Shodan-Lage Gebäudeautomation 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 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 6.562 Dienste belastbar der Gebäudeautomation zuzuordnen: 3.976 Weboberflächen von Herstellern (Gira HomeServer, Saia PCD, Sauter moduWeb, Elesta, Copeland/Dixell XWEB und weitere) und 2.586 offene Protokolldienste (KNXnet/IP, BACnet/IP, Niagara Fox). Die beiden größten Gruppen sind Gira HomeServer mit 3.003 und KNXnet/IP mit 2.458 Diensten. Österreich liegt je Einwohner mit 161 Diensten je Million gut dreimal so hoch wie Deutschland (51).

Der Angriff auf Kühlsteuerungen in Frankreich (11./12.10.2026, laut französischer Regierung rund 700 Supermärkte) betrifft genau diesen Bereich: Danfoss AK-SM und AK-SC sind Kälte- und Gebäudeautomation, und CERT-FR nennt seit 13.10.2026 auch Copeland xweb und Dixell xweb. Wir zählen in DACH 151 XWEB-Oberflächen belastbar, die Startseite antwortet bei 154 von 155 Rohtreffern ohne Anmeldung. Danfoss StoreView ist in DACH dagegen kaum echt sichtbar: 354 Rohtreffer, nach Abzug von Hostern und Honeypots bleiben einzelne.

Gesamtrisiko nach unserer Einschätzung: mittel, für einzelne Gruppen hoch (Copeland/Dixell XWEB in Gewerbekälte, Saia PCD und Sauter moduWeb in Heizung und Lüftung größerer Gebäude, KNXnet/IP ohne erkennbares KNX Secure). Das wahrscheinlichste Szenario mit spürbarem Schaden ist eine nachts verstellte Kälteanlage in einem Supermarkt oder Gewerbebetrieb über XWEB, nach dem Muster Frankreich (Einschätzung). „151 XWEB-Oberflächen in DACH gehören zu genau der Geräteklasse, die in Frankreich und jetzt in fünf weiteren Ländern angegriffen wurde, und fast alle zeigen ihre Startseite ohne Anmeldung und ohne TLS. Kältemanager, GLT-Stationen und KNX-Schnittstellen gehören hinter ein VPN, eine Portfreigabe ist keine Fernwartung“, sagt Max Gilg, OT-Cybersecurity-Experte aus Rosenheim.

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
Web/Hersteller belastbar	3.094	575	307
Protokolle belastbar	1.165	910	511
Summe belastbar	**4.259**	**1.485**	**818**
Gesamt wahrscheinlich	**4.315**	**1.513**	**838**
je Mio. Einwohner gesamt	51	161	91
Web/Hersteller je Mio. Einwohner	37	63	34
Protokolle je Mio. Einwohner	14	99	57
Region Web/Hersteller	Bayern 575	Salzburg 119, Tirol 74	nicht erhoben
Region Protokolle	Bayern 319	Salzburg 69, Tirol 61	nicht erhoben
Region gesamt	Bayern 894	Salzburg 188, Tirol 135	nicht erhoben
Gira HomeServer, X1, FacilityServer	2.612	337	54
KNXnet/IP 3671	1.134	853	471
Kälte: Copeland/Dixell XWEB	100	49	unter 5
Branche unklar: WAGO Web-Based Management	173	16	24
Branche unklar: Beckhoff ADS 48898	24	0	25
Branche unklar: Fernwartungsrouter	415	12	27

Hinweise zur Tabelle:

- „Wahrscheinlich“ = belastbar plus unsichere Gruppen (Rohwerte: BAB eibPort, Carel pCOWeb, Kieback&Peter Text, ABB free@home, Siemens Desigo, Distech ECLYPSE, LON/IP-852): Deutschland 4.259 + 56, Österreich 1.485 + 28, Schweiz 818 + 20. Nicht enthalten ist NETxAutomation (Produktfacette zeigt fremde Geräte). 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.
- Web/Hersteller und Protokolle können sich überschneiden: Ein Gira HomeServer kann zusätzlich einen KNXnet/IP-Dienst zeigen. Die Summe ist deshalb eine Obergrenze für Geräte, für Dienste ist sie exakt.
- Österreich liegt bei den Protokollen je Einwohner rund siebenmal so hoch wie Deutschland, vor allem durch KNXnet/IP (853). Die Schweiz liegt vorne bei Saia PCD (190).
- Fernwartungsrouter = Phoenix Contact TC ROUTER, Phoenix mGuard, mbCONNECT24, Teltonika (Rohwerte aus dem Report „Wasser und Abwasser“, Abschnitt 6). WAGO steht getrennt mit Werten aus dem Lauf Gebäudeautomation.

