Mindeststandard zur Authentisierung

Dokumenteninformation

Klassifikation:	Dienstgebrauch		
Versionsnummer:	2.1		
Dokumententitel:	Mindeststandard zur Authentisierung		
Dokumentennummer:	DOKID-4854		
Verantwortlicher:	Vorsitzender EG ISec		
Erstellt am:	07.10.2020	**Erstellt von:**	EG ISec
Nächste Überarbeitung:	01.04.2025	**Überarbeitung durch:**	EG ISec
Status:	Freigegeben	**Letzte Bearbeitung:**	15.03.2023
Freigabe am:		**Freigabe von:**	Netz-IT

Dokumentenverteiler

Berechtigte Rolle (Verteilerkreis)
ARD, ZDF, Deutschlandradio

Versionsverlauf

Datum	Version	Beschreibung	verändert durch
25.09.2020	0.8	Erstellung/Abstimmung des Dokuments in AG	Alessandro Benko, mdr
30.09.2020	0.9	Formatierungen/Dokumentenkopf	Michael Kalisch, rbb
07.10.2020	0.95	Ergänzungen nach CC Viko	Michael Kalisch
10.12.2020	0.97	Ergänzungen nach Kommentaren, BR, WDR, MDR	Michael Kalisch
11.12.2020	1.0	Dokument finalisiert nach Abstimmung in AG	Kalisch, Hoffmann, Gust, Rühle-Marx
29.01.2021	1.1	Anpassungen an Geltungsbereich nach Netz-IT vom 29.1.21	Kalisch, rbb
28.02.2023	2.0	Überarbeitung, Phishing resistente MFA	EG ISec
15.03.2023	2.1	Finale Version nach Abstimmung	EG ISec

Ergänzende Dokumente / Mitgeltende Unterlagen [1]

Dokumentennummer	Titel	Verantwortlicher

[1] In der Tabelle sind alle Dokumente einzutragen, die für dieses Dokument Gültigkeit besitzen, die aber im Dokument nicht explizit genannt werden. Einzutragen sind auch alle Dokumente, auf die im nachfolgenden Dokument explizit verwiesen wird.

1. Ziel

Dieses Dokument legt den Mindeststandard für den Umgang mit Benutzerkonten und Authentisierungsinformationen in den Rundfunkanstalten von ARD, ZDF und Deutschlandradio fest. Dieser Standard folgt dem Stand der Technik und orientiert sich an den Anforderungen des IT-Grundschutzkompendiums - Edition 2023 - des Bundesamtes für Sicherheit in der Informationstechnik.

2. Geltungsbereich

Die in diesem Dokument beschriebenen Anforderungen stellen einen sicherheitstechnischen Mindeststandard für den Umgang mit Benutzerkonten und Authentisierungsinformationen dar und gelten für ARD, ZDF und Deutschlandradio.

Die Umsetzung der in diesem Dokument beschriebenen und festgelegten Maßnahmen ist grundsätzlich technisch sicherzustellen. Sofern einzelne Anforderungen technisch nicht umgesetzt werden können, ist dies zu dokumentieren und es sind organisatorische Regelungen einzusetzen.

3. Abgrenzung

Die in diesem Mindeststandard dokumentierten Regelungen umfassen nicht das Identitäts- und Berechtigungsmanagement in seiner Gesamtheit, den Zutrittsschutz und die Protokollierung.

4. Allgemeine Regelungen

Die verwendeten Authentisierungsmethoden sind stets dem aktuellen Stand der Technik anzupassen.

4.1. Geheimhaltung

Authentisierungsinformationen, wie z.B. Passwörter, müssen stets geheim gehalten werden und dürfen nur dem zugewiesenen Benutzer persönlich bekannt sein. Falls der Verdacht besteht, dass diese offengelegt oder kompromittiert wurden, gelten die unter Punkt 7 genannten Anforderungen und Regelungen.

4.2. Sichere Eingabe bzw. Verwendung

Authentisierungsinformationen dürfen nur unbeobachtet eingegeben werden.

Gerätebasierte Authentisierungsmittel (z.B. Hardware-Token) dürfen nur im persönlichen Besitz genutzt werden, sind für den Zweck der Authentisierung mitzuführen und stets sicher zu verwahren.

4.3. Änderung voreingestellter Authentisierungsinformationen

Voreingestellte Authentisierungsinformationen (z. B. Standard- oder Initialkennungen und Passwörter des Herstellers bei Auslieferung von IT-Systemen) müssen vor der Inbetriebnahme des IT-Systems in den Produktivbetrieb geändert werden.

