CRA-MUSTER

Verfahren: Vernetzte Hackschnitzelheizung

Nach Maschinenverordnung und Cyber Resilience Act

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Beispiel	Nordwald Wärmetechnik GmbH (fiktiv), zwei Personen
Hinweis	Kostenfreies Muster, keine Rechtsberatung

Firmen, Personen und Daten sind frei erfunden. Reale Produkte dienen nur als technische Referenz.

1 So nutzen Sie das Verfahren

Gehen Sie die neun Schritte der Reihe nach durch. Zu jedem Schritt gibt es die passenden Dokumente zweimal: als leere Vorlage und als ausgefülltes Muster am Beispiel der Nordwald Wärmetechnik GmbH. Alle Dateien: ot-cyber.de/muster/cra-hackschnitzelheizung/

1.1 Das Beispiel

Nordwald Wärmetechnik GmbH (fiktiv) besteht aus zwei Personen: Michael Berger, Heizungsbaumeister und Geschäftsführer, und Jonas Weiß, Mechatroniker mit Schwerpunkt Steuerungstechnik. Der Betrieb bringt den Hackgutkessel NWT HACKTHERM 60 connect (18 bis 60 kW, Kesselklasse 5) unter eigener Marke in Verkehr und ist damit Hersteller. Gefertigt und entwickelt wird mit Partnern.

Partner	Leistung
Kesselbau Alpenrand GmbH	Kesselkörper, Austragung, Zellradschleuse
Schaltanlagen Hofer GmbH	Schaltschrank, Stückprüfung EN 60204-1
Datenwerk Embedded GmbH	Gateway, Portal, App, SBOM, Updates
Ingenieurbüro Lechner	PL-Berechnung, Validierung
Sichtwerk Security GmbH	Pentest, PSIRT-Bereitschaft, Meldeplattform
Prüfinstitut Feuerungstechnik Süd	Typprüfung EN 303-5, EMV

Die Partner liefern Leistungen. Die Pflichten aus Maschinenverordnung und CRA bleiben beim Hersteller und werden über Verträge, Meldewege und Nachweise abgesichert (D02, F03).

1.2 Fristen

Wann	Was
seit 11.09.2026	Meldepflicht nach Art. 14 CRA, auch für Produkte, die schon ausgeliefert sind
bis 19.01.2027	Maschinenrichtlinie 2006/42/EG
ab 20.01.2027	Maschinenverordnung (EU) 2023/1230
ab 11.12.2027	CRA vollständig, CE-Kennzeichnung auch nach CRA

2 Schritt 1: Einstufen

Gelten Maschinenverordnung und CRA, und sind wir Hersteller?

Wer: Berger (GF), Prüfung durch Weiß · Im Beispiel: Nov 2026

1. Wir sind betroffen, weil wir eine Gesamtheit von Maschinen erstellen: mehrere Maschinen, die so angeordnet und gesteuert sind, dass sie zusammen als eine Anlage funktionieren. Damit sind wir Hersteller nach Maschinenverordnung. Bei der Übergabe an den Kunden bringen wir diese Gesamtheit in Verkehr. Weil sie über Netzwerktechnik vernetzt ist, ist sie ein Produkt mit digitalen Elementen und fällt auch unter den CRA.

2. Rechtsakte und Fristen festlegen: MVO ab 20.01.2027, CRA vollständig ab 11.12.2027, Meldepflicht seit 11.09.2026.

3. CRA-Klasse bestimmen: Kernfunktion Wärmeerzeugung, keine Kategorie in Anhang III oder IV, also Standardprodukt.

4. Bewertungsverfahren wählen: interne Kontrolle in beiden Rechtsakten, keine notifizierte Stelle.

2.1 Welche Rolle haben wir? Drei Fälle

Fall A: eigener Name oder eigene Marke. Die Anlage geht unter unserem Namen oder unserer Marke an den Kunden, auch wenn Partner Teile fertigen.