1. Was dahinter steht: Anlagen und Geräte

Raum- und Hausautomation: Gira HomeServer 4, X1 und FacilityServer sind Visualisierungs- und Logikserver für KNX-Anlagen. Sie steuern Licht, Jalousien, Heizung je Raum, Szenen und teils Zutritt und Alarmmeldungen. Eingesetzt werden sie in Einfamilienhäusern, Bürogebäuden, Hotels und Arztpraxen (Herstellerangaben, Betreiber nicht erhoben). KNXnet/IP auf Port 3671 ist die IP-Schnittstelle der KNX-

Installation selbst, also der direkte Weg auf den Gebäudebus. Loxone Miniserver, eibPort und ABB free@home gehören in dieselbe Klasse.

Gebäudeleittechnik in größeren Liegenschaften: Saia PCD (Honeywell) und Sauter moduWeb sind Automationsstationen für Heizung, Lüftung, Klima und Kälte in Schulen, Kliniken, Bürogebäuden, Hallenbädern und kommunalen Gebäuden. Elesta (RCOWeb), Loytec, Trend und Honeywell WEBs (Niagara) sind weitere GLT-Plattformen. BACnet/IP und Niagara Fox sind die Protokolle, über die Leitstände und Automationsstationen miteinander sprechen.

Gewerbekälte: Copeland/Dixell XWEB und Danfoss StoreView bzw. AK-SM sind Systemmanager für Kühlstellen, Kühlschränke und Tiefkühltruhen im Lebensmittelhandel, in Gastronomie, Lagern und Laboren. Genau diese Gerätegruppe war in Frankreich das Ziel.

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 nennt 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“).
- Forescout fand am 22.10.2026 weltweit 12.976 exponierte Dienste von Kältesteuerungen auf 6.017 öffentlichen IP-Adressen in 99 Ländern, darunter 7.075 Copeland/Dixell XWEB, 4.697 Danfoss StoreView, 551 Copeland Site Supervisor und 513 CAREL pCOWeb. Rund 80 % der StoreView-Beobachtungen liefen mit Firmware älter als 4.3.1 (Vorfall-Lagebild OT-Cyber, Forescout über Euronews).
- 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).
- Zweite Welle: Am 02.11.2026 meldeten Supermärkte in Belgien, Schweden, Luxemburg, Irland und Estland manipulierte Kühl- und Tiefkühlanlagen, laut einem Installateur mit derselben Methode wie in Frankreich. In der Schweiz wurden laut Berichten Angriffsversuche bei einer Handelskette abgewehrt (Vorfall-Lagebild OT-Cyber, Stand 02.11.2026, Primärforensik nicht veröffentlicht).
- 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).

2.2 Ablauf des Angriffs, übertragen auf Gebäudeautomation

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

Schritt	Danfoss Frankreich	Gebäudeautomation DACH
Schritt 1, Finden	Weboberfläche per Suchmaschine	3.976 Weboberflächen per Titel
Schritt 2, Hineinkommen	offene Oberfläche, alte Firmware	Startseite 200 bei 3.023 Gira, 154 XWEB
Schritt 3, Altgeräte	AK-SM 800, AK-SC 355 ohne Updates	Jetty 2014 (Sauter), Niagara AX 3.7
Schritt 4, Eingreifen	Sollwert 50 °C, Dauer-Abtauung	Sollwerte, Lüftung, Licht, Kälte

Erläuterung je Schritt:

- Finden: In Frankreich reichte die Suche nach der Weboberfläche (LeMagIT, Reuters). In DACH sind alle gezählten Webgruppen über einen herstellertypischen Titel auffindbar. KNXnet/IP und BACnet/IP findet jede Suchmaschine über den Standardport.
- 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 3.023 von 3.028 Gira-Rohtreffern, bei allen 458 Saia PCD, allen 216 Sauter moduWeb und 154 von 155 XWEB. Alle diese Gruppen laufen ohne TLS. Ob dahinter Steuerfunktionen ohne Anmeldung erreichbar sind, ist nicht geprüft. KNXnet/IP hat ohne KNX Secure keine Anmeldung im Protokoll, KNX Secure war in der Vorarbeit nicht erkennbar.
- Altgeräte: Sauter moduWeb mit Jetty 7.6.16 von 2014 bei 75 Diensten (DE-Facette). Niagara Fox mit Version 3.7.44 bei 122 Rohtreffern (Niagara AX). Für XWEB ist die Firmware über Shodan meist nicht sichtbar, Shodan meldet vuln aus Versionsnummern bei 9 in DE und 40 in AT.
- Eingreifen: In Frankreich änderten die Angreifer Sollwert und Betriebsart. XWEB-Oberflächen sind genau dafür gebaut (Sollwerte, Abtauung, Alarme). Saia- und Sauter-Stationen steuern Heizkreise, Lüftungsanlagen und Kälte, Gira HomeServer und KNX Licht, Jalousien, Raumtemperatur und Szenen (Herstellerunterlagen).

