.
- Solarspitzengesetz in Kraft seit 25.02.2025 und § 14a EnWG: Steuerung über Smart-Meter-Gateway und Steuerbox ist der vorgesehene sichere Weg (bsi.bund.de, pv-magazine).
- BSI-CS 154 (13.10.2026): Empfehlung des BSI nach dem Danfoss-Angriff, ausdrücklich für Betreiber kleiner Anlagen, etwa Lebensmittelkühlung und Stromerzeugung (bsi.bund.de).

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), Bei sonnen gab es kein zweites Merkmal.
- Abzug je Land (Hoster, Herstellerfirma, Honeypot). Regionen ohne Abzug. Länderwerte im Ländervergleich sind die exakte Summe der Herstellerzeilen.
- Je Hersteller zählt nur eine Gruppe. Doppelzählungen zwischen Herstellern sind möglich, wenn ein Gerät mehrere Titel liefert (selten).
- HTTP 200 heißt nur, dass eine Seite antwortet. Ob Steuerfunktionen ohne Anmeldung erreichbar sind, ist nicht geprüft. CVEs aus Versionsnummern, Ausnutzbarkeit nicht geprüft.
- Cloud-angebundene Anlagen sind auf Shodan unsichtbar.
- 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.
- Danfoss-Angaben stammen ausschließlich aus unserem Vorfall-Lagebild (Stände 12.10. bis 14 Tage) und dem Blog „Hacker heizen Kühlschränke“ auf ot-cyber.de mit den dort genannten Quellen. Die Übertragung auf Heizen und Strom ist unsere Einschätzung.

12.1 Zählprotokoll: Rechenweg und wichtigste Gruppen

Grundlage ist unser internes Zählprotokoll mit Abfrage, Zeitpunkt, Länderwerten, Abzügen, Zugriffsart, Version und Gegenprobe je Gruppe.

Gruppe	DACH roh	Gegenprobe	Bewertung	zählt
SMA Sunny WebBox	1.796	94 %	belastbar	1.601
Fronius (Titel)	1.580	85 %	belastbar	1.527
Solar-Log	1.048	99 %	belastbar	1.003
OpenDTU	681	99 %	belastbar	599
Ochsner Web2Com	233	100 %	belastbar	228
Sauter moduWeb	216	64 %	belastbar	212
Stiebel Eltron ISG	211	84 %	belastbar	192
Solvis	210	Anmeldebereich	belastbar	172
Resol (Titel)	120	Titel	belastbar	103

- Geprüft, aber nicht gezählt (überwiegend Hoster, Firmen-IT, Honeypots oder Namensgleiche): Schneid MR (Text), Prozeda (Text), PlanET (Text), Nibe (Text).

Bewertungsregeln und Rechenweg:

- Belastbar: zweites Merkmal bestätigt (Schnittmenge mindestens 50 % bei Text, mindestens 30 % bei Titel), starkes Merkmal (Zertifikat, Produkt, Anmeldebereich) oder herstellerspezifischer Titel mit Fremdanteil unter 20 %.
- Fremdtreffer: mindestens 60 % Hoster, eigene Firmen-IT oder Honeypot, oder Schnittmenge unter 10 % ohne passenden Titel. Sonst unsicher.
- Wärme: Ochsner 228 + Sauter 212 + Stiebel Eltron 192 + Solvis 172 + Resol 103 + Technische Alternative 25 + HDG Bavaria 16 + KEBA KeEnergy 10 = 958.
- Strom: SMA 1.601 + Fronius 1.527 + Solar-Log 1.003 + OpenDTU 599 + Varta 142 + sonnen 116 + SolarView Linux 82 + Victron 64 + Solaranzeige 6 = 5.140.
- Je Hersteller zählt nur die stärkste Gruppe. SMA Power Reducer Box (118), weitere SMA-Geräte (361), Fronius Datalogger (37) und Ohmpilot (17) sind belastbar, aber nicht zusätzlich gezählt. Die SMA-Summe ist damit eher zu niedrig.
- Unsicher, zusätzlich 198: Viessmann Vitocom 39, iDM 24, Kermi 22, Kieback&Peter 15, Skytron 11, Engelmann 8, Heliotherm 7, ComAp 7, Buderus 6, EBV 6, EnviTec 6, Danfoss 5, Rest je 1 bis 4.
- Webtitel mit Branchenwort, unsicher: 111 (Heizung, Heizzentrale, Kesselhaus, Pelletheizung, Nahwärme und weitere, Überschneidungen möglich).

13. Hersteller ohne belastbare Treffer

- Fremdtreffer: Schneid, Prozeda, PlanET, NIBE, Wolf (Smartset, ISM7), Viessmann Vitogate (Titel), Alpha Innotec/Novelan, BSB-LAN, Buderus KM200, Gemina Termix, Guntamatic, Kamstrup, Kieback&Peter DDC4 (Text), Liebi, Lobaro, M-TEC, Oventrop, PEWO, Plum ecoNET, Remko, SOREL, Solvimus, Waterkotte, ratiotherm, ComAp, DEIF, E3/DC, Gantner, Huawei SmartLogger, INNIO myPlant, Janitza, MWM TPEM, Motortech, Next Kraftwerke, SenerTec, Sokratherm, Sungrow WiNet, agrikomp, MQTT-Suchworte (solar, inverter, opendtu, victron).
- Nur unsicher: Viessmann Vitocom, iDM, Kermi, Kieback&Peter, Heliotherm, Buderus, Danfoss ECL, Engelmann, Lingg & Janke, Windhager, Fröling, Hoval, Weishaupt, Dimplex, Remeha, Herz, Heizomat, Tecalor, EBV, Elvaco, Steca, Kostal, Kaco, SENEC, meteocontrol, Skytron, Ossberger, 2G, Tedom, EnviTec, Awite, Schmack.

- Ohne Treffer (Vorarbeit 02.11.2026): Vaillant, ETA, Hargassner, KWB, Ökofen, Solarfocus, Samson Trovis, SolarEdge, Growatt, GoodWe, Solax, Enphase, Contec SolarView Compact, BYD, LG ESS, Tesla, alle Wasserkraft-Hersteller.