NIS2-MUSTER

F-07 Risikoregister

Beispiel nach einem Jahr Betrieb, Stand 28.09.2027 · Musterwerk KWK-Service GmbH, BHKW-Service mit Fernwartung

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Musterbetrieb	Musterwerk KWK-Service GmbH, BHKW-Service mit Fernwartung (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

Alle bewerteten Risiken für den Dienst mit Wahrscheinlichkeit, Auswirkung, Maßnahmen und Restrisiko. Bewertung vor und nach Maßnahmen, Entscheidung der Geschäftsführung. Methode: W und A je 1 bis 4, Risiko = W × A, akzeptabel bis 4.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-07
Version, Status	2.3, freigegeben
Geltungsbereich	Musterwerk KWK-Service GmbH, alle Standorte, Systeme und Fernzugänge zu Kundenanlagen
Ersteller	Julia Hartl, ISB
Geprüft	Markus Wein, Vertretung ISB
Freigabe	Thomas Berger, Geschäftsführer, 28.09.2027
Nächste Prüfung	30.06.2028 oder bei wesentlicher Änderung
Vertraulichkeit	intern
Ablage	ISMS-Ordner im Cloud-Büropaket, Bereich 01 Lenkung

3 Risiken und Bewertung

So lesen Sie die Tabelle

Jede Zeile ist ein Risiko für den Dienst. „vorher“ ist das Risiko ohne Maßnahmen, „nachher“ mit Maßnahmen, jeweils Wahrscheinlichkeit mal Auswirkung, beides von 1 bis 4. Bis 4 ist das Risiko vertretbar, darüber braucht es weitere Maßnahmen oder eine Entscheidung der Geschäftsführung.

ID	Risiko	Werte	vorher	Maßnahmen	nachher	Entscheidung
R-01	Technikerkonto per Phishing übernommen	A-01, A-03	16	M-01, M-02, M-07	4	gemindert
R-02	Ransomware legt Leitwarte lahm	A-02, A-12	12	M-04, M-05, M-06	4	gemindert
R-03	Kundenrouter mit alter Firmware im Internet	K-01 bis K-91	12	M-03, M-08	3	gemindert

ID	Risiko	Werte	vorher	Maßnahmen	nachher	Entscheidung
R-04	Gemeinsame Zugangsdaten weitergegeben	A-03	9	M-02, M-03	2	gemindert
R-05	Hersteller-Fernzugang an uns vorbei	K-01 bis K-91	8	M-09, M-19	4	akzeptiert B-09
R-06	Ausfall Systemhaus im Vorfall	A-01, A-06	9	M-10, M-13	4	gemindert
R-07	Laptop mit Kundendaten verloren	A-04, A-12	9	M-11	2	gemindert
R-08	Leitwarte fällt aus, Störung unbemerkt	A-02, A-10	8	M-12, M-13	3	gemindert
R-09	Manipulierte Herstellersoftware auf Laptop	A-04	8	M-04, M-15	4	gemindert
R-10	Insider gibt Anlagendaten weiter	A-12	6	M-02, M-16	3	gemindert
R-11	Lücke in Fernwartungsplattform	A-03	12	M-08, M-14	4	gemindert
R-12	Mobilfunkausfall beim Kunden	K-01 bis K-91	6	M-12	4	akzeptiert B-09
R-13	Admin-Oberfläche Firewall aus Büronetz erreichbar	A-06	9	M-20	2	gemindert
R-14	Sprungserver ohne Aufzeichnung bei Ausfall	A-03	8	M-21	3	gemindert
R-15	Alte Konten nach Austritt aktiv	A-01, A-03	9	M-22	2	gemindert
R-16	KI-Assistent im Büropaket gibt Daten preis	A-01, A-12	6	M-23	3	gemindert
R-17	Brand, Wasser oder Stromausfall im Serverraum	A-02, A-10	8	M-26, M-13	3	gemindert
R-18	Mitarbeiter mit Zugriff handelt gegen uns	A-03, K-01 bis K-91	8	M-27, M-02, M-21	3	gemindert
R-19	Angreifer springt von einem Kunden zum nächsten	A-03, K-01 bis K-91	12	M-29, M-30	3	gemindert
R-20	Schadsoftware über USB-Stick	A-04	6	M-32, M-04	2	gemindert

Legende: Werte = betroffene Werte aus dem Inventar F-06 (A-Nummern); vorher und nachher = Risiko vor und nach den Maßnahmen, Risiko = W × A mit W = Wahrscheinlichkeit 1 bis 4 und A = Auswirkung 1 bis 4, akzeptabel bis 4; Maßnahmen = Nummern aus dem Maßnahmenplan F-08 (M-Nummern).

4 Bewertungsrunden

Datum	Anlass	Teilnehmende	Ergebnis
30.08.2026	Erstanalyse	Hartl, Wein, Berater	12 Risiken, 9 über 4
24.09.2026	Vorfall SV-2026-003	Hartl, MDR-Analyst	R-01 auf W 4 bestätigt, M-01 erweitert
05.02.2027	Pentestbericht	Hartl, Systemhaus, Pentester	3 neue Risiken
30.06.2027	Jahresbewertung	Berger, Hartl, Wein	alle bis auf R-05 und R-12 bei 4 oder darunter
20.09.2027	Externe Prüfung 14.09.2027	Berger, Hartl, Prüfer	gefahrenübergreifend ergänzt: R-17 bis R-20

R-05 und R-12 liegen nach Maßnahmen bei 4 und sind damit im akzeptablen Bereich; die Geschäftsführung hat sie zusätzlich ausdrücklich akzeptiert, weil weitere Senkung nur beim Kunden möglich ist. Nächste Bewertung: 30.06.2028 oder nach einem erheblichen Vorfall.

5 Begriffe und Abkürzungen

KI: künstliche Intelligenz

MDR: Dienst, der Alarme rund um die Uhr auswertet (Managed Detection and Response)

SV: Sicherheitsvorfall (Nummernkreis)

USB: USB-Anschluss

6 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	30.08.2026	Erste vollständige Analyse, 12 Risiken	T. Berger
1.2	24.09.2026	Nach SV-2026-003: R-01 neu bewertet	T. Berger
2.0	05.02.2027	Nach Pentest: R-13 bis R-15 neu	T. Berger
2.1	30.06.2027	Jährliche Bewertung, R-16 neu, Restrisiken akzeptiert (B-09)	T. Berger
2.2	28.09.2027	Gefahrenübergreifend ergänzt: R-17 bis R-20	T. Berger
2.3	28.09.2027	Lesehilfe zur Tabelle	T. Berger

Freigegeben: Thomas Berger, Geschäftsführer, 28.09.2027 (im Original unterschrieben). Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Musterbetrieb und Daten frei erfunden.