2.3 Danfoss Frankreich gegen Gebäudeautomation DACH

Merkmal	Danfoss Frankreich	Gebäudeautomation DACH
Gerätetyp	Kühlsteuerung, Systemmanager	GLT, KNX-Server, Kältemanager
Sichtbar per Shodan	rund 2.950 (FR, 12.10.)	6.562 (DACH, 02.11.)
davon in Deutschland	rund 20 (12.10.)	4.259
gleiche Gerätegruppe	AK-SM, AK-SC, xweb	XWEB 151, Danfoss netto unter 5
alte Webserver	veraltete Firmware	Jetty 2014 bei 75, Niagara AX
Startseite ohne Anmeldung	nicht belegt	HTTP 200 bei 3.851 Webdiensten
physische Wirkung	Wärme in Kühlschränken, Brände	Kälte, Heizung, Lüftung, Licht
Betreiber	Handelsketten, Dienstleister	Handel, Gewerbe, Kommunen, Haushalte
belegter Angriff	ja, rund 700 Märkte	in DACH nicht belegt

Erläuterung:

- „HTTP 200 bei 3.851“ = Gira 3.023 + Saia 458 + Sauter 216 + XWEB 154, Rohwerte vor Abzug.
- Danfoss in DACH: Der Titel „Danfoss StoreView“ liefert 354 Rohtreffer (DE 276, CH 76, AT unter 5). In Deutschland liegen davon 245 bei Hostern, 171 haben eine Honeypot-Markierung, in der Schweiz 59 bei Hostern und 42 mit Honeypot-Markierung. Netto bleiben nur einzelne in Österreich. Danfoss AK-SM (Text) liefert 0. Lesart: Fast alle Danfoss-Treffer in DACH sind Fallen oder Hosting, vermutlich nach dem Frankreich-Vorfall aufgestellt (Einschätzung, nicht geprüft).
- XWEB ist die engste Parallele: gleiche Gerätegruppe, im CERT-FR-Alert genannt, nur 4 Hoster unter den Rohtreffern, Startseite antwortet, kein TLS. Bayern 19, Salzburg unter 5, Tirol 5.

- Unterschied: In Frankreich hingen viele Märkte an wenigen Dienstleistern und gleicher Technik. In DACH ist die Gebäudeautomation über viele Hersteller und Integratoren verteilt. Ein Angriff trifft eher einzelne Liegenschaften als eine ganze Kette (Einschätzung).

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 Gewerbekälte verstellt	XWEB-Oberfläche	Ware verdorben, Brandgefahr	151	mittel bis hoch
S2 Heizung/Lüftung Großgebäude	Saia, Sauter, BACnet	Schule, Klinik kalt oder unbelüftet	770	mittel
S3 Licht, Jalousie, Zutritt	Gira HomeServer, KNX	Ausfall, Fehlschaltung, Türen	5.461	mittel
S4 KNX-Anlage gesperrt	KNXnet/IP 3671	Bus umprogrammiert, Neuinstallation	2.458	niedrig bis mittel
S5 Leitstand übernommen	Niagara Fox, Honeywell WEBs	viele Gebäude zugleich verstellt	39	niedrig
S6 Kälte in Laboren und Kliniken	XWEB, Carel pCOWeb	Proben, Medikamente verdorben	151 + 36 unsicher	niedrig bis mittel

Erläuterung je Szenario:

- S1 Gewerbekälte verstellt: Einstieg über Copeland/Dixell XWEB (151 belastbar, Startseite ohne Anmeldung). Der Angreifer setzt nachts Sollwerte hoch oder schaltet auf Dauer-Abtauung, genau wie in Frankreich. Folge: Kühlschränke und Tiefkühltruhen im Markt erwärmen sich, die Ware muss vernichtet werden, laut Staatsanwaltschaft Paris kam es dabei auch zu Entstehungsbränden. Für XWEB Pro sind 23 Schwachstellen veröffentlicht, behoben in Version 1.13 (Claroty Team82, 08/2026). Der Pentagon-Fall (Reuters 29.10.2026, Abtaumodus in mindestens sechs Commissaries Ende August) zeigt dasselbe Muster außerhalb Europas.
- S2 Heizung und Lüftung in Großgebäuden: Einstieg über Saia PCD Web (458), Sauter moduWeb (216, Jetty von 2014) oder BACnet/IP (96). Der Angreifer schaltet Lüftungsanlagen ab, verstellt Heizkreise oder Zeitprogramme. Folge: In Schulen und Kliniken fehlt Frischluft oder Wärme, bei Operationssälen und Reinräumen fällt die Raumluft aus dem Sollbereich, im Winter droht Frostschaden an Lüftungsregistern. Betreiber nicht erhoben, die Einsatzorte stammen aus Herstellerangaben.
- S3 Licht, Jalousie und Zutritt: Einstieg über Gira HomeServer (3.003, ohne TLS, Startseite 200) oder KNXnet/IP (2.458). Der Angreifer schaltet Licht und Jalousien, verstellt Raumtemperaturen oder öffnet über KNX angebundene Türen und Tore, soweit verbaut. Folge: Störung in Büros und Hotels, bei Zutritt ein Sicherheitsproblem. Ob Zutritt und Alarm in den gezählten Anlagen über KNX laufen, ist nicht geprüft.
- S4 KNX-Anlage gesperrt: Über einen offenen KNXnet/IP-Zugang ohne KNX Secure lassen sich Busgeräte technisch umprogrammieren und mit einem Geräteschlüssel sperren (Einschätzung, ein Fall in DACH ist nicht belegt). Folge: Der Elektriker muss Geräte tauschen oder neu programmieren, das Gebäude bleibt tagelang nur eingeschränkt nutzbar.
- S5 Leitstand übernommen: Niagara Fox (DE konservativ 0, AT 25, CH 7) und Honeywell WEBs (7) sind Leitstandsplattformen, die oft mehrere Liegenschaften bündeln. Ein Zugriff dort wirkt auf viele Gebäude gleichzeitig. Die deutsche Zahl ist wegen 125 Hostern und 88 Honeypots unter 152 Rohtreffern unsicher, die Vorarbeit kam ohne Hoster auf 31 bis 41.

