

Sicherheitsanforderung

IAM

Deutsche Telekom Gruppe

Version	6.0
Datum	01.12.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.69	Dokumententyp Sicherheitsanforderung
Version 6.0	Stand 01.12.2025	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.12.2025 - 30.11.2030	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung

Ein Identity- and Access Management (IAM) - Framework sorgt für eine zentrale Verwaltung von Identitäten und Zugriffsrechten für unterschiedliche Systeme und Applikationen. Authentifizierung und Autorisierung der User sind zentrale Funktionen des IAM-Frameworks. Das IAM-Framework befasst sich weiterhin mit der Verwaltung von Benutzerdaten, die einzelnen Personen zugeordnet sind. Dabei ist die Identität eine Sammlung von personenbezogenen Attributen, die die Person, die sich dieser Identität bedient, individualisiert. IAM stellt einen Oberbegriff für alle Prozesse und Anwendungen dar, die für die Administration von Identitäten und die Verwaltung von Zugriffsrechten auf verschiedenen Applikationen, Systeme und Ressourcen zuständig sind. Um für eine einfache und zentral administrierbare Lösung zu sorgen, kommen spezielle IAM-Architekturen zum Einsatz, die aus mehreren Softwarekomponenten bestehen.

Diese Sicherheitsanforderung ist für jedes IT-System anzuwenden, unabhängig davon wieviel Benutzer auf dem System eingerichtet sind oder dieses nutzen werden.

Copyright © 2025 by Deutsche Telekom AG.

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Inhaltsverzeichnis

1.	Einleitung	4
1.1.	Allgemeine Einleitung	4
1.2.	Geltungsbereich	5
1.3.	Definition IAM Framework	5
1.4.	Glossar	5
1.5.	Anmerkungen	8
2.	IAM Framework	9
2.1.	System	9
3.	Identity Management	12
3.1.	Identity Lifecycle Management	12
3.2.	Access Governance	16
3.3.	Identity Data Integration	20
3.4.	Accounts	22
3.5.	Credentials	26
4.	Access management	29
4.1.	Authentifizierung	29
4.2.	Autorisierung	30
4.3.	Privileged Account Management (PAM)	31
5.	Prozesse und Workflows	33
5.1.	Generelle Vorgaben für Prozesse und Workflows	33
5.2.	Joiner Prozess	33
5.3.	Mover Prozess	35
5.4.	Leaver Prozess	36
5.5.	Reconciliation-Prozess	38
5.6.	Prozess zur Ermittlung verwaister Accounts	39
5.7.	Recertification-Prozess	41
5.8.	Account Usage Review Prozess	42
5.9.	Genehmigungs-Workflow	43
5.10.	Self Service-Workflow	44
5.11.	Provisionierung von Authentifizierungs- und Autorisierungsinstanzen	44
6.	Anbindung Ziel-Applikationen	47
6.1.	Anforderungen an Ziel-Applikationen	47

1. Einleitung

1.1. Allgemeine Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus der Konzernrichtlinie Sicherheit (Group Security Policy) und der nachgelagerten Konzernrichtlinie für das Management von Identitäten, Rollen und Berechtigungen erstellt und deckt alle Aspekte eines IAM Frameworks ab. Die Sicherheitsanforderung dient unter anderem als Basis der untergeordneten IAM Sicherheitsanforderungen, welche zur Freigabe im PSA-Prozess verwendet werden. Sie dient darüber hinaus als Umsetzungsempfehlung für Vorgaben der Konzernrichtlinie Sicherheit (Group Security Policy) in Einheiten, die nicht am PSA-Verfahren teilnehmen.

Im Folgenden die IAM Sicherheitsanforderungen, welche sich ganz konkret auf einzelne Teilaspekte eines IAM Frameworks fokussieren:

- IAM Intern
 - Anforderungen an ein IAM Framework für interne Mitarbeiter und externe Arbeitskräfte
 - Verpflichtende Requirements: 01 – 74, 80
- IAM PK
 - Anforderungen an ein IAM Framework für Privatkunden
 - Verpflichtende Requirements: 01 – 11, 16 – 19, 21 – 25, 27 – 32, 33 – 39, 44 – 46, 55, 56, 58 – 62
- IAM GK
 - Anforderungen an ein IAM Framework für Geschäftskunden
 - Verpflichtende Requirements: 01 - 74, 80
- Angebundene Zielapplikationen
 - Anforderungen an IT/NT-Systeme, die sich an ein IAM Framework anbinden
 - Verpflichtende Requirements: 14 – 20, 22, 27 – 32, 75 – 80
- Nicht-angebundene Zielapplikationen:
 - Anforderungen an IT/NT-Systeme, die sich nicht an ein IAM Framework anbinden
 - Verpflichtende Requirements: 01 - 80

Diese Sicherheitsanforderung ist für jedes IT-System anzuwenden, unabhängig davon wieviel Benutzer auf dem System eingerichtet sind oder dieses nutzen werden.

Des Weiteren werden im Dokument einige Begriffe verwendet, die wie folgt definiert und entsprechend zu beachten sind:

- Mit dem Ausdruck **IT-/NT-Systeme** sind generell alle IT- und NT-Systeme einer Organisation gemeint. Sollten nun speziell die NT-Systeme Anforderungen aufgrund fehlender technischer Voraussetzungen nicht umsetzen können, so reduziert sich der Scope der jeweiligen Anforderung entsprechend.
- Der Begriff **Organisation** wird in diesem Dokument als Synonym für die folgenden Begriffe verwendet (Die Aufzählung ist nicht abschließend):
 - Konzern
 - Unternehmen
 - Konzern-/Unternehmens-Einheit
 - Behörde
- Für die Definition des Begriffs **Zielapplikation** siehe Glossar

Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten. Sollte die Einhaltung der beschriebenen Anforderungen in individuellen Fällen nicht oder nur eingeschränkt umsetzbar sein, ist gemeinsam mit einem Sicherheits- und/oder Datenschutzexperten (entsprechend der betroffenen Anforderung) eine Risikobewertung vorzunehmen und mögliche alternative Schutzmaßnahmen sind abzustimmen.

Sollte die Einhaltung bzw. Umsetzung der definierten Anforderungen in individuellen Fällen nicht oder nur eingeschränkt umsetzbar sein, ist gemeinsam mit einem verantwortlichen IAM Enterprise Architekten (entsprechend der betroffenen Organisations-Einheit) und Sicherheits- und/oder Datenschutzexperten (entsprechend der betroffenen Anforderung) eine Risikobewertung vorzunehmen und mögliche alternative Schutzmaßnahmen sind abzustimmen.

1.2. Geltungsbereich

Geltungsbereich

Die Sicherheitsanforderung gilt weltweit für alle Konzerneinheiten im Konzern Deutsche Telekom, nach Beschluss und Inkraftsetzung durch das für die jeweilige Gesellschaft zuständige Organ (Geschäftsführung und/oder Vorstand).

Lokale Anpassung

Bei der Umsetzung dieser Sicherheitsrichtlinie in den Konzerngesellschaften sind das jeweils vorrangige nationale und supranationale Recht und die jeweiligen kulturellen Gepflogenheiten sowie bestehende Beteiligungsrechte der zuständigen bzw. legitimierten Arbeitnehmervertretungsgremien zu beachten.

Review dieser Konzernrichtlinie

Diese Sicherheitsrichtlinie wird jährlich auf Änderungen überprüft.

1.3. Definition IAM Framework

Unter dem Begriff IAM Framework wird das koordinierte Zusammenwirken aller an einem Identity and Access Management (IAM) beteiligten Komponenten verstanden. Bei IAM Systemen innerhalb der Deutschen Telekom AG unterscheidet man grundsätzlich zwischen internen und externen IAM Frameworks. Diese Unterscheidung basiert auf den Identitäten bzw. Accounts, welche im jeweiligen IAM Framework verwaltet werden:

- **Internes IAM:** Identitäten und Accounts der Mitarbeiter einer Organisation
- **Externes IAM:** Identitäten und Accounts von Kunden. Außerhalb der Deutschen Telekom AG ist hier auch der Begriff Customer IAM gebräuchlich.

Die Komponenten müssen nicht zwangsläufig von einem Softwarehersteller bereitgestellt werden. Vielmehr werden standardisierte Schnittstellen zwischen Komponenten unterschiedlicher Hersteller zum Zwecke des Zusammenwirkens verwendet. Darüber hinaus sind auch Prozesse Bestandteil eines IAM Frameworks.

1.4. Glossar

Account (Benutzerkennung)

Konto eines Benutzers für ein Dienstleistungsangebot in einem Computernetzwerk: in der Regel besteht der Account aus einem Benutzernamen und einem zugehörigen Passwort; Synonyme: Benutzer, Benutzerkennung, Kennung, Benutzerkonto, Konto.

Dabei wird zwischen normalen, kritischen und privilegierten sowie Shadow-Accounts unterschieden:

- **Normaler Account:** Ist ein mit den notwendigen Zugriffsberechtigungen zur Erledigung der Aufgaben versehener Account
- **Kritischer Account:** Ein kritischer Account ist ein Account, welcher über kritische Zugriffsberechtigungen innerhalb eines IT-/NT-Systems verfügt. Diese Kritikalität leitet sich aus Data Privacy und Information Security Kriterien ab und ist mindestens dann gegeben, wenn ein Zugriff auf die folgenden Daten möglich ist:
 - sensible / kritische Daten (SCD) aus Sicht der Organisation
 - Personenbezogene Daten laut EU-DSGVO
- **Privilegiert Account:** Ein privilegierter Account ist ein Account, welcher über erweiterte Zugriffsberechtigungen innerhalb eines IT-/NT-Systems verfügt, z.B. für administrative Zwecke
- **Shadow-Accounts:** Account, der im Zuge eines fehlerhaften Workflows im System existiert, aber nicht korrekt an die passende Identität korreliert ist

Authentifizierungs- und Autorisierungs-Instanz / (Central) Access Layer

Eine Authentifizierungs- und Autorisierungs-Instanz wird auch als ein (Central) Access Layer bezeichnet. Diese Instanz stellt Dienste bereit, die von Zielapplikationen konsumiert werden, die sich an ein IAM Framework anbinden. Weiterhin stellt sie eine starke Authentifizierung sowie ein Security Monitoring sicher.

Corporate ID (CID)

Konzernweites eindeutiges Identifizierungsmerkmal einer Identität.

Diameter

Ein Authentifizierungs-, Autorisierungs- und Protokollierungs-Protokoll (Triple-A-System) für die Authentifizierung von Kommunikationspartnern in einem Netzwerk.

Entität

Eine Entität kann eine physische oder juristische Person, eine Organisation, ein aktiver oder passiver Gegenstand, ein Gerät, eine Software, ein Service, etc. oder eine Gruppe dieser Entitäten sein.

Identity- and Access Management (IAM)

IAM lässt sich mit dem Begriff Identitäts- und Zugriffsverwaltung übersetzen. IAM stellt einen Oberbegriff für alle Prozesse und Anwendungen dar, die für die Administration von Identitäten und die Verwaltung von Zugriffsrechten auf verschiedenen Zielapplikationen, Systemen und Ressourcen zuständig sind.

IAM Framework Intern

Ein IAM Framework, welches ausschließlich Identitäten und dazugehörige Accounts verwaltet, die innerhalb einer Organisation verwendet werden (Mitarbeiter, externe Arbeitskräfte, Service Accounts, etc.)

IAM Framework PK

Ein IAM Framework, welches Identitäten und dazugehörige Accounts verwaltet, die ihren Ursprung außerhalb der Organisation haben (Privatkunden)

IAM Framework GK

Ein IAM Framework, welches Identitäten und dazugehörige Accounts verwaltet, die ihren Ursprung außerhalb der Organisation haben (Geschäftskunden)

Identität

Das digitale Abbild einer Entität, welches durch geeignete Attribute eindeutig identifiziert werden kann.

Kerberos

Ein verteilter Authentifizierungsdienst (Netzwerkprotokoll) für offene und unsichere Computernetze

LDAPS

Netzwerkprotokoll zur Abfrage und Änderung von Informationen verteilter Verzeichnisdienste über verschlüsselte Kommunikationsverbindungen

OAuth2

Standardisierte, sichere API-Autorisierung für Desktop-, Web- und Mobile-Anwendungen

OpenID Connect (OIDC)

Dezentrales Authentifizierungssystem für webbasierte Dienste

Password (Passphrase, PIN)

Ein Passwort oder auch Kennwort ist eine Zeichenfolge, die zur Authentifizierung verwendet wird. Damit soll die Identität einer Person oder Instanz und daraus folgend die Zugriffsberechtigung auf eine Ressource nachgewiesen werden.

Prozess

Unter einem Prozess versteht man die Abfolge verschiedener, einzelner Tätigkeiten. Angestrebt wird hierbei die Erreichung eines vorherbestimmten Ziels. Zum Ablauf und zur Organisation eines Betriebes gehörend, können Prozesse auch Teil eines anderen Prozesses sein.

Quellapplikation

Als Quellapplikationen im Sinne des IAM Frameworks werden beispielsweise HR-Systeme bezeichnet, die die Daten für die Identitäten liefern.

Recertification Prozess

Verifizierung der Accounts und die dazugehörigen Zugriffsberechtigungen durch den Data Owner, der dann im Rahmen des Prozesses diese weiterhin genehmigen (rezertifizieren) oder aber zurückweisen kann. Im letzteren Fall werden Zugriffsberechtigungen entzogen und Accounts ggf. gelöscht.

Basierend auf den Empfehlungen der DSGVO und des BSI ist im IAM-Umfeld eine Rezertifizierung bereits gesetzlich vorgeschrieben. So kann die Einführung eines Rezertifizierungsprozesses ein Unternehmen vor Sicherheitsverletzungen und möglichen Bußgeldern schützen.

Reconciliation Prozess

Reconciliation bezeichnet den Vorgang der Konsistenz- und Kompatibilitätsprüfung über unterschiedliche Access Layer (beispielsweise Active Directory, unterschiedliche LDAP Server, etc.) hinweg. In einem IAM Framework steht der Prozess in Verbindung mit der Provisionierung und der Synchronisation von Accounts in die unterschiedlichen Access Layer.

Security Assertion Markup Language (SAML)

Ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen

System for Cross-domain Identity Management (SCIM)

Standard zum automatisierten Austausch von Identitäten und damit verbundenen Informationen zwischen verschiedenen IAM oder IT-/NT-Systemen

WebAuthN

WebAuthN ermöglicht die Authentifizierung von Benutzern ohne ein Passwort. Es handelt sich um einen W3C-Standard, der auf Public-Key-Verfahren und der Nutzung von Faktoren wie biometrischen Merkmalen, Hardware-Token oder Smartphones basiert.

Workflow

Als Workflow bezeichnet man einen Vorgang, der aus verschiedenen Prozessen und Aktivitäten aufgebaut ist. Der Workflow betrachtet dabei die operative Ebene.

Zielapplikation, angebunden

Angebundene Zielapplikationen im Sinne des IAM Frameworks sind IT-/NT-Systeme und Services, die sich in zwei Stufen an ein IAM Framework anbinden können:

- 1.Stufe: Nutzung der Lifecyclemanagement Prozesse für Identitäten und Accounts sowie der vom IAM Framework bereitgestellten Authentifizierungs-Instanz
- 2.Stufe: Zusätzlich zu den Services in der 1.Stufe wird auch das Management der Zugriffsberechtigungen des IAM Frameworks von der Applikation verwendet.

Zielapplikation, nicht-angebunden

Nicht-angebundene Zielapplikationen im Sinne des IAM Frameworks sind IT-/NT-Systeme und Services, die nicht an ein IAM Framework angebunden sind und aus diesem Grund nicht dessen Services nutzen. Infolgedessen werden die nicht-angebundenen Zielapplikationen wie ein IAM Framework im jeweiligen Kontext (Intern, PK, GK) eingestuft und entsprechende Security-Anforderungen gestellt.

Zugangskontrolle

Die Zugangskontrolle verhindert die Nutzung einer Datenverarbeitungsanlage durch Unbefugte. Während die Zutrittskontrolle den physikalischen Zutritt verhindert, unterbindet die Zugangskontrolle die Nutzung des Systems.

