BSI-ERSTMELDUNG · § 32 ABS. 1 NR. 1 BSIG

Detailcheckliste: Alle Felder der Erstmeldung

Was in den ersten 24 Stunden ins BSI-Meldeportal gehört: Feld für Feld, mit praktischem Hinweis.

Block 1 · Organisatorische Grunddaten: Wer meldet?

- [ ] **Identifikation der meldenden Einrichtung**
  Name, Rechtsform, Adresse, Handelsregisternummer. Nach BSI-Registrierung im Portal hinterlegt, vor dem Ernstfall prüfen, ob die Daten noch aktuell sind. Änderungen müssen binnen 2 Wochen gemeldet werden.
- [ ] **BSI-Registrierungsnummer / Portal-ID**
  Wird bei Erstregistrierung vergeben. Ohne gültige Registrierung keine Meldung möglich. Das Portal erfordert ELSTER-Authentifizierung. Zugangsdaten vor dem Ernstfall sichern und allen Beteiligten zugänglich machen.
- [ ] **Kontaktperson (Name, Funktion, 24/7-Erreichbarkeit)**
  BSI-Pflicht: rund um die Uhr erreichbare Kontaktstelle, auch an Wochenenden und Feiertagen. Primären Ansprechpartner plus Stellvertreter benennen, mit Privathandynummern, nicht nur Bürotelefon.
- [ ] **Meldezeitpunkt dokumentieren**
  Datum und Uhrzeit der Meldungsabgabe. Entscheidend für die Fristdokumentation. Sofort nach Abgabe Screenshot des bestätigten Eingangs anfertigen und archivieren.

Block 2 · Vorfallseinstufung: Was ist passiert?

- [ ] **Einstufung des Vorfalls**
  BSI-Portal-Kategorien: (A) Erheblicher Sicherheitsvorfall, meldepflichtig; (B) Sicherheitsvorfall, freiwillig; (C) Beinahevorfall, freiwillig. Nur Kategorie A ist Pflicht. Im Zweifel höher einstufen, die Herabstufung in der 72h-Folgemeldung ist jederzeit möglich.
- [ ] **Zeitpunkt der Kenntniserlangung**
  Der Moment, ab dem erstmals bekannt war, dass ein Vorfall vorliegt, nicht der Zeitpunkt des Analyseabschlusses. Die 24-Stunden-Frist läuft ab diesem Moment. Exaktes Datum und Uhrzeit sofort festhalten.
- [ ] **Kurzbeschreibung des Vorfalls (Freitext)**
  3 bis 5 Sätze: Art des Vorfalls, erstbekannte Auswirkungen, betroffene Systeme. Vollständigkeit ist nicht erforderlich, Pünktlichkeit hat Vorrang. „Weitere Details folgen in der 72h-Meldung" ist ausdrücklich zulässig.

Block 3 · Verdachtsangaben: Wie ist es passiert?

- [ ] **Verdacht auf rechtswidrige / böswillige Handlung (Ja / Nein)**
  Gesetzlich explizit gefordert in § 32 Abs. 1 Nr. 1 BSIG. Ransomware, Phishing, gezielter Angriff → Ja. Technischer Ausfall → Nein oder Unbekannt. Im Zweifel: Ja. Eine vorsichtige Einschätzung hat keine strafrechtlichen Konsequenzen.
- [ ] **Vermutete oder bekannte Ursache**
  Soweit in 24 Stunden bekannt: kompromittierte Zugangsdaten, ungepatchte Schwachstelle, Insider-Threat, technischer Defekt. Wenn unbekannt: „Ursache noch ungeklärt, Analyse läuft". Das genügt.

Block 4 · Auswirkungsangaben: Was ist betroffen?