- S6 Kälte in Laboren und Kliniken: Dieselben Kältemanager (XWEB, unsicher dazu Carel pCOWeb 36) stehen auch in Laboren, Apotheken und Kliniken (Herstellerangaben). Folge: Proben und temperaturgeführte Medikamente sind verloren. Der Anteil solcher Betreiber ist nicht erhoben.

4. Herstellerlandkarte mit Nischenherstellern

Hersteller	System	Einsatz
Gira	HomeServer 4, X1, FacilityServer	KNX-Visualisierung, Logik
Saia-Burgess (Honeywell)	PCD mit Web-Server	GLT, Heizung, Lüftung
Sauter (CH)	moduWeb, modu525	GLT, Heizzentralen
Elesta (CH)	RCOWeb	Raum- und Gebäudeautomation
Loxone (AT)	Miniserver	Haus- und Gebäudeautomation
Honeywell, Tridium	WEBs, Niagara	GLT-Leitstand
Loytec, Trend	Router, IQ3/IQ4	GLT
Siemens	Desigo, Synco OZW, PXC/PXM	GLT, Heizzentrale
Kieback&Peter	DDC4000	GLT
Copeland/Dixell	XWEB, Site Supervisor	Gewerbekälte
Danfoss	StoreView, AK-SM, AK-SC	Gewerbekälte
Carel	pCOWeb, PlantVisor, boss	Kälte, Klima
ABB, BAB Technologie, NETxAutomation	free@home, eibPort, NETx	KNX, Smart Building
WAGO, Beckhoff	Controller, ADS	SPS in GLT und Industrie

Anbindung und Quelle je Hersteller:

- Gira: Weboberfläche und KNXnet/IP (Shodan-Titel, Herstellerdoku nicht geprüft).
- Saia PCD und Sauter moduWeb: Web und BACnet/IP (Shodan-Titel, Herstellerdoku nicht geprüft).
- Copeland/Dixell XWEB: Weboberfläche, im CERT-FR-Alert genannt (CERTFR-2026-ALE-012, 13.10.2026).
- Danfoss: Weboberfläche StoreView, AK-SM/AK-SC (Danfoss, CERT-FR).
- Siemens Synco OZW und Kieback&Peter DDC4000: Web, Advisories siehe Abschnitt 8 (CISA).
- Niagara, Honeywell WEBs: Fox-Protokoll und Web (Shodan).
- WAGO, Beckhoff: Web-Based Management bzw. ADS, Branche nicht zuordenbar (Shodan).

5. Detailergebnis je Hersteller

Die Zuordnung zu einem Hersteller ist nicht zu 100 % sicher: Sie beruht auf Webtitel, Produktkennung, Protokoll und einer Gegenprobe über ein zweites Merkmal. „Belastbar“ geht in die Summen ein, alle anderen Zeilen nicht. Länderwerte nach Abzug, Regionen ohne Abzug.

