CRA-MUSTER

D07 Cybersecurity-Risikobewertung

Leere Vorlage · 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

Felder ausfüllen, mit Datum und Unterschrift freigeben, in der Ablage nach Dokumentenlenkung führen.

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.

So füllen Sie dieses Formular aus

Füllen Sie die Felder mit den Angaben Ihres Betriebs aus. Unter jeder Tabelle und neben jedem Feld steht ein Beispiel aus dem Musterbetrieb als Orientierung. Verweisen Sie auf Nachweise mit Nummer (z. B. Ticket oder Formular). Zum Schluss mit Datum und Unterschrift freigeben und nach der Dokumentenlenkung ablegen.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	
Version, Status	
Geltungsbereich	
Ersteller	
Geprüft	
Freigabe	
Nächste Prüfung	
Vertraulichkeit	
Ablage	

3 Rahmen der Bewertung

Feld	Eintrag	Beispiel aus dem Muster
Bestimmungsgemäße Verwendung		Wärmeerzeugung im Heizraum, Fernzugriff nur für …
Einsatzumgebung		Heizräume von Gewerbe, Kommunen, Landwirtschaft …
Werte		Sicherheitsfunktionen SF1 bis SF10, F-Programm, …

Feld	Eintrag	Beispiel aus dem Muster
Nutzungsdauer		15 bis 20 Jahre je Kessel; Bedrohungen über …
Methode		R = L × I, L und I je 1 bis 4; akzeptabel bis …
Anhang I Teil I		Zu jedem Punkt 2 a bis m ist in F01 …

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

Beispielzeile aus dem Muster: ID: C01 · Bedrohung: Übernahme Kundenkonto · Weg: Internet · R0: 9 · Maßnahmen: MFA, Ratenbegrenzung · R1: 4 · Bezug: 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.

Beschreiben Sie hier Ihren Stand, konkret und mit Datum. Beispiel aus dem Muster: 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.

5 Cyber-Safety-Nachweis

Beschreiben Sie hier Ihren Stand, konkret und mit Datum. Beispiel aus dem Muster: Schlimmster Fall: Ein Angreifer kontrolliert Portal und Gateway vollständig.

Bewertungsrunde	Anlass	Ergebnis

Bewertungsrunde	Anlass	Ergebnis

Beispielzeile aus dem Muster: Bewertungsrunde: 28.06.2027 · Anlass: NWT-VULN-2027-004 (MQTT-Bibliothek) · Ergebnis: C12 bestätigt, Monitoring täglich

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

Freigegeben (Name, Funktion, Datum, Unterschrift): _____ · Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Firma, Personen, Seriennummern und Daten frei erfunden.