Zugriffskontrolle

Die Zugriffskontrolle stellt sicher, dass ausschließlich befugte Personen Zugriff auf personenbezogene Daten, Programme, und Dokumente erhalten. Die Berechtigung ergibt sich aus der Aufgabenzuweisung und der Organisation des Betriebes. Wichtig: Der Vorgesetzte eines befugten Mitarbeiters verfügt nicht automatisch über eine Zugriffsberechtigung. Ein unbefugtes Lesen, Kopieren, Verändern oder Löschen personenbezogener Daten während ihrer Verarbeitung, Nutzung oder Speicherung soll ausdrücklich verhindert werden.

Zugriffsberechtigungen (Entitlements)

Als Zugriffsberechtigungen werden im Sinne des PSA zusammenfassend die Zutrittsberechtigungen, die Zugangsberechtigungen sowie Zugriffsrechte in einem IAM Framework bezeichnet.

Zutrittsberechtigung

Zutrittsberechtigung definiert Maßnahmen, die verhindern, dass unbefugte Personen den physikalischen Zutritt zu Datenverarbeitungsanlagen erhalten. Dazu zählen im weitesten Sinn Computer jeder Art - Server, PC, Notebook, Smartphone, Kopierer und andere Geräte, die sich zur Verarbeitung personenbezogener Daten eignen. Unbefugte Personen sind all jene, welche sich aufgrund der ihnen zugewiesenen Aufgaben nicht bei den entsprechenden Geräten auf-

halten müssen.

1.5. Anmerkungen

Dieses Dokument bildet die allgemeine Anforderungsbasis für die sichere Implementierung und den Betrieb eines IAM Frameworks. Aus ihm abgeleitet werden die Sicherheitsanforderungen für einzelne Teilaspekte eines IAM Frameworks wie in Kapitel 1.1 beschrieben. Die in diesem Dokument aufgeführten Anforderungen sind thematisch unterteilt, um eine strukturierte Übersichtlichkeit zu gewährleisten.

2. IAM Framework

2.1. System

Req 1	Eine Anmeldung an den Systemen eines IAM Frameworks aus betrieblichen Gründen muss mit mindestens zwei Authentisierungsmerkmalen (MFA) geschützt werden, die aus unterschiedlichen Faktoren stammen und Resilienz gegen Phishing-Angriffe sicherstellen.
-------	--

Ein IAM Framework ist eines der wichtigsten zentralen IT-/NT-Systeme, welches einen sehr hohen Schutzbedarf aufweist und daher besondere Sicherheitsmaßnahmen erfordert. Dieser hohe Schutzbedarf in Verbindung mit der Tatsache, dass 80% aller erfolgreichen Angriffe auf einer Kennwort-Attacke basieren, führen dazu, dass für alle Anmeldungen an IT-/NT-Systemen des IAM Frameworks aus betrieblichen Gründen eine Multi Factor Authentication verwendet werden muss. Diese Anforderung erweitert die Anforderung aus dem technischen Basisschutz dahingehend, dass für ein IAM Framework im Rahmen der Anmeldung aus betrieblichen Gründen eine MFA für alle Accounts und nicht nur für privilegierte (z.B. administrative) Accounts verwendet werden muss. Im Folgenden eine nicht abschließende Liste von Faktoren, die nicht als Bestandteil einer sicheren MFA definiert sind:

- Verwendung eines verwalteten Clients der Organisation
- Eine IP- oder MAC-Adresse eines Clients der Organisation

Dieses Requirement ist eine Erweiterung des Req. 19 („Benutzerkonten müssen gegen unautorisierte Nutzung durch Verwendung mindestens eines Authentisierungsmerkmals geschützt werden.“) aus dem Dokument „3.01 Technischer Basisschutz“.

Motivation: Reduzierung der Angriffsfläche.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.69-1/6.0

Req 2	Alle IT-Systeme des IAM Frameworks müssen mit einer dem Stand der Technik entsprechenden Endpoint Protection geschützt werden.
-------	--

Ein Malware-Schutz, der hauptsächlich auf einer Signatur-Erkennung beruht, bietet heutzutage keinen ausreichenden Schutz für die IT-Systeme eines IAM Frameworks, welches die direkte Kontrolle der Identitäten einer Organisation ausübt. Professionelle Angreifer bedienen sich modernster Malware, deren Signaturen nicht bekannt sind. In der Regel vergehen mehrere Monate, bis dann ein solcher Angriff erkannt wird und die Signaturen der verwendeten Malware für signaturbasierte Schutzmechanismen zur Verfügung stehen. Aus diesem Grund müssen alle IT-Systeme des IAM Frameworks mit einer modernen Endpoint Protection betrieben werden.

Beispiele von Merkmalen einer modernen Endpoint Protection sind u.a. die folgenden:

- Behaviour Monitoring
- Memory Scanning
- Network Monitoring
- Detect fileless and in-memory attacks
- Heuristic Detection
- Emulation/Sandboxing
- AV Scanner

Dieses Requirement ist eine Erweiterung des Req. 23 („Sicherheitssoftware muss stets aktuell gehalten werden.“) aus dem Dokument „3.61 Betrieb“.

Umsetzungsbeispiel: Umsetzung nach der Handreichung des Bundesverbandes IT-Sicherheit e.V. unter <https://www.teletrust.de/publikationen/broschueren/stand-der-technik/>

Motivation: Reduzierung der Angriffsfläche und Erkennung sowie frühzeitige Unterbindung von Angriffen

Umsetzungsbeispiel: Umsetzung nach der Handreichung des Bundesverbandes IT Sicherheit e.V. unter <https://www.teletrust.de/publikationen/broschueren/stand-der-technik/>.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-2/6.0

Req 3	Die IT-/NT-Systeme des IAM Frameworks müssen hochverfügbar konzeptioniert und betrieben werden.
-------	---

Ein IAM Framework muss jederzeit in der Lage sein, nach festgelegtem Service-Level Ad-hoc-Aktionen, wie das sofortige Deaktivieren von Accounts bei einem laufenden Angriff, durchzuführen. Darüber hinaus muss das IAM Framework sowohl bei Ausfällen als auch bei Lastspitzen zuverlässig verfügbar sein. Aus diesen Gründen müssen die Systeme des IAM Frameworks hochverfügbar konzeptioniert und betrieben werden.

Motivation: Sicherstellung der Verfügbarkeit des IAM Frameworks

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.69-3/6.0

Req 4	Das IAM Framework muss alle Vorgänge ohne Ausnahmen revisionssicher protokollieren.
-------	---

Der Begriff Revisionssicherheit bezieht sich auf elektronische Archivsysteme, die den Anforderungen des Handelsgesetzbuches (§ 239, § 257 HGB), der Abgabenordnung (§ 146, § 147 AO), der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) und anderen rechtlichen Vorgaben entsprechen. Die wesentlichsten Sicherheitsanforderungen sind:

- die Inhalte werden unverändert (originär) und fälschungssicher gespeichert,
- die Inhalte sind durch eine Suche wieder auffindbar,
- alle Aktionen im Archiv werden aus Gründen der Nachvollziehbarkeit protokolliert.

Motivation: Nach einem (erfolgreichen) Angriff gilt es im Nachhinein durch forensische Untersuchungen herauszufinden, wie die Angreifer vorgegangen sind. Dabei können eventuelle Schwachstellen identifiziert und mitigiert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-4/6.0

Req 5	Ein Notfall-Account muss im IAM Framework lokal angelegt werden, um bei einem Ausfall der Authentifizierungs-Instanz auf das IAM Framework zugreifen zu können.
-------	---

Zur Aufrechterhaltung des Geschäfts-Betriebs der Organisation muss es das IAM Framework ermöglichen, sich lokal mit einem Notfall-Account, unter Umgehung der Authentifizierungs-Instanz des IAM Frameworks, am IAM Framework anmelden zu können. Dieser Notfall-Account muss weitreichende Berechtigungen haben und muss bestmöglich, beispielsweise unter Verwendung sehr langer Kennwörter, vor unbefugtem Zugriff geschützt werden und darf nur im 4-Augen Prinzip eingesetzt werden. Die Nutzung dieses Notfall-Accounts ist an die Vorgaben eines Business Continuity Management Plans gebunden.

Eine mögliche Umsetzung ist die Verwendung eines Passworts in einem Tresor oder die Nutzung einer Privilege Access Management Lösung (PAM). Beide Lösungen in Verbindung mit organisatorischen Prozessen. Nicht zugelassene Lösungen sind Password Management Systeme, die nicht für die Verwaltung von privilegierten Accounts freigegeben sind, sowie Dokumente wie Excel-Arbeitsblätter, Textdateien, etc.

Motivation: Dieser Notfall-Account soll es ermöglichen, auch im Krisenfall auf die Daten des IAM Frameworks zuzugreifen und eventuelle weitere Schritte im Rahmen eines Business Continuity Managements durchführen zu können. Dadurch soll weiterer Schaden für die Organisation vermindert bzw. vermieden werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.69-5/6.0

Req 6	Das IAM Framework muss an ein Security Incident and Event Management System (SIEM) angebunden werden.
-------	---

Eine wirksame IT Security beinhaltet immer das Erkennen von Angriffen und Missbrauch der IT-/NT-Systeme der Organisation. Aus diesem Grund werden Security Incident and Event Management Systeme (SIEM) etabliert, um diese Erkennung zu gewährleisten bzw. signifikant zu verbessern und entsprechende Security Incidents prozessieren zu können. Der Erkennung des Missbrauchs von Accounts kommt hier eine immense Bedeutung zu. In einem Active Directory kann diese Überwachung beispielsweise durch den Microsoft Defender for Identity oder ähnliche Produkte realisiert werden, die entsprechende Incidents an ein zentrales SIEM weiterleiten. Aus diesem Grund muss ein IAM Framework an ein SIEM der Organisation angebunden werden. Für die Angriffs- und Missbrauchserkennung müssen entsprechend geeignete Use Cases auf Basis der Log-Daten des IAM Frameworks definiert und umgesetzt werden.

Motivation: Signifikante Verbesserung der Erkennung von Angriffen und Missbrauch, um diese so früh wie möglich zu unterbinden und somit die Identitäten nebst zugehörigen Accounts der Organisation zu schützen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-6/6.0

3. Identity Management

3.1. Identity Lifecycle Management

Req 7 Es dürfen nur standardisierte Identitätstypen verwendet werden.

Alle im IAM Framework verwendeten Identitätstypen müssen gemäß der Konzernrichtlinie IAM Governance der Deutschen Telekom AG standardisiert sein, da sich die Prozesse des IAM Frameworks darauf abstützen. Ein Angreifer, der seinen eigenen Identitätstyp in das IAM Framework einbringt, könnte Überwachungs- und Detektionsmaßnahmen umgehen. Aus diesem Grund dürfen in der Organisation nur freigegebene und standardisierte Identitätstypen verwendet werden, wie z.B.:

- Menschliche bzw. natürliche Identitäten
- Roboter Identitäten
- Juristische Identitäten
- Systemkomponenten (z.B. Hardware, Applikationen)
- IT/NT-Objekte (z.B. IoT-Geräte)

Motivation: Durch Standardisierung Erhöhung der Sicherheit

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-7/6.0

Req 8 Wenn private E-Mail-Adressen in IT-/NT-Systemen verwendet werden, dann müssen diese vor Verwendung verifiziert werden.

Angreifer versuchen auf verschiedenen Wegen sich valide Accounts zu verschaffen, die ihnen einen Zugriff auf IT-/NT-Systeme sowie auf die darin enthaltenen Daten ermöglichen. Ein Weg ist dabei die ungeprüfte Verwendung privater E-Mail-Adressen beispielsweise bei der Einstellung neuer Mitarbeiter oder bei der Anlage von Benutzerkonten etwa im PK Bereich. Des Weiteren kann eine unzureichend verifizierte Email-Adresse auch für unerlaubtes Exfiltrieren von Daten genutzt werden, etwa wenn beispielsweise die Personalabteilung das Arbeitszeugnis eines Mitarbeiters an eine private Email-Adresse versendet.

Aus diesen Gründen müssen private E-Mail-Adressen vor ihrer Verwendung ausreichend verifiziert werden, damit nachgewiesen ist, dass die Person, welche die private Email-Adresse angibt, auch über die volle Kontrolle diese Email-Adresse verfügt.

Die notwendige Verifikation richtet sich dabei nach den Informationen, die an diese Email-Adresse versendet werden. Gemäß der Datenschutz- und Sicherheitsempfehlungen der Deutschen Telekom AG muss eine Verifizierung einer privaten Email-Adresse mindestens bei Verwendung der Schutzklasse INTERN durchgeführt werden. Für andere Organisationen außerhalb der Deutschen Telekom AG müssen die dort geltenden Regelungen verbindlich beachtet werden.

Motivation: Schutz der Daten der Organisation

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-8/6.0

Req 9 Es dürfen nur ausreichend verifizierte Identitäten im IAM Framework verwendet werden.

Falls es einem Angreifer gelingt, eine neue Identität im IAM Framework anzulegen oder sich unter Nutzung einer

falschen Identität Zutritt zu Gebäuden und IT-/NT-Systemen der Organisation verschaffen kann, dann sind die IT-/NT-Systeme der Organisation gefährdet. Aus diesem Grund dürfen nur Identitäten im IAM Framework verwendet bzw. angelegt werden, die zuvor durch einen geeigneten Prozess verifiziert worden sind.

Internes IAM: Im Hinblick auf die Verifizierung von Mitarbeitern ist es angezeigt, die Identität und die berufliche Referenz, vor allem bei Personen mit sicherheitsrelevanten Aufgaben und Verantwortlichkeiten (z. B. bei Systemadministratoren, Sicherheitsbeauftragten oder Wachpersonal), zu validieren. Die jeweils eingesetzte Prüfungsmodalität und das Ergebnis müssen dokumentiert werden.

Zusätzlich zu den IT Security Anforderungen ergibt sich eine für die Organisation verpflichtende Verifizierung der Identitäten aus der Verordnung (EU) Nr. 910/2014, Artikel 26 (Anforderungen an fortgeschrittene elektronische Signaturen – muss u.a. eindeutig dem Unterzeichner zugeordnet sein und muss ihn identifizieren können).

Zur eindeutigen Feststellung der Identität sind die folgenden Verifizierungs-Methoden zugelassen:

- Eine automatische Verifizierung darf nur mit zertifizierten Videoidentverfahren und amtlichen Lichtbild-Ausweisen durchgeführt werden.
- Eine persönliche Verifizierung kann auf zwei Arten erfolgen:
 - In einem Videocall muss der mit der Prüfung beauftragte Mitarbeiter die Sicherheitsmerkmale des vorgezeigten amtlichen Lichtbild-Ausweises überprüfen und sicherstellen, dass die Person dem Eintrag auf dem amtlichen Lichtbild-Ausweis entspricht. Dabei muss eine sehr hohe Qualität des Videocalls gewährleistet sein
 - In einem persönlichen Gespräch muss der mit der Prüfung beauftragte Mitarbeiter die Sicherheitsmerkmale des vorgezeigten amtlichen Lichtbild-Ausweises überprüfen und sicherstellen, dass die Person dem Eintrag auf dem amtlichen Lichtbild-Ausweis entspricht

Die Organisation muss dafür Sorge tragen, dass die Mitarbeiter, die diese Prüfungen durchführen, eine sie dazu befähigende Schulung zur Erkennung der Sicherheitsmerkmale sowie Durchführung des Verifikationsprozesses erfolgreich absolvieren. Eine entsprechende Dokumentation muss vorgehalten und bei entsprechenden Audits, TÜV-Prüfungen, u.ä. vorgezeigt werden.

Aufgrund der eIDAS-Vorgaben und ETSI-Richtlinien für die Ausstellung von Signatur- und Emailverschlüsselungszertifikaten für Mitarbeiter müssen die zu Grunde liegenden Identitäten verifiziert und validiert sein. Aus diesem Grund muss sichergestellt sein, dass ein zu verwendendes Videoidentverfahren durch die Bundesnetzagentur (BNetzA) zertifiziert ist.

Die Verifizierung der Identitäten kann in einer dem IAM Framework vorgelagerten autoritativen Quelle (beispielsweise einem HR System) oder im IAM Framework selbst durchgeführt werden.

