

LEITFADEN · TOMORIS TOOLBOX

Incident Response: Playbook für Sicherheitsvorfälle in KMU

Phasen, Rollen, Entscheidungen mit Kriterien, Meldefristen und Vorfallprotokoll, nach NIST SP 800-61 Rev. 3, BSI DER.2.1 und den CISA-Playbooks

STAND

25.10.2026

UMFANG

PDF, 9 Seiten

ONLINE

tomoris.com/downloads/incident-response-playbook

AUF EINEN BLICK

24 h

Frühwarnung bei erheblichen Vorfällen (NISG 2026)

72 h

Meldung an CSIRT und Datenschutzbehörde

6

Funktionen des NIST CSF 2.0 im Modell

1

Vorfallleitung je Vorfall, laut NIST RS.MA-01 zu erwägen

FÜR WEN

- IT-Leitung und Administration, die Vorfälle technisch bearbeiten
- Informationssicherheitsbeauftragte, die die Behandlung koordinieren
- Geschäftsführung, die über Abschaltung, Meldung und Kommunikation entscheidet
- IT-Dienstleister, die Kunden im Vorfall unterstützen

WURUM ES GEHT

Ein Sicherheitsvorfall lässt keine Zeit, Zuständigkeiten erst zu klären. Dieses Playbook ordnet die Behandlung jedes Vorfalls, vom gekaperten Konto bis zum Datenabfluss: in welchen Phasen Sie vorgehen, wer welche Rolle hat, welche Entscheidungen anstehen und nach welchen Kriterien Sie sie treffen, welche Meldefristen laufen und wie Sie alles nachvollziehbar protokollieren. Grundlage sind NIST SP 800-61 Rev. 3, der Baustein DER.2.1 des BSI IT-Grundschutz-Kompendiums und die Playbooks der US-Behörde CISA. Für die Sofortmaßnahmen bei Ransomware, das Notfallhandbuch und die NIS2-Meldung gibt es eigene Downloads.

Dieser Leitfaden ist eine Empfehlung von TOMORIS und ersetzt weder einen Notfallplan noch Rechtsberatung oder forensische Unterstützung. Passen Sie Rollen, Kontakte und Kriterien an Ihr Unternehmen an. Ob eine Meldepflicht besteht, hängt von Ihrer Einrichtung und vom Vorfall ab; maßgeblich sind NISG 2026, NISV 2026 und DSGVO in der geltenden Fassung.

INHALT

01	Was ein Playbook leisten muss	2
02	Die Phasen im Überblick	3
03	Rollen im Vorfall	4
04	Ablauf Schritt für Schritt	5
05	Entscheidungen mit Kriterien	6
06	Meldefristen im Blick	7
07	Vorfallprotokoll zum Ausfüllen	7
08	Nachbereitung und Übung	8
09	Quellen	9

01

Was ein Playbook leisten muss

Warum Vorfallbehandlung vorbereitet sein muss und was das BSI verlangt

NIST beschreibt, wie sich Vorfälle verändert haben: Sie sind häufiger und richten mehr Schaden an, die Wiederherstellung dauert oft Wochen oder Monate. Vorfallbehandlung gehört deshalb in das gesamte Risikomanagement (SP 800-61 Rev. 3, Abschnitt 2.1). Playbooks geben für typische Lagen umsetzbare Schritte vor; dokumentierte Abläufe lassen sich üben und helfen beim Einarbeiten neuer Personen (Abschnitt 2.3).

Basis-Anforderungen des BSI (DER.2.1, Edition 2023)

DER.2.1.A1

Klar definieren, was ein Sicherheitsvorfall ist, und ihn von Störungen im Tagesbetrieb abgrenzen; alle Beteiligten kennen die Definition.

DER.2.1.A2	Richtlinie zur Behandlung von Sicherheitsvorfällen mit Verhaltensregeln je Vorfalldart, von der Leitung verabschiedet, allen bekannt, regelmäßig aktualisiert.
DER.2.1.A3	Verantwortlichkeiten und Ansprechpersonen festlegen, auch wer über eine forensische Untersuchung entscheidet, nach welchen Kriterien und wann; Kontaktdaten aktuell und leicht zugänglich.
DER.2.1.A4 bis A6	Betroffene Stellen zeitnah informieren und Meldepflichten beachten, Vorfall eingrenzen und beheben, Betriebsumgebung sicher wiederherstellen.

Dieses Playbook ist eine Empfehlung von TOMORIS für den allgemeinen Ablauf bei jeder Art von Sicherheitsvorfall. Sofortmaßnahmen bei Ransomware, das Notfallhandbuch für den Wiederanlauf und das Formular für die NIS2-Meldung stehen in eigenen Downloads.

