Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anleitung zur Mängel-Dokumentation in der Mängelliste

Version zu Mängelliste-Version 1.3 mit dem Stand: 06.2023

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	19.02.2024	WG 14	Initiale Fassung

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6166
E-Mail: kritische.infrastrukturen@bsi.bund.de
Internet: www.bsi.bund.de

Inhalt

1 Beschreibung

1.1 Einleitende Hintergrundinformation

Eine Kritische Infrastruktur im Sinne des BSI-Gesetzes (BSIG) und der BSI-Kritisverordnung (BSI-KritisV) betreibt, wer festgelegte qualitative und quantitative Kriterien erfüllt. Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) müssen gemäß § 8a Absatz 3 BSIG ihre Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, gegenüber dem BSI auf geeignete Weise nachweisen.

Nachweispflichtig sind alle Betreiber Kritischer Infrastrukturen gemäß BSI-KritisV, mit Ausnahme der in § 8d Absatz 2 BSIG genannten Betreiber.

Für jede nachweispflichtige Infrastruktur bzw. Anlage müssen KRITIS-Betreiber Nachweisdokumente beim BSI einreichen. Diese umfassen sowohl allgemeine Informationen über Art und Umfang der durchgeführten Prüfungen als auch eine Liste der aufgedeckten Sicherheitsmängel.

Das BSI kann zudem gemäß § 8a Absatz 3 BSIG „[...] die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln ggf. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder ggf. im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen." Sollten Fragen nicht final geklärt werden können, so kann das BSI sich außerdem durch eigene Vor-Ort-Prüfungen entsprechend § 8a Absatz 4 BSIG einen eigenen Eindruck von Sicherheitsvorkehrungen des KRITIS-Betreibers verschaffen.

1.2 Zielsetzung

Die Mängelliste ist Teil der Nachweisdokumente gemäß § 8a Absatz 3 BSIG und muss als Anlage zu den Nachweisformularen vom KRITIS-Betreiber an das KRITIS-Büro des BSI übersendet werden. Das vorliegende Dokument soll KRITIS-Betreibern und prüfenden Stellen eine Anleitung zur ordnungsgemäßen Dokumentation von Sicherheitsmängeln geben, die im Rahmen einer Nachweisprüfung, oder deren Aufbauprüfungen, aufgedeckt wurden.

Für die Erstellung der Mängelliste sind zwingend die *„Anforderungen nach § 8a Absatz 5 BSIG – Grundsätzliche Anforderungen im Nachweisverfahren (GAiN)*" zu beachten (siehe „D.AM.", „D.PE.12", „N.BN.01" und „N.AM.03"). Der Punkt „*N.BN.01*" verpflichtet zur Nutzung der vom BSI vorgegebenen Formulare: *„[...] sind zur Nachweiserbringung für alle Dokumente und Unterlagen vom Betreiber verpflichtend die aktuellen vom BSI zur Verfügung gestellten Formulare und Vorlagen im vorgegebenen Dateiformat zu verwenden. Das BSI veröffentlicht diese in jeweils aktueller Version und gibt gegebenenfalls Übergangsfristen an. Eine abweichende Einreichung kann nur in begründeten Ausnahmefällen mit schriftlicher Zustimmung des BSI erfolgen.*". Sämtliche Formulare zur Nachweiserbringung finden sich auf der Website des BSI unter KRITIS-Downloads: www.bsi.bund.de/kritis-downloads

Die Steigerung der Datenqualität im Rahmen der Sicherheitsmängelbehandlung und -beseitigung ist das Ziel dieses Dokuments. In diesem Zusammenhang wird die Einhaltung von Vorgaben bei Dokumentation der Mängel- und Maßnahmendaten vorausgesetzt, nicht zuletzt, um eine automatisierte Verarbeitung der Daten zu ermöglichen.

