

Sicherheitsanforderung

Machine Learning

Deutsche Telekom Gruppe

Version	4.0
Datum	01.07.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.81	Dokumententyp Sicherheitsanforderung
Version 4.0	Stand 01.07.2025	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.07.2025 - 30.06.2030	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung

Dieses Dokument beschreibt die Sicherheitsanforderungen an Machine Learning Algorithmen.

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
2.	KI-Komponenten	5
2.1.	Machine Learning Algorithmus	5
2.2.	Training des Machine Learning Algorithmus	8
2.3.	Betrieb des Machine Learning Algorithmus	10
2.4.	Zugriffe auf den Machine Learning Algorithmus	14
2.5.	Zugriffe des Machine Learning Algorithmus auf andere Systeme	27
3.	KI-Komponenten Nutzende Systeme	28
4.	Technischer Basisschutz von IT-/NT-Systemen	35
4.1.	Technisch-organisatorische Voraussetzungen für den Einsatz von Komponenten im System	35
4.2.	Grundlegende Systemhärtung	35
4.3.	Schutz der Verfügbarkeit und Integrität	39
4.4.	Schutz von Daten und Informationen	40
4.5.	Schutz von Sitzungen	41
4.6.	Authentifizierung und Autorisierung	42
4.7.	Protokollierung	43

1. Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus den im Konzern gültigen Sicherheitsrichtlinien erstellt. Es ist zu beachten, dass neben den Sicherheitsrichtlinien auch KI-Ethik Guidelines oder andere Maßgaben im Konzern existieren können, die ebenfalls beachtet werden müssen.

Die Sicherheitsanforderung dient u.a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung für Einheiten, die nicht am PSA-Verfahren teilnehmen. Diese Anforderungen müssen bereits während der Planungs- und Entscheidungsprozesse berücksichtigt werden. Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten.

Um eine einheitliche Verständnisgrundlage zu schaffen, werden im Folgenden einige zentrale Begriffe geklärt:

Begriff	Beschreibung
Künstliche Intelligenz (KI)	Oberbegriff für Methoden, die es Computern ermöglichen, menschenähnliche Intelligenz zu simulieren und Aufgaben zu erledigen, die normalerweise menschliches Denken erfordern.
KI-Komponente	Ein System, welches selbst KI implementiert. Z. B. ein Bilderkennungsalgorithmus, der über eine API angesprochen werden kann.
Machine Learning	Maschinelles Lernen ist ein Oberbegriff für die „künstliche“ Generierung von Wissen aus Erfahrung. Ein künstliches System lernt aus Beispielen und kann diese nach Beendigung der Lernphase verallgemeinern.
Machine Learning Algorithmus	Ein spezifischer Algorithmus, der im Rahmen des maschinellen Lernens verwendet wird, um z. B. Muster in Daten zu erkennen und Vorhersagen zu treffen.
Hyperparameter	Parameter, die den Lernprozess eines Machine Learning Algorithmus beeinflussen und vor dem Training festgelegt werden.
Dimensionalitätsreduktion	Ein Verfahren, bei dem die Anzahl der Merkmale oder Variablen in einem Datensatz reduziert wird, um die Komplexität zu verringern und die Effizienz von Machine Learning Algorithmen zu verbessern.

Wichtig zu beachten, ist ebenfalls, dass nicht jedes Produkt, jede einzelne Anforderung erfüllen muss. Dieses Dokument ist untergliedert in Anforderungen an KI-Komponenten und Anforderungen an Systeme, die KI-Komponenten verwenden.

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 abzustimmen.

2. KI-Komponenten

In diesem Dokument beschreibt eine KI-Komponente ein System, welches selbst KI implementiert. Z. B. ein Bilderkennungsalgorithmus, der über eine API angesprochen werden kann.