02

Die Phasen im Überblick

Vom bekannten Phasenmodell zum Modell nach NIST CSF 2.0

Phasen der Vorfalldbehandlung (bisheriges NIST-Modell, Eindämmung getrennt wie im CISA-Playbook)



Rev. 3 ordnet die Vorfalldbehandlung den sechs Funktionen des NIST Cybersecurity Framework 2.0 zu: Govern, Identify und Protect bereiten vor, Detect, Respond und Recover sind die eigentliche Behandlung; Erkenntnisse fließen laufend über die Kategorie Improvement zurück. NIST überlässt es ausdrücklich jeder Organisation, das Modell zu verwenden, das zu ihr passt. Dieses Playbook nutzt die bekannten Phasen und nennt die Kennungen aus Rev. 3.

03

Rollen im Vorfall

Wer entscheidet, wer bearbeitet, wer informiert

Rollen nach NIST SP 800-61 Rev. 3 (Abschnitt 2.2) und BSI DER.2.1

ROLLE	AUFGABE IM VORFALL
Geschäftsleitung	Beaufsichtigt die Behandlung, stellt Mittel bereit und entscheidet über folgenschwere Schritte wie das Abschalten oder Neuaufsetzen wichtiger Dienste.
Vorfallverantwortliche Person	Je Vorfall eine Person, die die Behandlung leitet, Aufgaben verteilt und das Protokoll führt (NIST RS.MA-01: incident lead).
Technik und IT-Betrieb	Prüfen, ob ein Vorfall vorliegt, sammeln und analysieren Daten, dämmen ein, finden die Ursache, stellen wieder her. Die Leitung des IT-Betriebs gibt Behebungsmaßnahmen frei (DER.2.1.A5).
Datenschutz, Recht	Prüfen Meldepflichten, Verträge und rechtliche Folgen; ob die Datenschutzbeauftragten einzubeziehen sind, ist zu prüfen (DER.2.1.A4).
Kommunikation	Stimmt Aussagen an Mitarbeitende, Kunden und Medien ab; nur Befugte geben Informationen weiter (DER.2.1.A9).
Personal, Betriebsrat	Personal ist beteiligt, wenn Mitarbeitende verdächtigt werden, einen Vorfall absichtlich verursacht zu haben (NIST 2.2); ob der Betriebsrat einzubeziehen ist, ist zu prüfen (DER.2.1.A4).
Externe	IR-Dienstleister, Cloud- und Internetanbieter mit vertraglich festgelegten Aufgaben, Rechten und Informationswegen (NIST 2.2).

Kontakte für den Vorfall (zum Ausfüllen, aktuell und leicht zugänglich halten)

ROLLE	NAME	ERREICHBAR UNTER	VERTRETUNG
Vorfallverantwortlich	_____	_____	_____
Geschäftsleitung	_____	_____	_____
IT-Betrieb	_____	_____	_____
Datenschutz	_____	_____	_____
IR-Dienstleister	_____	_____	_____
Zuständiges CSIRT	_____	_____	_____

04 —

Ablauf Schritt für Schritt

Von der ersten Meldung bis zum bestätigten Normalbetrieb

1 Meldung annehmen und prüfen

Meldungen kommen über feste, vertrauenswürdige Wege (DER.2.1.A9), auch von Dritten (NIST RS.MA-02). Kurz prüfen, ob tatsächlich ein Sicherheitsvorfall vorliegt, Schwere und Dringlichkeit abschätzen (NIST RS.MA-02).

2 Vorfall feststellen, Leitung benennen

Liegen die festgelegten Kriterien vor, den Vorfall erklären und eine verantwortliche Person benennen; bei Bedarf den IR-Dienstleister anfordern und andere Pläne wie den Notfallplan auslösen (NIST DE.AE-08, RS.MA-01).

3 Einstufen und priorisieren

Art des Vorfalls bestimmen, etwa Datenabfluss, Ransomware, Kontoübernahme oder Dienstausfall, nach einem einheitlichen Verfahren einstufen und priorisieren (NIST RS.MA-03, DER.2.1.A11).

4 Protokollieren und Beweise sichern

Jede Feststellung und Handlung mit Zeitpunkt festhalten, Aufzeichnungen vertraulich und unverändert aufbewahren; Daten sichern, die Art und Ursache erklären können (NIST RS.AN-06, RS.AN-07; DER.2.1.A6, A16).

5 Eindämmen

Betroffene Systeme und Netzbereiche isolieren, unberechtigte Zugriffe sperren, Kennwörter, Schlüssel und Dienstkonto bei Verdacht wechseln, privilegierte Zugänge entziehen (CISA-Playbook, Containment). Auswirkungen auf den Betrieb und auf die Beweissicherung abwägen.

