

MRIS.bd.2.3

Ausführungsplattformen

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

1 Beschreibung	3
1.1 Einleitung	3
1.2 Zielsetzung.....	3
1.3 Abgrenzung und Modellierung	3
2 Gefährdungslage.....	3
2.1 Seitwärtsbewegung über gemeinsame Geheimnisse und Netzwerkvertrauen.....	4
2.2 Manipulierte Images in der Lieferkette	4
2.3 Mandantenübergreifende Ausbreitung.....	4
3 Anforderungen	4
3.1 Basis-Anforderungen	5
MRIS.bd.2.3.A1 Einführung von Workload-Identitäten und identitätsbasierter Zugriffskontrolle (B)	5
3.2 Standard-Anforderungen	5
3.3 Anforderungen bei erhöhtem Schutzbedarf.....	5
MRIS.bd.2.3.A2 Einsatz signierter Container-Images und geschützter Ausführungsumgebungen (H)	5
MRIS.bd.2.3.A3 Umsetzung einer nachweisbaren Mandantentrennung (H)	5
4 Weiterführende Informationen	6

1 Beschreibung

1.1 Einleitung

Ausführungsplattformen stellen die Umgebung bereit, in der produktive Anwendungen und Dienste als Workloads laufen: Container-Orchestrierung, Virtualisierung und Cloud-Plattformen (IaaS, PaaS). Auf ihnen entscheidet sich, ob ein Angreifer nach einem ersten Zugriff weiterkommt.

Agentische Angreifer finden gemeinsame Geheimnisse, vertrauensvolle Netzbeziehungen und schwache Trennungen schneller, als es manuell möglich wäre, und nutzen sie in unauffälligen Einzelschritten aus. Wirksam sind hier strukturelle Barrieren: kryptografisch verifizierbare Identitäten statt Vertrauen in die Netzwerklage, signierte Images statt ungeprüfter Artefakte und nachweisbare Trennung zwischen Mandanten.

Dieser Baustein ist Teil der Bausteinfamilie MRIS.bd. Er enthält die Anforderungen, die an jeder einzelnen Ausführungsplattform umzusetzen sind.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, auf Ausführungsplattformen die Seitwärtsbewegung zwischen Diensten, das Einschleusen manipulierter Images und die Ausbreitung zwischen Mandanten durch harte strukturelle Barrieren zu verhindern.

1.3 Abgrenzung und Modellierung

Der Baustein MRIS.bd.2.3 Ausführungsplattformen ist auf jede Plattform anzuwenden, auf der produktive Anwendungen und Dienste betrieben werden, insbesondere Container-Orchestrierung, Virtualisierung und Cloud-Plattformen (IaaS, PaaS). Einzelne Anforderungen gelten nur unter einer Bedingung, etwa beim Betrieb von Containern oder mandantenfähigen Diensten. Trifft die Bedingung einer Anforderung auf einer Plattform insgesamt nicht zu, wird die Anforderung im IT-Grundschutz-Check als entbehrlich gekennzeichnet und begründet.

Der Baustein wird ergänzend zu den Bausteinen modelliert, die für diese Zielobjekte ohnehin anzuwenden sind, etwa SYS.1.5 Virtualisierung, SYS.1.6 Containerisierung und APP.4.4 Kubernetes. Er ersetzt keinen dieser Bausteine.

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

- die Cloud-Nutzung aus Sicht der Institution (siehe OPS.2.2 Cloud-Nutzung),
- die Identitäten von Benutzenden und KI-Agenten (siehe MRIS.bd.2.1 Identitäts- und Zugangssysteme und MRIS.bd.2.4 KI-Agenten) sowie
- Software-Stücklisten, Build-Provenance und Sicherheitstests in der Entwicklungs-Pipeline (siehe MRIS.bd.1.A7 und MRIS.bd.1.A8).

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.2.3 Ausführungsplattformen von besonderer Bedeutung.

2.1 Seitwärtsbewegung über gemeinsame Geheimnisse und Netzwerkvertrauen

Langlebige gemeinsame Geheimnisse und eine Autorisierung anhand der Netzwerklage ermöglichen es Angreifern, sich nach einem ersten Zugriff unbemerkt zwischen Diensten zu bewegen.

Service-Konten mit langlebigen, im Klartext abgelegten Zugangsdaten und Dienste, die einander allein aufgrund ihrer Netzwerklage vertrauen, sind der klassische Treibstoff für Lateral Movement. Wenn ein Angreifer einen einzigen Dienst übernimmt, dann kann er mit gefundenen Geheimnissen oder aus der vertrauten Netzzone heraus weitere Dienste ansprechen, ohne dass einzelne Zugriffe auffallen. Agentische Angreifer durchsuchen Konfigurationsdateien, Umgebungsvariablen und Code-Repositories systematisch nach solchen Geheimnissen und zerlegen die Ausbreitung in unauffällige Einzelschritte (siehe MRIS.bd.1, Kapitel 2.3).