2.1. Machine Learning Algorithmus

Req 1	Die Aufgabe des Algorithmus, der Kontext, in dem dieser verwendet werden soll, und die Rahmenbedingungen, unter denen der Algorithmus Entscheidungen treffen darf, müssen klar definiert sein.
-------	--

Damit ein Algorithmus verlässlich eingesetzt werden kann, ist es von entscheidender Bedeutung, dass die Aufgabe, die er erfüllen soll, klar definiert ist, dass der Kontext, in dem er verwendet werden soll, vollständig verstanden wird und dass genau geregelt ist, unter welchen Rahmenbedingungen der Algorithmus Entscheidungen treffen darf. Nur so kann sichergestellt werden, dass der Algorithmus die gewünschten Ergebnisse liefert und nicht zu unerwarteten oder unerwünschten Ergebnissen führt.

Benötigte Informationen für die Definition der Aufgabe:

- Klare und eindeutige Beschreibung der spezifischen Aufgabe
- Beispiel Input- und Output Daten

Benötigte Informationen für die Definition des Kontextes:

- Art der Daten, welche verarbeitet werden sollen
- Quelle der Trainings- und Testdaten
- Liste involvierter Stakeholder

Motivation: Durch eine klare Definition der Aufgabe, des Kontextes und der Rahmenbedingungen, unter denen der Algorithmus Entscheidungen treffen darf wird nicht nur das Risiko für unerwartete Ergebnisse minimiert, sondern auch eine bessere Überprüfbarkeit des Algorithmus gewährleistet.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Transparenz

ID: 3.81-1/4.0

Req 2	Der Prozess der Datensammlung und/oder der Datengenerierung muss klar dokumentiert sein. Das beinhaltet Trainings-, Validierungs- und Testdaten.
-------	--

Es ist von großer Bedeutung, dass der Prozess der Datensammlung und/oder der Datengenerierung klar dokumentiert wird, um die Transparenz, die Nachvollziehbarkeit sowie den Schutz von personenbezogenen Daten zu gewährleisten. Dies beinhaltet nicht nur die Dokumentation der Trainings-, Validierungs- und Testdaten, sondern auch die Beschreibung der verwendeten Methoden und Werkzeuge sowie der Auswahlkriterien für die Daten. Eine klare Dokumentation ist unerlässlich, um die Qualität der Daten sicherzustellen und mögliche Fehlerquellen zu identifizieren.

Relevante Informationen:

- Zeitstempel der Erhebung/Generierung
- Beschreibung der Datenquellen/-typen
- Methoden und Werkzeuge zur Datensammlung und/oder Datengenerierung
- Auswahlkriterien für die Daten

- Prozesse zur Datenaufbereitung und -bereinigung
- Prozesse zur Anonymisierung oder Pseudonymisierung von personenbezogenen Daten
- Prozesse zur Validierung und Überprüfung der Datenqualität
- Prozesse zur Aufteilung der Daten in Trainings-, Validierungs- und Testdaten
- Prozesse zur Aktualisierung und Wartung der Daten

Motivation: Eine klare Dokumentation des Prozesses der Datensammlung und/oder der Datengenerierung ist von entscheidender Bedeutung für die Qualität und Vertrauenswürdigkeit von Daten, die für das Trainieren und Testen des Algorithmus verwendet werden. Eine unzureichende Dokumentation kann zu Fehlern und Ungenauigkeiten in den Daten führen, die wiederum zu falschen Entscheidungen und unzuverlässigen Ergebnissen führen können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität
- Transparenz

ID: 3.81-2/4.0

Req 3	Die KI-Komponente und angeschlossene Systeme müssen gegen missbräuchliche Nutzung der KI-Komponente geschützt sein.
-------	---

Es muss eine Härtung stattfinden, damit die KI-Komponente, durch quasi legitime Nutzung, nicht missbraucht werden kann.

Beispiele für solche Angriffe sind:

- Task Escape Attacks - Verwendung des Large Language Models (LLM) für (potentiell maliziose) out-of-scope Aufgaben
- Data Exfiltration Attacks - Ausgabe von internen Informationen, die dem LLM durch zum Beispiel eine Datenbank zur Verfügung gestellt werden

Motivation: Machine Learning Algorithmen haben oft mehr Fähigkeiten, als von den Entwickelnden benötigt werden. Diese können potentielle Schwachstellen sein, da sie verwendet werden, um die KI-Komponente zu missbrauchen.