Externes IAM: Vor allem im PK Umfeld basieren sehr viele Prozesse auf der Registrierung einer Identität durch den Kunden im Rahmen eines Self-Service Workflow. Aus diesem Grund muss sich die notwendige Verifikation einer Identität dabei an den Informationen, zu denen der Kunde Zugriff erlangen wird, und an gesetzlichen Vorgaben orientieren. Dabei müssen sich Konzerneinheiten der Deutschen Telekom AG an die Vorgaben der Datenschutz- und Sicherheitsempfehlungen des Konzerns halten. Für andere Organisationen außerhalb der Deutschen Telekom AG müssen die dort geltenden Regelungen verbindlich beachtet werden.

Motivation: Erhöhung der IT-Sicherheit und Verringerung der Angriffsfläche

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.69-9/6.0

Req 10	Personen und IT/NT-Objekte müssen eindeutig und nachweisbar als digitale Identitäten abgebildet werden.
--------	---

Personen und IT/NT-Objekte müssen eindeutig und nachweisbar als digitale Identitäten abgebildet werden. Dafür müssen sie mit einem organisationsweit eindeutigen und unveränderbaren Identifizierungsmerkmal versehen werden. Innerhalb der Deutschen Telekom AG ist dies die Corporate ID (CID). Dieser Prozess erfolgt nach einheitlichen Regeln.

Ziel ist die Vergabe einer einzigen über alle Organisationseinheiten geltenden digitalen Identität pro Identitätstyp. Identitäten müssen ausreichend gegen Missbrauch und Diebstahl geschützt werden.

Als Subjekt sind im Kontext eines IAM Frameworks menschliche Lebewesen definiert, die in einem Bezug zur Organisation stehen. Als Beispiele sind hier interne oder externe Mitarbeiter genannt. Objekte beziehen sich auf technische Geräte wie beispielsweise einen Laptop oder ein Mobile Device. Um es Angreifern zu erschweren, Identitäten zu übernehmen, muss jeder Entität ihre eindeutige Identität in der Organisation zugeordnet werden, die Bestandteil des Identity Lifecycle Managements ist. Diese Eindeutigkeit muss auch beispielsweise bei gleichem Vornamen, Nachnamen und Geburtsdatum mehrerer Subjekte gegeben sein.

Folgende Abgrenzungen gelten:

- Interne IAM Frameworks bzw. Nicht-angebundene Zielapplikationen
 - Es dürfen keine personenbezogenen Daten aus den Personalstammdaten für das eindeutige und unveränderbare Identifizierungsmerkmal verwendet werden.
 - Personalnummern dürfen nichts als das eindeutige und unveränderbare Identifizierungsmerkmal verwendet werden, da sie ein personenbezogenes Datum darstellen und damit Rückschlüsse auf die Identität möglich sind.
- PK bzw. GK IAM Frameworks
 - Es dürfen keine personenbezogenen Daten aus den Kundenstammdaten für das eindeutige und unveränderbare Identifizierungsmerkmal verwendet werden.

Motivation: Durch Standardisierung Erhöhung der Sicherheit und Zuordnung der Identitäten was beispielsweise die forensische Untersuchung im Nachgang eines Incidents erleichtert.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.69-10/6.0

Req 11	Die Beziehung zwischen Identität und Account muss genau definiert sein.
--------	---

Die Zuordnung von Accounts zu Identitäten muss genau definiert und stets gegeben sein, da es ansonsten Angreifern gelingen kann, verwaiste Accounts zu übernehmen, um Angriffe durchzuführen.

Es gelten die folgenden Abgrenzungen für die Zuordnung von Accounts zu Identitäten:

- Interne IAM Frameworks bzw. nicht-angebundene Zielapplikationen
 - Jeder Account ist genau einer Identität zugeordnet (1:1, Account:Identität).
 - Jeder Identität können mehrere Accounts zugeordnet werden (1:n, Identität:Account).
- PK bzw. GK IAM Frameworks
 - Eine n:m Zuordnung (Identität:Account) ist erlaubt, es muss jedoch mindestens eine 1:1 (Identität:Account) vorliegen.
 - Standalone Accounts sind nicht erlaubt.

Motivation: Durch Standardisierung Erhöhung der Sicherheit

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-11/6.0

Req 12	Der Abgleich mit der autoritativen Datenquelle für Identitäten muss mindestens einmal täglich erfolgen.
--------	---

Eine autoritative Datenquelle für Identitäten ist z.B. ein zentrales HR-System oder ein zwischen HR- und IAM-System betriebenes System, was als Konsolidierungslayer dient.

Werden Identitätsdaten in Dateiform, z.B. CSV-Tabelle über eine Upload-Schnittstelle an das IAM-System geliefert, ist über eine Kombination von geeigneten Mechanismen wie Hashwertabgleich, Dateiverschlüsselung, verschlüsselte und eingeschränkte Kommunikationsbeziehung mittels Mutual TLS (mTLS), etc. die Integrität der Daten zu gewährleisten.

Motivation: Durch den täglichen Abgleich von Identitätsdaten werden Änderungen zuverlässig erkannt und die darauf basierenden Identity Lifecycle Prozesse sichergestellt.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.69-12/6.0

Req 13	Werden die erforderlichen Identitätsdaten nicht oder nur teilweise von der maßgeblichen Quelle für Identitätsdaten (autoritativen Quelle) geliefert, muss innerhalb von 3 Tagen ein Is-Loss-Prozess mit anschließendem Leaver-Prozess eingeleitet werden.
--------	---

Wird durch die maßgeblichen Quelle für Identitätsdaten (autoritativen Quelle) für Identitäten ein Identitätsdatensatz oder die zur Identitätsabbildung im IAM-System erforderlichen Datenfelder nicht geliefert, ist durch das IAM-System innerhalb von 3 Tagen ein Is-Loss-Prozess zu starten. Dieser Is-Loss-Prozess muss zum Ende der 3-Tagesfrist ein Austrittsdatum für die betroffene Identität eintragen, damit der Leaver-Prozess durchgeführt werden kann.

Der Is-Loss-Prozess sollte hierbei vorsehen, dass der verantwortliche Ansprechpartner der maßgeblichen Quelle für Identitätsdaten (autoritativen Quelle) darauf hingewiesen wird, um entsprechende Fehlerkorrekturen einzuleiten.

Motivation: Aus unterschiedlichen Gründen werden durch autoritativen Datenquellen für Identitäten ggf. keine Identitätsdaten an das IAM-System geliefert. Zum Beispiel wird bei einem Ausscheiden eines Employees der Datensatz im HR-System einfach gelöscht und kein Austrittsdatum gesetzt. Das würde dazu führen, dass alle auf die Identität gebundenen Assets wie Accounts, Zugänge, etc. bestehen bleiben und somit eine potentielle Angriffsfläche für Missbrauch bieten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

- Unbemerkt durchführbare Angriffe

ID: 3.69-13/6.0

3.2. Access Governance

Req 14	Die Zuweisung von Zugriffsberechtigungen muss eine aufgabenbedingte Funktionstrennung sicherstellen (Prinzip der Gewaltenteilung, Segregation of duties).
--------	---

Die zugewiesenen Zugriffsberechtigungen dürfen das Gebot der Funktionstrennung zwischen operativen und kontrollierenden Funktionen der Mitarbeiter nicht aufheben.

Zugriffsberechtigungen müssen derart strukturiert sein, dass keine Vermischung aus Rollen entsteht, welche die Tätigkeitsbereiche „operativ“ und „kontrollierend“ zusammenführt. Als Beispiel dafür sei genannt, dass derjenige Mitarbeiter, der Reisespesen genehmigt, nicht seine eigene Reisekostenabrechnung bearbeiten (und genehmigen) darf. Aus diesem Grund muss die Zuweisung der Zugriffsberechtigungen eine aufgabenbedingte Funktionstrennung sicherstellen.

Im Hinblick auf an ein IAM Framework angebundene Zielapplikationen gelten die folgenden Regelungen:

- Sobald die Implementierung des Prinzips Segregation of Duties innerhalb bzw. durch das IAM Framework sichergestellt wird, ist keine Umsetzung erforderlich.
- Wird das Prinzip der Segregation of Duties innerhalb der angebotenen Zielapplikation implementiert, so muss zusätzlich eine Übersicht der vergebenen Zugriffsberechtigungen an das zentrale IAM Framework übermittelt werden.

Motivation: Verhinderung der Möglichkeit des Missbrauchs und des Betrugs

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-14/6.0

Req 15	Redundante Zugriffsberechtigungen von Accounts, Gruppen und Rollen müssen im Rahmen von regelmäßigen Überprüfungen entfernt werden.
--------	---

In einem IAM Framework müssen die vergebenen Zugriffsberechtigungen jederzeit klar definiert und übersichtlich zugeordnet sein. Sollten dieselben Zugriffsberechtigungen einem Account, einer Gruppe und einer Rolle zugeordnet werden, so besteht die Gefahr, dass beispielsweise bei einem Mover Prozess nur die Zugriffsberechtigungen, die für die Gruppe und die Rolle konfiguriert sind, entfernt werden, die Zugriffsberechtigungen für den Account jedoch übersehen werden. Wird dieser Account von einem Angreifer übernommen, so besteht die Gefahr, dass durch die „vergessenen“ Zugriffsberechtigungen das Schadensausmaß vergrößert wird. Aus diesem Grund müssen redundante Zugriffsberechtigungen im Rahmen von regelmäßigen Überprüfungen entfernt werden.

Im Hinblick auf an ein IAM Framework angebundene Zielapplikationen gelten die folgenden Regelungen:

- Sobald das Entfernen von redundanten Zugriffsberechtigungen innerhalb bzw. durch das IAM Framework sichergestellt wird, ist keine Umsetzung erforderlich.
- Wird das Entfernen von redundanten Zugriffsberechtigungen innerhalb der angebotenen Zielapplikation implementiert, so muss zusätzlich eine Übersicht der vergebenen Zugriffsberechtigungen an das zentrale IAM Framework übermittelt werden.

Motivation: Begrenzung des Schadensausmaßes bei einem Sicherheitsvorfall

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.69-15/6.0

Req 16	Accounts dürfen nur auf die Daten zugreifen können, die für die Aufgabenerledigung unbedingt notwendig sind (Need To Know – Prinzip).
--------	---

Sollte ein Angreifer einen bestehenden Account übernehmen können, hat er Zugriff auf die Daten, für die der Account berechtigt ist. Damit das Schadensausmaß bei einem Sicherheitsvorfall begrenzt werden kann, dürfen die Accounts nur auf die Daten zugreifen, die für die Aufgabenerledigung der regulären Account-Inhaber unbedingt notwendig und erforderlich sind.

Im Hinblick auf an ein IAM Framework angebundene Zielapplikationen gelten die folgenden Regelungen:

- Sobald das Need to Know Prinzip innerhalb bzw. durch das IAM Framework sichergestellt wird, ist keine Umsetzung erforderlich.
- Wird das Need to Know Prinzip innerhalb der angebotenen Zielapplikation implementiert, so muss zusätzlich eine Übersicht der vergebenen Zugriffsberechtigungen an das zentrale IAM Framework übermittelt werden.

Dieses Requirement ist eine Erweiterung des Req. 23 („Die Berechtigungen von Benutzerkonten und Anwendungen müssen auf ein für deren Aufgaben notwendiges Minimum reduziert werden.“) aus dem Dokument „3.01 Technischer Basisschutz“.

Motivation: Begrenzung des Schadensausmaßes bei einem Sicherheitsvorfall

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.69-16/6.0

Req 17	Accounts dürfen nur die Aktionen auf den Daten ausführen können, die für die Aufgabenerledigung unbedingt notwendig sind (Least Privilege – Prinzip).
--------	---

Wird ein Account so konfiguriert, dass er vollen Zugriff auf die zu bearbeitenden Daten hat, so können Angreifer, die den Account übernehmen, die Daten nicht nur auslesen, sondern auch verändern oder löschen. Aus diesem Grund dürfen Accounts nur die Aktionen auf den Daten ausführen, die für die Aufgabenerledigung der regulären Account-Inhaber unbedingt notwendig und erforderlich sind.

Im Hinblick auf an ein IAM Framework angebundene Zielapplikationen gelten die folgenden Regelungen:

- Sobald das Least Privilege Prinzip innerhalb bzw. durch das IAM Framework sichergestellt wird, ist keine Umsetzung erforderlich.
- Wird das Least Privilege Prinzip innerhalb der angebotenen Zielapplikation implementiert, so muss zusätzlich ein Reporting an das zentrale IAM Framework erfolgen.

Dieses Requirement ist eine Erweiterung des Req. 23 („Die Berechtigungen von Benutzerkonten und Anwendungen müssen auf ein für deren Aufgaben notwendiges Minimum reduziert werden.“) aus dem Dokument „3.01 Technischer Basisschutz“.

Motivation: Begrenzung des Schadensausmaßes bei einem Sicherheitsvorfall und Sicherstellung der Integrität der Daten

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-17/6.0

Req 18	Zugriffsberechtigungen müssen atomar und voneinander abgegrenzt definiert sein.
--------	---

Um eine effektive und sichere Verwaltung der Zugriffsberechtigungen zu ermöglichen, müssen Zugriffsberechtigungen atomar und voneinander abgegrenzt sein. Andernfalls ist die Wahrscheinlichkeit sehr hoch, dass ein Account zu hohe Zugriffsberechtigungen besitzt, weil ein höheres Recht, das eigentlich gar nicht benötigt wird, zusammen mit niedrigeren Rechten in einer Zugriffsberechtigung vereint ist. Atomare Zugriffsberechtigungen können beispielsweise in Rollen zusammengefasst werden.

Im Hinblick auf an ein IAM Framework angebundene Zielapplikationen gelten die folgenden Regelungen:

- Sobald atomare und voneinander abgegrenzte Zugriffsberechtigungen innerhalb bzw. durch das IAM Framework sichergestellt werden, ist keine Umsetzung erforderlich.
- Werden atomare und voneinander abgegrenzte Zugriffsberechtigungen innerhalb der angebundenen Zielapplikation implementiert, so muss zusätzlich eine Übersicht der vergebenen Zugriffsberechtigungen an das zentrale IAM Framework übermittelt werden.

Motivation: Schutz der Daten der Organisation und Einhaltung des Need-To-Know sowie Least-Privilege Prinzips

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.69-18/6.0

Req 19	Zugriffsberechtigungen müssen eine verständliche Benennung und Beschreibung aufweisen.
--------	--

Um beispielsweise bei der Zuweisung von Zugriffsberechtigungen oder beim Durchlaufen eines Recertification-Prozesses die korrekten und notwendigen Zugriffsberechtigungen auswählen zu können, müssen Zugriffsberechtigungen eine verständliche Benennung und Beschreibung aufweisen.

Im Hinblick auf an ein IAM Framework angebundene Zielapplikationen gelten die folgenden Regelungen:

- Sobald die Benennung der Zugriffsberechtigungen innerhalb bzw. durch das IAM Framework sichergestellt wird, ist keine Umsetzung erforderlich.
- Wird die Benennung der Zugriffsberechtigungen innerhalb der angebundenen Zielapplikation implementiert, so muss zusätzlich eine Übersicht der vergebenen Zugriffsberechtigungen an das zentrale IAM Framework übermittelt werden.

Motivation: Sicherstellung des Least-Privileges Prinzips

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-19/6.0

Req 20 Die Erteilung und Änderung von Zugriffsberechtigungen muss mit Hilfe eines Genehmigungsworkflows durchgeführt werden.

Die Erteilung von Zugriffsberechtigungen muss nach dem Need-To-Know und Least-Privilege Prinzip passieren, damit die Daten der Organisation mit dem höchstmöglichen Sicherheitsniveau geschützt werden. Zur Sicherstellung dieses Schutzes muss die Erteilung und die Änderung der Zugriffsberechtigungen gemäß den Anforderungen im Kapitel „Genehmigungs-Workflow“ erfolgen. Andernfalls könnten Angreifer ihrem erstellten oder erbeuteten Account weitreichende Zugriffsberechtigungen zuweisen.

Im Hinblick auf an ein IAM Framework angebundene Zielapplikationen gelten die folgenden Regelungen:

- Sobald die Erteilung und Änderung der Zugriffsberechtigungen innerhalb bzw. durch das IAM Framework sichergestellt wird, ist keine Umsetzung erforderlich.
- Wird die Erteilung und Änderung der Zugriffsberechtigungen innerhalb der angebotenen Zielapplikation implementiert, so muss zusätzlich ein Reporting an das zentrale IAM Framework erfolgen.

