CRA-MUSTER

D07 Cybersecurity-Risikobewertung

Beispiel nach einem Jahr Betrieb, Stand 28.02.2028 · Nordwald Wärmetechnik GmbH, vernetzter Hackgutkessel NWT HACKTHERM 60 connect

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Musterbetrieb	Nordwald Wärmetechnik GmbH, vernetzter Hackgutkessel NWT HACKTHERM 60 connect (frei erfunden)
Hinweis	Kostenfreies Muster, keine Rechtsberatung

Firma, Personen, Daten und Nummern sind frei erfunden. So sieht das Dokument nach einem Jahr gelebtem Betrieb aus.

1 Zweck und Geltungsbereich

Risikobewertung nach Art. 13 CRA und IEC 62443-3-2, mit Nachweis zu MVO Anhang III 1.1.9 und 1.2.1: Kein Angriff über Netz oder Portal hebelt eine Sicherheitsfunktion aus. R = L × I, akzeptabel bis 4.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	NWT-CE-D07
Version, Status	1.6, freigegeben
Geltungsbereich	NWT HACKTHERM 60 connect (18 bis 60 kW), Steuerung, Gateway, Portal und App
Ersteller	Jonas Weiß, Technik und Product Security (PSO)
Geprüft	Ingenieurbüro Lechner (Safety), Sichtwerk Security (Security)
Freigabe	Michael Berger, Geschäftsführer, 28.02.2028
Nächste Prüfung	15.03.2029 oder bei wesentlicher Änderung
Vertraulichkeit	intern
Ablage	Technische Dokumentation NWT-TD-HT60C, aufbewahrt bis mindestens 10 Jahre nach Inverkehrbringen der letzten Einheit

3 Rahmen der Bewertung

Bestimmungsgemäße Verwendung: Wärmeerzeugung im Heizraum, Fernzugriff nur für Komfortfunktionen (D03)

Einsatzumgebung: Heizräume von Gewerbe, Kommunen, Landwirtschaft und Nahwärme; Kundennetz nicht vertrauenswürdig; Portal in einer Cloud in der EU

Werte: Sicherheitsfunktionen SF1 bis SF10, F-Programm, Sollwerte, Kundenkonten, Betriebsdaten, Gerätezertifikate, Signierschlüssel, Update-Kette

Nutzungsdauer: 15 bis 20 Jahre je Kessel; Bedrohungen über diese Zeit bewertet (D15)

Methode: R = L × I, L und I je 1 bis 4; akzeptabel bis 4, weil bis dahin kein Weg zu einer Sicherheitsfunktion führt (Cyber-Safety-Nachweis unten); Grenze von der Geschäftsführung freigegeben am 20.01.2027

Anhang I Teil I: Zu jedem Punkt 2 a bis m ist in F01 festgehalten, ob er gilt und wie er umgesetzt ist (Art. 13 Abs. 3 CRA)

4 Bedrohungen und Maßnahmen

So lesen Sie die Tabelle

Jede Zeile ist eine Bedrohung für Kessel, Gateway, Portal oder App. R0 ist das Risiko ohne Maßnahmen, R1 mit Maßnahmen, jeweils Wahrscheinlichkeit mal Auswirkung, beides von 1 bis 4. Ab einem R1 über 4 braucht es weitere Maßnahmen. Die Spalte Bezug zeigt, welche Anforderung des CRA die Maßnahme erfüllt.

ID	Bedrohung	Weg	R0	Maßnahmen	R1	Bezug
C01	Übernahme Kundenkonto	Internet	9	MFA, Ratenbegrenzung	4	I 2 d
C02	Lücke im Gateway ausgenutzt	Internet	8	keine offenen Ports, Patches	4	I 2 a, j
C03	Manipuliertes Update	Lieferkette	8	Signatur, Secure Boot	4	I 2 f
C04	Portal sendet Massenbefehle	Cloud	8	Grenzen im F-Teil, Freigabe	4	I 2 h, k
C05	Schadsoftware aus Kundennetz	LAN	9	Firewall, kein Eingang	3	I 2 i, j
C06	Lokaler Engineering-Zugriff	physisch	8	Plombe, F-Passwort	4	MVO 1.1.9
C07	Schadsoftware per USB	lokal	6	nur signierte Pakete	3	I 2 j
C08	Überlastung Gateway	Netz	6	Steuerung autark	2	I 2 h
C09	Abhören von Daten	Netz	4	TLS 1.3, Minimierung	2	I 2 e, g
C10	Missbrauch Servicezugang	Portal	8	Freigabe, MFA, Zeitlimit	4	I 2 d, l
C11	Schwache Passwörter	lokal	9	Geheimnis je Gerät	3	I 2 b
C12	Lücke in Fremdkomponente	alle	9	SBOM, Monitoring, P07	3	II 1 bis 3
C13	Schreiben über Modbus	LAN	6	nur lesend	2	I 2 j
C14	Diebstahl Signierschlüssel	intern	4	HSM, Vier-Augen; Rest bewusst angenommen	4	I 2 f
C15	Protokolle manipuliert	lokal	6	nur anhängen, Kopie	3	MVO 1.1.9
C16	Wartungsfreigabe erschlichen	Portal	8	Freigabe nur in App des Betreibers	4	I 2 d