Wird beispielsweise ein öffentlich zugängliches Large Language Model als KI-Komponente verwendet, muss sichergestellt werden, dass die Antworten des LLMs dem Kontext des Projektes entsprechen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Verfügbarkeit
- Vertraulichkeit
- Integrität

ID: 3.81-3/4.0

Req 4	Eingesetzte Basis-Algorithmen, die für Transfer-Learning verwendet werden, müssen aus vertrauenswürdigen Quellen bezogen werden und auf existierende KI-Komponenten Anforderungen (PSA Anforderungen in diesem Dokument) geprüft werden.
-------	--

Transfer-Learning bezeichnet alle Methoden, die es ermöglichen, das aus der Lösung eines bestimmten Problems gewonnene Wissen auf die Bearbeitung eines anderen Problems zu übertragen.

Um sicherzustellen, dass Transfer-Learning effektiv und sicher durchgeführt wird, ist es von entscheidender Bedeutung, dass die Basis-Algorithmen, die für diesen Prozess eingesetzt werden, aus vertrauenswürdigen Quellen stammen und den existierenden Anforderungen der KI-Komponenten (PSA Anforderungen in diesem Dokument) entsprechen. Es ist wichtig, dass diese Basis-Algorithmen regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie den neuesten Standards entsprechen und keine Sicherheitsrisiken darstellen. Darüber hinaus sollten bei der Auswahl von Basis-Algorithmen für Transfer-Learning auch Faktoren wie Leistung, Skalierbarkeit und Kompatibilität mit anderen Systemen berücksichtigt werden.

Motivation: Wenn die Basis-Algorithmen von unzuverlässigen oder unsicheren Quellen bezogen werden, kann dies zu Fehlern, Datenlecks und sogar zu Sicherheitsschwachstellen und neuen Angriffsszenarien führen. Außerdem können unzuverlässige Algorithmen die Performance der KI-Komponente beeinträchtigen und es schwieriger machen, die gewünschten Ergebnisse zu erzielen. Daher ist es wichtig, dass die Basis-Algorithmen aus vertrauenswürdigen Quellen stammen, um ein effektives und sicheres Transfer-Learning zu gewährleisten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität
- Transparenz

ID: 3.81-4/4.0

Req 5	Die Hyperparameter des Algorithmus müssen sorgfältig ausgewählt und dokumentiert werden, um eine Reproduzierbarkeit zu gewährleisten.
-------	---

Hyperparameter sind externe Konfigurationsvariablen, die für das Training von Machine Learning Algorithmen verwendet und vor dem Training eines Algorithmus manuell festgelegt werden. Beispiele für Hyperparameter sind die Anzahl der Knoten und Schichten in einem neuronalen Netz und die Anzahl der Zweige in einem Entscheidungsbaum. Hyperparameter bestimmen wichtige Merkmale wie die Modellarchitektur, die Lernrate und die Modellkomplexität.

Um sicherzustellen, dass die Ergebnisse eines Algorithmus reproduzierbar sind, ist es wichtig, die Hyperparameter sorgfältig auszuwählen und zu dokumentieren. Eine genaue Dokumentation der Hyperparameter ermöglicht auch eine weitere Verbesserung des Algorithmus durch Hyperparameteroptimierung. Sollte eine automatisierte Hyperparameteroptimierung verwendet werden, so muss auch dieser Prozess nachvollziehbar sein.

Motivation: Wenn die Hyperparameter eines Machine Learning Algorithmus nicht sorgfältig dokumentiert sind, kann dies zu Problemen bei der Reproduzierbarkeit und Optimierung des Algorithmus führen. Ohne eine genaue Dokumentation ist es schwer, die gleichen Ergebnisse zu erzielen, wenn der Algorithmus erneut ausgeführt wird, was die Zuverlässigkeit des Algorithmus beeinträchtigen kann. Darüber hinaus erschwert das Fehlen einer Dokumentation auch die Optimierung der Hyperparameter für bestmögliche Resultate.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Verfügbarkeit
- Integrität
- Transparenz

2.2. Training des Machine Learning Algorithmus

Req 6	Die gesammelten/generierten Daten müssen vor der Verwendung für Trainings-, Validierungs- und Testzwecke vorverarbeitet und bereinigt werden.
-------	---

Um die Genauigkeit und Zuverlässigkeit von Trainings-, Validierungs- und Testergebnissen zu gewährleisten, ist es notwendig, die gesammelten/generierten Daten vor der Verwendung sorgfältig zu überprüfen, zu bereinigen und zu normalisieren. Hierbei sollten fehlerhafte, unvollständige oder inkonsistente Daten entfernt oder korrigiert werden, um eine Verzerrung der Ergebnisse zu vermeiden. Zudem kann eine geeignete Vorverarbeitung der Daten, wie beispielsweise Feature-Extraktion oder Dimensionalitätsreduktion, die Effektivität von Machine Learning Algorithmen verbessern.