1.3 Abgrenzung

Über dieses Dokument hinausgehende Anforderungen können dem Dokument *„Anforderungen nach § 8a Absatz 5 BSIG – Grundsätzliche Anforderungen im Nachweisverfahren (GAiN)“*[1], oder weiteren Dokumenten wie den Orientierungshilfen (OH), bspw. dem Dokument „Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG“[2], entnommen werden. Die Art und Weise der Einreichung von Nachweisdokumenten, insbesondere der Mängelliste, ist nicht Gegenstand dieses Dokuments.

[1] www.bsi.bund.de/dok/8a5-bsig
[2] www.bsi.bund.de/dok/oh-nachweise

2 Anforderungen

Die aktuelle Vorlage der Mängelliste wird auf der BSI-Webseite zur Verfügung gestellt[3]. Die Anforderungen beziehen sich auf die Version 1.03 mit dem Stand 06.2023. Der grundsätzliche Aufbau dieser Vorlage ist in Abbildung 1 schematisch dargestellt. Das Tabellenblatt mit den aufgeführten Sicherheitsmängeln muss den Namen „Mängelliste“ tragen. Der Aufbau dieser Vorlage darf nicht verändert werden und muss damit unverändert übernommen werden. Dies betrifft sowohl die ersten vier Zeilen, als auch die Spalten. Lediglich darf im Ausnahmefall diese Tabelle um Spalten an der rechten Seite der Liste erweitert werden, sofern dies der Sache bzw. dem Verständnis dient.

2.1 Allgemeiner Aufbau der Vorlage

1	**Mängelliste**										**Mängelliste-Version: 1.3** **Stand: 06.2023**	
2	**Betreiber ID:**	**Stand dieser Mängelliste:**										
3	Mängelliste					Umsetzungsplan				Bewertung der Prüfenden		
4	ID	Mangelbeschreibung	Klassifizierung des Mangels: Thema	Klassifizierung des Mangels: Schwere	KRITIS-Bezug	KRITIS-Risiko	Maßnahmen	Verantwortliche	Termin	Status	Eignung der Maßnahme(n)	Begründung bei Nicht-Eignung
5												

Abbildung 1: Allgemeiner Aufbau der Mängelliste

Die zweite Zeile, beginnend mit „Betreiber ID:“, ist die **Kopfzeile**.

Die dritte Zeile unterteilt die darunterliegenden Felder in Abschnitte auf. Diese sind „**Mängelliste**“, „**Umsetzungsplan**“ und „**Bewertung der Prüfenden**“.

Die vierte Zeile ist die Überschriftenzeile für die Mängelinformationen.

Ab der fünften Zeile sind die Mangelinformationen durch den Prüfenden und den KRITIS-Betreiber zu dokumentieren.

2.2 Aufbau der Kopfzeile

Die Daten, die in der Kopfzeile anzugeben sind, werden nachfolgend erläutert.

„Betreiber ID“ in Zelle A2

- **Beschreibung**

  Eintrag der Betreiber- bzw. Institutions-ID, für den eine Mängelliste eingereicht wird. Diese ID wurde Ihnen im Rahmen der Registrierung als Kritische Infrastruktur zugewiesen.

- **Eingrenzung/Validitätsbereich**

  Diese ID besteht aus einer fünfstelligen Zeichenfolge

- **Beispielinhalt**

  „Betreiber ID: 3zci7“

„Stand dieser Mängelliste“ in Zelle C2

- **Beschreibung**

  Der Zeitpunkt, zu dem dieser Stand der Sicherheitsmängelbeseitigung gilt, ist hier aufzuführen. Diese Angabe ist demnach bei jeder Aktualisierung anzupassen.

- **Eingrenzung/Validitätsbereich**

  Der Zeitpunkt ist im Format TT.MM.JJJJ anzugeben, wobei „T“ für den Tag, „M“ für den Monat und „J“ für das Jahr steht.

- **Beispielinhalt**

  „Stand dieser Mängelliste: 31.12.2024“

[3] www.bsi.bund.de/dok/kritis-maengelliste

2.3 Aufbau der Abschnitte

Erläuterung der Daten der Kopfzeile der Mängelliste

Die unter der Kopfzeile aufgeführten Spalten sind in folgende Abschnitte unterteilt:

1. Mängelliste
2. Umsetzungsplan
3. Bewertung der Prüfenden

Diese Abschnitte werden in chronologischer Reihenfolge befüllt, wie in Abbildung 2 dargestellt.