Legende: C = Cyber-Bedrohung; Weg = Angriffsweg; R0 = Risiko vor den Maßnahmen; R1 = Risiko nach den Maßnahmen, jeweils R = L × I mit L = Wahrscheinlichkeit 1 bis 4 und I = Auswirkung 1 bis 4 (4 = Gefahr für Personen oder die ganze Flotte), akzeptabel bis 4; Bezug = Anforderung im CRA, z. B. „I 2 d“ = Anhang I Teil I Nr. 2 Buchst. d.

C14 bleibt bei 4: Der Schlüssel liegt im HSM und wird nur nach dem Vier-Augen-Prinzip genutzt; weniger ist mit vertretbarem Aufwand nicht erreichbar. Selbst ein gestohlener Schlüssel erreicht keine

Sicherheitsfunktion, weil das F-Programm nicht über die Update-Kette geändert wird. Annahme durch die Geschäftsführung am 28.02.2028.

5 Cyber-Safety-Nachweis

Schlimmster Fall: Ein Angreifer kontrolliert Portal und Gateway vollständig. Dann kann er nur Komfortsollwerte in festen Grenzen ändern. SF1 bis SF10 bleiben wirksam, weil Z1 keine Verbindung nach außen hat, das F-Programm Grenzwerte prüft und kein Bewegungsbefehl ohne lokale Quittierung ausgeführt wird. Geprüft im Pentest 02/2027 und 02/2028 (Sichtwerk).

Bewertungsrunde	Anlass	Ergebnis
28.06.2027	NWT-VULN-2027-004 (MQTT-Bibliothek)	C12 bestätigt, Monitoring täglich
20.10.2027	Aktiv ausgenutzte Lücke Portal (NWT-VULN-2027-006)	C04 und C10 geprüft, Grenzen hielten
20.11.2027	Neue Wartungsfreigabe	C16 neu, R1 = 4

6 Begriffe und Abkürzungen

CRA: Cyber Resilience Act, EU-Verordnung 2024/2847

HSM: Hardware-Sicherheitsmodul, schützt die Schlüssel zum Signieren

LAN: lokales Netzwerk

MFA: Anmeldung mit zweitem Faktor, z. B. Code aufs Handy

MQTT: Nachrichtenprotokoll zwischen Gerät und Portal

MVO: Maschinenverordnung (EU) 2023/1230, gilt ab 20.01.2027

NWT: Kürzel des Musterbetriebs in Dokument- und Ticketnummern

SBOM: Stückliste der Software: welche Bausteine in welcher Version enthalten sind

SF: Sicherheitsfunktion

TLS: Verschlüsselung der Verbindung

USB: USB-Anschluss

VULN: Schwachstellenticket (Nummernkreis)

7 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.01.2027	Erstbewertung	M. Berger
1.1	15.03.2027	Freigabe zum Inverkehrbringen	M. Berger

Version	Datum	Änderung	Freigabe
1.2	28.06.2027	Nach NWT-VULN-2027-004 neu bewertet	M. Berger
1.3	20.10.2027	Nach aktiv ausgenutzter Lücke im Portal (F06)	M. Berger
1.4	20.11.2027	Wartungsfreigabe im Portal bewertet (Gateway 1.5.0)	M. Berger
1.5	28.02.2028	Rahmen der Bewertung (Art. 13 Abs. 3), Annahme C14	M. Berger
1.6	28.02.2028	Lesehilfe zur Tabelle	M. Berger

Freigegeben: Michael Berger, Geschäftsführer, 28.02.2028 (im Original unterschrieben). Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Firma, Personen, Seriennummern und Daten frei erfunden.