Mögliche Bereinigungen und Vorverarbeitungen:

- Entfernen von Duplikaten
- Entfernen von Ausreißern
- Füllen von fehlenden Werten
- Normalisierung kann verwendet werden, um die Skalierung der Daten zu vereinheitlichen und somit vergleichbar zu machen
- Feature Engineering, die Vorbereitung von Daten für die Verarbeitung in Machine Learning Algorithmen, kann verwendet werden, um die relevanten Merkmale aus den Rohdaten zu extrahieren und die Dimensionalität der Daten zu reduzieren
- Entfernen von irrelevanten Merkmalen
- Jede Klasse von Daten (z. B. Hund und Katze) muss gleich oft im Datensatz repräsentiert sein

Motivation: Es ist wichtig, Daten vor der Verwendung für Trainings-, Validierungs- und Testzwecke sorgfältig zu bereinigen und vorzubereiten, um genaue und zuverlässige Ergebnisse zu erzielen. Unbereinigte oder unvollständige Daten können zu Verzerrungen und Fehlern in den Ergebnissen führen und die Effektivität des Machine Learning Algorithmus beeinträchtigen. Durch die Durchführung von Bereinigungen und Vorverarbeitungen kann sichergestellt werden, dass die Daten korrekt und konsistent sind, was zu einer höheren Genauigkeit und Zuverlässigkeit der Ergebnisse führt.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität
- Transparenz

ID: 3.81-6/4.0

Req 7	Die Daten, die für Trainings-, Validierungs- und Testzwecke verwendet werden, müssen im Hinblick auf die zugewiesene Aufgabe repräsentativ sein. Darüber hinaus müssen die Daten frei von möglichen Verzerrungen und Inkonsistenzen (Bias) sein.
-------	--

Um sicherzustellen, dass der Machine Learning Algorithmus genaue und zuverlässige Ergebnisse liefert, müssen die Daten, die für Trainings-, Validierungs- und Testzwecke verwendet werden, repräsentativ für die zugewiesene Aufgabe sein. Dies bedeutet, dass die Daten eine ausreichende Vielfalt und Abdeckung aufweisen sollten, um die verschiedenen Aspekte der Aufgabe abzudecken. Darüber hinaus ist es verpflichtend, dass die Daten frei von möglichen Verzerrungen und Inkonsistenzen (Bias) sind, die zu ungenauen oder unfairen Ergebnissen führen können. Beispiele für mögliche Verzerrungen sind eine ungleiche Verteilung von Datenpunkten in bestimmten Kategorien oder eine ungleiche Repräsentation von bestimmten Gruppen in den Daten.

Motivation: Es ist besonders notwendig, dass die Daten, die für einen Machine Learning Algorithmus verwendet werden, frei von Verzerrungen und Inkonsistenzen (Bias) sind, um genaue und faire Ergebnisse zu erzielen. Wenn die Daten verzerrt sind, können die Ergebnisse ebenfalls verzerrt sein und zu ungenauen oder unfairen Entscheidungen führen.