Abbildung 2: Chronologischer Ablauf mit Zuständigkeiten während der Erstellung einer Mängelliste

2.3.1 Abschnitt 1 – Mängelliste

Der **Abschnitt 1 (Mängelliste)** ist durch die Prüfenden zu erfassen. Wird eine Abweichung zu den Anforderungen gemäß § 8a Absatz 1 bzw. Absatz 1a BSIG festgestellt, handelt es sich um einen Sicherheitsmangel, der in der Mängelliste zu dokumentieren und in Bezug auf die Erbringung der kritischen Dienstleistung zu bewerten ist. Grundsätzlich sind alle Feststellungen, die ein Risiko darstellen oder eine korrigierende Maßnahme benötigen, die nicht ohne Zeit- oder Ressourcenaufwand umgesetzt werden können, in den Prüfbericht und der Mängelliste aufzunehmen. Die Sicherheitsmängel sowie deren Bewertung in Bezug auf die Erbringung der kritischen Dienstleistung sind zu erfassen, wobei jeder Sicherheitsmangel nachvollziehbar in seiner Art beschrieben sein muss. Für das BSI muss ersichtlich sein, warum der beschriebene Umstand einen Sicherheitsmangel darstellt. Für gängige Sicherheitsmängel ist eine einfache Beschreibung in der Regel ausreichend; für Sicherheitsmängel an nicht weit verbreiteten bzw. selten eingesetzten Systemen sind regelmäßig weitergehende Erläuterungen notwendig.

Identifizierte Sicherheitsmängel sind auch dann in die Mängelliste aufzunehmen, wenn diese durch den Betreiber direkt im Rahmen der Prüfung behoben werden. Die entsprechende erfolgte Behebung kann dann, wie in Abschnitt 2.3.2 erläutert, im Umsetzungsplan dokumentiert werden.

Wird im Rahmen der Prüfung auf bestehende zurückliegende Überprüfungen (beispielsweise im Rahmen von Zertifizierungen oder alten Nachweisprüfungen) zurückgegriffen und wurden in diesen Überprüfungen Sicherheitsmängel im Geltungsbereich der Kritischen Infrastruktur aufgedeckt, sind diese ebenfalls in der Mängelliste aufzuführen. Darüber hinaus sind nicht bereits vollständig abgestellte Mängel vorangegangener Nachweisprüfung(en) im Sinne des § 8a Absatz 3 BSIG im Verständnis des Punktes D.AM.03 nach GAiN aufzunehmen.

Die Daten, die im Abschnitt 1 – Mängelliste anzugeben sind, werden nachfolgend erläutert.

„ID“ in Spalte A

- **Beschreibung**

  Eindeutige Referenz oder Kennung, um die Kommunikation über die Sicherheitsmängel zu erleichtern.

  Sicherheitsmängel vorangehender Prüfungen, die zum Zeitpunkt der aktuellen Prüfung aus Sicht des Prüfers nicht vollständig behobenen sind, sind mit der ID, samt Präfix "ALT-[JAHR]-" in die aktuelle Mängelliste zu übernehmen. Darüber hinaus sind die Anforderungen gemäß § 8a Absatz 5 BSIG1, D.AM.03 zu berücksichtigen, die eine Plausibilitätsprüfung durch die Prüfenden zur Abstellung aller vorangegangener Sicherheitsmängel fordert.

Sicherheitsmängel sonstiger vorangehender Prüfungen (wie beispielsweise Zertifizierungen), die zum Zeitpunkt der aktuellen Prüfung aus Sicht des Prüfers nicht vollständig behoben sind und im Geltungsbereich der Kritischen Infrastruktur liegen, sind mit der ID, samt Präfix „[Prüfung]-[JAHR]-“ (vgl. Anforderungen gemäß § 8a Absatz 5 BSIG1, N.AM.03) in die aktuelle Mängelliste zu übernehmen.