4.4. Gültigkeitsdauer

Die Gültigkeitsdauer der Authentisierung ist zu befristen und auf einen angemessenen Zeitraum zu beschränken.

4.5. Verwendung zentraler Authentifizierungsdienste

Es sind vorrangig zentrale Authentifizierungsdienste zu verwenden.

4.6. Sichere Speicherung und Übermittlung von Authentisierungsinformationen

Authentisierungsinformationen müssen verschlüsselt gespeichert und übertragen werden. Ihre Verarbeitung ist technisch so abzusichern, dass eine unberechtigte Kenntnisnahme (z.B. Auslesen) ausgeschlossen bzw. unter nachvollziehbarer Risikobewertung und -behandlung wesentlich erschwert ist.

Darüber hinaus ist eine Verknüpfung von Authentisierungsinformationen mit programmierbaren Funktionstasten von Tastaturen oder Mäusen unzulässig.

4.7. Schutz vor unbefugten Anmeldeversuchen

Es sind geeignete Maßnahmen einzurichten, um ein manuelles bzw. automatisiertes Ausprobieren von Passwortkombinationen oder anderen Authentisierungsinformationen zu unterbinden (z.B. Begrenzung von oder Zeitverzögerung nach nicht erfolgreichen Anmeldeversuchen, Schutz vor unberechtigtem Zugriff auf Passwortdateien).

Außerdem sollte dem Benutzer der Zeitpunkt der letzten Anmeldung angezeigt werden.

4.8. Hinterlegung von Authentisierungsinformationen

Sollten Authentisierungsinformationen physisch oder digital hinterlegt werden, sind diese sicher zu verwahren (z.B. freigegebene Passwortmanager, versiegelter Umschlag im Tresor).

5. Konten

5.1. Personenbezogene Konten

Zur Identifizierung einer für die Nutzung eines IT-Systems berechtigten Person sind personenbezogene Konten einzurichten. Das jeweilige Konto muss eindeutig einer natürlichen Person zugeordnet sein.

5.2. Funktions- bzw. Gruppenkonten

Die Vergabe und das Einrichten von Funktions- bzw. Gruppenkonten („Nicht-personalisierten Konten“) sind nur in Ausnahmefällen zulässig, wenn eine Aufgabe mittels eines personenbezogenen Kontos nicht oder nur unter nachvollziehbarer Risikobewertung und -behandlung durchgeführt werden kann. Sofern ein Funktions- bzw. Gruppenkonto zum Einsatz kommt, muss eine eindeutige Zuordnung des Benutzers auf anderem Wege (z.B. Dienstplan, Zuordnungstabelle) gewährleistet werden. Es ist sicherzustellen, dass für jedes Funktions- bzw. Gruppenkonto ein Verantwortlicher festgelegt ist.

5.3. Technische Konten

Technische Konten (z.B. System- oder Dienstkonten) dürfen nur bei zwingenden technischen Gründen eingerichtet werden. Eine interaktive Anmeldung ist technisch zu unterbinden.

Für jede Schnittstelle bzw. jede technische Anwendung ist nach Möglichkeit ein eigenes technisches Konto anzulegen.

Es ist sicherzustellen, dass für jedes technische Konto ein Verantwortlicher festgelegt ist.

6. Authentisierungsinformationen

6.1. Passwörter

Änderung von Initialpasswörtern

Bei der Einrichtung von personenbezogenen Konten sowie Funktions- bzw. Gruppenkonten ist ein Initialpasswort anzulegen. Eine Änderung bei der Erstanmeldung ist technisch zu erzwingen. Das Passwort zur Erstanmeldung darf dabei nicht einer nachvollziehbaren Bildungsregel unterliegen und ist auf sicherem Weg und vertraulich zu übermitteln.

6.1.1.Mehrfachverwendung

Für jeden Authentifizierungsdienst/Zugang ist ein eigenständiges Passwort festzulegen. Passwörter dürfen nicht mehrfach verwendet werden. Insbesondere dienstliche und private Authentisierungsinformationen sind strikt zu trennen.

6.1.2.Allgemeine Komplexitätsanforderungen

Es ist technisch sicherzustellen, dass ausschließlich komplexe Passwörter verwendet werden. Insbesondere Trivialpasswörter (z.B. „password“), gängige Zeichenketten und Tastaturmuster („123456“, „asdf“) sowie Passwörter, die nur unwesentlich von den vorherigen Passwörtern abweichen, dürfen nicht verwendet werden.