Motivation: Schutz der Unternehmensdaten und Minimierung der Angriffsfläche

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-20/6.0

Req 21 Die Provisionierung von Zugriffsberechtigungen in angebundene Zielapplikationen muss zeitnah erfolgen.

Im Rahmen eines Lateral Movements eines Angreifers nach der erfolgreichen Übernahme eines IT-/NT-Systems sind besonders die Accounts von Interesse, die hohe bzw. sehr weitreichende Zugriffsberechtigungen auf Daten und IT-/NT-Systeme innehaben. Um die Wahrscheinlichkeit der Ausnutzung solcher hohen bzw. weitreichenden Zugriffsberechtigungen zu minimieren, müssen erstellte, geänderte und entzogene Zugriffsberechtigungen zeitnah in angebundene Zielapplikationen provisioniert werden. Der Ablauf der Provisionierung muss entsprechend durch das IAM Framework überwacht werden. Darüber hinaus müssen Prozesse im Fehlerfall initiiert werden, damit die Provisionierung sichergestellt wird. Die Ergebnisse der Provisionierungsläufe müssen protokolliert werden.

Dabei gelten die folgenden Regularien:

- **Push Mechanismus:** Direkt nach der Erteilung/Änderung der Zugriffsberechtigungen im IAM Framework müssen diese in die angebotenen Zielapplikationen provisioniert werden. Dies gilt für interne, PK und GK IAM Frameworks gleichermaßen.
- **Pull Mechanismus:** Die angebotene Zielapplikation muss alle 30 Minuten auf erstellte, geänderte bzw. entzogene Zugriffsberechtigungen im IAM Framework prüfen und diese provisionieren. Für PK und GK IAM Frameworks kann diese Zeitspanne bis zu 6 Stunden betragen. Als Beispiel für einen Pull Mechanismus dienen hier in einem LDAP hinterlegt Gruppen, anhand derer die Zugriffsberechtigungen innerhalb einer angebotenen Zielapplikation vergeben werden.
- **Nicht-angebunden Zielapplikationen:** Bei Zielapplikationen, die nicht an ein IAM Framework angebunden sind, müssen erstellte, geänderte und entzogene Zugriffsberechtigungen sofort angewendet werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-21/6.0

Req 22	Bei der Verwendung Token-basierter Protokolle dürfen die Token nur gemäß dem jeweils definierten Standard verwendet werden.
--------	---

Um eine Vergrößerung der Angriffsfläche Token-basierter Protokolle, wie beispielsweise OAuth2, SAML oder OpenID Connect (OIDC) zu verhindern, dürfen die jeweiligen Token nur gemäß der jeweiligen Protokoll-Spezifikation verwendet und nicht verändert werden.

Die folgenden Anforderungen für das jeweilige Protokoll müssen umgesetzt werden:

- OAuth2
 - **Access Token:** Ein Access Token wird für die Autorisierung des Clients für eine bestimmte Ressource verwendet.
- OIDC
 - **ID Token (Session Token):** Das ID-Token ist ein Sicherheitstoken, das ausschließlich Informationen über die Authentifizierung eines Endbenutzers durch einen Autorisierungsserver enthält. ID Token dürfen für weitergehenden Informationen, wie beispielsweise der Autorisierung oder der zugeordneten Zugriffsberechtigungen, nicht verwendet werden.
 - **Access Token:** Ein Access Token wird für die Autorisierung des Clients für eine bestimmte Ressource verwendet.
- SAML
 - **Authentication Assertion:** Die Authentication Assertion enthält Informationen bezüglich der Identifizierung des Benutzers und gibt die Zeit der Authentifizierung sowie die dabei verwendete Authentifizierungsmethode an.
 - **Attributes Assertion:** Die Attributes Assertion enthält beispielsweise Informationen bezüglich der Rollen, die dem Benutzer zugewiesen sind.
 - **Authorization Assertion:** In der Authorization Assertion wird angegeben, ob der Benutzer die Ressource benutzen darf oder die Verwendung, beispielsweise aufgrund einer fehlerhaften Authentifizierung, nicht gestattet wurde.

Motivation: Schutz der Daten der Organisation, Minimierung der Angriffsfläche sowie Erhöhung der Sicherheit durch Standardisierung

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-22/6.0

3.3. Identity Data Integration

Req 23 Bei der Anbindung von Quellapplikationen an ein IAM Framework müssen sich beide Systeme gegenseitig authentifizieren.

Über nicht gesicherte Schnittstellen des IAM Frameworks kann es einem Angreifer gelingen, gefälschte Identitäten und/oder Accounts in das IAM Framework zu importieren. Sollte der Angreifer erfolgreich sein, so sind alle nachgelagerten Zielapplikationen, die die entsprechenden Accounts verwenden sowie potenziell das IAM Framework selbst nicht mehr gesichert und es könnten beispielsweise Daten der Zielapplikationen exfiltriert werden. Aus diesem Grund müssen sich Quellapplikationen und das IAM Framework gegenseitig authentifizieren.

Motivation: Schutz der Zielapplikationen sowie der darin befindlichen Daten und des IAM Frameworks vor Angreifern, die mit selbst erstellten Identitäten bzw. Accounts ihr Ziel erreichen wollen

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-23/6.0

Req 24 Nur autorisierte Quellapplikationen dürfen an das IAM Framework angebunden werden.

Nur autorisierte Quellapplikationen dürfen Daten in das IAM Framework exportieren, damit die Integrität und Authentizität der importierten Daten sichergestellt werden kann. Als Beispiel sei hier ein SAP-System genannt, dessen Daten die Grundlage für die zu verwaltenden Identitäten darstellen. Eine autorisierte Quellapplikation wird wie folgt definiert:

- Schriftlich dokumentierte Schnittstellenvereinbarung zwischen der Quellapplikation und dem IAM Framework
- Abgeschlossenes PSA Verfahren der Quellapplikation mit Freigabe durch die Security sowie des Datenschutzes
- Freigabe der IT

Motivation: Um einen Missbrauch durch einen Angreifer zu erschweren bzw. zu verhindern, dürfen nur autorisierte Quellapplikationen Daten in das IAM Framework exportieren. Somit müsste der Angreifer erst die Quellapplikation(en) kompromittieren, ehe er gefälschte Identitäten in das IAM Framework einbringen kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten

ID: 3.69-24/6.0

Req 25 Es muss sichergestellt sein, dass ein Objekt aus genau einer Quellapplikation importiert wird.

Ein Objekt eines IAM Frameworks darf nicht aus verschiedenen Quellapplikationen importiert werden, damit eine 1:1 Zuordnung innerhalb des IAM Frameworks erreicht wird, d.h. der Import eines Objekts muss genau einer Quellapplikation zugeordnet sein. Ein Objekt darf jedoch mit Informationen aus anderen Quellapplikationen angereichert werden, solange die Nachvollziehbarkeit der Anreicherung (welche Information stammt aus welcher Quellapplikation?) gegeben ist und die Informationen aus der autoritativen Quelle, aus der das Objekt an sich importiert wurde, nicht überschrieben werden. Es muss sichergestellt werden, dass die Attribute eines Objekts sich nicht überschreiben bzw. widersprechen. Eine Anreicherung darf nur einen ergänzenden Charakter haben.

Motivation: Es soll einem Angreifer erschwert werden, kompromittierte Quellapplikationen zu missbrauchen, um nicht autorisierte Identitäten im IAM Framework zu erstellen

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

3.4. Accounts

Req 26 Inaktive Accounts müssen nach 35 Tagen deaktiviert werden.

Um einem Missbrauch inaktiver Accounts durch einen Angreifer vorzubeugen bzw. diesen zu entdecken, müssen inaktive Accounts idealerweise nach 30 Tagen, spätestens nach 35 Tagen deaktiviert werden.

Motivation: Minimierung der Angriffsfläche und Detektion von Angriffen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-26/6.0

Req 27 Es dürfen nur freigegebene und standardisierte Account-Typen verwendet werden.

Freigegebene und standardisierte Account-Typen und deren Verwendung erleichtern die Detektion von Angriffen, wenn beispielsweise ein Angreifer einen Service Account für die Anmeldung an einem Client Rechner verwendet. Aus diesem Grund dürfen nur freigegebene und standardisierte Account-Typen verwendet werden. Beispiele von Standardisierten Account-Typen sind die folgenden:

- Privilegierte Accounts (z.B. für Administratoren)
- Normale Benutzer-Accounts im Active Directory oder in einer beliebigen Zielapplikation
- Externe Accounts (z.B. für Fremddienstleister oder Partner)
- Service-Accounts (Dienste-Konto, welches für Zielapplikationen benötigt wird)
- Roboter-Accounts (auch als "Bots" bezeichnet; sie werden beispielsweise zum Automatisieren von Routine-Aufgaben eingesetzt)
- Geräte-Accounts (beispielsweise IoT-Devices)
- Funktions-Accounts (z.B. Empfang im Gebäude oder Schulungsrechner)

Motivation: Detektion von Angriffen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-27/6.0

Req 28 Benutzerkonten müssen die eindeutige Identifizierung des Benutzers sicherstellen. Geteilte Benutzerkonten oder Gruppenkonten sind verboten.

Benutzer müssen eindeutig von einem System identifiziert werden können. Dies wird typischerweise dadurch erreicht, dass für jeden Benutzer ein individuelles Benutzerkonto genutzt wird. Sogenannte Gruppenkonten, d.h. die Nutzung eines Benutzerkontos für mehrere Personen dürfen nicht verwendet werden. Eine Ausnahme dieser Anforderung sind die sogenannte Maschinenkonten. Diese werden für Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt und können damit nicht einer einzelnen Person zugewiesen werden.

Solche Benutzerkonten müssen individuell pro System oder pro Anwendung vergeben werden. Hierbei ist allerdings

sicherzustellen, dass eine missbräuchliche Nutzung solcher Benutzerkonten nicht möglich ist. Möglichkeiten, um eine missbräuchliche Nutzung solcher Benutzerkonten durch Personen zu verhindern, sind:

- Konfiguration eines, den Sicherheitsanforderungen entsprechendem Passwortes, dass nur einem kleinstmöglichen Kreis von Administratoren bekannt ist.
- Konfiguration des entsprechenden Benutzerkontos, so dass dies nur lokal verwendet werden kann und eine interaktive Anmeldung nicht möglich ist.
- Verwendung eines Verfahrens mit öffentlichem und privatem Schlüssel oder Zertifikaten für die Authentifizierung des entsprechenden Benutzerkontos.
- Einschränkung des Zugriffs über ein Netz auf legitimierte Systeme.

Motivation: Die eindeutige Identifizierung eines Benutzers ist Voraussetzung, um einem Benutzer Berechtigungen zuweisen zu können, die für die Durchführung seiner Aufgaben auf dem System notwendig sind. Nur so kann eine adäquate Zugriffskontrolle auf Daten und Dienste eines Systems erreicht und der missbräuchliche Zugriff verhindert werden.

Des Weiteren wird hierdurch ermöglicht, dass Tätigkeiten und Aktionen auf einem System protokolliert und einem Benutzer zugeordnet werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-28/6.0

Req 29 Die Benutzernamen von Accounts müssen pseudonymisiert sein.

Angriffe wählen als Ziel ihrer Bemühungen in der Regel Accounts, die ihnen auf dem Weg zur Erreichung ihres Ziels hilfreich sind. Darunter fallen sämtliche privilegierte Accounts, aber auch Accounts, die Zugriff auf bestimmte Daten haben. Üblicherweise haben sie diese Informationen, wie beispielsweise den Namen eines für Überweisungen zuständigen Mitarbeiters der Organisation, bereits im Vorfeld recherchiert und machen sich gezielt auf die Suche nach diesem Account.

Aus diesem Grund müssen die Benutzernamen von Accounts pseudonymisiert sein.

Nachfolgend eine nicht abschließende Auflistung unerlaubter Benutzernamen:

- Personalnummern, etwa aus SAP HR Systemen
- Eine Kombination von Nachnamen und Vornamen, auch die Verwendung von Teilen davon oder Abkürzungen
- Generell die Verwendung von Merkmalen, die auf Account-Inhaber bzw. Funktionalität des Accounts schließen lassen

Gerade im Active Directory Umfeld ist es zwar jedem Benutzer möglich, die Informationen jedes beliebigen Accounts auszulesen, also auch einem Angreifer. Dies ist jedoch erst möglich, nachdem man sich erfolgreich angemeldet hat, so dass ein pseudonymisierter Benutzername durchaus u.a. vor dem oben skizzierten Szenario schützt.

Für IAM Systeme im Privatkundenumfeld (PK) siehe weiterführende Informationen auf den [Webseiten der Gilde Wiki Sicherheitsanforderungen](#).

Motivation: Verringerung der Angriffsfläche

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-29/6.0

Req 30 Für privilegierten Zugang zu IT-/NT-Systemen müssen separate personenbezogene Accounts eingerichtet und verwendet werden.

Die Nutzung eines zentralen privilegierten Accounts durch mehrere Personen führt dazu, dass Vorgänge nicht der ausführenden Person eindeutig zugeordnet werden können. Daher muss für jede Identität, welche privilegierte Zugriffsberechtigungen benötigt, ein zusätzlicher separater privilegierter (administrativer) personenbezogener Account eingerichtet und genutzt werden.

Dieses Requirement ist eine Erweiterung des Req. 22 („Benutzerkonten müssen die eindeutige Identifizierung des Benutzers sicherstellen.“) aus dem Dokument „3.01 Technischer Basisschutz“.

Motivation: Die eindeutige Identifizierung eines Benutzers ist Voraussetzung, um einem Benutzer Berechtigungen zuweisen zu können, die für die Durchführung seiner Aufgaben auf dem System notwendig sind. Nur so kann eine adäquate Zugriffskontrolle auf Daten und Dienste erreicht und der missbräuchliche Zugriff verhindert werden. Darüber hinaus ist so eine bessere Detektion von Angriffen auf privilegierte Accounts gegeben.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.69-30/6.0

Req 31 Privilegierte Benutzerkonten müssen von einem zentralen IAM verwaltet werden.

Privilegierte Benutzerkonten unterliegen aufgrund ihrer Bedeutung für die IT-Sicherheit einer besonderen Aufmerksamkeit.

Jedes privilegierte Benutzerkonto muss einer natürlichen Person zugeordnet sein und mit einem eindeutigen Identifier (z. B. Corporate ID) abgespeichert werden. Für jede Applikation ist ein separates privilegiertes Benutzerkonto anzulegen.

Motivation: Privilegierte Benutzerkonten verfügen über weitreichende Berechtigungen, um Systemeinstellungen zu ändern oder andere kritische Funktionen auszuführen. Das Ziel von Angreifern ist es, sich Zugang zu solchen Benutzerkonten zu verschaffen. Aufgrund der verschärften Bedrohungslage mit der daraus folgenden Gesetzgebung (z. B. KRITIS, NIS2) muss für diese Benutzerkonten ein effektiver Lifecycle-Prozess (Joiner, Mover, Leaver) sichergestellt sein.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-31/6.0

Privilegierte Benutzerkonten unterliegen aufgrund ihrer besonderen Bedeutung für die IT-Sicherheit einer besonderen Aufmerksamkeit. Um unrechtmäßige Nutzung mittels Logging und Monitoring frühzeitig erkennen und Gegenmaßnahmen einleiten zu können, müssen privilegierte Benutzerkonten anhand eindeutiger Namenskonventionen identifiziert werden können.

Privilegierte Benutzerkonten müssen folgende Bedingungen erfüllen:

Lokale privilegierte Benutzerkonten:

- Systembedingte Standard-Benutzerkonten müssen deaktiviert werden.
- Lokale privilegierte Benutzerkonten müssen personalisiert angelegt werden, d. h. sie müssen sich über einen eindeutigen, pseudonymisierenden Identifier einer natürlichen Person zuordnen lassen. Gruppenaccounts bzw. gemeinsam genutzte Accounts sind nicht zulässig.
- Diese Benutzerkonten müssen mit den drei Buchstaben **adm** beginnen, gefolgt von einer eindeutigen, personenbeziehbaren ID (z. B. Corporate ID). Sollte dies technisch nicht möglich sein, kann eine alternative personenbeziehbare ID verwendet werden.