- **Eingrenzung/Validitätsbereich**

  Um den Sicherheitsmangel eindeutig zu identifizieren, darf die vergebene Kennzeichnung nicht für die Beschreibung eines anderen Sicherheitsmangels verwendet werden. Die IDs müssen also **eindeutig** sein. Sinnvoll ist die Verwendung des Jahres der Prüfung mit einer fortlaufenden Zahl.

- **Beispielinhalt**

  „2023-1“, „2023-2“, „2023-3“ bzw. „1“, „2“, „3“ oder „GA-1“, „GA-2“, „SA-1“, „EM-1“

  (Zur Info: EM=Empfehlung, GA=geringfügige Abweichung, SA=schwerwiegende Abweichung)

  Beispiel: Sicherheitsmangel 3 aus Nachweis 2020 ist bei der Nachweisprüfung 2022 als nicht vollständig behoben identifiziert, so ist dieser Sicherheitsmangel in der Mängelliste 2022 als „ALT-2020-3“ zu übernehmen. (vgl. Anforderungen gemäß § 8a Absatz 5 BSIG1, N.AM.03)

  Sicherheitsmängel aus sonstigen hinzugezogenen Prüfungen sind mit Bezug auf die Prüfung **für Dritte nachvollziehbar** anzugeben. Bspw.: *„ISO27001-2021-1“, „ISO27001-2021-2“, „C5-2022-1“, „SOC2-2022-1“.*

„Mangelbeschreibung“ in Spalte B

- **Beschreibung**

  Eine für **Dritte nachvollziehbare** und **verständliche** Beschreibung des Sicherheitsmangels mit zusammenfassender Überschrift. Insbesondere ist darauf zu achten, dass keine unternehmensspezifischen Abkürzungen verwendet werden, oder diese sind alternativ zu erläutern.

  Wesentlich ist, dass dem BSI ausreichende Informationen zur Bewertung der jeweiligen Sicherheitsmängel zur Verfügung stehen. Dies stellt die Grundlage für das BSI dar, zu entscheiden, ob die vom KRITIS-Betreiber im Umsetzungsplan vorgesehenen Schritte zur Behebung der Mängel angemessen und ausreichend sind.

- **Eingrenzung/Validitätsbereich**

  Freitextfeld

- **Beispielinhalt**

  „Die Unternehmens-richtlinie zur Passwortkomplexität wird auf den ERP-Systemen nicht angewendet. User, aber insbesondere Administratoren, sind organisatorisch verpflichtet, komplexe Kennwörter zu verwenden. Dies wird jedoch nicht technisch durchgesetzt.“

„Klassifizierung des Mangels: Thema“ in Spalte C

- **Beschreibung**

  Klassifizierung des Sicherheitsmangels anhand untenstehender Auswahlliste.

  Kategorien aus Anhang E der Orientierungshilfe zu Nachweisen (Version 1.2)[2]:

  „Für die thematische Klassifizierung von Sicherheitsmängeln sollen folgende Kategorien genutzt werden:

  1. Informations-Sicherheits-Management-System (ISMS)

  2. Asset Management

  3. Continuity- und Notfallmanagement für die kDL

  4. Technische Informationssicherheit

4.1 Absicherung von Netzübergängen

4.2 Sichere Interaktion im Internet

4.3 Sichere Software (insbesondere Vermeidung von offenen Sicherheitslücken)

4.4 Sichere und zuverlässige Hardware

4.5 Sichere Authentisierung

4.6 Verschlüsselung

4.7 Sonstiges

5. Personelle und organisatorische Sicherheit

6. Bauliche/physische Sicherheit

7. Vorfallserkennung und -bearbeitung

8. Überprüfung im laufenden Betrieb

9. Lieferanten, Dienstleister und Dritte

10. Branchenspezifische Technik und (Kern-) Komponenten (Beschaffung, Entwicklung, Einsatz, Betrieb und Wartung).“

- **Eingrenzung/Validitätsbereich**
  Die Sicherheits-mängel sind ausschließlich in die genannten und in der Mängelliste vorhandenen Kategorien einzuordnen.