2.2 Manipulierte Images in der Lieferkette

Unsignierte oder ungeprüfte Images können manipulierte Komponenten unbemerkt in den Produktivbetrieb bringen.

Container werden aus Images gestartet, die aus Registries bezogen und häufig automatisiert aktualisiert werden. Wenn eine Plattform Images ohne Prüfung von Herkunft und Integrität startet, dann gelangen manipulierte Basis-Images oder kompromittierte Build-Ergebnisse unbemerkt in den Produktivbetrieb. Eine Prüfung, die Verstöße nur protokolliert, aber nicht blockiert, bietet dabei keinen Schutz.

2.3 Mandantenübergreifende Ausbreitung

Ist die Mandantentrennung nur auf Anwendungsebene umgesetzt, genügt ein einzelner Fehler, damit ein Angreifer aus einem Mandanten auf andere zugreift.

Mandantenfähige Dienste verarbeiten Daten mehrerer Kunden oder Organisationseinheiten auf gemeinsamer Infrastruktur. Wenn die Trennung nur auf Anwendungsebene über eine Mandanten-Kennung im Code umgesetzt ist, dann hebt ein einzelner Anwendungsfehler sie vollständig auf. Ein Angreifer, der in einem Mandanten Fuß fasst, kann so auf Daten anderer Mandanten zugreifen, unabhängig davon, wie schnell die Institution reagiert.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins MRIS.bd.2.3 Ausführungsplattformen 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	Entwickler

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.2.3.A1 Einführung von Workload-Identitäten und identitätsbasierter Zugriffskontrolle (B)

Privilegierte Service-Konten und Workloads MÜSSEN mit kryptografisch verifizierbaren, kurzlebigen Identitäten ausgestattet werden. Die Kommunikation zwischen kritischen Diensten MUSS anhand dieser Workload-Identität autorisiert werden. Die Netzwerklage allein DARF NICHT als Autorisierungsgrundlage dienen. Langlebige, im Klartext gespeicherte gemeinsame Geheimnisse DÜRFEN auf kritischen Kommunikationspfaden NICHT eingesetzt werden. Die Kommunikation zwischen produktiven Diensten SOLLTE durchgängig mit mTLS abgesichert werden. Die Umstellung SOLLTE stufenweise erfolgen, beginnend mit den privilegierten Workloads.

3.2 Standard-Anforderungen

Für diesen Baustein sind keine Standard-Anforderungen definiert.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

MRIS.bd.2.3.A2 Einsatz signierter Container-Images und geschützter Ausführungsumgebungen (H)

Falls auf der Plattform produktive Container betrieben werden, dann SOLLTEN diese ausschließlich aus signierten, vor dem Start geprüften Images aus kontrollierten Registries gestartet werden. Die Prüfung SOLLTE technisch über die Plattform durchgesetzt werden, etwa mit Admission-Controller-Policies. Falls Workloads einen besonders hohen Schutzbedarf haben, dann SOLLTEN geschützte Ausführungsumgebungen (Confidential Computing) mit Remote-Attestation eingesetzt werden.

MRIS.bd.2.3.A3 Umsetzung einer nachweisbaren Mandantentrennung (H)

Falls mandantenfähige Dienste betrieben werden, dann SOLLTEN Daten, Netzwerke und Rechenressourcen je Mandant getrennt werden. Die Datentrennung SOLLTE mit mandantenspezifischen Schlüsseln umgesetzt werden. Die Wirksamkeit der Trennung SOLLTE durch regelmäßige, möglichst automatisierte Tests nachgewiesen werden. Falls ein mandantenübergreifender Zugriff festgestellt wird, dann SOLLTE dieser unverzüglich unterbunden werden.

4 Weiterführende Informationen

Das Framework „Mythos-resistente Informationssicherheit (MRIS)“ (Version 2.0) und der „MRIS Implementation Guide“ (Version 2.0) beschreiben die Mythos-Härtungs-Controls MHC-04, MHC-06 und MHC-07, die diesem Baustein zugrunde liegen, mit Reifegrad-Pfad, Kennzahlen und typischen Fehlern.

Das BSI stellt mit dem Kriterienkatalog C5:2026 Anforderungen an Cloud-Dienste bereit, die insbesondere die Mandantentrennung stützen. Die Projekte SPIFFE und SPIRE der Cloud Native Computing Foundation beschreiben kryptografisch verifizierbare Workload-Identitäten; das Projekt Sigstore der Open Source Security Foundation stellt Werkzeuge für die Signatur und Prüfung von Artefakten wie Container-Images bereit.