CRA SAMPLE

D07 Cybersecurity risk assessment

Example after one year of operation, status 28.02.2028 · Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect

Publisher	OT-Cyber.de, Max Gilg, Rosenheim
Sample company	Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect (fictitious)
Note	Free sample, not legal advice

Company, people, data and numbers are fictitious. This is how the document looks after one year of operation.

1 Purpose and scope

Risk assessment under Article 13 CRA and IEC 62443-3-2, with evidence for MR Annex III, sections 1.1.9 and 1.2.1: no attack via the network or portal can defeat a safety function. R = L × I, acceptable up to 4.

2 Document control

Field	Entry
Document no.	NWT-CE-D07
Version, status	1.6, approved
Scope	NWT HACKTHERM 60 connect (18 to 60 kW), controller, gateway, portal and app
Author	Jonas Weiß, Engineering and Product Security (PSO)
Checked by	Ingenieurbüro Lechner (safety), Sichtwerk Security (security)
Approval	Michael Berger, Managing Director, 28.02.2028
Next review	15.03.2029 or in the event of a substantial modification
Confidentiality	internal
Filing	Technical documentation NWT-TD-HT60C, retained for at least 10 years after the last unit is placed on the market

3 Scope of the assessment

Intended use: Heat generation in the boiler room, remote access for convenience functions only (D03)

Operating environment: Boiler rooms in commercial, municipal, agricultural and local heating network settings; customer network not trusted; portal hosted in a cloud within the EU

Assets: Safety functions SF1 to SF10, F program, setpoints, customer accounts, operating data, device certificates, signing keys, update chain

Service life: 15 to 20 years per boiler; threats assessed over this period (D15)

Method: R = L × I, L and I each 1 to 4; acceptable up to 4, because up to this level no path leads to a safety function (cyber safety evidence below); threshold approved by management on 20.01.2027

Annex I, Part I: For each of points (2)(a) to (m), F01 records whether it applies and how it is implemented (Article 13(3) CRA)

4 Threats and measures

How to read the table

Each row is a threat to the boiler, gateway, portal or app. R0 is the risk without measures, R1 the risk with measures, in each case likelihood times impact, both rated from 1 to 4. Any R1 above 4 requires further measures. The Reference column shows which CRA requirement the measure fulfils.

ID	Threat	Path	R0	Measures	R1	Reference
C01	Customer account takeover	Internet	9	MFA, rate limiting	4	I 2 d
C02	Gateway vulnerability exploited	Internet	8	no open ports, patches	4	I 2 a, j
C03	Tampered update	Supply chain	8	Signature, Secure Boot	4	I 2 f
C04	Portal sends mass commands	Cloud	8	Limits in F section, authorisation	4	I 2 h, k
C05	Malware from customer network	LAN	9	Firewall, no inbound connections	3	I 2 i, j
C06	Local engineering access	physical	8	Seal, F password	4	MR 1.1.9
C07	Malware via USB	local	6	signed packages only	3	I 2 j
C08	Gateway overload	Network	6	Control system autonomous	2	I 2 h
C09	Data interception	Network	4	TLS 1.3, minimisation	2	I 2 e, g
C10	Misuse of service access	Portal	8	Authorisation, MFA, time limit	4	I 2 d, l
C11	Weak passwords	local	9	Unique secret per device	3	I 2 b
C12	Vulnerability in third-party component	all	9	SBOM, monitoring, P07	3	II 1 to 3
C13	Writing via Modbus	LAN	6	read-only	2	I 2 j
C14	Theft of signing key	internal	4	HSM, four-eyes principle; residual risk consciously accepted	4	I 2 f
C15	Logs tampered with	local	6	append-only, copy	3	MR 1.1.9
C16	Maintenance authorisation obtained by deception	Portal	8	Authorisation only in operator's app	4	I 2 d

Legend: C = cyber threat; R0 = risk before measures; R1 = risk after measures, R = L × I with L = likelihood 1 to 4 and I = impact 1 to 4, acceptable up to 4; Reference = CRA requirement, e.g. "I 2 d" = Annex I, Part I, point (2)(d).

C14 remains at 4: the key is stored in the HSM and used only under the four-eyes principle; a lower value cannot be achieved with reasonable effort. Even a stolen key cannot reach a safety function, because the F program is not modified via the update chain. Accepted by management on 28.02.2028.

5 Cyber safety evidence

Worst case: an attacker has full control of the portal and gateway. Even then, they can only change convenience setpoints within fixed limits. SF1 to SF10 remain effective, because Z1 has no external connection, the F program checks limit values and no motion command is executed without local acknowledgement. Verified in the penetration tests 02/2027 and 02/2028 (Sichtwerk).

Assessment round	Trigger	Result
28.06.2027	NWT-VULN-2027-004 (MQTT library)	C12 confirmed, daily monitoring
20.10.2027	Actively exploited portal vulnerability (NWT-VULN-2027-006)	C04 and C10 checked, limits held
20.11.2027	New maintenance authorisation	C16 added, R1 = 4

6 Terms and abbreviations

CRA: Cyber Resilience Act, Regulation (EU) 2024/2847

HSM: hardware security module, protects the signing keys

LAN: local area network

MFA: multi-factor authentication

MQTT: messaging protocol between device and portal

MR: Machinery Regulation (EU) 2023/1230, applies from 20 January 2027

NWT: abbreviation of the sample company in document and ticket numbers

SBOM: software bill of materials: which components in which version

SF: safety function

TLS: encryption of the connection

USB: USB port

VULN: vulnerability ticket (number range)

7 Revision history and approval

Version	Date	Change	Approval
1.0	20.01.2027	Initial assessment	M. Berger
1.1	15.03.2027	Approval for placing on the market	M. Berger

Version	Date	Change	Approval
1.2	28.06.2027	Reassessed following NWT-VULN-2027-004	M. Berger
1.3	20.10.2027	Following actively exploited vulnerability in the portal (F06)	M. Berger
1.4	20.11.2027	Maintenance authorisation in the portal assessed (Gateway 1.5.0)	M. Berger
1.5	28.02.2028	Scope of the assessment (Article 13(3)), acceptance of C14	M. Berger
1.6	28.02.2028	Reading guide for the table	M. Berger

Approved: Michael Berger, Managing Director, 28.02.2028 (signed in the original). Free sample from OT-Cyber.de, not legal advice. Company, persons, serial numbers and data are entirely fictitious.