

# MRIS.bd.2.2

## Datensicherungssysteme

MRIS.bd: Benutzerdefinierte Schicht — Mythos-resistente Informationssicherheit

Systembaustein der Bausteinfamilie MRIS.bd

**Benutzerdefinierter Baustein — keine offizielle Anforderung des BSI**

Version 2.0 | Stand: 19.09.2026 | Autor: Richard Peddi

Lizenz: CC BY-SA 4.0 — die Verwendung in IT-Sicherheitskonzepten nach IT-Grundschutz ist ausdrücklich erwünscht; Bearbeitungen und Weitergabe erfolgen unter denselben Bedingungen

# Inhaltsverzeichnis

|                                                                                   |          |
|-----------------------------------------------------------------------------------|----------|
| <b>1 Beschreibung .....</b>                                                       | <b>3</b> |
| 1.1 Einleitung .....                                                              | 3        |
| 1.2 Zielsetzung.....                                                              | 3        |
| 1.3 Abgrenzung und Modellierung .....                                             | 3        |
| <b>2 Gefährdungslage.....</b>                                                     | <b>3</b> |
| 2.1 Manipulation von Sicherungen über kompromittierte Administrationsrechte ..... | 4        |
| 2.2 Abschluss des Angriffs vor der Erkennung .....                                | 4        |
| <b>3 Anforderungen .....</b>                                                      | <b>4</b> |
| 3.1 Basis-Anforderungen .....                                                     | 5        |
| MRIS.bd.2.2.A1 Trennung der Administration des Datensicherungssystems (B) .....   | 5        |
| MRIS.bd.2.2.A2 Technische Durchsetzung der Unveränderlichkeit (B) .....           | 5        |
| 3.2 Standard-Anforderungen .....                                                  | 5        |
| 3.3 Anforderungen bei erhöhtem Schutzbedarf .....                                 | 5        |
| <b>4 Weiterführende Informationen.....</b>                                        | <b>5</b> |

# 1 Beschreibung

## 1.1 Einleitung

Datensicherungssysteme speichern oder verwalten die Sicherungskopien, auf die eine Institution nach einem erfolgreichen Angriff angewiesen ist. Dazu gehören Backup-Server, Speichersysteme für Sicherungskopien und Backup-Dienste in der Cloud.

KI-gesteuerte Angriffe können abgeschlossen sein, bevor Erkennung und Reaktion greifen. Dann hängt der Schaden davon ab, ob sich die Daten aus unveränderten Sicherungen wiederherstellen lassen. Unveränderliche Sicherungen sind eine harte strukturelle Barriere: Ihre Schutzwirkung hängt nicht von der Erkennungsgeschwindigkeit ab, sondern davon, dass Angreifer sie auch mit administrativen Rechten nicht löschen oder verändern können.

Dieser Baustein ist Teil der Bausteinfamilie MRIS.bd. Er setzt die im Prozessbaustein MRIS.bd.1 Mythos-resistente Härtung des ISMS festgelegten Vorgaben zur unveränderlichen Datensicherung technisch an den einzelnen Datensicherungssystemen um.

## 1.2 Zielsetzung

Ziel dieses Bausteins ist es, Datensicherungssysteme so abzusichern, dass Sicherungskopien auch nach einer Kompromittierung der Produktionsumgebung weder gelöscht noch verändert werden können.

## 1.3 Abgrenzung und Modellierung

Der Baustein MRIS.bd.2.2 Datensicherungssysteme ist auf jedes System anzuwenden, das Datensicherungen speichert oder verwaltet, etwa Backup-Server, Speichersysteme für Sicherungskopien und Backup-Dienste in der Cloud.

Der Baustein wird ergänzend zu den Bausteinen modelliert, die für diese Zielobjekte ohnehin anzuwenden sind, etwa SYS.1.8 Speicherlösungen. Er ersetzt keinen dieser Bausteine.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- das Datensicherungskonzept (siehe CON.3 Datensicherungskonzept),
- die Vorgaben zu unveränderlichen Sicherungskopien und Wiederherstellungstests (siehe MRIS.bd.1.A3 Vorhalten unveränderlicher Datensicherungen mit regelmäßigen Wiederherstellungstests) sowie
- die phishing-resistente Anmeldung an Administrationszugängen (siehe MRIS.bd.2.1 Identitäts- und Zugangssysteme).