  Nur zulässige Kategorien lassen sich über eine Auswahlliste in der Spalte „C“ selektieren. Ein Umgehen dieser Auswahl ist nicht zulässig und führt zu einer inkonsistenten Mängelliste.

- **Beispielinhalt**
  Über die Auswahlliste wird die entsprechende Kategorie ausgewählt, bspw. *„4. Technische Informationssicherheit“*.

„Klassifizierung des Mangels: Schwere“ in Spalte D

- **Beschreibung**
  Schwere des Sicherheitsmangels (Auswahlliste)
  Definition der Sicherheitsmängelkategorien in Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSI (Version 1.2)[2], Kapitel 5.7.2:
  „*Für die Klassifizierung der Schwere der Sicherheitsmängel sind Sicherheitsmängelkategorien zu definie-ren und im gesamten Prüfbericht einheitlich zu verwenden. In der Mängelliste des Nachweisdokuments, das an das BSI gesendet wird, müssen jedoch einheitliche Sicherheitsmängelbewertungen vorgenommen werden. Abweichungen in der Kategorie „Schwerwiegend“ und „Geringfügig“ müssen in der Mängelliste aufgenommen werden, „Empfehlungen“ sollten aufgenommen werden.“*

- **Eingrenzung/Validitätsbereich**
  Die Schwere der Sicherheitsmängel ist ausschließlich in den genannten und in der Mängelliste vorhandenen Kategorien einzuordnen. Diese sind:
  – Schwerwiegende/-r oder erhebliche/-r Abweichung/Sicherheitsmangel
  – Geringfügige/-r Abweichung/Sicherheitsmangel
  – Empfehlung

  Nur zulässige Kategorien lassen sich über eine Auswahlliste in der Spalte „D“ selektieren. Ein Umgehen dieser Auswahl ist nicht zulässig und führt zu einer inkonsistenten Mängelliste.

- **Beispielinhalt**

  Über die Auswahlliste wird der entsprechende Wert ausgewählt, bspw. „Schwerwiegende/-r oder erhebliche/-r Abweichung/Sicherheitsmangel“.

„KRITIS-Bezug“ in Spalte E

- **Beschreibung**

  Benennung der Auswirkung des Sicherheitsmangels.

  „Eine Benennung des Teils der KRITIS inklusive einer konkreten Referenz auf die geprüfte Anlage, auf den der Sicherheitsmangel sich konkret auswirkt, bzw. auswirken kann. Bei weitreichenden Auswirkungen beschränkt auf die wichtigsten Teilsysteme oder eine überblicksartige Beschreibung.“

  Sofern sich die Nachweisprüfung über mehrere Anlagen erstreckt bzw. es sich eine gemeinsame Anlage handelt, ist eine konkrete Referenz auf die geprüfte Anlage, auf die sich der Sicherheitsmangel auswirkt bzw. auswirken kann anzugeben. Bei weitreichenden Auswirkungen beschränkt auf die wichtigsten Teilsysteme oder eine überblickartige Beschreibung.

- **Eingrenzung/Validitätsbereich**

  Freitextfeld

- **Beispielinhalt**

  „ERP-System zur Behandlung/Bestellung/Distribution/Inverkehrbringen.“

  Im Falle von mehreren geprüften Anlagen innerhalb einer Nachweiserbringung: *„ERP-System für die Anlage X zur Behandlung/Bestellung/Distribution/Inverkehrbringen.“*

„KRITIS-Risiko“ in Spalte F

- **Beschreibung**

  Bewertung des Sicherheitsmangels im Hinblick auf die Erbringung der kritischen Dienstleistung: textuelle Beschreibung.

  Die Beschreibung soll **für Dritte verständlich** sein. Bezieht sich der Mangel auf konkrete Prozesse, Systeme oder Dienste, sind diese und ihre Relevanz für die Kritische Infrastruktur kurz zu erläutern.