Beispielsweise kann eine ungleiche Verteilung von Datenpunkten in bestimmten Kategorien dazu führen, dass der Algorithmus diese Kategorien nicht angemessen berücksichtigt oder dass er falsche Schlussfolgerungen zieht. Darüber hinaus kann eine ungleiche Repräsentation von bestimmten Gruppen in den Daten zu unfairen Entscheidungen führen, die auf Vorurteilen oder Diskriminierung beruhen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität
- Transparenz

ID: 3.81-7/4.0

Req 8	Tätigkeiten, wie das Trainieren des Machine Learning Algorithmus, müssen klar dokumentiert werden.
-------	--

Es ist notwendig, Tätigkeiten, wie das Trainieren des Machine Learning Algorithmus, genau zu dokumentieren, um bei Fehlern oder Sicherheitsverletzungen eine effektive Fehlerbehebung und Rückverfolgbarkeit zu gewährleisten. Dabei sind folgende Informationen zu erfassen:

- Name der Person, die das Training durchführt
- Zeitstempel des Trainings
- Verwendeter Datensatz
- Änderungen an Trainings-, Validierungs- und Testdaten
- Name der Person, die die Änderungen durchführt
- Zeitstempel der Änderungen

Motivation: Durch eine präzise Dokumentation können potenzielle Sicherheitsrisiken frühzeitig erkannt und behoben werden, bevor sie zu größeren Problemen führen. Zudem ermöglicht eine klare Identifikation der Ereignisse eine schnelle und effektive Reaktion auf Sicherheitsvorfälle.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Transparenz

ID: 3.81-8/4.0

Req 9	Schutzbedürftige Daten, wie Trainings-, Validierungs- und Testdaten, sowie Hyperparameter und Implementierung des Algorithmus müssen während der Speicherung und der Übertragung vor nicht autorisierter Einsichtnahme, Veränderung und Löschung geschützt sein.
-------	--

Um die Integrität und Vertraulichkeit von Daten, die für das Training, die Validierung und den Test von Algorithmen verwendet werden, sowie die Hyperparameter und die Implementierung des Algorithmus selbst, während der Speicherung und der Übertragung zu gewährleisten, ist es unerlässlich, geeignete Sicherheitsmaßnahmen zu ergreifen. Dazu gehören die Verwendung von Verschlüsselungstechniken, Zugriffskontrollen und regelmäßige Überprüfungen der Sicherheitsmaßnahmen. Es ist außerdem notwendig, sicherzustellen, dass alle Personen, die Zugriff auf diese Daten haben, über die Bedeutung der Datensicherheit informiert sind und sich an die entsprechenden Compliance Vor-

gaben halten.

Motivation: Unberechtigter Zugriff auf Trainings-, Validierungs- und Testdaten kann zu einer unbemerkten Manipulation dieser führen. Wird dann der Algorithmus mit dem manipulierten Datensatz trainiert, kann unvorhergesehenes Verhalten eintreten und die Integrität des Algorithmus ist nicht mehr gewährleistet.

Geschieht unberechtigter Zugriff auf die Hyperparameter oder auf die Implementierung des Algorithmus, können Änderungen vorgenommen werden, die schwerwiegende Folgen haben können. Außerdem bieten diese Informationen die Möglichkeit für das Klonen des Algorithmus.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Vertraulichkeit
- Integrität
- Transparenz

ID: 3.81-9/4.0

2.3. Betrieb des Machine Learning Algorithmus

Req 10	Die Ergebnisse des Algorithmus müssen kontinuierlich überprüft und validiert werden, um sicherzustellen, dass sie korrekt sind und den Erwartungen entsprechen. Falls die Ergebnisse des Algorithmus vom erwarteten Verhalten abweichen, so muss dies umgehend behoben werden.
--------	--

Es ist essenziell, dass die Ergebnisse des Algorithmus regelmäßig überprüft und validiert werden, um sicherzustellen, dass sie nicht nur korrekt sind, sondern auch den Erwartungen entsprechen. Eine ungenaue oder fehlerhafte Ausgabe kann schwerwiegende Konsequenzen haben. Daher ist es notwendig, dass der Algorithmus kontinuierlich überwacht wird, um mögliche Probleme frühzeitig zu erkennen und zu beheben. Das kann durch regelmäßige Funktions- und Penetrationstests erfolgen.

Außerdem ist es notwendig, dass der Algorithmus stets das erwartete Verhalten zeigt. Sollte es jedoch zu Abweichungen kommen, müssen diese umgehend identifiziert und behoben werden, um eine zuverlässige Funktionsweise des Algorithmus sicherzustellen. Dazu ist es erforderlich, dass der betroffene Machine Learning Algorithmus außer Betrieb genommen wird, solange das Fehlverhalten nicht behoben wurde.

