

MRIS.bd.2.1 Identitäts- und Zugangssysteme

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 KI-gestütztes Phishing auf Spear-Phishing-Niveau	4
2.2 Umgehung über Rückfall- und Wiederherstellungsverfahren	4
3 Anforderungen	4
3.1 Basis-Anforderungen	5
MRIS.bd.2.1.A1 Durchsetzung phishing-resistenter Authentisierung (B)	5
3.2 Standard-Anforderungen	5
MRIS.bd.2.1.A2 Protokollierung von Authentisierungsvorgängen (S)	5
3.3 Anforderungen bei erhöhtem Schutzbedarf	5
4 Weiterführende Informationen.....	5

1 Beschreibung

1.1 Einleitung

Identitäts- und Zugangssysteme entscheiden darüber, wer sich im Informationsverbund anmelden darf. Dazu gehören Identitätsanbieter (Identity Provider, IdP), Verzeichnisdienste, Fernzugänge wie VPN-Gateways, Systeme für privilegierte Zugänge (Privileged Access Management, PAM) sowie Anwendungen mit eigener Anmeldung.

Agentische KI-Modelle machen individualisiertes Phishing auf dem Niveau gezielter Spear-Phishing-Kampagnen für jeden Angreifer verfügbar. Authentisierungsverfahren, deren Schutz darauf beruht, dass Benutzende eine Täuschung erkennen, verlieren dadurch an Wirksamkeit. Phishing-resistente Verfahren nach FIDO2/WebAuthn binden den Authentisierungsnachweis kryptografisch an den echten Dienst und wirken unabhängig von der Qualität der Täuschung.

Dieser Baustein ist Teil der Bausteinfamilie MRIS.bd. Er setzt die im Prozessbaustein MRIS.bd.1 Mythos-resistente Härtung des ISMS festgelegten Regelungen zur phishing-resistenten Authentisierung technisch an den einzelnen Systemen um.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, die in der Authentisierungsrichtlinie festgelegten phishing-resistenten Verfahren an jedem Identitäts- und Zugangssystem technisch durchzusetzen, schwächere Rückfallverfahren auszuschließen und Authentisierungsvorgänge so zu protokollieren, dass die Wirksamkeit messbar wird.

1.3 Abgrenzung und Modellierung

Der Baustein MRIS.bd.2.1 Identitäts- und Zugangssysteme ist auf jeden Identitätsanbieter, jeden Verzeichnisdienst, jeden Fernzugang (etwa VPN) und jedes System für privilegierte Zugänge (PAM) anzuwenden, außerdem auf jede Anwendung mit eigener Anmeldung, für deren Zugänge nach MRIS.bd.1.A2 phishing-resistente Verfahren festgelegt sind. Delegiert eine Anwendung die Anmeldung an einen Identitätsanbieter, genügt die Modellierung auf den Identitätsanbieter.

Der Baustein wird ergänzend zu den Bausteinen modelliert, die für diese Zielobjekte ohnehin anzuwenden sind, etwa APP.2.1 Allgemeiner Verzeichnisdienst, APP.2.2 Active Directory Domain Services, APP.2.3 OpenLDAP und NET.3.3 VPN. Er ersetzt keinen dieser Bausteine.

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

- die Authentisierungsrichtlinie mit Geltungsbereich, zugelassenen Verfahren und Ausnahmeprozess (siehe MRIS.bd.1.A2 Festlegung phishing-resistenter Multi-Faktor-Authentisierung),
- das allgemeine Identitäts- und Berechtigungsmanagement (siehe ORP.4 Identitäts- und Berechtigungsmanagement) sowie
- die Identitäten von Diensten und KI-Agenten (siehe MRIS.bd.2.3 Ausführungsplattformen und MRIS.bd.2.4 KI-Agenten).

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.2.1 Identitäts- und Zugangssysteme von besonderer Bedeutung.

2.1 KI-gestütztes Phishing auf Spear-Phishing-Niveau

Agentische KI-Modelle erzeugen individualisierte, sprachlich fehlerfreie Phishing-Kampagnen in beliebiger Zahl, sodass die Erkennbarkeit für Benutzende als Schutz entfällt.

Überzeugende, auf einzelne Personen zugeschnittene Phishing-Nachrichten setzten bisher Recherche und Handarbeit voraus. Agentische KI-Modelle übernehmen beides automatisiert, einschließlich täuschend echter Anmeldeseiten, die eingegebene Zugangsdaten und Einmalcodes in Echtzeit an den echten Dienst weiterreichen. Wenn ein Authentisierungsverfahren darauf beruht, dass Benutzende die Täuschung erkennen, dann genügt eine einzige erfolgreiche Nachricht, um Passwort und Einmalcode zu erbeuten. Verfahren wie SMS-Codes, Einmalpasswörter aus Apps oder einfache Push-Bestätigungen schützen gegen diese Weiterleitung nicht.

2.2 Umgehung über Rückfall- und Wiederherstellungsverfahren

Bleiben schwächere Verfahren als Rückfalloption aktiv oder ist die Wiederherstellung von Authentisierungsmitteln ungesichert, weichen Angreifer gezielt auf diese Pfade aus.

Ein phishing-resistentes Verfahren schützt nur, wenn es nicht umgangen werden kann. In der Praxis bleiben SMS-Codes oder einfache Push-Bestätigungen häufig als Rückfalloption aktiv, und neue Authentisierungsmittel werden über einen Helpdesk-Prozess ohne verlässliche Identitätsprüfung ausgegeben. Wenn ein Angreifer eine solche Rückfalloption auslösen oder sich am Helpdesk als betroffene Person ausgeben kann, dann ist auch das stärkste Verfahren wirkungslos. Agentische KI-Modelle erleichtern gerade diese Täuschung, etwa durch geklonte Stimmen bei telefonischen Rückfragen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins MRIS.bd.2.1 Identitäts- und Zugangssysteme 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.2.1.A1 Durchsetzung phishing-resistenter Authentisierung (B)

Auf dem System MÜSSEN die Verfahren aktiviert werden, die in der Authentisierungsrichtlinie für seine Zugänge festgelegt sind. Die Anmeldung über diese Zugänge MUSS technisch auf die festgelegten Verfahren beschränkt werden. Nicht zugelassene Verfahren DÜRFEN auch als Rückfalloption NICHT angeboten werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

MRIS.bd.2.1.A2 Protokollierung von Authentisierungsvorgängen (S)

Das bei einer Anmeldung verwendete Authentisierungsverfahren SOLLTE protokolliert werden. Die Registrierung und die Änderung von Authentisierungsmitteln SOLLTEN protokolliert werden.

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-03, das diesem Baustein zugrunde liegt, mit Reifegrad-Pfad, Kennzahlen und typischen Fehlern.

Die Spezifikation Web Authentication (WebAuthn) des W3C und die Spezifikationen der FIDO Alliance beschreiben die technischen Grundlagen phishing-resistenter Verfahren. Die NIST-Richtlinie SP 800-63B beschreibt Anforderungen an Authentisierungsverfahren einschließlich ihrer Widerstandsfähigkeit gegen Phishing.