- **Eingrenzung/Validitätsbereich**

  Freitextfeld

- **Beispielinhalt**

  „Eine Übernahme eines privilegierten Kontos kann erhebliche Auswirkungen auf die Verfügbarkeit der kDL haben, jedoch ist der administrative Zugriff nur aus einem isolierten und gesicherten Adminnetz möglich. Nicht privilegierte Konten haben eingeschränkte Rechte und können nur geringe Störungen hervorrufen. Anomalien würden von einem SIEM erkannt und zeitnah kontrolliert werden.“

2.3.2 Abschnitt 2 – Umsetzungsplan

Der **Abschnitt 2 (Umsetzungsplan)** ist durch den/die KRITIS-Betreiber zu erfassen. Die entsprechend einzureichenden Daten werden nachfolgend erläutert.

Die Daten, die im Abschnitt 2 – Umsetzungsplan anzugeben sind, werden nachfolgend erläutert.

„Maßnahmen“ in Spalte G

- **Beschreibung**

  Eine **für Dritte nachvollziehbare** und **verständliche** Beschreibung geplanter Maßnahmen zur plausiblen Abstellung des Sicherheitsmangels. Sind mehrere Maßnahmen zur Beseitigung eines Sicherheitsmangels erforderlich, so sind jeweilige Maßnahmen in separate Zeilen aufzuteilen.

- **Eingrenzung/Validitätsbereich**

  Freitextfeld

- **Beispielinhalt**

  „Die Übernahme der Kennwortrichtlinien wird als Change beim ERP-Hersteller beauftragt“

Sollten zwei oder mehrere Maßnahmen zur Behebung eines Sicherheitsmangels erforderlich sein, so sind diese in separaten Zeilen in den Feldern „Maßnahmen“ bis „Status“ zu dokumentieren. Dabei bleiben die Felder innerhalb des Abschnitts Mangelliste leer und zeigen somit die Zugehörigkeit zum vorherigen Sicherheitsmangel an. Alle Spalten einer Maßnahme im Abschnitt Umsetzungsplan müssen dokumentiert werden. Die Angabe mehrerer Maßnahmen zu einem Sicherheitsmangel ist beispielhaft in Abbildung 3 dargestellt.

Mängelliste

Betreiber ID: **Stand dieser Mängelliste:**

Mängelliste						Umsetzungsplan			
ID	Mangelbeschreibung	Klassifizierung des Mangels: Thema	Klassifizierung des Mangels: Schwere	KRITIS-Bezug	KRITIS-Risiko	Maßnahmen	Verantwortliche	Termin	Status
1	Beispielabweichung A	4. Technische Informationssicherheit	Geringfügige/-r Abweichung/Sicherheitsmangel	Bezug der Abweichung A	Risiko der Abweichung A	Maßnahme 1 zur Abweichung A sieht vor, dass…	IT-SiBe	30.06.2023	90%
						Maßnahme 2 zur Abweichung A sieht vor, dass…	Administrator	30.09.2023	60%
						Maßnahme X zur Abweichung A sieht vor, dass…	…	…	…
2	Beispielabweichung B	2. Asset Management	Geringfügige/-r Abweichung/Sicherheitsmangel	Bezug der Abweichung B	Risiko der Abweichung B	Maßnahme zur Abweichung B	…	…	…

Abbildung 3: Mehrere Maßnahmen zu einer Abweichung dokumentieren.

„Verantwortliche“ in Spalte H

- **Beschreibung**

  Benennung der verantwortlichen Rolle bzw. Funktion zur Abstellung des Sicherheitsmangels.

- **Eingrenzung/Validitätsbereich**

  Freitextfeld

- **Beispielinhalt**

  „IT-SiBe, ERP-Hersteller, ERP-Administration“

„Termin“ in Spalte I

- **Beschreibung**

  Je Maßnahme ist ein geplanter Abschlusstermin zu benennen. Dieser geplante Abschlusstermin ist das Enddatum der Umsetzung zur **vollständigen** Umsetzung der Maßnahme.