## 2 Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein MRIS.bd.2.2 Datensicherungssysteme von besonderer Bedeutung.

## 2.1 Manipulation von Sicherungen über kompromittierte Administrationsrechte

**Wird die Datensicherung mit Rechten der Produktionsumgebung verwaltet, können kompromittierte Administrationskonten Sicherungen löschen, verschlüsseln oder ihre Unveränderlichkeit aufheben.**

Angreifer, die Administrationsrechte in der Produktionsumgebung erlangt haben, suchen gezielt nach den Sicherungen, bevor sie Daten verschlüsseln oder verändern. Wenn die Datensicherungssysteme über dieselben Konten, Verzeichnisdienste oder Zugangsdaten verwaltet werden wie die Produktionsumgebung, dann genügt ein einziger kompromittierter Zugang, um die Wiederherstellbarkeit zu zerstören. Dasselbe gilt, wenn sich die Unveränderlichkeit mit denselben Administratorrechten wieder abschalten lässt: Die Sicherungen sind dann nur dem Anschein nach geschützt.

## 2.2 Abschluss des Angriffs vor der Erkennung

**KI-gesteuerte Angriffe können abgeschlossen sein, bevor Erkennung und Reaktion greifen; dann entscheidet allein die Wiederherstellbarkeit über den Schaden.**

Agentische Angriffe führen Aufklärung, Rechteausweitung und Verschlüsselung in einer Geschwindigkeit aus, die menschliche Reaktionsketten nicht erreichen (siehe MRIS.bd.1, Kapitel 2.2). Wenn der Schutz der Datensicherung darauf baut, einen Angriff rechtzeitig zu erkennen und zu stoppen, dann bleibt bei einem schnellen Angriff keine Zeit dafür. Agentische Integritätsangriffe können Daten zudem unauffällig verändern, sodass auch jüngere Sicherungen bereits manipulierte Stände enthalten.

## 3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins MRIS.bd.2.2 Datensicherungssysteme aufgeführt. Der ISB ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

| Zuständigkeiten         | Rollen     |
|-------------------------|------------|
| Grundsätzlich zuständig | IT-Betrieb |
| Weitere Zuständigkeiten | –          |

Genau eine Rolle sollte Grundsätzlich zuständig sein. Darüber hinaus kann es noch Weitere Zuständigkeiten geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt.

### **3.1 Basis-Anforderungen**

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

#### **MRIS.bd.2.2.A1 Trennung der Administration des Datensicherungssystems (B)**

Das Datensicherungssystem MUSS über eigene, von der Produktionsumgebung getrennte Zugriffswege und Berechtigungen verwaltet werden. Zugangsdaten für die Administration des Datensicherungssystems SOLLTEN NICHT in der Produktionsumgebung hinterlegt werden.

#### **MRIS.bd.2.2.A2 Technische Durchsetzung der Unveränderlichkeit (B)**

Falls Sicherungskopien unveränderlich vorgehalten werden, dann MUSS die Unveränderlichkeit technisch erzwungen werden. Die Aufbewahrungssperre MUSS so konfiguriert werden, dass sie während der Aufbewahrungsfrist auch mit administrativen Rechten nicht aufgehoben werden kann. Die Aufbewahrungs- und Sperreinstellungen SOLLTEN dokumentiert werden.

### **3.2 Standard-Anforderungen**

Für diesen Baustein sind keine Standard-Anforderungen definiert.

### **3.3 Anforderungen bei erhöhtem Schutzbedarf**

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

## **4 Weiterführende Informationen**

Das Framework „Mythos-resistente Informationssicherheit (MRIS)“ (Version 2.0) und der „MRIS Implementation Guide“ (Version 2.0) beschreiben das Mythos-Härtungs-Control MHC-08, das diesem Baustein zugrunde liegt, mit Reifegrad-Pfad, Kennzahlen und typischen Fehlern.

Der Baustein CON.3 Datensicherungskonzept des IT-Grundschutz-Kompendiums beschreibt die grundlegenden Anforderungen an die Datensicherung, auf denen dieser Baustein aufsetzt.