Maschinenverordnung: volle Herstellerpflichten. CRA: volle Herstellerpflichten.

Fall B: Gesamtheit von Maschinen, ohne eigene Produktmarke. Wir kombinieren Kessel, Raumaustragung, Zellradschleuse und Steuerung verschiedener Lieferanten zu einer Anlage und übergeben sie beim Kunden funktionsfähig. Das ist bei uns der entscheidende Grund, die eigene Marke kommt dazu.

Maschinenverordnung: Hersteller der Gesamtheit, eigener Name auf dem Typenschild, eigene Erklärung. CRA: Hersteller der Gesamtanlage, wenn sie vernetzt ist; für Steuerung und Gateway stützen wir uns auf Erklärung, SBOM und Updates der Lieferanten.

Fall C: reiner Einbau fertiger Geräte ohne Veränderung. Wir bauen ein fertiges, CE-gekennzeichnetes Gerät nach Herstelleranleitung ein, ohne es mit anderen Maschinen zu einer Anlage zu verbinden und ohne Software oder Sicherheitseinstellungen zu ändern.

Keine Herstellerpflichten, nur Händler- und Montagepflichten. Wer Sicherheitsfunktionen abschaltet, Fernzugänge selbst einrichtet oder Software ändert, prüft neu: Das kann eine wesentliche Änderung sein.

Nicht maßgeblich ist, ob die Anlage bei uns oder beim Kunden zusammengebaut wird. Eine Anlage nur für den eigenen Betrieb fällt nicht unter den CRA, wohl aber unter die Maschinenverordnung. Wie Behörden die Montage beim Kunden im Einzelfall sehen, ist noch nicht abschließend geklärt; die Herstellerrolle deshalb schriftlich mit Kunde und Lieferanten festlegen.

Ergebnis: Regelwerksmatrix, Normenliste und Bewertungsverfahren stehen fest.

Nr.	Dokument	Vorlage und Beispiel
D01	Einstufung, Rechtsrahmen und Bewertungsverfahren	leer und ausgefüllt

3 Schritt 2: Betrieb aufstellen

Wie decken zwei Personen alle Herstellerpflichten ab?

Wer: Berger, Weiß, Partnerfirmen · Im Beispiel: Nov 2026

1. Rollen mit Vertretung verteilen: Geschäftsführung und CE bei Berger, Technik, Safety und Product Security bei Weiß.

2. Partner vertraglich binden: Meldewege, Supportzusage 15 Jahre, Aufbewahrung, Quellcode-Hinterlegung.

3. Meldefähigkeit herstellen: Zugang zur ENISA-Meldeplattform, Bereitschaft, Notfallkarte, Meldeübung.

4. Schulungen planen und nachweisen.

Ergebnis: Organisation steht, der Betrieb kann Schwachstellen und Vorfälle fristgerecht melden.

Nr.	Dokument	Vorlage und Beispiel
D02	Rollen, Unterauftragnehmer und Pflichtenverteilung	leer und ausgefüllt
D16	Notfallkarte: Meldung nach Art. 14 CRA	leer und ausgefüllt
F03	Unterauftragsvereinbarung: Anhang CRA und MVO	leer und ausgefüllt
F06	Meldeprotokoll nach Art. 14 CRA	leer und ausgefüllt
F12	Schulungsnachweis	leer und ausgefüllt

4 Schritt 3: Anlage beschreiben

Was genau bringen wir in Verkehr, und wofür?

Wer: Weiß, Freigabe Berger · Im Beispiel: Dez 2026

1. Produktdaten, Baugruppen und Schnittstellen festhalten.

2. Bestimmungsgemäße Verwendung und vorhersehbare Fehlanwendung beschreiben, auch beim Fernzugriff.

3. Grenzen und Lebensphasen festlegen, einschließlich Update und Außerbetriebnahme.

4. Anforderungen mit Quelle in die Anforderungsliste aufnehmen.

Ergebnis: Anlagenbeschreibung und Anforderungsliste als Grundlage für alle weiteren Schritte.