Zentrale privilegierte Benutzerkonten:

- Zentrale privilegierte Benutzerkonten werden über das zentrale IAM-System provisioniert und sind personalisiert, d. h. sie lassen sich einer natürlichen Person zuordnen.
- Das privilegierte Benutzerkonto muss mit dem A-Account Namen (nur Corporate ID ohne führendes 'A') der jeweiligen Person beginnen, gefolgt von einem E und zwei Ziffern.
 1. Werden unterschiedliche Access-Layer (z.B. Active Directories) in verteilten Infrastrukturen durch ein zentrales IAM-System provisioniert, ist darauf zu achten dass sich die privilegierten Benutzerkonten in der Namenskonvention durch zusätzliche Parameter unterscheiden. Siehe Beispiele.
 2. In hybriden Infrastrukturen (Microsoft Active Directory und Microsoft Entra ID) können Abweichungen bei der Namensgebung zur Unterscheidung der privilegierten Benutzerkonten in den unterschiedlichen Accesslayern vorgenommen werden. Siehe Beispiele.
- Pro Person können mehrere privilegierte Benutzerkonten angelegt werden.
- Für jede Anwendung, für die ein privilegiertes Benutzerkonto benötigt wird, ist ein eigenes Benutzerkonto zu verwenden.

Motivation: Die Benennung privilegierter Benutzerkonten muss der konzernweiten Namenskonvention folgen, um diese z. B. im Rahmen des Monitorings im SIEM (Security Information & Event System) aus der Masse der Benutzerkonten effizient identifizieren und filtern zu können.

Umsetzungsbeispiel: Lokale privilegierte Benutzerkonten:

Privilegierte Benutzerkonten müssen mit den drei Buchstaben **adm** beginnen, damit bei einer Sortierung der User-Liste aller privilegierten Benutzeraccounts zusammenhängend dargestellt werden.

Beispiel: A-Account: A123456789

- Lokales privilegiertes Benutzerkonto: **adm123456789**

Zentrale privilegierte Benutzeraccounts:

Der Privilegierte Account muss mit dem A-Account Namen der jeweiligen Person beginnen, gefolgt von einem E und zwei Ziffern.

Beispiel: A-Account: A123456789

- Zentrales privilegiertes Benutzerkonto (Microsoft Active Directory & Entra ID): A123456789**E01**,A123456789

E02,A123456789E03, ...

- Zentrales privilegiertes Benutzerkonto in verteilter Infrastruktur:[Frei zu definierender Parameter aus min. 2 Zeichen]123456789E01->XY123456789E01,XY123456789E02,XY123456789E03, ...
- Zentrales privilegiertes Benutzerkonto in hybrider Infrastruktur (nur Entra ID, Cloud only privilegierte Accounts):C123456789E01,C123456789E02,C123456789E03, ...

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-32/6.0

Req 33 Für Active Directory basierte Service Accounts müssen Group Managed Service Accounts verwendet werden.

In der Regel verwalten die Betreiber von IT-/NT-Systemen die Passwörter der im IT-/NT-System verwendeten Service-Accounts. Trotz der Komplexitäts-Anforderungen an die dabei zu verwendenden Passwörter ist es teilweise möglich, diese per Brute-Force-Attacken zu knacken.

Aus diesem Grund müssen Zielapplikationen bzw. Applikationen eines IAM Frameworks, die an ein Active Directory angebunden sind, group Managed Service Accounts (gMSA) verwenden. Bei der Verwendung eines gMSA wird die Kennwortverwaltung automatisch im Active Directory durchgeführt, ohne dass die Betreiber des IT-/NT-Systems darauf Einfluss nehmen können. Dadurch wird die Wahrscheinlichkeit einer erfolgreichen Brute-Force-Attacke erheblich minimiert.

Eine Dokumentation bezüglich gMSA ist hier zu finden: <https://learn.microsoft.com/de-de/windows-server/identity/ad-ds/manage/group-managed-service-accounts/group-managed-service-accounts/group-managed-service-accounts-overview>

Motivation: Verhinderung von Brute-Force-Attacken auf Kennwörter von Service Accounts

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.69-33/6.0

3.5. Credentials

Req 34 Es dürfen keine öffentlich bekannten Kennwörter verwendet werden.

Angreifer verwenden oftmals (gekaufte) Kennwort-Datenbanken oder Rainbow-Tables, um Kennwörter bzw. deren Hashes mit Hilfe von Brute-Force Attacken oder anderen Techniken zu ermitteln und diese für ihre Angriffe zu verwenden. Aus diesem Grund dürfen öffentlich bekannte Kennwörter in der Organisation nicht verwendet werden.

Zur Ermittlung öffentlich bekannter Kennwörter kann man sich im Internet verfügbarer Dienste wie beispielsweise „ID Guard“ der Deutschen Telekom Security GmbH bedienen, um etwa bei der turnusmäßigen Kennwort-Änderung eines Accounts das neue Kennwort dahingehend zu prüfen, ob es öffentlich bekannt ist. Bei der Nutzung von Diensten im Internet muss sichergestellt sein, dass dabei nur ein verschlüsselter Hash des Passwortes – und nicht das Passwort selbst – übertragen wird.

Dieses Requirement ist eine Erweiterung des Req. 25 („Falls Passwörter als Authentisierungsmerkmal genutzt wer-

den, muss ein Schutz gegen Online-Angriffe wie Wörterbuch- und Brute-Force-Attacken vorhanden sein, der das Erraten von Passwörtern stark erschwert.“) aus dem Dokument „3.01 Technischer Basisschutz“.

Motivation: Reduzierung der Sicherheitsvorfälle bzw. Minimierung der Angriffsfläche.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.69-34/6.0

Req 35	Falls Passwörter als Authentisierungsmerkmal für technische Accounts genutzt werden, müssen diese mindestens 30 Zeichen lang sein und drei der folgenden Zeichenkategorien beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.
--------	--

Technische Accounts, wie beispielsweise Service Accounts oder Roboter Accounts, sind in der Regel ein lohnendes Ziel für Angreifer, da Ihre Kennwörter einmal gesetzt und sehr selten – wenn überhaupt – geändert werden. Dies bedeutet, je länger solch ein Account verwendet wird, desto höher steigt die Wahrscheinlichkeit, dass das dazugehörige Kennwort durch einen Angreifer herausgefunden wird.

Aus diesem Grund müssen Kennwörter von technischen Accounts eine stärkere Password Policy erfüllen:

- Länge des Kennwortes: 30 Zeichen
- Verwendung von 3 von 4 Zeichenklassen (a-z, A-Z, 0-9, Sonderzeichen)

Dieses Requirement ist eine Erweiterung des Req. 27 („Falls Passwörter als Authentisierungsmerkmal genutzt werden, müssen diese mindestens 12 Zeichen lang sein und drei der folgenden Zeichenkategorien beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.“) aus dem Dokument „3.01 Technischer Basisschutz“.

Motivation: Minimierung der Angriffsfläche.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.69-35/6.0

Req 36	Wenn PGP bzw. S/MIME Zertifikate verwendet werden, so müssen diese identitätsbezogen und validiert sein.
--------	--

PGP bzw. S/MIME E-Mail-Verschlüsselung und -Signierung beruht auf der Verwendung von Zertifikaten einer PKI. Um den verschlüsselten E-Mail Austausch mit Empfängern außerhalb der eigenen Organisation sicherzustellen, werden in der Regel Zertifikate einer öffentlichen PKI verwendet. Um das fälschliche Ausstellen von Zertifikaten bzw. einen Missbrauch der Zertifikate zu verhindern, müssen diese Zertifikate identitätsbezogen sein und die Identitäten müssen gemäß den Anforderungen des Requirements “Es dürfen nur ausreichend verifizierte Identitäten im IAM Framework verwendet werden“ validiert sein.

Motivation: Verhinderung des Missbrauchs von Zertifikaten bzw. des fälschlichen Ausstellens von Zertifikaten

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

- Unberechtigte Modifikation von Daten

ID: 3.69-36/6.0

4. Access management

4.1. Authentifizierung

Req 37	Eine Authentifizierungs- und Autorisierungsinstanz darf nur standardisierte und etablierte Protokolle verwenden.
--------	--

Selbst entwickelte Protokolle sind in der Regel mit Fokus auf Funktionalität und nicht mit dem Fokus auf Sicherheit programmiert, so dass sie anfällig für Angriffe sind. Aus diesem Grund muss eine Authentifizierungs- und Autorisierungsinstanz standardisierte und etablierte Protokolle verwenden. Geeignete Protokolle für die Authentifizierung und Autorisierung sind beispielsweise die folgenden:

- OpenID Connect
- OAuth2
- SAML
- Kerberos
- WebAuthN
- Diameter

Dieses Requirement ist eine Erweiterung des Req. 1 („Software- und Hardware-Komponenten, für die es keine Wartung oder Pflege durch den Lieferanten, Hersteller oder Entwickler gibt, dürfen nicht verwendet werden.“) aus dem Dokument „3.01 Technischer Basisschutz“.

Motivation: Verringerung der Angriffsfläche und damit einhergehende Minimierung der Anzahl von Sicherheitsvorfällen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.69-37/6.0

Req 38	Eine Authentifizierungs- und Autorisierungsinstanz muss es ermöglichen, sich mit mehreren unterschiedlichen Authentifizierungsmethoden anmelden zu können.
--------	--

Für eine starke Authentifizierung ist es erforderlich, dass die Anmeldung mit mehreren unterschiedlichen Authentifizierungsmethoden möglich ist (Multi Factor Authentication, MFA). Eine MFA ist in der Regel für Angreifer nicht so leicht zu umgehen wie beispielsweise die alleinige Authentifizierung mit Benutzername und Kennwort.

Aus diesem Grund muss eine Authentifizierungs- und Autorisierungs-Instanz in einem IAM Framework es ermöglichen, sich mit mehreren unterschiedlichen Authentifizierungsmethoden anmelden zu können. Dabei sollten mehrere Methoden zur Auswahl stehen, die dann für eine Authentifizierung genutzt werden können.

Nachfolgend eine nicht abschließende Liste mit sicheren Authentifizierungsmethoden bzw. MFA Faktoren, die für eine sichere Authentifizierung miteinander kombiniert werden können:

- Username/Passwort
- Biometrische Faktoren:
 - Fingerabdruck
 - Handvenenscan
 - Iris Scan
 - Gesichtserkennung

- Smartcards, FIDO2 (bzw. zertifikatsbasierte Authentifizierung mit einem HW Token)
- Zertifikate (inkl. SSH Certificates)
- Authentication Apps auf dem Company Phone
- OneTime Token
 - Hardware
 - Software
 - QR Code

Wird die Authentifizierungsmethode Username/Passwort verwendet, so muss eine weitere Authentifizierungsmethode, wie z.B. eine Smartcard mit PIN, für die Authentifizierung verwendet werden.

Motivation: Schutz der Ziel-Applikationen und der darin befindlichen Daten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

ID: 3.69-38/6.0

Req 39 Unsichere Authentifizierungsmethoden dürfen nicht eingesetzt werden.

Unsichere Authentifizierungsmethoden ermöglichen es nicht nur einem Angreifer, sich unerlaubt an IT-/NT-Systemen anzumelden, sondern verweigern auch potenziell dem regulären Benutzer den Zugang aufgrund ihrer Unzuverlässigkeit oder Ungenauigkeit.

Aus diesem Grund dürfen unsichere Authentifizierungsmethoden nicht eingesetzt werden. Als Beispiel dafür seien die folgenden genannt:

- Verhaltensbasierte Token
 - Gesten
 - Keyboard Stroke
 - Voice Print
- Biometrische Token
 - Hand Topography
 - Retina Scan
 - Hand Geometry

Motivation: Verringerung der Angriffsfläche.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.69-39/6.0

4.2. Autorisierung

Req 40 Die Autorisierung eines Benutzers muss eindeutig und reproduzierbar erfolgen.

Treten bei der Zuweisung von Zugriffsberechtigungen an einen Account im Zuge der Autorisierung inkonsistente Zustände in der Art auf, dass von Zeit zu Zeit erhöhte Zugriffsberechtigungen erteilt werden, die für die durchzuführen-

den Aufgaben nicht benötigt werden, so können Angreifer diesen Umstand gezielt ausnutzen. Aus diesem Grund muss die Autorisierung eines Benutzers eindeutig und reproduzierbar erfolgen.

Motivation: Verringerung der Angriffsfläche und Sicherstellung Least-Privilege-Prinzip.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.69-40/6.0

4.3. Privileged Account Management (PAM)

Req 41	Die Provisionierung des PAM muss automatisiert und ausschließlich durch das IAM Framework erfolgen.
--------	---

Die Möglichkeit der Erstellung privilegierter Accounts muss verringert werden, um es dem Angreifer zu erschweren, seine vorhandenen Rechte auszuweiten. Privilegierte Accounts dürfen nicht in der PAM Lösung selbst erstellt werden, d.h. es darf keine Möglichkeit geben, privilegierte Accounts am genehmigten Prozess vorbei on the Fly in der PAM Lösung zu erstellen, um diese für den Zugriff auf zu administrierende IT-/NT-Systeme zu verwenden. Falls die PAM Lösung ein eigenes Identity Management betreibt, so sind alle Requirements für ein internes IAM Framework zu erfüllen. Aus diesem Grund muss die Provisionierung von weitreichenden Zugriffsberechtigungen bzw. von privilegierten Accounts automatisiert und ausschließlich durch das IAM Framework erfolgen.

Motivation: Reduzierung der Möglichkeiten des Angreifers um seine Rechte auszuweiten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.69-41/6.0

Req 42	Es muss möglich sein, Accounts und Zugriffsberechtigungen zeitlich limitiert bzw. befristet zu vergeben.
--------	--

Ein Angreifer strebt danach, die volle Kontrolle über das Angriffsziel zu erhalten. Dies erreicht er u.a. durch die Übernahme von Konten mit privilegierten Zugriffsberechtigungen. Verkürzt man nun die Zeitspanne, in der die privilegierten Zugriffsberechtigungen zur Verfügung stehen bzw. einem Account zugewiesen sind, in dem man einen Start- und einen Endzeitpunkt für die Nutzung dieser Zugriffsberechtigungen setzt, so verringert man die Möglichkeiten für den Angreifer, eben jene Zugriffsberechtigungen zu erlangen. Aus diesem Grund muss es möglich sein, Accounts und Zugriffsberechtigungen zeitlich limitiert zu vergeben.

Motivation: Verringerung der Angriffsfläche zur Erlangung privilegierter Zugriffsberechtigungen bzw. von Privilege Escalation

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.69-42/6.0

Req 43	Wenn eine automatische Rotation von Passwörtern durch die PAM Lösung angeboten wird, muss diese genutzt werden.
--------	---

Ein automatisiertes Ändern von Passwörtern durch die PAM Lösung macht es einem Angreifer nahezu unmöglich, erbeutete Credentials zu verwenden. Die Passwörter werden nach einmaliger Nutzung durch die PAM Lösung geändert und verschlüsselt im Passwort Tresor abgelegt. Auf die Art und Weise kennt nicht einmal der berechtigte privilegierte Benutzer das Kennwort. Aus diesem Grund muss die automatische Rotation von Passwörtern benutzt werden, wenn die PAM Lösung dies anbietet.

Dabei müssen die folgenden Anforderungen berücksichtigt werden:

- Länge des Kennwortes: 30 Zeichen
- Verwendung 3 von 4 Zeichenklassen (a-z, A-Z, 0-9, Sonderzeichen)
- Ein Passwort gilt für genau eine Benutzeranmeldung

Motivation: Verhinderung der Ausspähung von Credentials von privilegierten Accounts durch einen Angreifer und somit Reduzierung der Angriffsfläche

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-43/6.0

Req 44	Die Zuteilung der privilegierten Accounts und der damit verbundenen Zugriffsberechtigungen muss mit Hilfe eines Genehmigungsworkflows durchgeführt werden.
--------	--

Privilegierte Accounts – insbesondere die damit verbundenen Zugriffsberechtigungen – sind ein begehrtes Ziel von Angreifern. Denn mit ihnen ist es in der Regel möglich, Zugriff auf andere Accounts und damit verbundene Daten zu bekommen. Um einem Missbrauch vorzubeugen, muss die Zuteilung der privilegierten Accounts und der damit verbundenen Zugriffsberechtigungen mit Hilfe eines Genehmigungsworkflows erfolgen. Dabei müssen die Sicherheitsanforderungen der Kapitel „Generelle Vorgaben für Prozesse und Workflows“ sowie „Genehmigungs-Workflow“ erfüllt werden, sofern die PAM Lösung den Genehmigungsworkflow selbst realisiert. Andernfalls muss der Genehmigungsworkflow des jeweiligen IAM Frameworks verwendet werden, der die PAM Lösung provisioniert.