Sicherheit	Hersteller/Gruppe	DE	AT	CH	Bayern	Salzburg	Tirol
belastbar	Gira HomeServer, X1, FacilityServer	2.612	337	54	491	53	39
belastbar	Saia PCD Web	154	114	190	31	58	13
belastbar	Sauter moduWeb	121	60	35	20	unter 5	15
belastbar	Copeland/Dixell XWEB (Kälte)	100	49	unter 5	19	unter 5	5
belastbar	Elesta RCOWeb	90	unter 5	19	unter 5	0	0
belastbar	Loxone Miniserver (Produkt)	8	7	5	unter 5	unter 5	unter 5
belastbar	Honeywell WEBs (Niagara)	6	0	unter 5	7	0	0
belastbar	Danfoss StoreView (Kälte)	0	unter 5	0	unter 5	0	0
belastbar	Trend IQ3	unter 5	0	0	0	0	0
belastbar	Loytec	unter 5	unter 5	unter 5	0	0	unter 5
belastbar	**Summe Web/Hersteller**	**3.094**	**575**	**307**	**575**	**119**	**74**
belastbar	KNXnet/IP 3671	1.134	853	471	295	55	53
belastbar	BACnet/IP mit Banner	31	32	33	12	unter 5	8
belastbar	Niagara Fox	0	25	7	12	10	0
belastbar	**Summe Protokolle**	**1.165**	**910**	**511**	**319**	**69**	**61**
unsicher	NETxAutomation	58	7	9	nicht erhoben		
unsicher	ABB free@home	18	unter 5	0	unter 5	0	0
unsicher	eibPort	17	unter 5	unter 5	7	0	0
unsicher	Carel pCOWeb (Kälte)	10	15	11	8	7	0
unsicher	Kieback&Peter (Text)	5	7	unter 5	0	0	unter 5
unsicher	LON/IP-852	unter 5	0	unter 5	0	0	0
unsicher	Siemens Desigo	unter 5	unter 5	unter 5	unter 5	0	0
unsicher	Distech ECLYPSE	unter 5	0	0	0	0	0
nicht gezählt	Siemens Synco OZW (Abfragefehler)	nicht gezählt					

- Geprüft, aber nicht gezählt (überwiegend Hoster, Firmen-IT, Honeypots oder Namensgleiche): Loxone (Text), Priva (Text), iSMA, GFR (Text), Neuberger (Text), DEOS (Text), Siemens PXG3, BACnet mit HikCentral.

Zugriffsart, alte Versionen, vuln (Rohwerte DACH):

- Gira: 3.028 roh, alle ohne TLS, Startseite 200 bei 3.023. Titel-Facette zu 99 % Produkttitel (HomeServer 4 2.366, X1 211, FacilityServer 4 201).
- Saia PCD Web: 458 roh, 99 % bestätigt, alle 200, alle ohne TLS.
- Sauter moduWeb: 216 roh, 100 % bestätigt, alle 200, ohne TLS. Jetty 7.6.16 (2014) bei 75 (DE-Facette).
- Copeland/Dixell XWEB: 155 roh (Titel XWEB, EVO, PRO), nur 4 Hoster, 200 bei 154, ohne TLS. Shodan-vuln bei 9 DE und 40 AT. Im CERT-FR-Alert seit 13.10.2026.
- Elesta: 113 roh, 82 % mit Titel bestätigt, 200 bei 89, 401 bei 4.
- Honeywell WEBs: 59 roh, davon 52 in DE bei Hostern, 200 bei 46.
- Danfoss StoreView: 354 roh, Abzug siehe Abschnitt 2.3.

- KNXnet/IP: 2.463 roh, ohne TLS, kein KNX Secure erkennbar (Vorarbeit).
- BACnet/IP: 123 roh mit Banner, 22 davon HikCentral (Videosystem, ausgeschlossen). Erkennbare Produkte u. a. Kieback&Peter DDC4000, Siemens PXC/PXM.
- Niagara Fox: 186 roh. DE 152 roh, davon 125 Hoster und 88 Honeypot-Markierung, deshalb konservativ 0. Die Vorarbeit kam ohne Hoster auf 31 bis 41, davon Niagara AX 3.7/3.8. Version 3.7.44 bei 122.
- Fremdtreffer: Loxone Text 1.179 roh (2 % bestätigt), Priva Text 1.350 roh (2 %), iSMA 77 (4 %, 32 Hoster), GFR 89 (überwiegend OpenSSH), NETxAutomation 124 roh (Produktfacette zeigt u. a. HP iLO, deshalb unsicher).

6. Branche unklar: Fernzugänge und generische Protokolle

Rohwerte, nicht in den Summen. Fernwartungsrouter und Protokolle aus dem Report „Wasser und Abwasser“ (Abschnitt 6), WAGO und Beckhoff aus dem Lauf Gebäudeautomation.