Nr.	Dokument	Vorlage und Beispiel
D03	Anlagenbeschreibung	leer und ausgefüllt
F01	Anforderungsliste	leer und ausgefüllt

5 Schritt 4: Sicher konstruieren

Wie bleibt die Heizung sicher, auch wenn jemand angreift?

Wer: Weiß mit Ingenieurbüro und Software-Partner · Im Beispiel: Dez 2026

1. Sicherheitssteuerung mit Zertifikat nach IEC 62443-4-2 auswählen.

2. Sicherheitsfunktionen SF1 bis SF10 mit PLr festlegen.

3. Grundsatz: STB, Ablaufsicherung, Sicherheitsventil und Löschung wirken ohne Software und Netzwerk.

4. Zonen und Conduits nach IEC 62443 planen, Fernwartung nur nach Freigabe, signierte Updates.

Ergebnis: Steuerungs- und Sicherheitskonzept sowie Netzwerkarchitektur.

Nr.	Dokument	Vorlage und Beispiel
D04	Steuerungs- und Sicherheitskonzept	leer und ausgefüllt
D05	Netzwerk- und Systemarchitektur	leer und ausgefüllt

6 Schritt 5: Risiken beurteilen

Welche Gefahren bleiben, und sind sie akzeptabel?

Wer: Weiß, Berger, Ingenieurbüro, Security-Partner · Im Beispiel: Jan 2027

1. Gefährdungen nach EN ISO 12100 für alle Lebensphasen bewerten und mit dem Drei-Stufen-Verfahren mindern.

2. Cyber-Bedrohungen nach IEC 62443-3-2 bewerten und CRA Anhang I zuordnen.

3. Nachweisen, dass ein Angriff keine Sicherheitsfunktion aushebelt (MVO Anhang III 1.1.9, 1.2.1).

4. Restrisiken für die Anleitung festhalten.

Ergebnis: Zwei Risikobeurteilungen mit gemeinsamem Cyber-Safety-Nachweis.

Nr.	Dokument	Vorlage und Beispiel
D06	Risikobeurteilung Maschinensicherheit	leer und ausgefüllt
D07	Cybersecurity-Risikobewertung	leer und ausgefüllt

7 Schritt 6: Prozesse einführen

Was muss im Betrieb dauerhaft laufen?

Wer: Weiß (PSO), Berger, Software-Partner · Im Beispiel: Dez 2026 bis Mär 2027

1. 20 Prozesse nach Prozesshandbuch einführen: Entwicklung, SBOM, Schwachstellen, Updates, Änderungen, Marktbeobachtung.

2. Lieferanten und Komponenten bewerten.

3. Richtlinie zur koordinierten Offenlegung und security.txt veröffentlichen.

4. Jedes Release mit SBOM und Security-Freigabe ausliefern.

Ergebnis: Gelebte Prozesse mit Nachweisen für die technische Dokumentation.

Nr.	Dokument	Vorlage und Beispiel
D08	Prozesshandbuch	leer und ausgefüllt
D14	Richtlinie zur koordinierten Offenlegung	leer und ausgefüllt
F02	Lieferanten- und Komponentenbewertung	leer und ausgefüllt
F04	SBOM-Freigabe	leer und ausgefüllt
F14	Release-Freigabe Security	leer und ausgefüllt

8 Schritt 7: Prüfen und validieren

Funktioniert alles so, wie geplant?

Wer: Weiß, Ingenieurbüro, Prüflabor, Partner · Im Beispiel: Jan bis Mär 2027

1. Typprüfung EN 303-5 und EMV beim akkreditierten Labor.

2. Jede Sicherheitsfunktion mit Fehlerinjektion validieren.

3. Penetrationstest und Kommunikationsausfalltest.

4. Stückprüfung je Seriennummer einführen.

Ergebnis: Prüfberichte, Validierungsprotokolle, Stückprüfprotokoll.

