CRA SAMPLE

F02 Supplier and component 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

Due diligence for third party components (Article 13(5) CRA): assessment of suppliers and components with regard to security, support throughout the support period and vulnerability status. Annually and on change (P05).

2 Document control

Field	Entry
Document no.	NWT-CE-F02
Version, status	1.3, 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 Supplier and component assessment: overview

Component	Supplier	Support until	Vulnerabilities 2027	Rating
Safety controller	Controller manufacturer	2037, successor planned	1 medium, patched	A
Gateway hardware	Datenwerk	2034, redesign 2033	none	A
Gateway operating system	Linux with long term support	annual major version	4, all patched	A
MQTT library	Open source project	actively maintained	1 high (NWT-VULN-2027-004)	B, daily monitoring
TLS library	Open source project	long term branch	2, patched	A
Portal platform	Datenwerk, cloud in the EU	ongoing	1 actively exploited (NWT-VULN-2027-006)	B, measures
App	Datenwerk	ongoing	none	A
Signing HSM	Datenwerk, service	contract until 2032	none	A

Criteria: Supplier's security process, origin and maintenance of the component, support throughout the support period or planned replacement, vulnerability status, reporting channels to us

Rating: A without conditions, B with conditions, C not approved

Conditions B: MQTT library: daily monitoring, replacement review 2028; portal: additional web application firewall rules, external test per major version

4 Terms and abbreviations

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

HSM: hardware security module, protects the signing keys

MQTT: messaging protocol between device and portal

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

TLS: encryption of the connection

VULN: vulnerability ticket (number range)

5 Revision history and approval

Version	Date	Change	Approval
1.0	10.12.2026	Initial assessment	M. Berger
1.1	15.03.2027	Status at placing on the market	M. Berger
1.2	20.11.2027	Annual assessment	M. Berger
1.3	28.02.2028	Criterion: support throughout the support period	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.