Gruppe	DE	AT	CH	Bewertung
WAGO Web-Based Management	173	16	24	Produkt belastbar
Beckhoff ADS 48898	24	0	25	Branche unklar
Beckhoff (Text)	8	unter 5	6	unsicher
Phoenix Contact TC ROUTER	186	11	10	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
Modbus/TCP 502	1.197	123	159	Branche unklar
Siemens S7 102	206	69	unter 5	Branche unklar
CODESYS 2455	55	5	27	Branche unklar
OPC UA 4840	42	5	unter 5	Branche unklar

Hinweise:

- WAGO-Controller und Beckhoff-Steuerungen sind in der Gebäudeautomation verbreitet, aber ebenso in Maschinen und Wasserwirtschaft. Der Anteil Gebäude ist mit Shodan nicht bestimmbar.
- 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).
- Organisationen, Seitentitel und Zertifikatsinhalte wurden ausgewertet, aber bewusst nicht aufgeführt. Gruppen unter 5 Diensten in einer Region nennen wir im ganzen Report nur als „unter 5“ oder „einzelne“.
- Modbus: zusätzlich 569 Dienste mit Honeypot-Markierung (DE 383, CH 185), ausgeschlossen.
- Weitere geprüfte Einzelgruppen mit sehr kleinen Zahlen (je unter 5): Wiesemann & Theis Web-IO, Belimo (Text).

7. Risikomatrix

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

Gruppe	DACH	Nähe zu Danfoss	Szenario	Risiko
Copeland/Dixell XWEB	151	sehr eng: gleiche Geräteklasse	S1, S6	hoch
Saia PCD Web	458	eng: offen, ohne TLS	S2	hoch
Sauter moduWeb	216	eng: Webserver 2014	S2	mittel bis hoch
KNXnet/IP	2.458	mittel: Protokoll ohne Anmeldung	S3, S4	mittel bis hoch
Gira HomeServer	3.003	mittel: offen, ohne TLS	S3	mittel
Niagara Fox, Honeywell WEBs	39	mittel: Niagara AX alt	S5	mittel
Elesta RCOWeb	112	gering bis mittel	S2	mittel
BACnet/IP	96	mittel	S2	mittel
Danfoss StoreView	unter 5	gleiche Geräteklasse	S1	niedrig (kaum echt)
Loxone, Loytec, Trend	30	gering	S3	niedrig
WAGO, Beckhoff (Branche unklar)	262	nicht bewertbar	S2	nicht bewertbar

Begründung:

- XWEB hoch: im CERT-FR-Alert namentlich genannt, 23 veröffentlichte Schwachstellen in XWEB Pro, Startseite ohne Anmeldung, kein TLS, kaum Hoster. Das ist der Danfoss-Fall in anderer Marke.
- Saia hoch: 458 Dienste, alle ohne TLS und mit antwortender Startseite, Einsatz in Liegenschaften mit vielen Menschen. Die Advisory-Lage ist nicht geprüft.
- Sauter: Webserver von 2014, Heizzentralen und Lüftung größerer Gebäude.
- KNXnet/IP: große Zahl und kein KNX Secure erkennbar. Folge meist Störung und Aufwand, selten Gefahr für Menschen.
- Gira: größte Gruppe, aber überwiegend Wohnen und kleines Gewerbe, Schaden je Anlage begrenzt (Einschätzung).
- Einschätzung gesamt: Gut 6.500 offen erreichbare Gebäudeautomations-Dienste in DACH, davon 151 aus genau der Geräteklasse, die in Frankreich und am 02.11.2026 in fünf weiteren Ländern angegriffen wurde. Das ist die direkteste Übertragung des Frankreich-Musters aller drei Reports.

8. Belegte Vorfälle und Advisories

Datum	Ort	Vorfall
11./12.10.2026	Frankreich	Kühlsteuerungen, rund 700 Märkte
02.11.2026	BE, SE, LU, IE, EE	zweite Welle Supermarktkälte
Ende 08/2026	USA	Gefriertruhen auf Militärbasen
18.10.2026	Österreich	Angriff auf IT von Loxone
22.10.2026	weltweit	Forescout: 12.976 Kältedienste offen

Was passiert ist und Quelle:

- 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.

- Zweite Welle (02.11.2026): manipulierte Kühl- und Tiefkühlanlagen in Supermärkten in Belgien, Schweden, Luxemburg, Irland und Estland, Angriffsversuche in der Schweiz abgewehrt. Danfoss StoreView und Copeland/Dixell XWEB laut Forescout bei Euronews, je Kette nicht bestätigt (Vorfall-Lagebild OT-Cyber).
- USA (Ende August 2026): Reuters berichtet am 29.10.2026, das Pentagon behandle Ausfälle von Kühlschränken und Gefriertruhen in mindestens sechs Commissaries auf Militärbasen als mutmaßlichen Hack, die Anlagen liefen im Abtaumodus. US Cyber Command ermittelt mit (Vorfall-Lagebild OT-Cyber).
- Loxone (18.10.2026): Der Hersteller meldet einen Cyberangriff auf interne Unternehmenssysteme, Kundeninstallationen laufen laut Hersteller weiter. Ein behaupteter Datenabfluss ist vom Hersteller nicht bestätigt (Vorfall-Lagebild OT-Cyber).
- Forescout (22.10.2026): 12.976 exponierte Dienste von Kältesteuerungen auf 6.017 IP-Adressen in 99 Ländern, davon 7.075 Copeland/Dixell XWEB. Shadowserver sah zuletzt 1.173 Copeland XWEB Pro/Evo (Vorfall-Lagebild OT-Cyber).
- DACH: Eingriffe in Gebäudeautomation oder Gewerbekälte sind öffentlich nicht belegt (Recherche 02.11.2026).

Advisories:

- Copeland XWEB Pro: 23 Schwachstellen, davon 21 hoch, behoben in Version 1.13 (Claroty Team82, 08/2026).
- Danfoss AK-SM 800A: CVE-2025-41450 bis 41452 (Claroty Team82, 09.08.2026), behoben ab Firmware R4.3.1.
- 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.
- Viessmann Vitogate 300: CVE-2025-9494/9495 (ICSA-25-266-04), behoben mit Firmware 3.1.0.1.
- Zu Gira HomeServer, Saia PCD, Sauter moduWeb, Elesta und KNXnet/IP ist die Advisory-Lage für diesen Report nicht geprüft.

9. Regionallage Bayern, Salzburg, Tirol

Region	Web/Hersteller	Protokolle	Summe
Bayern	575	319	894
Salzburg	119	69	188
Tirol	74	61	135

- Bayern: Gira 491, KNXnet/IP 295, Saia 31, Sauter 20, XWEB 19, BACnet 12, Niagara Fox 12, Honeywell WEBs 7. Bayern stellt 19 % der Gira-Dienste in Deutschland.
- Salzburg: Saia 58 (über die Hälfte der österreichischen Saia-Dienste), KNXnet/IP 55, Gira 53, Niagara Fox 10, dazu einzelne XWEB- und Loxone-Dienste.
- Tirol: KNXnet/IP 53, Gira 39, Sauter 15 (ein Viertel der österreichischen Sauter-Dienste), Saia 13, BACnet 8, XWEB 5.
- Grenzregion: Die Häufung von Saia in Salzburg und Sauter in Tirol deutet auf Liegenschaften mit klassischer GLT hin, etwa Hotels, Seilbahnen, Schulen und Kliniken (Einschätzung, Betreiber nicht erhoben). Kälte über XWEB: 27 Dienste in den drei Regionen.
- Regionen sind ohne Abzug gezählt, deshalb können einzelne Regionswerte über dem Länderwert liegen (Honeywell WEBs Bayern 7 gegen DE 6, bei Danfoss einzelne in Bayern gegen DE 0).

10. Empfehlungen nach SANS Five ICS Critical Controls

- CC1 ICS Incident Response: Für Kälteanlagen in Märkten und Laboren eine nachts erreichbare Rufbereitschaft beim Kältefachbetrieb und eine Temperaturalarmierung unabhängig vom Systemmanager festlegen. Danfoss-Lehre: Der Angriff lief nachts, entdeckt wurde er erst morgens (Berichte vom 12.10.2026). Für GLT: Handbetrieb von Heizung und Lüftung dokumentieren, KNX-Projektdatei und Gerätepasswörter offline sichern.
- CC2 Defensible Architecture: Keine Portfreigabe für XWEB, StoreView, Saia, Sauter, Gira HomeServer und KNXnet/IP. CERT-FR: Geräte ohne Sicherheitsupdates gehören gar nicht ins Internet (CERTFR-2026-ALE-012). GLT-Netz vom Büro- und Gästenetz trennen.
- CC3 ICS Network Visibility & Monitoring: Facility Manager, Kältefachbetriebe und Integratoren gleichen ihre Anlagen regelmäßig mit Shodan-Daten ab. Sollwertänderungen, Abtaubefehle außerhalb des Plans und KNX-Programmierzugriffe als Sicherheitsereignis behandeln.
- CC4 Secure Remote Access: Fernwartung nur über VPN mit Mehrfaktor-Anmeldung, so wie CERT-FR es nach dem Danfoss-Angriff fordert. HTTP abschalten, Werkspasswörter ändern, KNX Secure nutzen, wo die Geräte es können.
- CC5 Risk-Based Vulnerability Management: Zuerst XWEB auf Version 1.13 oder neuer und AK-SM 800A auf R4.3.1, Altgeräte ohne Updates ersetzen. Dann Sauter moduWeb (Jetty von 2014) und Niagara AX, danach Synco OZW, DDC4000 und Vitogate 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. Bei Kälte die Abtauzeiten, bei GLT Sollwerte und Zeitprogramme prüfen.