- **Eingrenzung/Validitätsbereich**

  Der geplante Termin zur Umsetzung der Maßnahme ist konkret als Datum anzugeben. Sollte eine Quartalsangabe gewünscht sein, so ist das letzte Datum des jeweiligen Quartals zu benennen. Die Angabe hat im Format TT.MM.JJJJ (T=Tag, M=Monat, J=Jahr) zu erfolgen.

  Ein Umgehen dieser Auswahl ist nicht zulässig und führt zu einer inkonsistenten Mängelliste.

- **Beispielinhalt**

  „01.01.2023“ oder „31.12.2023“

„Status“ in Spalte J

- **Beschreibung**

  Dieser Status spiegelt die Umsetzung der jeweiligen Maßnahme zur Abstellung des Sicherheitsmangels wider.

- **Eingrenzung/Validitätsbereich**

  Der Fortschritt zur Umsetzung der Maßnahme ist in Prozentwert anzugeben, im ganzzahligen Wertebereich zwischen 0 % und 100 %.

  Eine Maßnahme, deren Umsetzung noch nicht begonnen hat, ist mit 0 % zu kennzeichnen. Maßnahmen, die zur Abstellung von Mängeln geführt haben, sind im Verlauf mindestens einmal mit 100 % dem BSI im Rahmen des Mängelmonitorings vorzulegen.

  Ein Umgehen dieser Auswahl ist nicht zulässig und führt zu einer inkonsistenten Mängelliste.

- **Beispielinhalt**

  „1 %“, „5 %“ oder „10 %“ bzw. „50 %“

2.3.3 Abschnitt 3 – Bewertung der Prüfenden

Der **Abschnitt 3 (Bewertung der Prüfenden)** ist durch den/die Prüfenden zu bewerten und auszufüllen. Diese Bewertung bezieht sich auf die vom KRITIS-Betreiber genannten Maßnahmen zur Abstellung des Sicherheitsmangels und soll sicherstellen, dass das Verständnis über den Sicherheitsmangel beim Betreiber und der/den Prüfenden übereinstimmt sowie dass die durch den Betreiber festgelegten Maßnahmen geeignet sind, den Mangel adäquat zu beseitigen. Die Daten, die im Abschnitt 3 –Bewertung der Prüfenden anzugeben sind, werden nachfolgend erläutert.

„Eignung der Maßnahme(n)“ in Spalte K

- **Beschreibung**

  Eine prüfende Person beurteilt unter Berücksichtigung der Ergebnisse der Prüfung, ob die vom KRITIS-Betreiber geplanten Maßnahmen geeignet sind, um die identifizierten Sicherheitsmängel zu beseitigen. Halten die Prüfenden eine oder mehrere Maßnahmen in der Beurteilung für ungeeignet, müssen diese Prüfenden eine kurze Begründung in der Liste hinzufügen. (vgl. Anforderungen gemäß § 8a Absatz 5 BSIG, D.PE.12)

- **Eingrenzung/Validitätsbereich**

  Auswahlfeld mit möglichen Optionen:

  „Maßnahme(n) ist/sind geeignet.“

  „Maßnahme(n) ist/sind nicht geeignet.“

- **Beispielinhalt**

  „Maßnahme(n) ist/sind geeignet.“ bzw. „Maßnahme(n) ist/sind nicht geeignet.“

„Begründung bei Nicht-Eignung“ in Spalte L

- **Beschreibung**

  Eine Begründung ist nur dann erforderlich, sofern die Maßnahme als **nicht geeignet** bewertet wird. Die Bewertung muss hierbei nachvollziehbar begründet werden. (vgl. Anforderungen gemäß § 8a Absatz 5 BSIG, D.PE.12)

- **Eingrenzung/Validitätsbereich**

  Freitextfeld

- **Beispielinhalt**

  „Die aufgeführte Maßnahme aus dem dokumentierten Sachverhalt erfüllt nicht den Stand der Technik, da die eingesetzten kryptologischen Algorithmen als veraltet und ‚gebrochen' gelten."