Motivation: Reduzierung der Angriffsfläche und damit verbundener Schutz der privilegierten Accounts und den damit verbundenen Zugriffsberechtigungen. Gleichzeitig erhält man somit eine Nachvollziehbarkeit der Nutzung privilegierter Accounts, um im Verdachtsfall forensische Untersuchungen durchführen zu können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-44/6.0

5. Prozesse und Workflows

5.1. Generelle Vorgaben für Prozesse und Workflows

Req 45	Alle automatisierten Prozess- und Workflow-Schritte eines IAM Frameworks müssen überwacht und entsprechende Fehler bzw. Abweichungen müssen alarmiert werden.
--------	---

Um die Verfügbarkeit des IAM Frameworks zu gewährleisten und Angreifer, die Fehler in der Prozess- bzw. Workflow-Kette ausnutzen, zu erkennen, muss ein permanentes Monitoring aller automatisierten Prozess- und Workflow-Schritte eines IAM Frameworks implementiert sein. Erkannte Fehler bzw. Abweichungen müssen alarmiert werden. Dieses Monitoring sollte idealerweise durch ein SIEM, sofern technisch umsetzbar, realisiert werden.

Motivation: Erhöhung der Verfügbarkeit des IAM Frameworks sowie frühzeitige Detektion von Angriffsversuchen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-45/6.0

Req 46	Alle Prozesse und Workflows des IAM Frameworks müssen dokumentiert und freigegeben sein.
--------	--

Gerade bei einem IAM Framework gilt es, auf die Sicherheit der Prozesse zu achten, so dass es nicht möglich ist, durch organisatorische oder prozessuale Fehler Einfluss auf das IAM Framework zu nehmen bzw. das IAM Framework missbrauchen zu können. Aus diesem Grund müssen alle Prozesse dokumentiert und durch das jeweilige Sicherheitsmanagement der Organisation freigegeben sein.

Motivation: Reduzierung der Möglichkeiten für einen Angreifer, Fehler in der Prozesskette für einen Missbrauch auszunutzen. Weiterhin Erhöhung der Verfügbarkeit des IAM Frameworks, da weniger fehlerhafte Prozesse zu weniger Ausfällen im IAM Framework führen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-46/6.0

5.2. Joiner Prozess

Req 47	Es muss ein Joiner Prozess etabliert sein.
--------	--

Für einen Angreifer kann es von Vorteil sein, wenn er sich im Rahmen seines Angriffes selbständig neue Identitäten nebst Accounts erstellen kann. Diese können beispielsweise für weitere Privilege Escalations oder Verschleierung von Daten Exfiltration genutzt werden. Darüber hinaus gibt es gesetzliche und regulatorische Vorgaben, die bestimmte Eigenschaften von Identitäten und Accounts einfordern. Aus diesem Grund muss ein Joiner Prozess für neue Mitarbeiter einer Organisation etabliert sein, der dokumentiert und im Rahmen des PSA Prozesses durch den Datenschutz sowie IT Security freigegeben wurde.

Dieser Joiner Prozess muss die Anforderungen dieses Kapitels umsetzen und die folgenden Schritte für ein internes IAM Framework enthalten:

- Import der Identitäten/der Identitätsdaten aus autorisierten Quellapplikationen
- Erstellung notwendiger Accounts, Credentials, Zertifikate, etc. durch automatisierte Prozesse sowie Provisionierung derselben unter Beachtung der dafür notwendigen Security Requirements
- Sichere Übermittlung der notwendigen Informationen an den neuen Mitarbeiter

Für IAM Frameworks aus dem PK bzw. GK Umfeld müssen ähnliche Prozesse nur mit anderen Anforderungen erstellt werden. Folgende Fragestellungen können dabei helfen:

- Wie erstellt der Kunde seine Identität/seinen Account?
- Mit welchen Informationen soll die Identität/der Account angereichert werden?
- Wie wird seine E-Mail-Adresse verifiziert?
- Welche Daten der Identität sind notwendig? Wie werden diese verifiziert?

Nicht-angebundene Zielapplikationen, die von internen Mitarbeitern genutzt werden, müssen die Anforderungen für ein internes IAM Framework erfüllen.

Motivation: Verringerung der Angriffsfläche

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-47/6.0

Req 48	Die Aktivierung aller Accounts sowie Zutritts- und Zugangsmittel, die dem neuen Mitarbeiter zugewiesen wurden, muss bis spätestens 30 Tage nach Aushändigung an den Verantwortlichen für die Ausgabe erfolgen.
--------	--

Falls nach 30 Tagen keine Aktivierung aller zugewiesenen Accounts sowie Zutritts- und Zugangsmittel durch den neuen Mitarbeiter erfolgt ist, so müssen die Accounts sowie Zutritts- und Zugangsmittel gelöscht bzw. invalidiert werden. Diese Maßnahme verringert die Anzahl bereitgestellter, aber nicht aktivierter bzw. nicht genutzter Accounts sowie Zutritts- und Zugangsmittel. Andernfalls könnten diese durch Angreifer missbräuchlich ausgenutzt werden. Die Überwachung der Frist muss durch das jeweilige IAM Framework sichergestellt werden.

Motivation: Verringerung der Möglichkeiten für den Angreifer, sich unerlaubt Zutritt in Räumlichkeiten und Zugang zu IT-/NT-Systemen zu verschaffen

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-48/6.0

Req 49	Bei Erstellung von Accounts für neue Mitarbeiter dürfen standardmäßig keine kritischen Zugriffsberechtigungen gesetzt werden.
--------	---

Zur Vermeidung überflüssiger bzw. zu großer Zugriffsberechtigungen und der Reduzierung der Gefahr, dass Angreifer „vergessene“ Accounts für Angriffe auf IT-/NT-Systeme verwenden, dürfen neu angelegte Accounts für neue Mitarbeiter standardmäßig nicht mit kritischen Zugriffsberechtigungen konfiguriert werden. Dieses Requirement gilt sowohl für angebundene bzw nicht-angebundene Zielapplikationen sowie für alle IAM Frameworks (Intern, PK, GK).

Motivation: Reduzierung der Gefahr, dass vergessene oder übersehene Accounts für Angriffe missbraucht werden können. Des Weiteren werden so die notwendigen Zugriffsberechtigungen auf ein Mindestmaß reduziert, damit nicht

versehentlich Accounts mit zu großen Zugriffsberechtigungen ausgestattet werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-49/6.0

5.3. Mover Prozess

Req 50	Es muss ein Mover Prozess etabliert sein.
--------	---

Für einen Angreifer kann es von Vorteil sein, wenn er im Rahmen seines Angriffes Accounts mit sehr hohen bzw. weitreichenden Zugriffsberechtigungen, die aus einem Wechsel des Arbeitsplatzes eines Mitarbeiters innerhalb der Organisation ohne einen etablierten Mover Prozess resultieren, verwenden kann. Diese können beispielsweise für weitere Privilege Escalations oder Verschleierung von Daten Exfiltration genutzt werden. Aus diesem Grund muss ein Mover Prozess für interne Mitarbeiter einer Organisation etabliert sein, der dokumentiert und im Rahmen des PSA Prozesses durch den Datenschutz sowie IT Security freigegeben wurde. Dieser Mover Prozess muss die Anforderungen dieses Kapitels für ein internes IAM Framework erfüllen.

Nicht-angebundene Zielapplikationen, die von internen Mitarbeitern genutzt werden, müssen ebenfalls die Anforderungen dieses Kapitels für ein internes IAM Framework erfüllen.

Motivation: Verringerung der Angriffsfläche

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-50/6.0

Req 51	Bei einem Wechsel des Arbeitsplatzes innerhalb der Organisation muss der Recertification-Prozess für den betreffenden Mitarbeiter durchgeführt werden.
--------	--

Sollte ein Mitarbeiter innerhalb der Organisation seinen Arbeitsplatz wechseln und die Zugriffsberechtigungen sowie Zutritts- und Zugangsberechtigungen, die für die alte Aufgabe notwendig waren, nicht gelöscht bzw. deaktiviert werden, so wäre ein Angreifer, nachdem er die Identität und die damit verbundenen Accounts übernommen hat, in der Lage, wesentlich mehr IT-/NT-Systeme zu kompromittieren und bspw. Daten zu exfiltrieren als es mit den notwendigen Zugriffsberechtigungen des Mitarbeiters möglich gewesen wäre.

Aus diesem Grund muss bei einem Wechsel des Arbeitsplatzes innerhalb der Organisation der Recertification Prozess durchgeführt werden, dabei gelten die folgenden Bedingungen:

- spätestens drei Arbeitstage nach dem Wechsel des Arbeitsplatzes muss der Prozess durchgeführt werden
- nicht mehr benötigte Zugriffsberechtigungen sowie Zutritts- und Zugangsberechtigungen müssen gelöscht bzw. deaktiviert werden.

Der Recertification Prozess muss Bestandteil des Mover Prozesses sein.

Motivation: Reduzierung des Schadensmaßes bei einem Sicherheitsvorfall und Einschränkung der Möglichkeiten für einen Angreifer.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-51/6.0

Req 52	Bei einer Neuzuweisung von Zugriffsberechtigungen sowie Zutritts- und Zugangsberechtigungen im Rahmen eines Wechsels des Arbeitsplatzes in der Organisation müssen diese innerhalb von 30 Tagen durch den Mitarbeiter persönlich aktiviert werden.
--------	--

Falls nach 30 Tagen keine Aktivierung aller zugewiesenen Accounts sowie Zutritts- und Zugangsmittel durch den Mitarbeiter bei einem Arbeitsplatzwechsel erfolgt ist, müssen die Accounts sowie Zutritts- und Zugangsmittel gelöscht bzw. invalidiert werden. Diese Maßnahme verringert die Anzahl bereitgestellter, aber nicht aktivierter bzw. nicht genutzter Accounts sowie Zutritts- und Zugangsmittel. Andernfalls könnten diese durch Angreifer missbräuchlich genutzt werden. Die Überwachung der Frist muss durch das jeweilige IAM Framework sichergestellt werden.

Motivation: Verringerung der Möglichkeiten für den Angreifer, sich unerlaubt Zutritt in Räumlichkeiten und Zugang zu IT-/NT-Systemen zu verschaffen

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.69-52/6.0

5.4. Leaver Prozess

Req 53	Es muss ein Leaver Prozess etabliert sein.
--------	--

Für einen Angreifer kann es von Vorteil sein, wenn er im Rahmen seines Angriffes Accounts mit sehr hohen bzw. weitreichenden Zugriffsberechtigungen für Privilege Escalations oder Verschleierung von Daten Exfiltration nutzen kann, die nach dem Austritt eines Mitarbeiters aus der Organisation nicht mindestens deaktiviert wurden.

Aus diesem Grund muss ein Leaver Prozess für ausscheidende Mitarbeiter einer Organisation etabliert sein, der dokumentiert und im Rahmen des PSA Prozesses durch den Datenschutz sowie IT Security freigegeben wurde. Dieser Leaver Prozess muss die Anforderungen für einen Leaver Prozess aus diesem Kapitel für ein internes IAM Framework erfüllen.

Für IAM Frameworks aus dem PK bzw. GK Umfeld müssen ähnliche Prozesse nur mit anderen Anforderungen erstellt werden. Folgende Fragestellungen können dabei helfen:

- Wie deaktiviert/löscht der Kunde seine Identität/seinen Account?
- Soll er dies überhaupt können?
- Wie lange ist die Aufbewahrungsfrist der Daten

Nicht-angebundene Zielapplikationen, die von internen Mitarbeitern genutzt werden, müssen die Anforderungen für ein internes IAM Framework erfüllen.

Motivation: Verringerung der Angriffsfläche

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-53/6.0

Req 54 Bei einer längeren Abwesenheit des Mitarbeiters müssen Zugriffsberechtigungen sowie Zutritts- und Zugangsmittel deaktiviert werden.

Ist ein Mitarbeiter beispielsweise aufgrund eines Sabbaticals oder Elternzeit sowie einem absehbaren Krankheitsverlauf längere Zeit abwesend, so müssen entweder zu Beginn einer geplanten Abwesenheit oder zum Zeitpunkt des Bekanntwerdens einer ungeplanten Abwesenheit alle Zugriffsberechtigungen sowie Zutritts- und Zugangsmittel deaktiviert werden. Andernfalls könnten diese von Angreifern unbemerkt verwendet werden.

Motivation: Reduzierung der Angriffsfläche und Verhinderung von Sicherheitsvorfällen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.69-54/6.0

Req 55 Beim Austritt eines Mitarbeiters müssen am Austrittstag alle Zugriffsberechtigungen sowie Zutritts- und Zugangsmittel zurückgegeben und deaktiviert werden.

Zur Verhinderung, dass Zugriffsberechtigungen sowie Zutritts- und Zugangsmittel des ausgeschiedenen Mitarbeiters über sein Austrittsdatum hinaus missbräuchlich verwendet werden, müssen diese am Austrittstag sämtlich deaktiviert werden.

Dabei müssen die folgenden Bedingungen eingehalten werden:

- Deaktivierung sämtlicher Accounts, Zugangs-Token sowie Authentifizierungs-Faktoren um 23:59 Uhr des Austrittsdatums (Gültig ist die Zeitzone, in der der Mitarbeiter beschäftigt war)
- Rückgabe sämtlicher physikalischer Authentifizierungsfaktoren und Zugangstoken spätestens beim letztmaligen Verlassen des Arbeitsplatzes
- Private Schlüssel für Verschlüsselung müssen 6 Monate sicher aufbewahrt werden, damit etwa verschlüsselte Dokumente wieder hergestellt werden können.

Motivation: Reduzierung der Angriffsfläche und Vermeidung von Sicherheitsvorfällen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.69-55/6.0

Req 56 Nach dem Austritt eines Mitarbeiters aus der Organisation müssen alle ihm zugeordneten Accounts nach spätestens 30 Tagen deprovisioniert werden.

Alle Accounts eines ausgeschiedenen Mitarbeiters müssen spätestens nach 30 Tagen aus den Zielapplikationen sowie den Authentifizierungs- und Autorisierungsinstanzen deprovisioniert werden. Andernfalls können sie durch einen Angreifer (nach Aktivierung) verwendet werden, um bspw. unerlaubten Zugriff auf geschützte Daten zu bekommen. Dabei ist darauf zu achten, die Accounts lediglich zu deprovisionieren, nicht jedoch im IAM Framework zu löschen.

Motivation: Reduzierung der Angriffsfläche und Vermeidung von Sicherheitsvorfällen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.69-56/6.0

Req 57 Es muss ein Emergency Leaver Prozess etabliert sein.

Zum sofortigen Abwenden eines Schadens von der Organisation, etwa durch Nutzung kompromittierter Accounts für die Daten Exfiltration während eines Angriffs, muss es möglich sein, Accounts und/oder Identitäten umgehend, d.h. binnen maximal 5 Minuten nach Erkennung und Bestätigung des Angriffs, zu deaktivieren, so dass kein weiterer Schaden verursacht werden kann. Aus diesem Grund muss ein Emergency Leaver Prozess definiert sein.

Motivation: Reduzierung des Schadensausmaßes bei Sicherheitsvorfällen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.69-57/6.0

Req 58 Wenn ein Active Directory verwendet wird, so müssen die E-Mail-Adresse und der User Principal Name (UPN) des ausgeschiedenen Mitarbeiters mindestens 6 Monate gesperrt werden, bevor sie wiederverwendet werden dürfen.

Zur Sicherstellung des Zugriffs auf Daten eines ausgeschiedenen Mitarbeiters werden die ihm zugeordnete E-Mail-Adresse und die UPN benötigt. Aus diesem Grunde müssen die E-Mail-Adresse und der UPN des ausgeschiedenen Mitarbeiters mindestens 6 Monate gesperrt werden, ehe sie wieder verwendet werden dürfen.

Motivation: Sicherstellung des Zugriffs auf benötigte Daten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.69-58/6.0

5.5. Reconciliation-Prozess

Req 59 Es muss ein Reconciliation-Prozess etabliert sein.