6 Ausmaß und Ursache ermitteln

Ablauf rekonstruieren, Schwachstellen und Angriffswege bestimmen, auch auf nicht offensichtlich betroffenen Systemen nach Spuren und Hintertüren suchen (NIST RS.AN-03, RS.AN-08). Neue Spuren erweitern Analyse und Eindämmung (CISA-Playbook).

7 Beseitigen

Alle betroffenen Systeme und Dienste erfassen, Schadsoftware entfernen, kompromittierte Konten sperren, ausgenutzte Schwachstellen schließen (NIST RS.MI-02); Maßnahmen vorher von der Leitung des IT-Betriebs freigeben lassen (DER.2.1.A5).

8 Wiederherstellen und bestätigen

Sicherungen vor der Verwendung auf Integrität prüfen (NIST RC.RP-03), Systeme mit allen Patches wiederherstellen, alle Zugangsdaten ändern, Benutzende in Funktionstests einbeziehen und danach gezielt überwachen (DER.2.1.A6). Ende des Vorfalls nach Kriterien erklären (NIST RC.RP-06).

Angreifer nicht vorwarnen: Die CISA rät, Betroffene telefonisch statt per E-Mail zu informieren, für die Abstimmung einen Kanal außerhalb der möglicherweise kompromittierten Systeme zu nutzen und Schadsoftware-Proben nicht bei öffentlichen Analysediensten hochzuladen.

05

Entscheidungen mit Kriterien

Die wichtigsten Weichenstellungen und wer sie trifft

Entscheidungen im Vorfall (Zuordnung „wer“: Empfehlung von TOMORIS)

ENTSCHEIDUNG	KRITERIEN LAUT QUELLE	WER
Sofort eindämmen oder weiter beobachten?	Ob Schaden begrenzen oder Aufklären wichtiger ist (DER.2.1.A10); Folgen für den Betrieb, Dauer und Wirksamkeit, Folgen für Beweise; Risiko, den Angreifer zu warnen, gegen Risiko, ihn länger im Netz zu lassen (CISA).	Vorfallverantwortliche mit Geschäftsleitung
Systeme vom Netz, Dienste abschalten?	Über folgenschwere Schritte wie das Abschalten oder Neuaufsetzen wichtiger Dienste kann laut NIST die Leitung entscheiden (NIST 2.2); betroffene Komponenten vom Netz nehmen (DER.2.1.A6).	Geschäftsleitung
Forensik beiziehen?	Kriterien und Zuständigkeit vorab festlegen (DER.2.1.A3); Beweissicherung mit Nachweiskette etwa, wenn eine Strafverfolgung möglich ist (NIST RS.AN-07).	Geschäftsleitung nach Empfehlung der Technik
Melden an Behörden?	Gesetzliche Meldepflichten prüfen (DER.2.1.A4); NISG 2026, DSGVO; Polizei nach den Kriterien im Plan und mit Freigabe der Leitung (NIST RS.CO-02).	Geschäftsleitung, Datenschutz
Kunden und Öffentlichkeit informieren?	Empfänger der Dienste bei Beeinträchtigung unverzüglich unterrichten (§ 34 Abs. 3 NISG 2026); Betroffene bei hohem Risiko (Art. 34 DSGVO); öffentliche Aussagen nur über freigegebene Wege (NIST RC.CO-04).	Geschäftsleitung, Kommunikation
Wiederanlauf starten?	Festgelegte Kriterien für den Beginn der Wiederherstellung anwenden, mögliche Betriebsstörungen berücksichtigen (NIST RS.MA-05).	Vorfallverantwortliche, IT-Betrieb

06 —

Meldefristen im Blick

Was bei erheblichen Vorfällen und bei Datenschutzverletzungen läuft

Meldefristen: 24 und 72 Stunden ab Kenntnisnahme, Abschlussbericht ab Meldung



24 Stunden

Frühwarnung an das CSIRT

Unverzüglich, spätestens innerhalb von 24 Stunden: für wesentliche und wichtige Einrichtungen bei erheblichen Cybersicherheitsvorfällen (§ 34 Abs. 2 Z 1 NISG 2026).



72 Stunden

Meldung an CSIRT und DSB

Meldung mit erster Bewertung an das CSIRT (§ 34 Abs. 2 Z 2 NISG 2026); bei Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden an die Datenschutzbehörde (Art. 33 Abs. 1 DSGVO).



1 Monat

Abschlussbericht

Spätestens einen Monat nach der Meldung. Dauert der Vorfall noch an, zunächst ein Fortschrittsbericht, der Abschlussbericht dann binnen eines Monats nach Ende der Vorfallsbehandlung (§ 34 Abs. 2 Z 4 und 5 NISG 2026).

Erheblich ist ein Vorfall nach § 35 Abs. 1 NISG 2026, wenn er schwerwiegende Betriebsstörungen oder finanzielle Verluste für die Einrichtung verursacht hat oder verursachen kann oder andere durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann; die NISV 2026 legt dazu weitere Kriterien fest. Die DSGVO-Meldung entfällt nur, wenn die Verletzung voraussichtlich zu keinem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Prüfen Sie beide Pflichten parallel und früh. Felder und Ablauf der NIS2-Meldung stehen in der Vorlage „NIS2-Vorfallmeldung“, die Pflichten im Leitfaden „NIS2-Meldepflichten“.

07 —

Vorfallprotokoll zum Ausfüllen

Stammdaten und Tagebuch des Vorfalls, vertraulich aufbewahren

Stammdaten des Vorfalls

FELD	EINTRAG
Vorfallnummer	_____
Festgestellt am, um, durch	_____
Vorfallverantwortliche Person	_____
Art (Datenabfluss, Ransomware, Kontoübernahme, Dienstausschlag, Sonstiges)	_____
Betroffene Systeme, Dienste, Daten	_____

Meldepflicht NISG 2026 geprüft am, Ergebnis _____

Meldepflicht DSGVO geprüft am, Ergebnis _____

Ende des Vorfalls erklärt am, durch _____

Tagebuch: jede Feststellung und Handlung mit Zeitpunkt (NIST RS.AN-06, DER.2.1.A16)

DATUM, UHRZEIT	BEOBACHTUNG ODER MASSNAHME	ENTSCHEIDUNG	WER
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

08 —

Nachbereitung und Übung

Aus jedem Vorfall lernen und den Ablauf üben

- ☐ Abschlussbericht erstellt: Vorfall, Maßnahmen zur Behandlung und Wiederherstellung, Lehren (NIST RC.RP-06).
- ☐ Ausgewertet: Wie schnell wurde der Vorfall erkannt und behoben, funktionierten die Meldewege, reichten die Informationen, wirkten Erkennung und Maßnahmen (DER.2.1.A17)?
- ☐ Alle Beteiligten haben ihre Erfahrungen berichtet; Prozesse und Abläufe angepasst (DER.2.1.A18).
- ☐ Ursache beseitigt, Schwachstellen in Infrastruktur und Abläufen erfasst, Rollen und Befugnisse geklärt, Schulungsbedarf und Werkzeuge verbessert (CISA, Post-Incident).
- ☐ Erkennung nachgeschärft: Regeln und Protokollierung für die beobachteten Angriffstechniken ergänzt, blinde Flecken geschlossen (CISA, Post-Incident).
- ☐ Geschäftsleitung informiert: jährlich über alle Vorfälle, bei sofortigem Handlungsbedarf umgehend (DER.2.1.A17).
- ☐ Handlungsanweisungen für vergleichbare Vorfälle erstellt und bekannt gemacht (DER.2.1.A17).

- ☐ Eskalationswege in Übungen erprobt (DER.2.1.A14), bei erhöhtem Schutzbedarf auch Planspiele (A22); Erkenntnisse aus Übungen eingearbeitet (NIST ID.IM-02).
- ☐ Playbook und Kontakte regelmäßig überprüft und aktualisiert (DER.2.1.A7, NIST ID.IM-04).

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

IT-Notfallkarte

tomoris.com/tools/notfallkarte

NIS2-Meldefristen-Rechner

tomoris.com/tools/meldefristen-rechner

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

09

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management (April 2025)**
Abschnitte 2.1 bis 2.3, Tabelle der CSF-Kategorien DE, RS, RC und ID.IM, gelesen am 25.10.2026
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3...
- 2 **BSI IT-Grundschutz-Kompodium, Baustein DER.2.1 Behandlung von Sicherheitsvorfällen (Edition 2023)**
Anforderungen A1 bis A22, gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 3 **CISA: Cybersecurity Incident & Vulnerability Response Playbooks (November 2021)**
Incident Response Playbook: Vorbereitung, Eindämmung, Nachbereitung, gelesen am 25.10.2026
www.cisa.gov/sites/default/files/publications/Federal_Governmen...
- 4 **NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS**
§ 34 Berichtspflichten, § 35 erheblicher Cybersicherheitsvorfall, gelesen am 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 5 **NISV 2026, BGBl. II Nr. 290/2026**
§§ 5 bis 7 Erheblichkeit, gelesen am 25.10.2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 6 **Verordnung (EU) 2016/679 (DSGVO), deutsche Fassung auf EUR-Lex**
Art. 33 und 34, gelesen am 25.10.2026
eur-lex.europa.eu/eli/reg/2016/679/oj/deu