6.1.3.Personenbezogene Konten / Funktions- bzw. Gruppenkonten

Es gelten folgende Anforderungen sofern die Bedingungen aus 4.7 erfüllt sind:

	Standardprivilegien	**erhöhte Privilegien**
Passwortlänge	min. 10 Zeichen	min. 15 Zeichen
Komplexität	3 aus den folgenden 4 Merkmalen: - Großbuchstabe - Kleinbuchstabe - Ziffer - Sonderzeichen	3 aus den folgenden 4 Merkmalen: - Großbuchstabe - Kleinbuchstabe - Ziffer - Sonderzeichen
Passworthistorie	8 Passwörter (d. h. die letzten acht Passwörter dürfen nicht verwendet werden)	8 Passwörter (d. h. die letzten acht Passwörter dürfen nicht verwendet werden)
Passwortalter	- mindestens 1 Tag - maximal 365 Tage	- mindestens 1 Tag - maximal 365 Tage
Zusätzliche Hinweise	- Zeichensatz beschränkt auf internationale Standardzeichen - Bei technischer Möglichkeit sollte eine Multi-Faktor-Authentisierung verwendet werden.	- Zeichensatz beschränkt auf internationale Standardzeichen - Bei technischer Möglichkeit ist eine Multi-Faktor-Authentisierung zu implementieren. In diesem Fall kann eine reduzierte Passwortlänge (min. 10 Zeichen) zum Einsatz kommen.

6.1.4.Technische Konten

Die folgenden Anforderungen gelten für technische Konten (Punkt 5.3.):

Passwortlänge	mind. 25 Zeichen (siehe auch 2)
Komplexität	- mind. 1 Großbuchstabe - mind. 1 Kleinbuchstabe - mind. 1 Ziffer - mind. 1 Sonderzeichen
Passworthistorie	8 Passwörter (d. h. die letzten acht Passwörter dürfen nicht verwendet werden)
Zusätzliche Hinweise	- Zeichensatz beschränkt auf internationale Standardzeichen - Passwort muss zufällig mit maximaler Sicherheit generiert werden

6.1.5.Einsatz von Passwortmanagern

Für die sichere Hinterlegung und Verwaltung von Authentisierungsinformationen wird die Verwendung von Passwortmanagern empfohlen, die hinsichtlich der Sicherheit dem Stand der Technik und den Vorgaben der Rundfunkanstalten entsprechen. Für das Masterpasswort gelten die beschriebenen Komplexitätsanforderungen bezüglich Benutzerkonten mit erhöhten Privilegien (Punkt 6.1.3).

6.2. Multi-Faktor-Authentisierung

In den folgenden Fällen sind mindestens zwei voneinander unabhängige Authentisierungsfaktoren einzusetzen:

- Fernzugriffe auf Ressourcen und IT-Systeme der Rundfunkanstalt aus externen oder öffentlichen Netzen
- Zugriffe auf cloudbasierte Ressourcen der Rundfunkanstalt in externen oder öffentlichen Netzen
- Benutzerkonten mit erhöhten Privilegien (Punkt 6.1.3)

6.2.1 Anforderungen an Verfahren zur Multi-Faktor-Authentisierung

Sofern technisch möglich, müssen „Phishing-resistente“ MFA-Verfahren zur Anwendung kommen. Hierbei ist insbesondere bei Clouddiensten zu beachten, dass die Sicherheit des gewählten Verfahrens bei allen Arten von Anmeldeszenarien auf allen Gerätetypen gewährleistet ist.

6.3. Passwortlose Authentisierungsmethoden

6.3.1. Hardware-Token

Bei der Verwendung von Hardware-Token ist darauf zu achten, dass Verarbeitung und Speicherung der Authentisierungsinformationen dem Stand der Technik entsprechen.

6.3.2.Biometrie

Bei biometrischen Authentisierungsverfahren ist darauf zu achten, dass Erfassung, Verarbeitung und Speicherung der Authentisierungsinformationen dem Stand der Technik entsprechen.

6.3.3.PIN-Verfahren

Da es sich bei PIN-Verfahren um Zahlenkombinationen handelt, sind Maßnahmen gegen Brute-Force-Angriffe zu implementieren (siehe 4.7).

6.4. Passwortbasierte Verschlüsselung

Beim Einsatz einer passwortbasierten Verschlüsselung (bspw. ZIP-Archive, Office-Dokumente, PDFs) gelten die Anforderungen an die Passwortlänge und –Komplexität der Konten mit erhöhten Rechten, um einen in diesem Fall möglichen Offline-Angriff auf absehbare Zeit zu verhindern.

7. Offenlegung bzw. Kompromittierung von Authentisierungsinformationen

Sofern der Verdacht besteht, dass Authentisierungsinformationen wie bspw. Passwörter kompromittiert oder offengelegt wurden (z.B. durch Schadsoftware) stellt dies in jedem Fall einen Sicherheitsvorfall dar, der umgehend gemäß den in den Rundfunkanstalten definierten Prozessen zu Informationssicherheitsvorfällen gemeldet werden muss. Gleiches gilt für einen Manipulationsverdacht im Zusammenhang mit einer Multi-Faktor-Authentisierung, der ebenfalls umgehend als Informationssicherheitsvorfall zu melden ist.

Ein Passwort muss zwingend gewechselt werden, wenn es offengelegt wurde oder der Verdacht dazu besteht. Geräte- oder softwarebasierte Authentisierungsmittel und/oder -informationen sind bei bestätigter oder vermuteter Manipulation umgehend wieder in einen vertrauenswürdigen Zustand zu versetzen.

8. Zurücksetzen von Zugangsdaten

Das Zurücksetzen von Authentisierungsinformationen darf nur erfolgen, wenn die Identität des Benutzers glaubhaft überprüft worden ist. Dieser Vorgang kann durch einen Passwort-Self-Service unterstützt und realisiert werden. Weiterhin sind dabei die Regelungen bzgl. Initialpasswörtern gemäß Punkt 6.1anzuwenden.

Anhang Definitionen

Identifizierung: Unter Identifizierung versteht man das Behaupten einer Identität gegenüber einem IT-System. Ein Benutzer identifiziert sich an einem IT-System, indem er z.B. eine Benutzerkennung eingibt.

Authentisierung: Authentisierung bezeichnet den Nachweis einer behaupteten Identität. Ein Benutzer kann sich z.B. durch Passworteingabe, Vorhalten einer Chipkarte oder einen Abgleich biometrischer Merkmale an einem IT-System authentisieren.

Authentifizierung: Authentifizierung stellt die Überprüfung der im Rahmen einer Authentisierung übermittelten Identitätsnachweise dar. Ein IT-System gleicht hierzu bspw. die durch den Benutzer übermittelten Informationen mit einer Datenbank ab.

Authentisierungsinformationen: Hierunter sind alle Informationen zu verstehen, die ein Benutzer bzw. ein IT-System zum Zwecke seiner Authentisierung anbringt. Am verbreitetsten sind hierbei Passwörter oder Zahlencodes, die für den einmaligen Einsatz generiert werden.

Gerätebasierte Authentisierungsmittel: Unter dem Begriff sind körperlichen Gegenstände zusammengefasst, die zum Zweck der Authentisierung eingesetzt werden. Dies umfasst z.B. Chipkarten, Hardwaretoken sowie Geräte zum Generieren von Einmal-Passwörtern.

Softwarebasierte Authentisierungsmittel: Hierunter sind Softwarekomponenten zu verstehen, die Informationen zum Zweck der Authentisierung bereitstellen (z.B. Authenticator-Applikationen).

Phishing-Resistente MFA:

Eine Phishing-resistente Multi-Faktor-Authentifizierung (MFA) ermöglicht einen Authentifizierungsprozess, bei dem ein Angreifer nicht in der Lage ist, durch Phishing, Social-Engineering oder auf anderem Wege abgefangene Zugangsdaten und/oder MFA-Faktoren für eine Authentisierung zu nutzen. Dienstanbieter und Benutzer müssen Beweise für ihre Identität vorlegen, die im Vorfeld vereinbart wurden, eine Vertrauensbeziehung sicherstellen und sich nicht während des Authentifizierungsprozesses von Dritten missbrauchen lassen.

Damit werden nicht nur Phishing- bzw. Spear-Phishing-Angriffe verhindert, es können beispielsweise auch Brute-Force-, Man-in-the-Middle- oder Replay-Angriffe abgewehrt werden.

In der Praxis wird zur Umsetzung einer Phishing-resistenten Multi-Faktor-Authentifizierung (MFA) während eines kryptografischen Registrierungsprozesses ein Public-Key-Kryptoverfahren etabliert, bei dem der Private-Key in einem geschützten Speicher gesichert wird, der nur den jeweiligen Parteien zur Verfügung steht. In der Regel ist dies ein FIDO-Sicherheitsschlüssel, eine Smartcard oder eine geeignete Sicherheitshardware (z.B. TPM oder HSM).