Reconciliation bezeichnet den Vorgang der Konsistenz- und Kompatibilitätsprüfung über unterschiedliche Access Layer (beispielsweise Active Directory, unterschiedliche LDAP Server, etc.) hinweg. In einem IAM Framework steht der Prozess in Verbindung mit der Provisionierung und der Synchronisation von Accounts in die unterschiedlichen Access Layer. Insbesondere doppelte Accounts derselben Identität bilden ein hohes Risiko für intransparente Zugriffsberechtigungen.

Aus diesem Grund muss ein Reconciliation-Prozess etabliert werden, der das IAM Framework untersucht und regelmäßig ausgeführt wird.

Handelt es sich bei dem IT-/NT-System um eine nicht-angebundene Zielapplikation, so muss ein entsprechender Report bezüglich der Durchführung des Reconciliation Prozesses inklusive der Ergebnisse erstellt und zur Verfügung gestellt werden.

Motivation: Verhinderung von Sicherheitsvorfällen wie beispielsweise Data Exfiltration, Lateral Movement, Privilege Escalation.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-59/6.0

5.6. Prozess zur Ermittlung verwaister Accounts

Req 60	Es muss ein Prozess etabliert werden, der verwaiste Accounts ermittelt.
--------	---

Verwaiste Accounts werden von keiner Identität für eine Anmeldung verwendet und werden in der Regel nicht überwacht, d.h. sie sind keiner Identität zugeordnet. Angreifer nutzen diese „vergessenen“ Accounts in der Regel, um sich unerlaubt an Zielapplikationen anzumelden und dort beispielsweise Daten zu exfiltrieren. Aus diesem Grund muss ein Prozess etabliert werden, der das IAM Framework auf verwaiste Accounts untersucht und regelmäßig ausgeführt wird. Generell ist solch ein Prozess Teil des Reconciliation Prozesses.

Handelt es sich bei dem IT-/NT-System um eine nicht-angebundene Zielapplikation, so muss ein entsprechender Report bezüglich der Durchführung des Prozesses zur Ermittlung verwaister Accounts inklusive der Ergebnisse erstellt und zur Verfügung gestellt werden.

Motivation: Verhinderung von Sicherheitsvorfällen wie beispielsweise Data Exfiltration, Lateral Movement, Privilege Escalation.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-60/6.0

Req 61	Verwaiste Accounts müssen spätestens innerhalb von 5 Werktagen nach Erlangen der Kenntnis deaktiviert und eine verantwortliche Stelle alarmiert werden.
--------	---

Bei jedem verwaisten Account, der im Rahmen des Reconciliation-Prozesses ermittelt wird, ist anzunehmen, dass er

potenziell für einen Angriff verwendet werden kann. Aus diesem Grund muss jeder ermittelte verwaiste Account ohne zeitlichen Verzug, innerhalb von 5 Werktagen nach Erlangen der Kenntnis, deaktiviert und eine verantwortliche Stelle alarmiert werden.

Motivation: Verhinderung von Sicherheitsvorfällen wie beispielsweise Data Exfiltration, Lateral Movement, Privilege Escalation.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-61/6.0

Req 62	Der Prozess zum Erkennen verwaister Accounts muss spätestens alle 30 Tage ausgeführt werden.
--------	--

Je eher ein verwaister Account ermittelt werden kann, desto geringer ist die Wahrscheinlichkeit, dass er für einen Angriff verwendet wurde bzw. in Gegenwart oder Zukunft verwendet wird. Daher muss der Prozess zum Erkennen verwaister Accounts spätestens alle 30 Tage ausgeführt werden.

Motivation: Erkennung potenzieller Angriffe sowie Reduzierung der Angriffsfläche.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-62/6.0

Req 63	Wenn verwaiste Accounts entdeckt worden sind, so muss untersucht werden, ob sie für eine Anmeldung verwendet worden sind.
--------	---

Ermittelte verwaiste Accounts könnten in der Vergangenheit für Angriffe missbraucht worden sein, die nicht durch andere Maßnahmen der Detektion erkannt wurden. Aus diesem Grund muss bei jedem ermittelten verwaisten Account ermittelt werden, ob er für einen Angriff verwendet worden ist bzw. gerade für laufende Angriffe missbraucht wird.

Motivation: Erkennung potenziell laufender Angriffe und Verbesserung der Detektion von Angriffen sowie Mitigation von eventuellen Schwachstellen, die für einen Angriff verwendet worden sind.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-63/6.0

5.7. Recertification-Prozess

Req 64 Es muss ein Recertification Prozess etabliert sein.

In der Praxis kann es vorkommen, dass einem Account nicht benötigte Zugriffsberechtigungen zugeordnet sind. Dies kann beispielsweise durch nicht korrekt definierte Mover Prozesse oder durch ein Zuweisen der Zugriffsberechtigungen außerhalb der definierten Prozesse geschehen. Aus diesem Grund muss ein Recertification-Prozess etabliert sein, der ausnahmslos für alle Accounts durchgeführt wird und die folgenden Anforderungen in diesem Kapitel erfüllt.

Motivation: Reduzierung des Schadensausmaßes bei einem Angriff und Sicherstellung der Integrität der Daten in den Zielapplikationen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.69-64/6.0

Req 65 Der Recertification Prozess muss regelmäßig durchgeführt werden.

Je eher erhöhte oder falsche Zugriffsberechtigungen in einem IAM Framework ermittelt werden, desto geringer ist die Wahrscheinlichkeit, dass Angreifer oder Mitarbeiter Daten einsehen oder verändern können, für die sie normalerweise nicht berechtigt sind. Aus diesem Grund muss der Recertification-Prozess spätestens alle 12 Monate durchgeführt werden. Je nach Kritikalität der Zielapplikation bzw. der darin befindlichen Daten sollten für diesen Zeitraum kürzere Abstände gewählt werden.

Für nicht-angebundene Zielapplikationen muss der Recertification-Prozess spätestens alle 3 Monate durchgeführt werden. Ein entsprechender Report bezüglich der Durchführung des Recertification-Prozesses inklusive der Ergebnisse muss erstellt und zur Verfügung gestellt werden.

Zielapplikation	Zyklus
Zielapplikation an ein zentrales, internes IAM angebunden	1 x jährlich / alle 12 Monate
Applikationen mit Internal Control System - Relevanz (ICS IT) bzw. TOP66 Applikationen	2 x jährlich / alle 6 Monate
Zielapplikationen, die nicht an ein zentrales, internes IAM angebunden sind	4 x jährlich / alle 3 Monate

Motivation: Reduzierung des Schadensausmaßes bei einem Angriff und Sicherstellung der Integrität der Daten in den Zielapplikationen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

Req 66	Nicht benötigte Zugriffsberechtigungen müssen spätestens innerhalb von 5 Werktagen nach Erlangen der Kenntnis entfernt werden.
--------	--

Nicht benötigte Zugriffsberechtigungen stellen einen Verstoß gegen das Least-Privilege-Prinzip dar und können für Daten Exfiltration im Rahmen eines Angriffs missbraucht werden. Aus diesem Grund müssen nicht benötigte Zugriffsberechtigungen im Rahmen des Recertification-Prozesses ohne zeitlichen Verzug, spätestens innerhalb von 5 Werktagen nach Erlangen der Kenntnis, entfernt werden, um die Wahrscheinlichkeit für einen Missbrauch dieser erhöhten Zugriffsberechtigungen zu minimieren. Startzeitpunkt für die Frist ist der durchlaufene Recertification-Prozess.

Motivation: Reduzierung des Schadensausmaßes bei einem Angriff und Sicherstellung der Integrität der Daten in den Zielapplikationen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

Req 67	Der Recertification-Prozess muss im Mover Prozess etabliert sein.
--------	---

Je eher erhöhte oder falsche Zugriffsberechtigungen in einem IAM Framework ermittelt werden, desto geringer ist die Wahrscheinlichkeit, dass Angreifer oder Mitarbeiter Daten einsehen oder verändern können, für die sie normalerweise nicht berechtigt sind. Aus diesem Grund muss der Recertification-Prozess im Mover Prozess so etabliert werden, dass bei einem Wechsel eines Mitarbeiters der Recertification Prozess anlassbezogen durchlaufen wird.

Motivation: Reduzierung des Schadensausmaßes bei einem Angriff und Sicherstellung der Integrität der Daten in den Zielapplikationen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

5.8. Account Usage Review Prozess

Req 68	Es muss ein Account Usage Review Prozess etabliert sein.
--------	--

Sollte beispielsweise ein Mitarbeiter die Organisation verlassen, so müssen die direkt seiner Identität zugeordneten Accounts entfernt werden. Aus diesem Grund muss jederzeit sichergestellt sein, dass eine Übersicht vorliegt, aus der hervorgeht, in welchem IT-/NT-System der jeweilige Account verwendet wird, damit es möglich ist, den jeweiligen Account zu deprovisionieren.

Motivation: Verhinderung des Abflusses von Daten und Verhinderung der Übernahme verwaister Accounts.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-68/6.0

5.9. Genehmigungs-Workflow

Req 69 Es muss ein Genehmigungs-Workflow etabliert sein.

In einem IAM Framework werden in der Regel in einem Genehmigungs-Workflow Zugriffsberechtigungen auf Antrag erteilt oder verweigert. Darüber hinaus können jedoch auch andere Bereiche in einem IAM Framework mit einem Genehmigungs-Workflow ausgestattet werden. Dies dient dazu, die im Genehmigungs-Workflow erteilten Zugriffsberechtigungen (um beim Beispiel zu bleiben) nachvollziehbar und sicher für den betreffenden Account zu provisionieren, um es für einen Angreifer zu erschweren, sich Zugriffsberechtigungen für den von ihm übernommen Account zuzuweisen. Aus diesem Grund muss ein Genehmigungs-Workflow etabliert sein, der die folgenden Anforderungen in diesem Kapitel erfüllt.

Motivation: Vorbeugung der Erschleichung von (weitreichenden) Zugriffsberechtigungen zur Verhinderung von bspw. Daten Exfiltration und Manipulation sowie Identitätsmissbrauch.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.69-69/6.0

Req 70 Die Rollen Antragsteller und Genehmigender müssen von verschiedenen natürlichen Identitäten wahrgenommen werden.

Im Rahmen eines Genehmigungs-Workflows üben die in der Rolle des Genehmigenden Tätigen eine kontrollierende Funktion aus, indem sie entscheiden, ob der Antragsteller beispielsweise die beantragten Zugriffsberechtigungen benötigt oder nicht. Diese Kontrollfunktion kann von technischen Identitäten, etwa Robotern („Bots“), nur sehr eingeschränkt ausgeübt werden. Zudem können technische, automatisierte Prozesse von Angreifern manipuliert werden. Aus diesem Grund müssen die Rollen Antragsteller und Genehmigender von natürlichen Identitäten wahrgenommen werden. Darüber hinaus müssen die Rollen Antragsteller und Genehmigender von verschiedenen natürlichen Identitäten wahrgenommen werden. Damit wird verhindert, dass sich Antragsteller selbständig Zugriffsberechtigungen zuweisen können.

Motivation: Verhinderung der Manipulation von Genehmigungs-Workflows mit anschließender illegaler Zuweisung von (erhöhten) Zugriffsberechtigungen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-70/6.0

Req 71	Bei der Vergabe von kritischen Zugriffsberechtigungen muss das 4-Augen Prinzip für die Rolle des Genehmigenden verwendet werden.
--------	--

Gerade bei der Vergabe von kritischen Zugriffsberechtigungen muss das 4-Augen Prinzip für die Rolle des Genehmigenden in der Form umgesetzt werden, dass mindestens zwei verschiedene natürliche Identitäten die Vergabe kritischer Zugriffsberechtigungen genehmigen müssen. Dies soll es zusätzlich erschweren, sich Zugriffsberechtigungen auf für die Organisation kritische Infrastrukturen und Daten zu erschleichen.

Für die Deutsche Telekom AG sind Definitionen für kritische Zugriffsberechtigungen in der Konzernrichtlinie Sicherheit in Kapitel 3.3 „Technik & Produkte“ (Stichwort „Rollen und Zugriffsrechte“) sowie in Kapitel 3.6 „Geschäftskontinuität“ (Stichwort „Business Continuity Management“) zu finden.

Motivation: Vorbeugung der Erschleichung von (weitreichenden) Zugriffsberechtigungen zur Verhinderung von bspw. Daten Exfiltration und Manipulation sowie Identitätsmissbrauch.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.69-71/6.0

5.10. Self Service-Workflow

Req 72	Die Selbstregistrierung einer Identität bzw. eines Accounts darf nicht möglich sein.
--------	--

Angrifer dürfen nicht in der Lage sein, sich eigene Identitäten nebst Accounts in einem internen IAM Framework erstellen zu können (Selbstregistrierung). Ansonsten könnten diese Accounts für Angriffe auf die Zielapplikationen verwendet werden. Dieses Requirement beruht darüber hinaus auf Anforderungen seitens der internen Revision sowie externer Wirtschaftsprüfer einer Organisation.

GK IAM: Wird das IAM für Geschäftskunden durch die Organisation selbst betrieben, so dürfen Mitarbeiter nicht in der Lage sein, sich analog zu einem internen IAM Framework eigene Identitäten und Accounts erstellen zu können. Wird das GK IAM durch den Kunden betrieben, so gelten die Sicherheitsanforderungen des Kunden.

PK IAM: Die Selbstregistrierung von Identitäten und Accounts durch Privatkunden ist erlaubt.

Motivation: Reduzierung der Angriffsfläche und damit einhergehende Verringerung der Eintrittswahrscheinlichkeit von Sicherheitsvorfällen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-72/6.0

5.11. Provisionierung von Authentifizierungs- und Autorisierungsinstanzen

Req 73	Bei der Provisionierung von Authentifizierungs- und Autorisierungsinstanzen müssen standardisierte und etablierte Protokolle unter Nutzung einer aktuellen Verschlüsselungstechnologie verwendet werden.
--------	--

Selbst entwickelte Protokolle sind der Regel mit Fokus auf Funktionalität und nicht mit dem Fokus auf Sicherheit programmiert, so dass sie anfällig für Angriffe sind. Aus diesem Grund müssen bei der Provisionierung von Authentifizierungs- und Autorisierungsinstanzen standardisierte und etablierte Protokolle unter Nutzung einer aktuellen Verschlüsselungstechnologie verwendet werden. Ein Beispiel hierfür ist SCIM. Darüber hinaus verringert der Einsatz standardisierter Protokolle einen potenziellen Vendor-Lock-in und ermöglicht so einen einfacheren Wechsel zu einem anderen Anbieter eines IAM Frameworks, falls dies in Zukunft erforderlich ist.

Dieses Requirement ist eine Erweiterung des Req. 14 („Schutzbedürftige Daten müssen bei der Übertragung sowie Speicherung gegen unberechtigte Einsichtnahme und Veränderung geschützt werden.“) aus dem Dokument „3.01 Technischer Basisschutz“.

Motivation: Verringerung der Angriffsfläche und damit einhergehende Minimierung der Anzahl von Sicherheitsvorfällen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-73/6.0

Req 74	Das IAM Framework und die jeweilige Authentifizierungs- und Autorisierungs-Instanz müssen sich bei der Provisionierung gegenseitig authentifizieren.
--------	--

Auch und gerade bei der Kommunikation zwischen zwei IT-/NT-Systemen muss eine gegenseitige Authentifizierung der Kommunikationspartner sichergestellt sein, so dass bspw. ein Man-in-the-Middle Angriff nicht durchgeführt werden kann. Weiterhin wird so verhindert, dass ein Angreifer seine eigenen Accounts in die Authentifizierungs- und Autorisierungsinstanz einbringen kann. Aus diesen Gründen müssen sich das IAM Framework und die jeweilige Authentifizierungs- und Autorisierungs-Instanz bei der Provisionierung gegenseitig authentifizieren.

Motivation: Verhinderung von Man-In-the-Middle-Attacken und Einbringung von gefälschten Accounts in die Authentifizierungs- und Autorisierungs-Instanz.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-74/6.0

Req 75	Pro Authentifizierungs- und Autorisierungs-Instanz darf nur genau ein Provisionierungssystem verwendet werden.
--------	--

Sollten zwei oder mehr IAM Frameworks Objekte in der Authentifizierungs- und Autorisierungs-Instanz provisionieren bzw. schreibend verändern, so ist die Gefahr vorhanden, einen inkonsistenten Zustand herbeizuführen und/oder die Verfügbarkeit der Authentifizierungs- und Autorisierungs-Instanz zu reduzieren. Aus diesem Grund darf pro Authentifizierungs- und Autorisierungs-Instanz nur genau ein IT-System provisionierend verwendet werden.