11. Regulatorischer Bezug

- NIS2 Deutschland: NIS2UmsuCG in Kraft seit 06.12.2025 (usd.de, secjur.com). Krankenhäuser und große Lebensmittelhändler können erfasst sein, die Gebäudeautomation ist dann Teil ihrer Risikomaßnahmen. Für Wohngebäude und kleines Gewerbe meist nicht einschlägig (Einschätzung).
- Österreich: NISG 2026 in Kraft seit 01.10.2026 (WKO). Schweiz: Meldepflicht an das BACS seit 01.04.2025.
- CRA (VO (EU) 2024/2847): KNX-Server, GLT-Stationen und Kältemanager mit Netzanbindung sind Produkte mit digitalen Elementen. Hersteller müssen Updates über die Lebensdauer liefern und Schwachstellen melden. Für Altgeräte gilt der CRA nicht rückwirkend (Vorfall-Lagebild OT-Cyber). Eine Einstufung in Anhang III ist nicht geprüft.
- BSI-CS 154 (13.10.2026): Empfehlung des BSI nach dem Danfoss-Angriff, ausdrücklich für Betreiber kleiner Anlagen, etwa Lebensmittelkühlung (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 (Titel, Favicon, Produktkennung, Protokoll-Banner). Rechenweg im internen Zählprotokoll dokumentiert.
- Abzug je Land (Hoster, Herstellerfirma, Honeypot). Regionen ohne Abzug. Länderwerte im Ländervergleich sind die exakte Summe der Herstellerzeilen.
- Web/Hersteller und Protokolle werden getrennt gezählt, ein Gerät kann in beiden vorkommen.
- 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 und Anlagen hinter VPN sind auf Shodan unsichtbar.
- Siemens Synco OZW konnte wegen eines Abfragefehlers (HTTP 429) nicht gezählt werden.
- Danfoss-Angaben stammen ausschließlich aus unseren Vorfall-Lagebildern und dem Blog „Hacker heizen Kühlschränke“ auf ot-cyber.de mit den dort genannten Quellen. Die Übertragung auf Gebäudeautomation ist unsere Einschätzung.
- 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.

12.1 Zählprotokoll: Rechenweg und wichtigste Gruppen

Gruppe	DACH roh	Gegenprobe	Bewertung	zählt
Gira HomeServer, X1, FacilityServer	3.028	99 % Produkttitel	belastbar	3.003
KNXnet/IP 3671	2.463	Protokoll	belastbar	2.458
Saia PCD Web	458	99 %	belastbar	458
Danfoss StoreView	354	Hoster/Honeypot	belastbar netto	unter 5
Sauter moduWeb	216	100 %	belastbar	216
Niagara Fox	186	Protokoll	belastbar konservativ	32
Copeland/Dixell XWEB	155	Titel, 4 Hoster	belastbar	151
BACnet/IP mit Banner	123	ohne HikCentral	belastbar	96
Elesta RCOWeb	113	82 % Titel	belastbar	112

Bewertungsregeln und Rechenweg:

- Belastbar: zweites Merkmal bestätigt (Schnittmenge mindestens 50 % bei Text, mindestens 30 % bei Titel), starkes Merkmal (Zertifikat, Produkt, Protokoll-Banner) 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.
- Web/Hersteller: Gira 3.003 + Saia 458 + Sauter 216 + XWEB 151 + Elesta 112 + Loxone 20 + Honeywell WEBs 7 + Loytec 5 + Danfoss und Trend je unter 5 = 3.976.
- Protokolle: KNXnet/IP 2.458 + BACnet/IP 96 + Niagara Fox 32 = 2.586.
- Gesamt: 3.976 + 2.586 = 6.562.
- Unsicher, nicht in der Summe: NETxAutomation 74, Carel pCOWeb 36, eibPort 22, ABB free@home 20, Kieback&Peter 15, LON/IP-852 5, Siemens Desigo 5, Distech ECLYPSE unter 5.

13. Hersteller ohne belastbare Treffer

- Fremdtreffer: Loxone (Text), Priva (Text), iSMA, GFR, Neuberger, DEOS, Weinzierl, Siemens PXG3, BACnet mit HikCentral (Videosystem), Niagara Web-Titel, COMEXIO (Text), RESOL (Text, Namensgleiche).
- Nur unsicher: NETxAutomation, Carel pCOWeb, eibPort, ABB free@home, Kieback&Peter (Text), LON/IP-852, Siemens Desigo, Distech ECLYPSE.
- Ohne Treffer (02.11.2026): Johnson Controls Metasys, Schneider Electric EcoStruxure Building und SmartStruxure, Honeywell Excel Web, Viessmann Vitogate, Jung Smart Visu, Kieback&Peter DDC4000 (Titel), Carel PlantVisor und boss, Danfoss AK-SM, Trend IQ4 (Titel), Dixell (Text), Eliwell, Wurm Frigolink, Trane Tracer SC, Eckelmann E*LDS (netto 0), Technische Alternative C.M.I., Stiebel Eltron ISG, TROX X-AIRCONTROL, Hoval (netto 0), Gira HomeServer (Text), Wiesemann & Theis Web-Thermometer.
- Nicht gezählt (Abfragefehler): Siemens Synco OZW.