NIS2-MUSTER

F-09 Erstaufnahme Sicherheitsereignisse

Beispiel nach einem Jahr Betrieb, Stand 20.08.2027 · 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

Jedes Sicherheitsereignis wird sofort mit Uhrzeit, Quelle, Beobachtung und Sofortmaßnahmen aufgenommen, auch wenn es sich später als harmlos erweist. Das Register zeigt, dass der Meldeweg gelebt wird.

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	MW-ISMS-F-09
Version, Status	1.5, 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, 20.08.2027
Nächste Prüfung	30.06.2028 oder bei wesentlicher Änderung
Vertraulichkeit	intern
Ablage	ISMS-Ordner im Cloud-Büropaket, Bereich 01 Lenkung

3 Ereignisregister

Vorgang	Eingang	Quelle	Beobachtung	Bewertung F-10
SV-2026-001	28.08.2026	MDR	Anmeldeversuche auf Plattform	nicht erheblich
SV-2026-002	14.09.2026	Mitarbeiterin	Phishing-Mail gemeldet, nicht geklickt	nicht erheblich
SV-2026-003	22.09.2026	MDR	Kontoübernahme Techniker	erheblich, gemeldet
SV-2027-001	09.03.2027	Kunde	Router K-41 neu gestartet, Ursache Stromausfall	kein Sicherheitsvorfall
SV-2027-002	02.06.2027	MDR	Schadsoftware auf Laptop blockiert	nicht erheblich
SV-2027-003	16.06.2027	Hersteller	Lücke in Plattform-Software gemeldet	nicht erheblich, F-18
SV-2027-004	19.08.2027	Bereitschaft	Unbekannte Sitzung auf Sprungserver	nicht erheblich, Testkonto Systemhaus

4 Beispiel einer Erstaufnahme: SV-2026-003

Eingang: 22.09.2026, 06:42 Uhr, MDR-Dienst per Telefon und E-Mail

Beobachtung: Anmeldung am Konto des Servicetechnikers S. Kraus aus dem Ausland um 03:15 Uhr, danach neue Weiterleitungsregel im Postfach

Betroffen: Cloud-Konto S. Kraus (A-01), Postfach mit Wartungsberichten mehrerer Kunden (A-12)

Sofortmaßnahmen: 06:50 Konto gesperrt und Sitzungen beendet (Systemhaus); 06:55 Konto auf der Fernwartungsplattform gesperrt (Rufbereitschaft)

ISB alarmiert: 06:58 Uhr

Aufgenommen: P. Neumann, Rufbereitschaft

Lehre aus SV-2027-004: Testkonten der Lieferanten werden vorab angekündigt und mit Ablaufdatum angelegt (F-15). Seitdem keine unangekündigte Sitzung mehr.

5 Begriffe und Abkürzungen

ISB: Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter

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

SV: Sicherheitsvorfall (Nummernkreis)

6 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	20.07.2026	Erstfassung im Projektstart	T. Berger
1.1	22.09.2026	SV-2026-003 aufgenommen	T. Berger
1.2	11.12.2026	SV-2026-001/002 nachgetragen	T. Berger
1.3	09.03.2027	SV-2027-001	T. Berger
1.4	17.06.2027	SV-2027-002 und 003	T. Berger
1.5	20.08.2027	SV-2027-004	T. Berger

Freigegeben: Thomas Berger, Geschäftsführer, 20.08.2027 (im Original unterschrieben). Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Musterbetrieb und Daten frei erfunden.