Motivation: Durch kontinuierliche Überwachung des Verhaltens des Algorithmus können potentielle Probleme frühzeitig erkannt und darauf reagiert werden. Bleibt eine solche Überprüfung aus, werden Verhaltensänderungen nicht erkannt und können nicht behoben werden.

Umsetzungsbeispiel: Abhängig vom Einsatzgebiet, beispielsweise bei Bilderkennung, können stichprobenartige Überprüfungen ausreichend sein. Wird jedoch eine KI-Komponente verwendet, um produktive Systeme, wie Netzelemente, Server, Applikationen, etc. zu konfigurieren, sollte die von der KI-Komponente getroffene Entscheidung zuvor auf einem Testsystem überprüft werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität

ID: 3.81-10/4.0

Sicherheitsrelevant sind jegliche Ereignisse, die Auswirkungen auf die Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) eines Systems haben können oder dessen mißbräuchliche Verwendung anzeigen. Systeme müssen das Auftreten von sicherheitsrelevanten Ereignissen protokollieren.

Um eine Zuordnung und Auswertung dieser Ereignisse zu ermöglichen, müssen diese zusammen mit einer eindeutigen Systembezeichnung (z. B. Hostname, IP- oder MAC-Adresse) und dem genauen Zeitpunkt des Auftretens ("Zeitstempel") protokolliert werden. Der Zeitstempel eines protokollierten Ereignisses muss mindestens folgende Informationen beinhalten:

- Datum des Ereignisses (Jahr, Monat, Tag)
- Uhrzeit des Ereignisses (Stunden, Minuten, Sekunden)
- Zeitzone, auf die sich diese Zeitangaben beziehen

Die Sicherheitsrelevanz konkreter Ereignisse ergibt sich individuell aus Art und Funktion des Systems sowie den darin verarbeiteten Daten. Daher kann keine einheitliche Liste aus Ereignissen, die Sicherheitsrelevanz besitzen, vorgegeben werden. Relevante Ereignisse müssen passend zum System identifiziert werden. Die folgende Auflistung enthält typische sicherheitsrelevante Ereignisse und ist entsprechend als eine grundlegende Orientierungshilfe bei der Identifikation der sicherheitsrelevanten Ereignisse für ein bestimmtes System zu verstehen.

Sicherheitsrelevantes Ereignis	Informationen, die zum Ereignis zu protokollieren sind
Fehlerhafte Anmeldeversuche	• betroffenes Benutzerkonto, • Anzahl der Fehlversuche • Quelle des Zugriffs (IP-Adresse, Client-ID/Client-Name, lokale Konsole, ...)
Systemzugriffe über Benutzerkonten (einschliesslich System-Konten bzw. technischer Benutzerkonten)	• betroffenes Benutzerkonto • Startzeit/Endzeit des Zugriffs (Anmeldung/Abmeldung) • Quelle des Zugriffs (IP-Adresse, Client-ID/Client-Name, lokale Konsole, ...)
Änderungen an Benutzerkonten (einschliesslich System-Konten bzw. technischer Benutzerkonten)	• Benutzerkonto, mit dem die Änderung vorgenommen wurde • Benutzerkonto, an dem die Änderung vorgenommen wurde • Art der vorgenommenen Änderung (Neueinrichtung, Aktivierung, Deaktivierung, Löschung, Passwort-Rücksetzung, ...)
Änderungen der Rollenzuweisungen/Berechtigungen von Benutzerkonten (einschliesslich System-Konten bzw. technischer Benutzerkonten)	• Benutzerkonto, mit dem die Änderung vorgenommen wurde • Benutzerkonto, an dem die Änderung vorgenommen wurde • Bezeichnung der betroffenen Rolle / Typ der betroffenen Berechtigung • Art der vorgenommenen Änderung (Rolle/Berechtigung hinzugefügt, Rolle/Berechtigung entfernt, ...)