Motivation: Erhöhung der Verfügbarkeit der Authentifizierungs- und Autorisierungs-Instanz und Verringerung von inkonsistenten Zuständen, die die Security bzw. die Produktion der Organisation beeinträchtigen können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

ID: 3.69-75/6.0

6. Anbindung Ziel-Applikationen

6.1. Anforderungen an Ziel-Applikationen

Req 76	Es muss die zentrale Authentifizierungs- und Autorisierungs-Instanz des IAM Framework inklusive des zentralen Rollenshops verwendet werden.
--------	---

Zur Sicherstellung einer starken Authentifizierung und Autorisierung sowie eines zentralen Security Monitorings muss die zentrale Authentifizierungs- und Autorisierungs-Instanz des IAM Frameworks verwendet werden.

Nachfolgend eine Liste von Protokollen, die von einer zentralen Authentifizierungs- und Autorisierungs-Instanz gemäß den IAM Security Requirements angeboten werden sollten:

- OAuth2
- OpenID Connect
- SAML
- Kerberos
- WebAuthN
- Diameter

Motivation: Hoher Schutz der verwendeten Accounts sowie bessere Detektion eines Missbrauchs der Accounts.

Durch die zentrale Verwaltung der Identität für Konten und deren Berechtigungen müssen diese nur einmalig und nicht für jedes System separat gepflegt werden. Aus Sicht der Sicherheit hat dies den Vorteil, dass ein Benutzerkonto und dessen Berechtigungen nur an einer zentralen Stelle bekannt ist. Diese Informationen können so von zentraler Stelle an die angebundenen Systeme weitergeleitet (Provisionierung), zentral verwaltet (Kontenabstimmung/Reconciliation) und zentral gelöscht (Deprovisionierung) werden. Hierdurch wird das Risiko gesenkt, dass Konten auf Grund der Existenz auf vielen Systemen bei Änderung oder Löschung auf Systemen vergessen werden und dadurch über falsche Berechtigungen verfügen oder weiterhin auf das System zugreifen können.

Umsetzungsbeispiel: Etablierung eines zentralen Accesslayers mit einem zentralen Rollenshop für Berechtigungen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-76/6.0

Req 77	Nach einem Logout bzw. nach Ablauf der Session-Lifetime muss die Session bzw. das Token invalidiert werden.
--------	---

Während der Laufzeit einer aktiven Session mit einer Web-Applikation wird unter anderem die Gültigkeit der Session in einem Token gespeichert. Dies geschieht beispielsweise durch Speicherung der Session Daten in einem Cookie oder einem JSON Web-Token (JWT). Nach Beendigung der Session eines Users durch einen aktiven Logout oder den Ablauf der Session muss das dazugehörige Token, in welchem die Daten der Session gespeichert sind, invalidiert werden.

Dieses Requirement ist eine Erweiterung der Req. 17 („Das System muss Benutzern ermöglichen sich von ihrer Sitzung abzumelden.“) und Req. 18 („Sitzungen müssen nach einer dem Verwendungszweck angepassten Zeit der Inaktivität beendet werden.“) aus dem Dokument „3.01 Technischer Basisschutz“.

Motivation: Angreifer könnten das Token übernehmen und ggfs. für eine Replay-Attacke missbrauchen, um beispiels-

weise Daten der Organisation auszuleiten oder den Account für weitere Angriffe zu missbrauchen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-77/6.0

Req 78	Ein Notfall-Account muss in der Zielapplikation lokal angelegt werden, um bei einem Ausfall der Authentifizierungs- und Autorisierungs-Instanz des IAM Frameworks auf die Zielapplikation zugreifen zu können.
--------	--

Zur Aufrechterhaltung des Geschäfts-Betriebs der Organisation muss es die Zielapplikation ermöglichen, sich im Notfall lokal, unter Umgehung der Authentifizierungs- und Autorisierungs-Instanz des IAM Frameworks, mit einem Notfall-Account anmelden zu können. Dieser Notfall-Account muss weitreichende Berechtigungen haben und muss bestmöglich vor unbefugtem Zugriff geschützt werden. Der Notfall-Account muss mindestens die Kennwortrichtlinie für Service Accounts erfüllen (siehe Dokumente „3.01 Technischer Basisschutz von IT-/NT-Systemen“, Requirement „Falls Passwörter als Authentisierungsmerkmal für technische Accounts genutzt werden, müssen diese mindestens 30 Zeichen lang sein und drei der folgenden Zeichenkategorien beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.“). Die Nutzung dieses Notfall-Accounts ist an die Vorgaben eines Business Continuity Management Plans gebunden.

Motivation: Dieser Notfall-Account soll es ermöglichen, auch im Krisenfall auf die Daten der Zielapplikation zuzugreifen und eventuelle weitere Schritte im Rahmen eines Business Continuity Managements durchführen zu können. Dadurch soll weiterer Schaden für die Organisation vermindert bzw. vermieden werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.69-78/6.0

Req 79	Wird eine Zielapplikation an einen Active Directory Forest mit mehreren Domains angebunden, so muss die Zielapplikation Multidomainfähigkeit unterstützen.
--------	--

Alle Zielapplikationen, die bereits jetzt oder zukünftig an einen Active Directory Forest mit mehreren Domains angebunden sind bzw. werden, müssen so gestaltet sein bzw. werden, dass sie Multi-Domain fähig sind. Multi-Domainfähigkeit bedeutet in diesem Zusammenhang, dass Accounts und deren Gruppen aus mehreren Domänen eines Active Directory Forests in einer Zielapplikation verwendet werden können.

Ist die Zielapplikation an einem zentralen Access Layer, der durch das IAM Framework bereitgestellt wird, angeschlossen, so ist es die Aufgabe des zentralen Access Layers, die Multi-Domain-Fähigkeit sicher zu stellen.

Zielapplikationen mit nachfolgend aufgelisteten rechtlichen und/oder vertraglichen Ausnahmen, die dadurch bedingt nur an eine einzelne Domäne angebunden werden dürfen, sind von diesem Requirement ausgenommen:

- German Eyes Only (GEO)
- VS-NfD (Geheimschutz)

Motivation: : Verhinderung der Anlage von sogenannten Dubletten-Accounts als Bypass zu rechtlichen und/oder vertraglichen Regularien

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-79/6.0

Req 80 Bei Nutzung einer zentralen Authentifizierungs- und Autorisierungs-Instanz muss sichergestellt werden, dass Benutzer-Accounts sich nicht nativ an einer Zielapplikation anmelden können.

Mit der Anbindung der Zielapplikation an ein IAM Framework werden in der Regel alle lokal vorhandenen Accounts – bis auf den Notfall-Account – aus der Zielapplikation entfernt. Sollte dies nicht erfolgt sein, so ist ein Angreifer unter Nutzung eines lokalen Accounts in der Lage, auf die Zielapplikation zuzugreifen und beispielsweise Daten zu exfiltrieren. Aus diesem Grund muss bei Nutzung einer zentralen Authentifizierungs- und Autorisierungs-Instanz sichergestellt werden, dass sich nur der Notfall-Account nativ an der Zielapplikation anmelden kann.

Motivation: Verringerung der Angriffsfläche

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.69-80/6.0

Req 81 Eine Zielapplikation muss für alle Accounts bevorzugt den Login via "passwortloser Authentifizierung" über zentral bereitgestellte Accesslayer anbieten.

Passwortlose Authentifizierung ist eine Authentifizierungsmethode, die es einem Benutzer ermöglicht, Zugang zu einer Anwendung oder einem IT-System zu erhalten, ohne ein Passwort einzugeben oder ein anderes wissensbasiertes Geheimnis einzugeben. Stattdessen liefert der Benutzer eine andere Form des Nachweises, z. B. einen Fingerabdruck. Die passwortlose Authentifizierung wird häufig in Verbindung mit der Multi-Faktor-Authentifizierung (MFA) und Single Sign-On-Lösungen eingesetzt, um die Benutzerfreundlichkeit zu verbessern, die Sicherheit zu erhöhen und die Kosten und Komplexität des IT-Betriebs zu reduzieren.

Folgende Voraussetzungen müssen umgesetzt werden, um eine sichere passwortlose Authentifizierung zu realisieren:

Es sind nur FIDO2-konforme Sicherheitsschlüssel, gerätegebundene Passkeys und zertifikatsbasierte Authentifizierung (CBA) zulässig. Ergänzt werden müssen diese Verfahren immer durch eine zusätzliche Multi-Faktor-Authentifizierung (MFA), wobei entweder eine PIN mit mindestens acht Ziffern oder biometrische Merkmale wie Fingerabdrücke oder Gesichtserkennung zulässig sind. Für die Erfassung der biometrischen Merkmale dürfen nur sichere, zertifizierte Komponenten verwendet werden, die in die Hardware integriert sind.

Die Nutzung muss auf zentral freigegebene Authenticators beschränkt werden, die anhand ihrer Authenticator Attestation GUID (AAGUID) identifiziert und freigegeben werden. Cloud-synchronisierbare Passkeys sowie Bluetooth-basierte CTAP-Verbindungen (BLE) sind generell ausgeschlossen. Gerätegebundene Passkeys dürfen nur in für Nutzung freigegebenen Hardwaresicherheitsmodulen (HSM) wie z.B. Trusted Plattform Modul, Secure Enclave, Trusted Execution Environment, etc. verwendet werden.

FIDO2-Schlüssel müssen mindestens eine Level-2-Zertifizierung der FIDO Alliance aufweisen. Darüber hinaus ist ein vollständiger Lifecycle-Prozess zu etablieren, der Registrierung, Konfiguration, Benutzerzuordnung, regelmäßige Überprüfung sowie Deaktivierung bei Verlust, Defekt oder Nutzerwechsel umfasst. Bei Versand von vorprovisionierten Geräten mit drahtloser Schnittstelle (z. B. NFC) ist diese vorübergehend zu deaktivieren.

Die Nutzung passwortloser Verfahren ist ausschließlich auf verwalteten Endgeräten oder verwalteten Authenticator-Apps (z.B. per MDM-Lösungen wie Microsoft Intune) und definierten Sicherheits- und Compliance-Richtlinien beschränkt. Die jeweils aktuelle Liste zugelassener Authenticators ist zu dokumentieren, regelmäßig zu aktualisieren und im Auditfall nachzuweisen.

Motivation: Einfache Authentifizierungsmethoden, die nur Kombinationen aus Benutzernamen und Kennwort erfordern, sind von Natur aus anfällig. Angreifer können Anmeldedaten erraten oder stehlen und sich mit verschiedenen Techniken Zugang zu sensiblen Informationen und IT-Systemen verschaffen, z. B.:

- *Brute-Force-Methoden* - Verwendung von Programmen zur Generierung zufälliger Kombinationen aus Benutzernamen und Kennwort oder Ausnutzung gängiger schwacher Kennwörter wie 123456
- *Credential Stuffing* - Verwendung gestohlener oder durchgesickelter Anmeldedaten eines Kontos, um Zugang zu anderen Konten zu erhalten (Personen verwenden oft dieselbe Benutzername/Kennwort-Kombination für viele Konten)
- *Phishing* - Verwendung von gefälschten E-Mails oder Textnachrichten, um ein Opfer dazu zu bringen, seine Anmeldedaten zu übermitteln
- *Keylogging* - Installation von Malware auf einem Computer, um Tastatureingaben von Benutzernamen und Kennwort zu erfassen
- *Man-in-the-Middle-Angriffe* - Abfangen von Kommunikationsströmen (z. B. über öffentliches WiFi) und Abspielen von Anmeldedaten

Selbst wenn ein Kennwort mit einer zusätzlichen aber möglicherweise phishbaren Multifaktor Authentifizierung geschützt ist, stellt das Kennwort für sich ein Sicherheitsrisiko dar.

Umsetzungsbeispiel: Als sichere Passwortlose Authentifizierungsmethoden werden aktuell folgende Multifaktor Authentifizierungen angesehen:

- Hardware-basierende Zertifikate (z. B. myCard, TPM-Chip mit Hello 4 Business)
- Hardware OTP Generator (z. B. RSA Key, FIDO2 Sicherheitsschlüssel)
- gemanagte OTP Software App mit Push Notifications oder Number Matching (z. B. Microsoft Authenticator)

Der telekom.de-Entra ID Tenant unterstützt die passwortlose Authentifizierung via [myCard](#). Die Möglichkeit der Nutzung von gerätegebundenen Passkeys via Microsoft Authenticator und FIDO2-Keys ist aktuell in Vorbereitung.

Eine englischsprachige Anleitung um sich als Anwendung am telekom.de-Entra ID Tenant anzubinden, findet sich im Wiki unter <https://wiki.telekom.de/spaces/IA/ME/pages/1563181642/How+to+onboard+to+AzureAD+CAIMAN>.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-81/6.0

Req 82	Eine Zielapplikation muss bei kritischen Funktionen, Ereignissen oder dem Zugriff auf sensible Informationen eine Step-up-Authentifizierung mittels Multi-Faktor-Authentifizierung erzwingen.
--------	---

Die Step-up-Multi-Faktor-Authentifizierung ist eine Sicherheitskonzeption, bei der eine zusätzliche Authentifizierungsebene eingeführt wird, um den Zugriff oder das Durchführen bestimmter Aktionen oder den Zugriff auf sensible Inhalten besonders abzusichern. Vereinfacht gesagt findet eine erneute Überprüfung der Identität durch eine Multi-Faktor-Authentifizierung statt, wenn verschiedene Bedingungen erfüllt sind.

Die Step-up-Multi-Faktor-Authentifizierung beginnt wie jede andere Authentifizierungsmethode mit einer standardmäßigen Anmeldung (z.B. Single Sign On). So können Benutzer Routineaufgaben ohne zusätzlichen Aufwand ausführen.

Sobald das System jedoch etwas Ungewöhnliches oder etwas Riskantes feststellt oder kritische bzw. privilegierte Funktionen aufgerufen werden oder sensible Informationen abgerufen werden, müssen zusätzliche Verifizierungsschritte mittels Multifaktor-Authentifizierung erzwungen werden.

Motivation: Die Step-up-Multi-Faktor-Authentifizierung ist eine effektive Methode, um den Zugriff auf kritische Funktionen, Ereignisse oder den Zugriff auf sensible Informationen zusätzlich abzusichern. Die Sicherheit wird durch eine zusätzliche Authentifizierungsebene erheblich erhöht.

Identitätsdiebe können Phishing-E-Mails versenden, um ahnungslosen Benutzern ihre Anmeldedaten & -Token zu stehlen oder sich als Autoritätspersonen ausgeben und Anmeldedaten oder Zugriff anfordern. Eine optimal eingesetzte Step-up-Multi-Faktor-Authentifizierung senkt das daraus resultierende Risiko auf ein akzeptables Niveau.

Umsetzungsbeispiel: Hier ist ein typischer Arbeitsablauf im Detail:

- Der Benutzer authentifiziert sich am System.
 - Das System überprüft, ob die Anmeldedaten korrekt sind.
 - Wenn sie gültig sind, erhält der Benutzer Zugriff auf das System in seinem rollenspezifischen Kontext.
 - Wenn das System während der Sitzung eine riskante Aktivität identifiziert, wie z. B. den Zugriff auf sensible Daten oder kritische Funktionen müssen folgende Schritte erzwungen werden:
1. Das System fordert den Benutzer auf, eine erneute Verifizierung mittels Multi-Faktor-Authentifizierung durchzuführen.
 - Für privilegierte Zugriffe/Aktionen ist zu beachten, dass nur Faktoren mit hoher Resilienz gegen Phishing verwendet werden dürfen (siehe Req. 21 der Sicherheitsanforderung 3.01 Technischer Basischutz in IT-/NT-Systemen).
 2. Der Benutzer gibt den zusätzlichen Nachweis an, der für die Benutzerauthentifizierung erforderlich ist
 3. Wenn der zusätzliche Nachweis korrekt ist, erhält der Benutzer Zugriff auf die Ressource oder kann die Aktion ausführen. Entspricht der Nachweis nicht den gesetzten Anforderungen, wird der Zugriff verweigert.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.69-82/6.0