- [ ] **Betroffene Dienstleistung(en)**
  Welche der im BSI registrierten Dienste sind betroffen? Bezug zur Sektorzugehörigkeit herstellen. Diese Angaben aus der Registrierung für den Ernstfall schriftlich vorhalten.
- [ ] **Betroffene IT-Systeme und Anlagenteile**
  Welche Systeme, Server, Anwendungen, Netzwerksegmente sind betroffen? Grobe Kategorisierung genügt für die Erstmeldung, eine vollständige Systemliste ist nicht erforderlich.
- [ ] **Anzahl betroffener Nutzer (Schätzwert)**
  Interne und externe Nutzer. Schätzwert ist ausreichend, z. B. „ca. 200 interne Mitarbeitende, externe Kunden nicht betroffen". Exakte Zahlen folgen in der 72h-Meldung.
- [ ] **Schweregrad / Lageeinstufung**
  BSI-Kategorien: Kritisch / Hoch / Mittel. Im Ernstfall eher höher einschätzen, die Herabstufung in der Folgemeldung ist unkompliziert. Zu niedrige Ersteinstufung kann als Verharmlosung gewertet werden.
- [ ] **Erwartete Dauer der Störung**
  Soweit abschätzbar. „Derzeit unklar, Wiederherstellung läuft" ist eine ausdrücklich zulässige Antwort für die Erstmeldung, es gibt keine Verpflichtung zur Prognose unter Unsicherheit.

Block 5 · Grenzüberschreitende Wirkung: Wer sonst ist betroffen?

- [ ] **Verdacht auf grenzüberschreitende Auswirkungen (Ja / Nein)**
  Gesetzlich explizit gefordert in § 32 Abs. 1 Nr. 1 BSIG. Betrifft der Vorfall Systeme oder Dienste in anderen EU-Ländern oder Dritte im Ausland? Wenn unklar: Nein angeben und in der 72h-Meldung präzisieren.
- [ ] **Betroffene Drittstaaten oder Partner**
  Nur wenn bereits bekannt: welche anderen Länder oder Organisationen könnten mitbetroffen sein? Wenn unbekannt: Feld leer lassen oder „wird ermittelt" eintragen.

Block 6 · Schadensabwehr: Was wurde getan?

- [ ] **Ergriffene Sofortmaßnahmen**
  Was wurde bis zum Zeitpunkt der Meldung unternommen? Netzwerksegmentierung, System-Abschaltung, Passwort-Reset, Backup-Aktivierung, IR-Dienstleister aktiviert. Kurz und faktisch, eine Bewertung der Wirksamkeit ist nicht erforderlich.
- [ ] **Wurde die Beeinträchtigung verhindert oder eingedämmt?**
  Das BSI-Portal fragt explizit: Ja / Nein / Teilweise, mit kurzem Freitext. Ehrliche Einschätzung zum Zeitpunkt der Meldung, Aktualisierung in der 72h-Meldung möglich.

Block 7 · Parallele Meldepflichten: Was noch?

- [ ] **Datenschutzrelevanz prüfen**
  Sind personenbezogene Daten betroffen? → Zusätzlich Meldung an die zuständige Datenschutzbehörde (Landes-DSB oder BfDI) innerhalb 72 Stunden nach Art. 33 DSGVO. Beide Meldungen koordiniert vorbereiten.
- [ ] **Cyber-Versicherung informieren**
  Viele Cyber-Policen verlangen unverzügliche Benachrichtigung, oft 24 bis 48 Stunden nach Kenntnis. Verspätete Meldung kann zur Leistungskürzung führen. Versicherungsvertrag und Schadennummer vorhalten.
- [ ] **Interne Eskalation dokumentieren**
  Wer wurde intern informiert: Geschäftsführung, IT-Leitung, externe IR-Dienstleister, Anwalt? Zeitstempel der internen Benachrichtigungen schriftlich festhalten, sie werden bei einer BSI-Prüfung angefordert.

> ⚠ **Frist-Erinnerung**
>
> Die 24-Stunden-Frist beginnt mit der ersten Kenntnis, nicht mit dem Ende der Analyse. Unvollständige Meldungen sind zulässig und besser als verspätete. Spätere Präzisierung erfolgt in der 72h-Folgemeldung.

Rechtsgrundlage: § 32 Abs. 1 Nr. 1 BSIG n. F. (NIS2UmsuCG). Orientierungshilfe auf Basis der gesetzlichen Anforderungen und der BSI-Portaldokumentation. Ersetzt keine Rechtsberatung.

BSI-Meldeportal: portal.bsi.bund.de · Stand: September 2026