Nr.	Dokument	Vorlage und Beispiel
F09	Validierungsprotokoll Sicherheitsfunktion	leer und ausgefüllt
F10	Stückprüfprotokoll	leer und ausgefüllt

9 Schritt 8: Dokumentieren und erklären

Was braucht es für die CE-Kennzeichnung?

Wer: Berger (Unterschrift), Weiß · Im Beispiel: Mär 2027

1. Technische Dokumentation vollständig zusammenstellen.

2. Nutzerinformationen veröffentlichen, mit vereinfachter Konformitätserklärung nach Anhang VI und dem Ende des Unterstützungszeitraums je Einheit (15 Jahre ab Übergabe).

3. Checkliste abarbeiten, dann die gemeinsame EU-Konformitätserklärung unterschreiben: mit dem Satz, dass die Erfüllung von Anhang I nachgewiesen ist, Geltung ab 11.12.2027 und Normen mit Ausgabe.

4. Typenschild, CE-Kennzeichnung und Supportende-Etikett anbringen.

Ergebnis: Unterschriebene Erklärung, CE-Kennzeichnung, Freigabe zum Inverkehrbringen.

Nr.	Dokument	Vorlage und Beispiel
D09	Technische Dokumentation: Inhaltsverzeichnis	leer und ausgefüllt
D10	Checkliste bis zum Inverkehrbringen	leer und ausgefüllt
D11	EU-Konformitätserklärung	leer und ausgefüllt
D12	Typenschild und Kennzeichnung	leer und ausgefüllt
D13	Nutzerinformationen nach CRA Anhang II	leer und ausgefüllt
D15	Erklärung zum Unterstützungszeitraum	leer und ausgefüllt

10 Schritt 9: Ausliefern und betreuen

Was gilt nach dem Verkauf, über den ganzen Unterstützungszeitraum?

Wer: Weiß (Service, PSO), Berger · Im Beispiel: ab Mär 2027

1. Inbetriebnahme mit Sicherheits-Erstkonfiguration.
2. Schwachstellen behandeln, Nutzer informieren, Updates kostenlos bereitstellen.
3. Änderungen auf wesentliche Veränderung prüfen.
4. Korrekturmaßnahmen umsetzen und Behörden informieren, wenn nötig.

Ergebnis: Konformität und Sicherheit über den gesamten Unterstützungszeitraum.

Nr.	Dokument	Vorlage und Beispiel
F05	Schwachstellenticket	leer und ausgefüllt
F07	Sicherheitshinweis an Nutzer	leer und ausgefüllt
F08	Änderungsantrag	leer und ausgefüllt
F11	Inbetriebnahmeprotokoll	leer und ausgefüllt
F13	Korrekturmaßnahme und Behördenkontakt	leer und ausgefüllt

11 Wichtige Hinweise

• Die Musterdokumente sind interne Nachweise. In der Konformitätserklärung stehen Rechtsakte, Normen und Spezifikationen; eine Vermutungswirkung entsteht nur über harmonisierte Normen mit Fundstelle im Amtsblatt.

• Für den CRA und für MVO Anhang III 1.1.9 gibt es am 05.11.2026 noch keine gelistete harmonisierte Norm. IEC 62443, EN 40000-1-2 und FprEN 50742 werden als Spezifikationen genutzt und die Lösungen in der Dokumentation begründet.

• Risikozahlen, PL-Kennwerte, Fristen und Supportdauer sind begründete Beispielwerte. Jeder Hersteller bewertet sein eigenes Produkt.

• Kleinst- und Kleinunternehmen: Für eine verpasste 24-Stunden-Frühwarnung gibt es kein Bußgeld (Art. 64 Abs. 10 Buchst. a CRA). Die Meldepflicht selbst gilt.

• Vor jeder Erklärung den Stand von Amtsblatt, Normen und nationalem Durchführungsgesetz prüfen.

Alle Vorlagen und Beispiele: ot-cyber.de/muster/cra-hackschnitzelheizung/ · Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung.