JUMBO BLOCK REPORT

Meldepflichten im Vorfall – NIS-2, KRITIS-DachG, CRA und DSGVO



Handbuch · Version 1.0.0
Oktober 2026
ZANNI GROUP · Andreas Zanni e.K. · Brauhof 12 · 44866 Bochum · jumboblock.org

Inhalt

1. Überblick
2. Grundbegriffe
3. Arbeitsablauf
4. Vorfallakte anlegen und öffnen
5. Vorfall, Meldepflichten und Erheblichkeit
6. Fristen und Meldewege
7. Meldungen erstellen und abgeben
8. Zeitleiste
9. Bericht
10. Datei, Prüfkette und Signatur
11. Zusammenspiel mit anderen Programmen
12. Sicherheit und Technik
13. Fehlerbehebung

1. Überblick

REPORT unterstützt Einrichtungen und Unternehmen dabei, die Meldepflichten bei einem Sicherheitsvorfall vollständig und fristgerecht zu erfüllen. Ab dem Zeitpunkt der Kenntnisnahme überwacht REPORT alle in Betracht kommenden Fristen nach NIS-2 (§ 32 BSIG), KRITIS-Dachgesetz (§ 18 KRITIS-DachG), Cyber Resilience Act (Art. 14 CRA) und DSGVO (Art. 33), erstellt die Meldetexte mit den gesetzlichen Pflichtangaben und hält jede abgegebene Meldung unveränderlich fest.

Alle Angaben und Handlungen werden in einer Vorfallakte gespeichert. Jede relevante Handlung wird als Eintrag in einer Hash-Kette festgehalten; der daraus gebildete Prüfwert steht in jeder Meldung und in jedem Bericht. So lässt sich die Akte nachträglich nicht unbemerkt verändern.

Vollständig offline: REPORT läuft im Browser, auch direkt vom USB-Stick (`file://`). Es gibt keine Server-Verbindung, kein Konto und keine Cloud. Die Vorfallakte ist mit Ihrem Passwort verschlüsselt.

Arbeitshilfe, keine Rechtsberatung: REPORT bildet die Meldepflichten nach dem angegebenen Rechtsstand ab. Maßgeblich sind die Gesetzestexte und die Vorgaben von BSI, BBK und Aufsichtsbehörden. Die Meldungen selbst werden über die Meldeportale der zuständigen Stellen abgegeben.

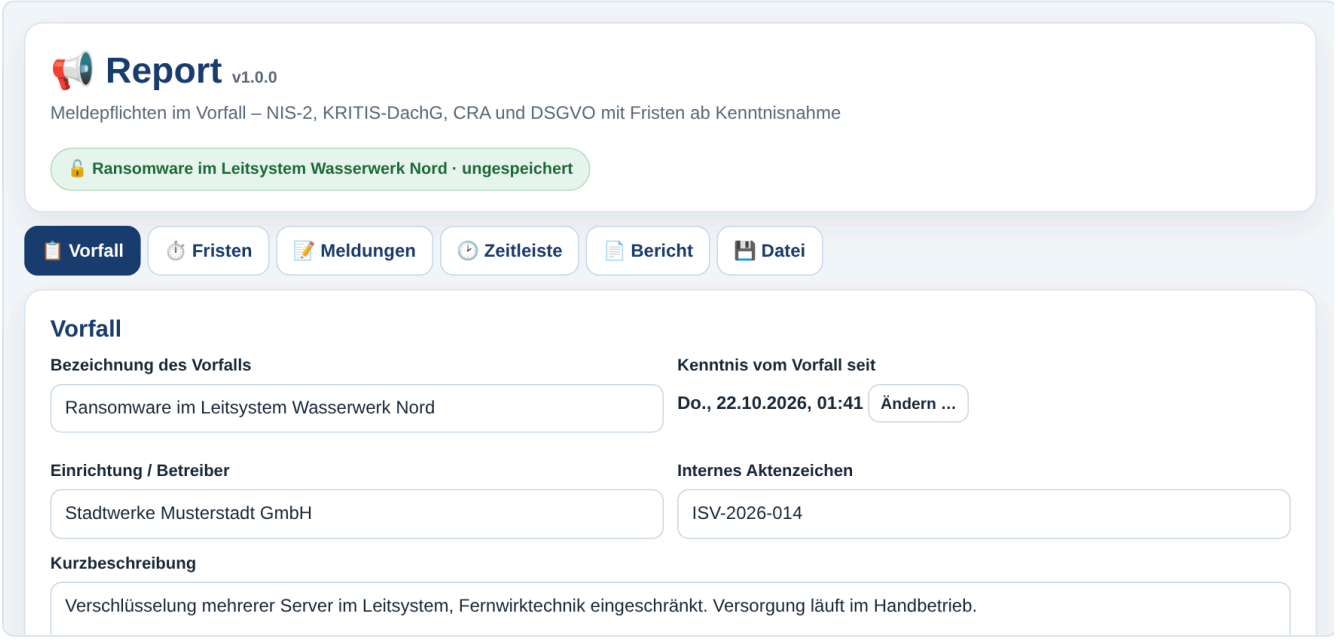


Abb. 1: Arbeitsbereich von REPORT mit den sechs Reitern

Bereich	Aufgabe
Vorfall	Angaben zum Vorfall, Kenntnisnahme, in Betracht kommende Meldepflichten und Bewertung der Erheblichkeit
Fristen	Alle Meldungen mit Rechtsgrundlage, spätester Abgabe und Stand; Meldewege
Meldungen	Meldetexte erstellen, kopieren und als abgegeben festhalten
Zeitleiste	Ereignisse und Maßnahmen, auch aus dem Lagebuch von JUMBO BLOCK LOGBOOK
Bericht	Dokumentation des Vorfalls zum Drucken oder als PDF
Datei	Speichern, Sperren, Prüfkette, Signatur und Prüfung

2. Grundbegriffe

Begriff	Bedeutung
Vorfallakte	Verschlüsselte Datei (.dbm) mit allen Angaben, Bewertungen, Meldungen, der Zeitleiste und der Prüfkette eines Vorfalls
Kenntnisnahme	Zeitpunkt, zu dem die Einrichtung vom Vorfall Kenntnis erlangt hat. Er setzt alle Fristen in Gang und lässt sich nur mit Begründung ändern.
Erheblicher Sicherheitsvorfall	Nach § 2 Nr. 11 BSIG ein Vorfall, der schwerwiegende Betriebsstörungen oder finanzielle Verluste verursacht hat oder verursachen kann oder Dritte erheblich beeinträchtigt. Nur erhebliche Vorfälle sind nach § 32 BSIG zu melden.
Meldung	Eine Stufe einer Meldepflicht, z. B. Frühwarnung, Vorfallsmeldung oder Abschlussmeldung, mit eigener Frist und eigenen Pflichtangaben
Meldetext	Von REPORT erzeugter Text mit allen Pflichtangaben zum Übertragen in das Meldeportal
Abgabe	Festgehaltene Abgabe einer Meldung mit Zeitpunkt, Meldeweg, Vorgangsnummer und genauem Wortlaut. Danach ist die Meldung unveränderlich.
Prüfkette	Hash-Kette aller relevanten Handlungen in der Vorfallakte
Prüfwert	Nummer und SHA-256-Hash des letzten Eintrags der Prüfkette, z. B. „Nr. 18 · SHA-256 dcc579…“. Er steht in jeder Meldung und jedem Bericht.
Prüfdatei	Datei mit den Hashes der Prüfkette ohne Inhalte, signierbar mit JUMBO BLOCK CRYPT

3. Arbeitsablauf

1. **Vorfallakte anlegen** – sobald ein Sicherheitsvorfall bekannt wird; Kenntnisnahme genau festhalten (Kapitel 4).
2. **Pflichten bestimmen** – Einstufung nach NIS-2, KRITIS, CRA und DSGVO angeben und die Erheblichkeit bewerten (Kapitel 5).
3. **Fristen überwachen** – der Reiter *Fristen* zeigt, welche Meldung bis wann fällig ist (Kapitel 6).
4. **Melden** – Meldetext erstellen, in das Meldeportal übertragen, Abgabe mit Vorgangsnummer festhalten (Kapitel 7).
5. **Dokumentieren** – Ereignisse und Maßnahmen in der Zeitleiste führen, Einträge aus dem Lagebuch übernehmen (Kapitel 8).
6. **Stand sichern** – Akte regelmäßig speichern; wichtige Stände signieren (Kapitel 10).
7. **Abschließen** – Abschluss- bzw. Fortschrittsmeldungen abgeben, Vorfall als abschließend bearbeitet markieren und Bericht erstellen (Kapitel 9).

Alle Meldungen sind unverzüglich abzugeben – die angezeigten Fristen sind Höchstfristen. Im Zweifel vorsorglich fristgerecht melden; die Frühwarnung kann mit den zu diesem Zeitpunkt verfügbaren Informationen abgegeben werden.

4. Vorfallakte anlegen und öffnen

1. Unter *Neuer Vorfall* die Bezeichnung eingeben, z. B. „Ransomware im Leitsystem Wasserwerk Nord“.
2. *Kenntnis vom Vorfall seit* genau eintragen – Datum und Uhrzeit.
3. Einrichtung bzw. Betreiber und internes Aktenzeichen ergänzen.
4. Passwort mit mindestens 12 Zeichen zweimal eingeben und *Vorfallakte anlegen* klicken.



Abb. 2: Neuen Vorfall anlegen

> Ohne Passwort lässt sich die Akte nicht mehr öffnen – es gibt keine Wiederherstellung.

Die Startseite zeigt außerdem den Rechtsstand der Regeltabelle, nach der REPORT die Fristen berechnet.

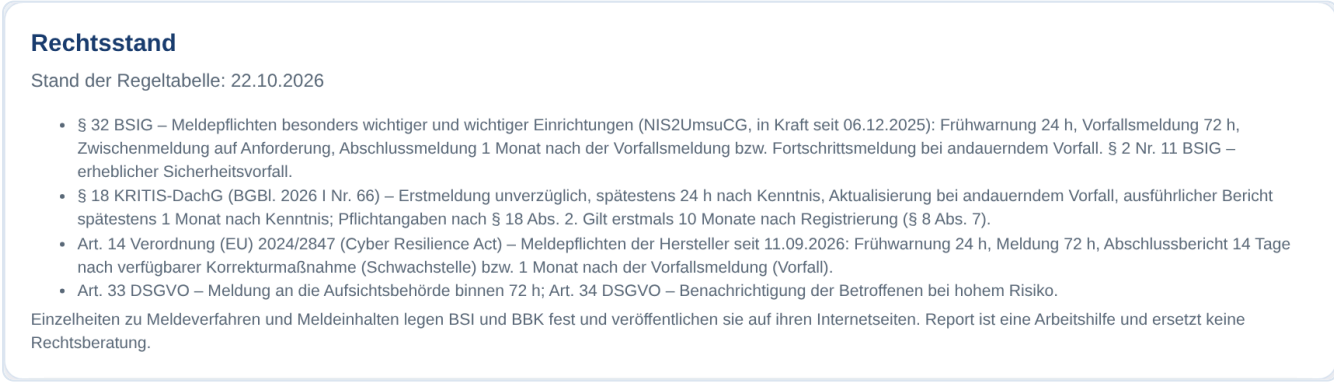


Abb. 3: Rechtsstand der Regeltabelle

Öffnen, sperren, wiederherstellen

- *Vorfallakte öffnen* liest eine vorhandene Datei; danach wird das Passwort abgefragt.
- Die Akte sperrt sich nach 15 Minuten ohne Eingabe. Zum Weiterarbeiten genügt das Passwort.
- Bis zum Speichern wird die Akte zusätzlich verschlüsselt im Browser zwischengespeichert. Nach einem Absturz bietet die Startseite den Stand zur Wiederherstellung an.

5. Vorfall, Meldepflichten und Erheblichkeit

Vorfall

Im Reiter *Vorfall* stehen Bezeichnung, Kenntnisnahme, Einrichtung, Aktenzeichen, Kurzbeschreibung und die meldende Stelle als Kontakt für Rückfragen. Diese Angaben werden in alle Meldetexte übernommen.

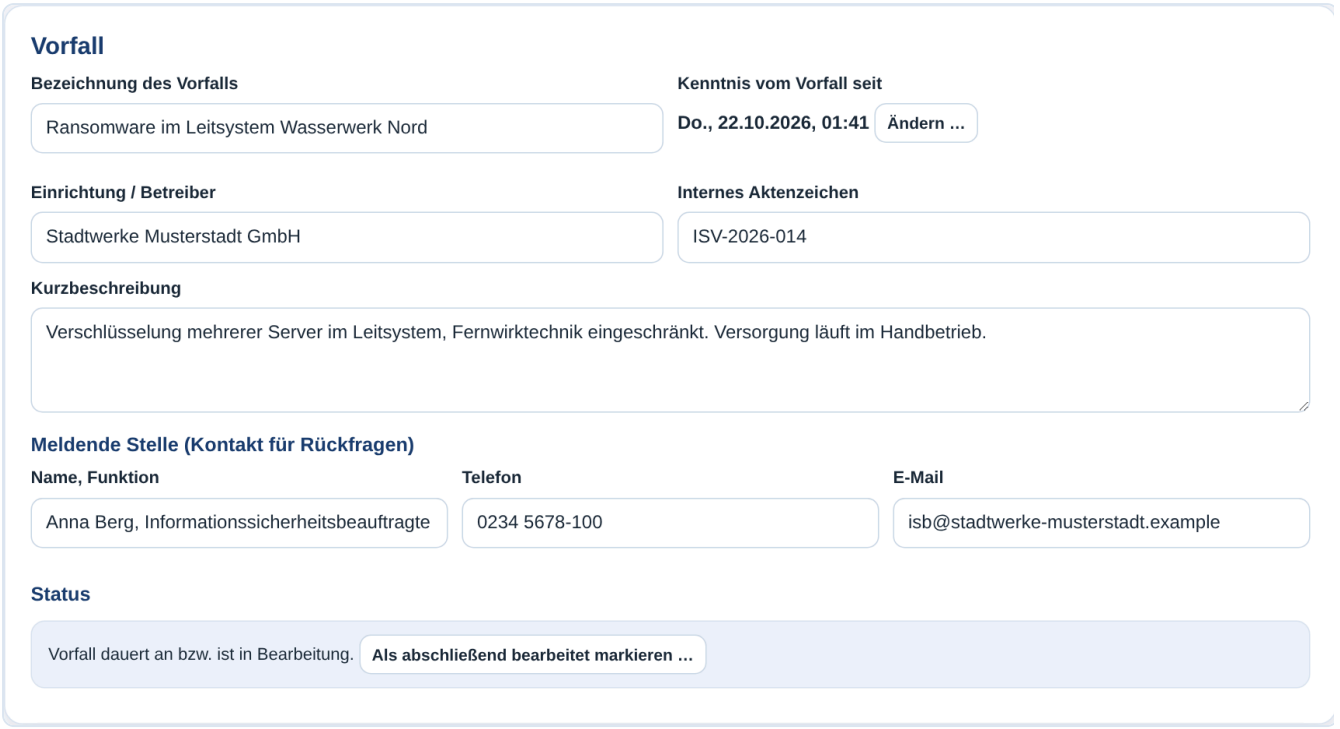


Abb. 4: Angaben zum Vorfall

Ändern … neben der Kenntnisnahme verlangt eine Begründung; die Änderung wird mit altem und neuem Zeitpunkt in der Prüfkette festgehalten. Alle Fristen werden neu berechnet.

Welche Meldepflichten kommen in Betracht?



Abb. 5: Einstufung nach NIS-2, KRITIS, CRA und DSGVO

Frage	Wirkung
NIS-2: Einstufung nach BSIG	Besonders wichtige oder wichtige Einrichtung – Meldepflichten nach § 32 BSIG bei erheblichen Sicherheitsvorfällen
KRITIS: Betreiber einer kritischen Anlage	Kritische Anlage, kritische Dienstleistung und Datum der Registrierung beim BBK. Die Meldepflicht nach § 18 KRITIS-DachG gilt erstmals zehn Monate nach der Registrierung; Anlage und Dienstleistung fließen auch in NIS-2-Meldungen ein (§ 32 Abs. 3 BSIG).
CRA	Für Hersteller von Produkten mit digitalen Elementen: aktiv ausgenutzte Schwachstelle (Art. 14 Abs. 1) und/oder schwerwiegender Vorfall (Art. 14 Abs. 3); dazu Produkt und Zeitpunkt einer verfügbaren Korrektur- oder Abhilfemaßnahme
DSGVO	Verletzung des Schutzes personenbezogener Daten: ja, unklar oder nein. Bei „unklar“ zeigt REPORT die Frist mit dem Hinweis „Meldepflicht prüfen“.

Erheblichkeit

Die Bewertung folgt § 2 Nr. 11 BSIG: schwerwiegende Betriebsstörung, finanzielle Verluste, erhebliche Schäden Dritter – bei KRITIS-Anlagen zusätzlich die erhebliche Beeinträchtigung der kritischen Dienstleistung. Jede Frage wird mit ja, nein oder noch unklar beantwortet; REPORT zeigt sofort das Ergebnis.

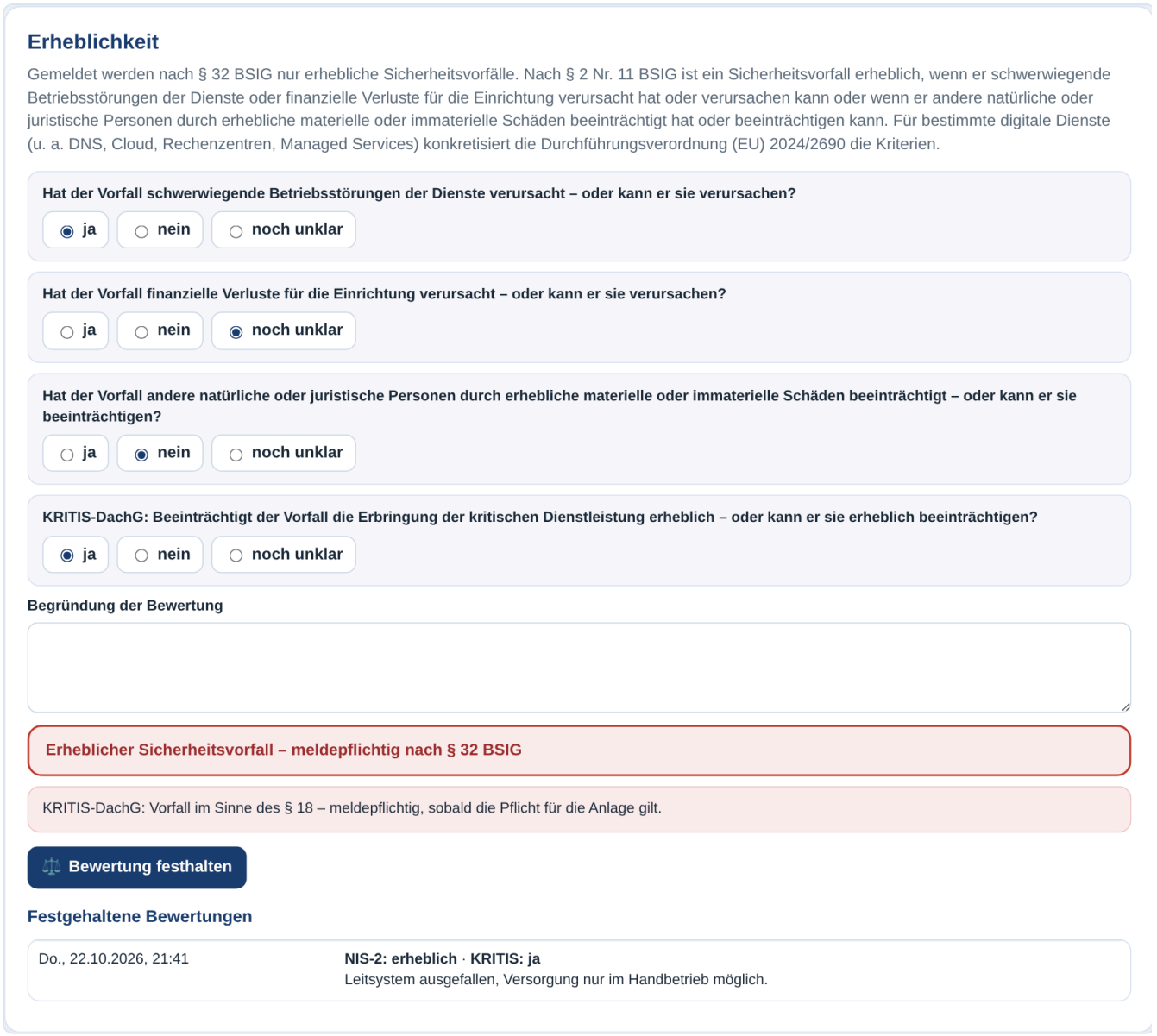


Abb. 6: Bewertung der Erheblichkeit mit Ergebnis und festgehaltener Bewertung

Bewertung festhalten speichert Antworten, Ergebnis und Begründung mit Zeitpunkt in der Prüfkette. Bei neuen Erkenntnissen wird die Bewertung wiederholt; alle Bewertungen bleiben in der Liste *Festgehaltene Bewertungen* erhalten.

Status

Ist der Vorfall abschließend bearbeitet, markieren Sie ihn mit *Als abschließend bearbeitet markieren …*. Das steuert die Abschluss- und Fortschrittsmeldungen. *Wieder öffnen* nimmt die Markierung zurück; beides wird protokolliert.

6. Fristen und Meldewege

Der Reiter *Fristen* listet alle Meldungen, die sich aus den Angaben ergeben, mit Rechtsgrundlage, spätestem Abgabezeitpunkt und Stand. Monatsfristen rechnet REPORT vorsichtig bis zur gleichen Uhrzeit am entsprechenden Tag des Folgemonats.

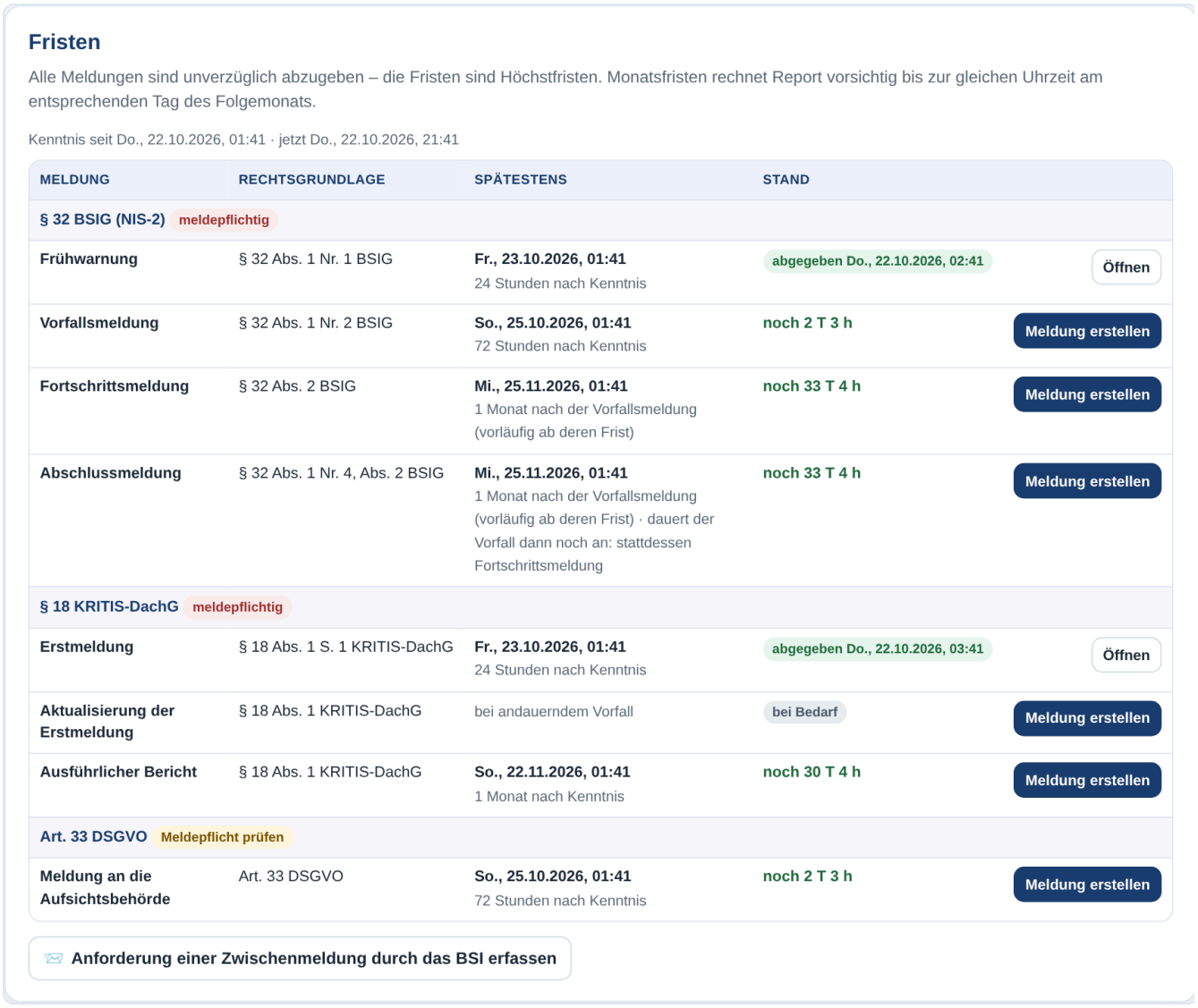


Abb. 7: Fristen mit Stand und Schaltflächen zum Erstellen der Meldungen

Regelung	Meldungen und Fristen
§ 32 BSIG (NIS-2)	Frühwarnung 24 h · Vorfallsmeldung 72 h · Zwischenmeldung auf Anforderung des BSI · Abschlussmeldung 1 Monat nach der Vorfallsmeldung bzw. Fortschrittsmeldung, solange der Vorfall andauert
§ 18 KRITIS-DachG	Erstmeldung 24 h · Aktualisierung bei andauerndem Vorfall · ausführlicher Bericht 1 Monat nach Kenntnis
Art. 14 CRA – Schwachstelle	Frühwarnung 24 h · Schwachstellenmeldung 72 h · Abschlussbericht 14 Tage nach Verfügbarkeit der Korrektur- oder Abhilfemaßnahme
Art. 14 CRA – Vorfall	Frühwarnung 24 h · Vorfallsmeldung 72 h · Abschlussbericht 1 Monat nach der Vorfallsmeldung
Art. 33 DSGVO	Meldung an die Aufsichtsbehörde 72 h

Die Spalte *Stand* zeigt die verbleibende Zeit, „überfällig seit …“ oder „abgegeben“ mit Zeitpunkt. Hängt eine Frist von einer früheren Meldung ab, rechnet REPORT vorläufig ab deren Frist und nach der Abgabe ab dem tatsächlichen Zeitpunkt.

Zwischenmeldung auf Anforderung

Fordert das BSI eine Zwischenmeldung an (§ 32 Abs. 1 Nr. 3 BSIG), halten Sie die Anforderung mit *Anforderung einer Zwischenmeldung durch das BSI erfassen* fest – mit Datum, Frist und Bemerkung. Die Zwischenmeldung erscheint dann mit dieser Frist.

Meldewege

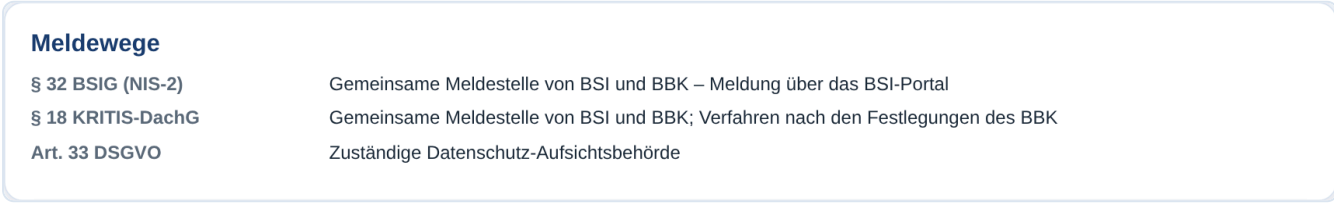


Abb. 8: Meldewege der in Betracht kommenden Meldungen

7. Meldungen erstellen und abgeben

Eine Meldung wird im Reiter *Fristen* über *Meldung erstellen* oder im Reiter *Meldungen* über die Auswahl und *Meldung anlegen* begonnen. Das Formular enthält die gesetzlichen Pflichtangaben der jeweiligen Stufe; Pflichtfelder sind mit * gekennzeichnet. Angaben aus dem Reiter *Vorfall* und aus früheren Meldungen sind vorausgefüllt.

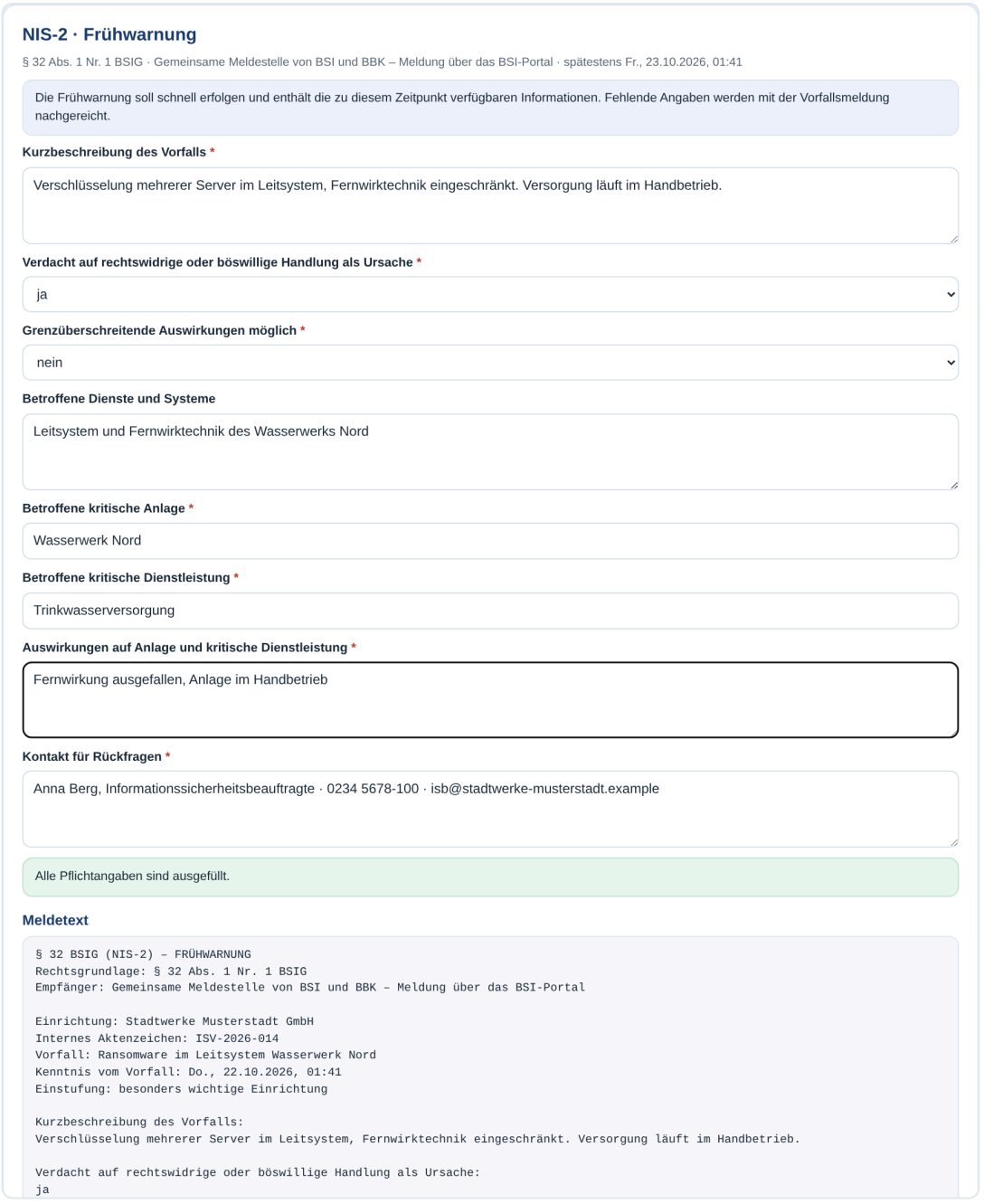


Abb. 9: NIS-2-Frühwarnung mit Pflichtangaben und Meldetext

1. Felder ausfüllen bzw. prüfen. Darunter zeigt REPORT, ob alle Pflichtangaben vorhanden sind.
2. Der *Meldetext* entsteht laufend aus den Angaben. Er beginnt mit Rechtsgrundlage, Empfänger und Kopfdaten und endet mit der Zeile *Prüfwert der Vorfallakte*.

3. *Meldetext kopieren* und in das Meldeportal übertragen. Die Prüfwert-Zeile bitte mit übertragen, z. B. in ein Freitextfeld – sie verankert den Stand der Akte bei der empfangenden Stelle.
4. Nach der Abgabe *Als abgegeben festhalten …* klicken.

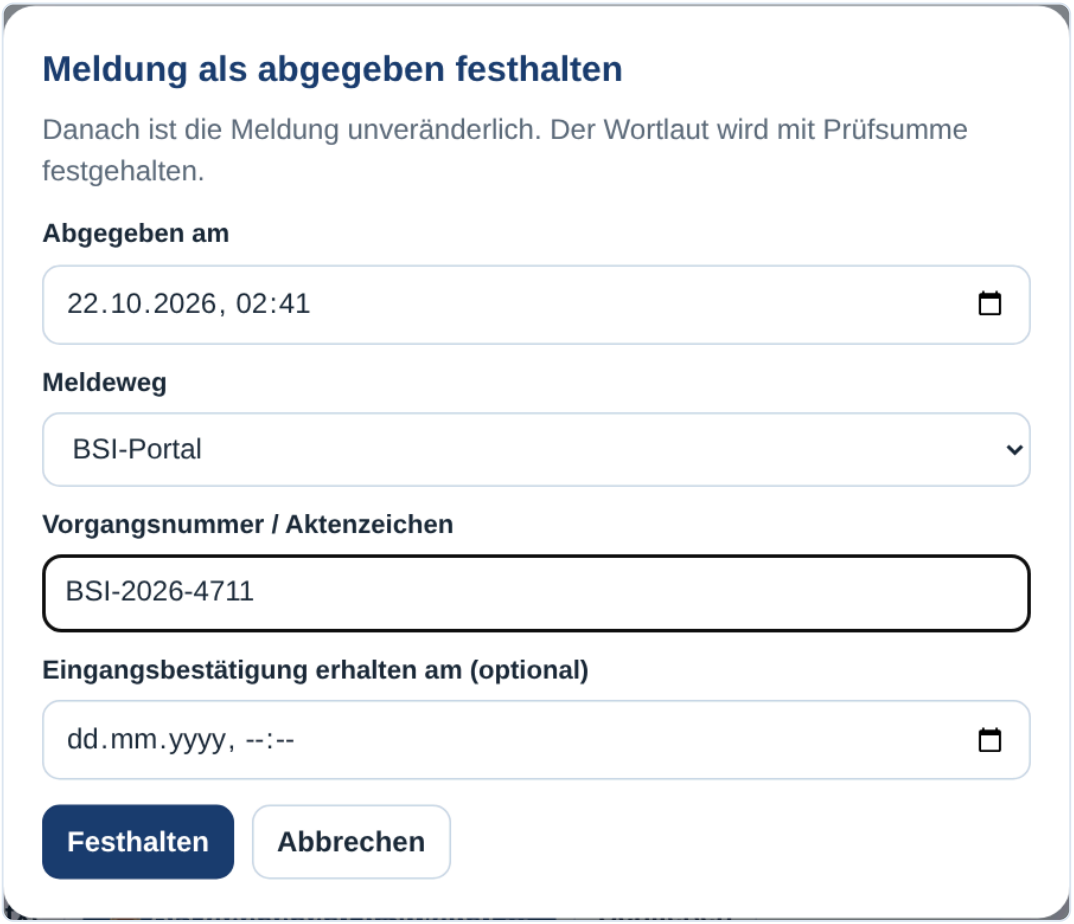


Abb. 10: Abgabe festhalten mit Zeitpunkt, Meldeweg und Vorgangsnummer

Im Dialog tragen Sie Abgabezeitpunkt, Meldeweg, Vorgangsnummer bzw. Aktenzeichen und gegebenenfalls den Eingang der Bestätigung ein. Wurde der Meldetext vorher kopiert und danach noch geändert, fragt REPORT, welcher Wortlaut abgegeben wurde – der zuletzt kopierte oder der aktuelle. REPORT hält genau diesen Wortlaut mit seiner Prüfsumme fest.

Danach ist die Meldung unveränderlich. Mehrfach mögliche Meldungen wie Zwischenmeldungen und Aktualisierungen lassen sich erneut anlegen.



Abb. 11: Übersicht der Meldungen mit Stand und Abgabe

Noch nicht abgegebene Meldungen bleiben als Entwurf in der Akte. Änderungen an Entwürfen werden beim Speichern übernommen, aber erst die Abgabe wird unveränderlich festgehalten.

8. Zeitleiste

Die Zeitleiste sammelt Ereignisse und Maßnahmen für die Meldungen und den Abschlussbericht. REPORT trägt Kenntnisnahme und abgegebene Meldungen selbst ein.

- Eigene Einträge mit Zeit, Art (Ereignis, Maßnahme, Entscheidung, Kommunikation, Meldung, Sonstiges) und Inhalt über *Eintrag hinzufügen*.
- Einträge werden nicht gelöscht, sondern mit Begründung gestrichen. Sie bleiben in der Prüfkette erhalten.

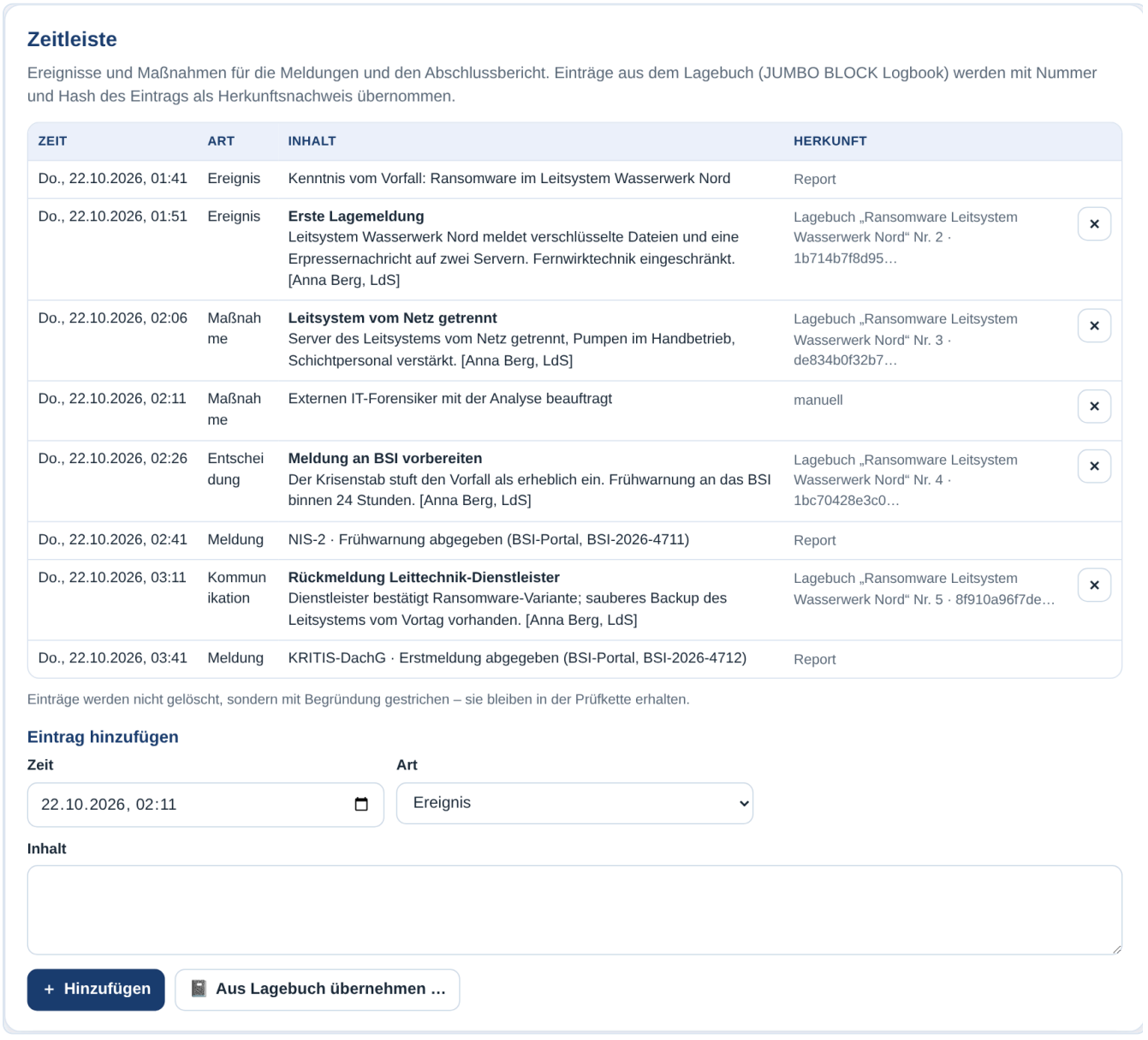


Abb. 12: Zeitleiste mit eigenen Einträgen und Einträgen aus dem Lagebuch

Aus dem Lagebuch übernehmen

Aus Lagebuch übernehmen … öffnet eine Lagebuch-Datei von JUMBO BLOCK LOGBOOK mit deren Passwort – nur lesend; das Lagebuch wird nicht verändert. REPORT prüft die Hash-Kette des Lagebuchs und listet die Einträge.

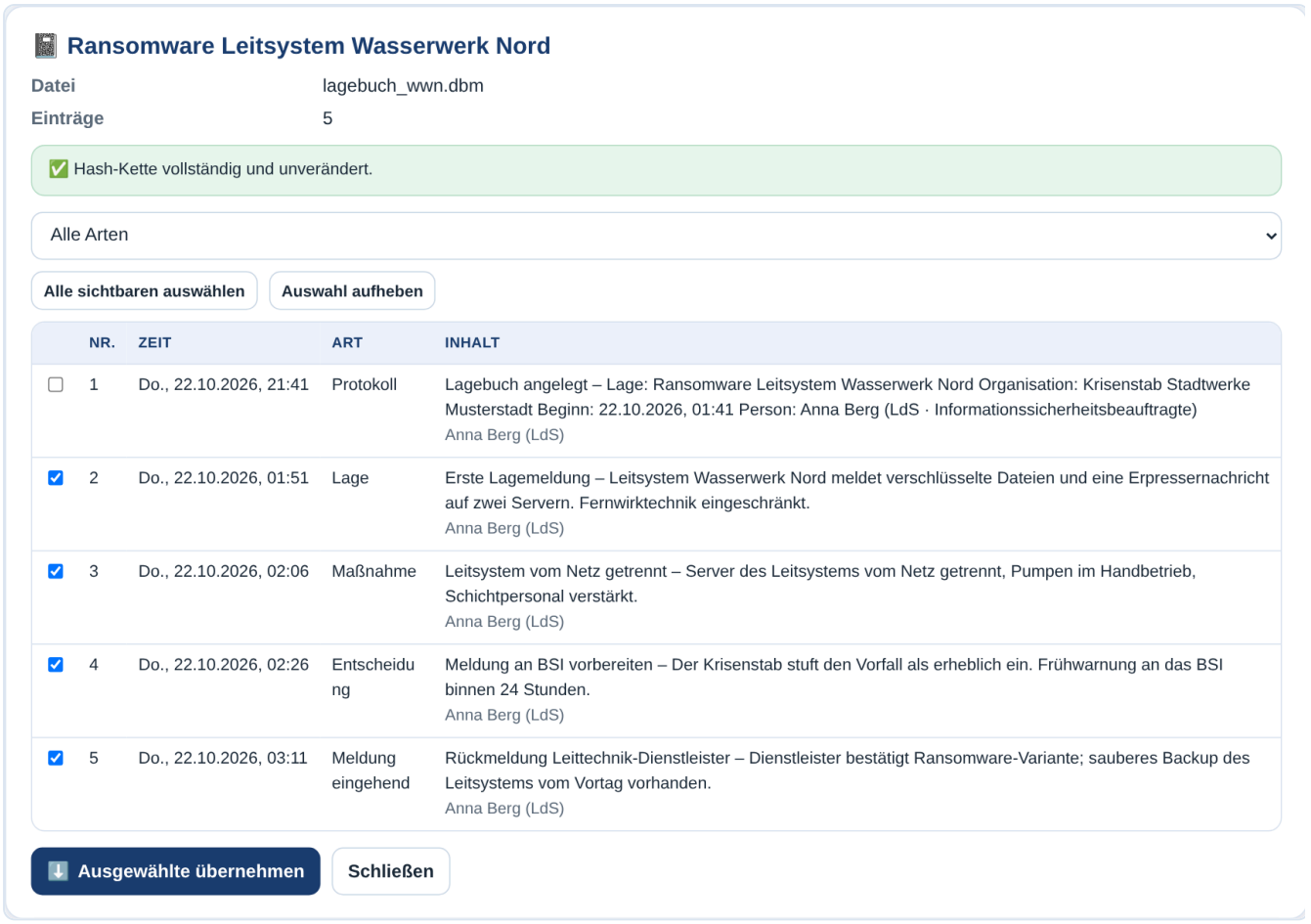


Abb. 13: Auswahl von Einträgen aus dem Lagebuch

Gewünschte Einträge ankreuzen (Filter nach Art, *Alle sichtbaren auswählen*) und *Ausgewählte übernehmen* klicken. Jeder übernommene Eintrag trägt Lagebuch, Nummer und Hash als Herkunftsnachweis. Bereits übernommene Einträge werden nicht doppelt aufgenommen.

9. Bericht

Der Reiter *Bericht* erzeugt die Dokumentation des Vorfalls. *Drucken / PDF* druckt sie oder speichert sie als PDF.



Vorfallbericht – Meldepflichten

Ransomware im Leitsystem Wasserwerk Nord

Prüfwert der Vorfallakte: Nr. 22 · SHA-256 e90f8d60bee3ba9551a5bbcb19852d36a0b57fa44fff4ba9e8539c8d8a96da1c
Prüfbar mit der Vorfallakte in JUMBO BLOCK Report (Reiter „Datei“ → Prüfen). Prüfkette: vollständig und unverändert

1. Vorfall

Einrichtung	Stadtwerke Musterstadt GmbH
Internes Aktenzeichen	ISV-2026-014
Kenntnis vom Vorfall	Do., 22.10.2026, 01:41
Abschließend bearbeitet	nein – andauernd
Kurzbeschreibung	Verschlüsselung mehrerer Server im Leitsystem, Fernwirktechnik eingeschränkt. Versorgung läuft im Handbetrieb.
Kontakt	Anna Berg, Informationssicherheitsbeauftragte · 0234 5678-100 · isb@stadtwerke-musterstadt.example
Kritische Anlage	Wasserwerk Nord – Trinkwasserversorgung (registriert 1.9.2025)

2. Meldepflichten und Erheblichkeit

NIS-2	besonders wichtige Einrichtung
KRITIS-DachG	Betreiber einer kritischen Anlage
CRA	nicht betroffen
DSGVO	unklar

Bewertet am	Ergebnis	Begründung
Do., 22.10.2026, 21:41	NIS-2: ja · KRITIS: ja	Leitsystem ausgefallen, Versorgung nur im Handbetrieb möglich.

Abb. 14: Vorfallbericht mit Prüfwert-Zeile

Abschnitt	Inhalt
1. Vorfall	Alle Angaben zum Vorfall, Kenntnisnahme, Status, meldende Stelle
2. Meldepflichten und Erheblichkeit	Einstufung und alle festgehaltenen Bewertungen
3. Fristen	Alle Meldungen mit Frist und Stand, Rechtsstand der Regeltabelle
4. Abgegebene Meldungen im Wortlaut	Jede Abgabe mit Zeitpunkt, Meldeweg, Vorgangsnummer und genauem Text
5. Zeitleiste	Alle nicht gestrichenen Einträge mit Herkunft
6. Signaturen	Signierte Stände der Akte
7. Prüfkette	Alle Einträge der Prüfkette mit Hash

Jede Seite trägt in der Fußzeile den Prüfwert der Akte zum Zeitpunkt des Drucks.

10. Datei, Prüfkette und Signatur

Vorfallakte speichern



Abb. 15: Vorfallakte mit Speichern, Sperren und automatischem Speichern

Schaltfläche	Wirkung
Speichern / Speichern unter …	Speichert die Akte verschlüsselt. In Chrome und Edge wird beim nächsten Speichern dieselbe Datei überschrieben; mit *Automatisch speichern* nach jeder Änderung.
Sperren	Entfernt den Schlüssel aus dem Arbeitsspeicher
Passwort ändern	Neues Passwort; danach speichern
Schließen	Schließt die Akte; bei ungespeicherten Änderungen fragt REPORT nach

Prüfkette und Prüfwert

Jede relevante Handlung – Anlage, Angaben, Kenntnisnahme, Bewertung, Anforderung, Zeitleiste, Streichung, Abgabe, Abschluss, Passwortänderung, Signatur – wird als Eintrag mit Zeitpunkt und SHA-256-Hash festgehalten. Der Prüfwert ist der Hash des letzten Eintrags. Liegt er bei einer Behörde, im Lagebuch oder in einer Signatur, lässt sich die Akte nachträglich nicht unbemerkt verändern.

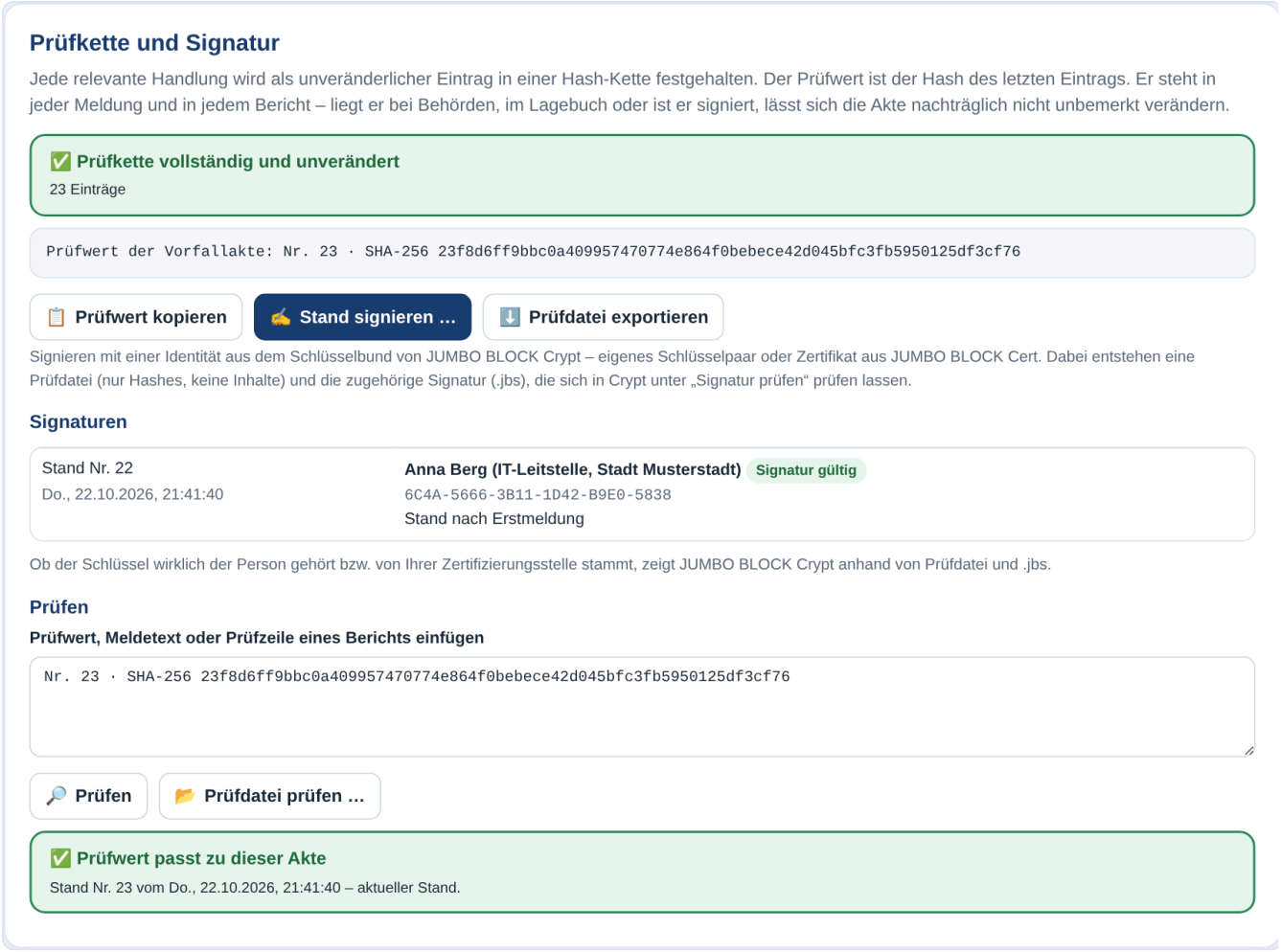


Abb. 16: Prüfkette, Signatur und Prüfung

Stand signieren

Stand signieren … öffnet einen Schlüsselbund von JUMBO BLOCK CRYPT (nur lesend) und signiert den aktuellen Prüfwert mit einer Identität – eigenes Schlüsselpaar oder Zertifikat aus JUMBO BLOCK CERT. Optional wird ein Vermerk angegeben, z. B. „Stand nach Erstmeldung“.



Abb. 17: Stand der Akte signieren

Dabei entstehen eine **Prüfdatei** (nur Hashes, keine Inhalte) und die zugehörige **Signaturdatei (.jbs)**. Beide lassen sich weitergeben – z. B. an Geschäftsführung, Aufsicht oder Versicherung – und in CRYPT unter *Signatur prüfen* prüfen. Die Signatur wird zusätzlich in der Akte vermerkt.

Prüfen

Unter *Prüfen* lässt sich ein Prüfwert, ein vollständiger Meldetext oder die Prüfzeile eines Berichts einfügen. REPORT zeigt, ob der Prüfwert zu dieser Akte passt und – bei einem Meldetext – ob der Wortlaut mit einer abgegebenen Meldung übereinstimmt. *Prüfdatei prüfen …* vergleicht eine Prüfdatei mit der Akte. *Prüfdatei exportieren* erzeugt eine Prüfdatei ohne Signatur.

Prüfkette (Protokoll)

NR.	ERFASST	VORGANG	HASH
23	Do., 22.10.2026, 21:41:40	Stand Nr. 22 signiert von Anna Berg – Stand nach Erstmeldung	`23f8d6ff9bbc0a40…`
22	Do., 22.10.2026, 21:41:37	Zeitleiste: Do., 22.10.2026, 03:11 – Rückmeldung Leittechnik-Dienstleister – Dienstleister bestätigt Ransomware-Variante; sauberes Backup des Leitsystems vom Vortag vorhanden. [Anna Berg, LdS] [Lagebuch „Ransomware Leitsystem Wasserwerk Nord“ Nr. 5 · 8f910a96f7de…]	`e90f8d60bee3ba95…`
21	Do., 22.10.2026, 21:41:37	Zeitleiste: Do., 22.10.2026, 02:26 – Meldung an BSI vorbereiten – Der Krisenstab stuft den Vorfall als erheblich ein. Frühwarnung an das BSI binnen 24 Stunden. [Anna Berg, LdS] [Lagebuch „Ransomware Leitsystem Wasserwerk Nord“ Nr. 4 · 1bc70428e3c0…]	`ffbaacad1a7c8e5b…`
20	Do., 22.10.2026, 21:41:37	Zeitleiste: Do., 22.10.2026, 02:06 – Leitsystem vom Netz getrennt – Server des Leitsystems vom Netz getrennt, Pumpen im Handbetrieb, Schichtpersonal verstärkt. [Anna Berg, LdS] [Lagebuch „Ransomware Leitsystem Wasserwerk Nord“ Nr. 3 · de834b0f32b7…]	`16fa971b309ae6f4…`
19	Do., 22.10.2026, 21:41:37	Zeitleiste: Do., 22.10.2026, 01:51 – Erste Lagemeldung – Leitsystem Wasserwerk Nord meldet verschlüsselte Dateien und eine Erpressernachricht auf zwei Servern. Fernwirktechnik eingeschränkt. [Anna [Lagebuch „Ransomware Leitsystem Wasserwerk Nord“ Nr. 2 · 1b714b7f8d95…]	`1b42928b94093665…`
18	Do., 22.10.2026, 21:41:32	Zeitleiste: Do., 22.10.2026, 02:11 – Externen IT-Forensiker mit der Analyse beauftragt	`6420368bae43d01a…`
17	Do., 22.10.2026, 21:41:30	Zeitleiste: Do., 22.10.2026, 03:41 – KRITIS-DachG · Erstmeldung abgegeben (BSI-Portal, BSI-2026-4712)	`ec40a832980633b6…`
16	Do., 22.10.2026, 21:41:30	Meldung abgegeben: KRITIS-DachG · Erstmeldung – Do., 22.10.2026, 03:41 · BSI-Portal · BSI-2026-4712 · SHA-256 323aefab2c47a0b6…	`3ec7a01ce05dbb14…`
15	Do., 22.10.2026, 21:41:29	Zeitleiste: Do., 22.10.2026, 02:41 – NIS-2 · Frühwarnung abgegeben (BSI-Portal, BSI-2026-4711)	`2a4ab6167b447c05…`
14	Do., 22.10.2026, 21:41:29	Meldung abgegeben: NIS-2 · Frühwarnung – Do., 22.10.2026, 02:41 · BSI-Portal · BSI-2026-4711 · SHA-256 6ce3bd28f1b9b967…	`be43f9df42126338…`
13	Do., 22.10.2026, 21:41:25	Erheblichkeit bewertet: NIS-2 ja · KRITIS ja – Leitsystem ausgefallen, Versorgung nur im Handbetrieb möglich.	`614877cba0ef680e…`
12	Do., 22.10.2026, 21:41:25	Angabe: dsgvo = unklar	`af48f719bd7a9df3…`
11	Do., 22.10.2026, 21:41:25	Angabe: registriert = 2025-09-01	`b473a06a1…`

Abb. 18: Prüfkette (Protokoll)

11. Zusammenspiel mit anderen Programmen

Programm	Zusammenspiel
JUMBO BLOCK LOGBOOK	Einträge des Lagebuchs werden mit Nummer und Hash in die Zeitleiste übernommen. Das Lagebuch wird nur gelesen.
JUMBO BLOCK CRYPT	Identitäten des Schlüsselbunds signieren den Stand der Akte; Prüfdatei und Signatur werden in CRYPT geprüft.
JUMBO BLOCK CERT	Personenzertifikate der eigenen Zertifizierungsstelle als Identität im Schlüsselbund
JUMBO BLOCK KRITIS	Grundlagen und Selbsteinschätzung zu KRITIS-DachG, NIS-2 und CRA vor einem Vorfall

12. Sicherheit und Technik

Bereich	Umsetzung
Vorfallakte	AES-256-GCM, PBKDF2-SHA-256 mit 600 000 Durchläufen; zusätzliche SHA-256-Prüfsumme der Datei
Prüfkette	SHA-256 je Eintrag über den kanonisch geordneten Inhalt einschließlich des Vorgänger-Hashs; Beginn mit „GENESIS“
Abgaben	Wortlaut und SHA-256-Prüfsumme des abgegebenen Meldetexts
Signatur	ECDSA oder RSA mit der Identität aus dem Schlüsselbund von CRYPT; Format kompatibel zu CRYPT
Fristen	Regeltabelle mit Rechtsstand 22.10.2026; Stunden- und Tagesfristen exakt, Monatsfristen bis zum gleichen Tag und zur gleichen Uhrzeit des Folgemonats
Datenschutz	Keine Netzwerkverbindung, keine Telemetrie; Zwischenspeicherung nur verschlüsselt

Grenzen

- REPORT ersetzt keine rechtliche Prüfung. Einzelheiten zu Meldeverfahren und Meldeinhalten legen BSI, BBK und die Aufsichtsbehörden fest.
- REPORT übermittelt keine Meldungen selbst; die Abgabe erfolgt über die Portale der zuständigen Stellen.
- Die Fristen hängen an der richtig erfassten Kenntnisnahme und an der Uhr des Geräts.
- Änderungen der Rechtslage nach dem angegebenen Rechtsstand sind nicht berücksichtigt.

13. Fehlerbehebung

Problem	Ursache und Lösung
Eine erwartete Meldung fehlt in den Fristen	Angaben im Reiter *Vorfall* prüfen: Einstufung, Erheblichkeit, KRITIS-Registrierung (Pflicht erst 10 Monate danach), CRA-Kästchen, DSGVO.
CRA-Abschlussbericht ohne Frist	Zeitpunkt der verfügbaren Korrektur- oder Abhilfemaßnahme im Reiter *Vorfall* eintragen.
„Der Zeitpunkt liegt vor der Kenntnisnahme“	Abgabezeitpunkt prüfen oder die Kenntnisnahme mit Begründung korrigieren.
„Prüfwert passt NICHT zu dieser Akte“	Prüfwert gehört zu einer anderen Akte oder wurde falsch übertragen. Format: „Nr. 12 · SHA-256 …“.
„Der Wortlaut entspricht keiner als abgegeben festgehaltenen Meldung“	Der eingefügte Text wurde verändert oder die Abgabe noch nicht festgehalten.
Lagebuch lässt sich nicht übernehmen	Passwort des Lagebuchs prüfen. Ist die Hash-Kette des Lagebuchs verletzt, zeigt REPORT einen Hinweis.
„Signierer passt nicht zum Schlüssel“	Prüfdatei und Signaturdatei gehören nicht zusammen. Beide Dateien desselben Signiervorgangs verwenden.
Akte nach Absturz verloren	Startseite neu laden; der zwischengespeicherte Stand wird zur Wiederherstellung angeboten.