Nutzung/Initiierung von kritischen Systemfunktionen	• Benutzerkonto, mit dem die Nutzung vorgenommen wurde • Bezeichnung/Typ der genutzten Systemfunktion
Zugriff auf sensible Daten ("Sensitive Data"), die im System verarbeitet werden	• Benutzerkonto, mit dem der Zugriff vorgenommen wurde • Bezeichnung des betroffenen Datenfelds (der Inhalt des Datenfelds sollte dabei nicht mit protokolliert werden, um einen Datenabfluss über Log-Dateien zu verhindern) • Art des Zugriffs (Lesen, Ändern, Löschen, ...)
Abnormaler Anstieg in der Auslastung von Systemressourcen, wie etwa Arbeitsspeicher, CPU, Netzwerk oder Festplattenzugriffen über einen längeren Zeitraum	• Schwellwert der betroffenen Systemressource • Dauer der Überschreitung des Schwellwerts • Höhe der Überschreitung des Schwellwerts Es müssen abhängig vom individuellen System sinnvolle Schwellwerte definiert werden.
Sonstige Ereignisse, die für versuchte oder erfolgreiche Angriffe gegen das System Hinweise liefern können *)	• individuell abhängig von der Art des Ereignisses

*) Dies erfordert eine Identifizierung der wichtigsten, für das System typischerweise zu erwartenden Angriffsformen und die Sicherstellung, dass zu deren Erkennung relevante Ereignisse durch das System tatsächlich protokolliert werden. In der Regel kann das nur durch den Entwickler/Hersteller des Systems gewährleistet werden.

Bei der Protokollierung müssen die jeweils geltenden gesetzlichen und betrieblichen Bestimmungen beachtet werden. Letztere umfassen insbesondere auch Vereinbarungen, die mit den betrieblichen Sozialpartnern getroffen wurden. Diese Bestimmungen besagen unter anderem, dass die Protokollierung von Ereignissen nur zweckgebunden erfolgen darf. Die Protokollierung von Ereignissen zum Zweck der Arbeitskontrolle von Mitarbeitern ist nicht zulässig.

Zudem muss - wie für jegliche Daten, die von einem System verarbeitet werden - auch für Protokollierungsdaten ein angemessener Schutzbedarf berücksichtigt und umgesetzt werden; dies gilt für die Speicherung, die Übertragung sowie den Zugriff. Insbesondere falls Wirkdaten in den Protokollierungsdaten enthalten sind, muss derselbe Schutzbedarf berücksichtigt werden, der auch für die reguläre Verarbeitung dieser Wirkdaten innerhalb des Quell-Systems Anwendung findet.

Motivation: Die Protokollierung von sicherheitsrelevanten Ereignissen ist eine Grundvoraussetzung, um laufende Angriffe oder auch Angriffe im Nachhinein erkennen zu können. Nur so ist es möglich, sinnvolle Maßnahmen zur Erhaltung oder auch Wiederherstellung der Systemsicherheit durchzuführen. Des Weiteren dienen die Protokollierungsdaten der Beweissicherung, um rechtlich gegen Angreifer vorgehen zu können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-33/9.0

Req 12 Für sicherheitsrelevante Protokollierungsdaten, die lokal erfasst werden, müssen geltende Aufbewahrungszeiträume und Löschfristen eingehalten werden.

Aus Sicht der IT-Sicherheit wird auf einem System die lokale Erfassung von sicherheitsrelevanten Protokollierungsdaten nicht zwingend gefordert. Da lokal erfasste Protokollierungsdaten bei Systemstörungen beschädigt oder von einem erfolgreichen Angreifer gezielt manipuliert werden können, sind sie für sicherheitstechnische bzw. forensische Analysen nur bedingt belastbar. Entsprechend ist für die IT-Sicherheit relevant, dass Protokollierungsdaten an einen separaten Log Server weitergeleitet werden.

Eine lokale Erfassung kann dennoch erfolgen; beispielsweise falls bei der Erzeugung der Protokollierungsdaten eine

lokale Speicherung aufgrund technischer Abläufe zunächst unabdingbar ist oder es begründete betriebliche Interessen gibt, Protokollierungsdaten auch lokal vorzuhalten.

Folgende Grundregelung ist bei einer lokalen Erfassung von Protokollierungsdaten zu berücksichtigen:

- Sicherheitsrelevante Protokollierungsdaten müssen für einen Zeitraum von 90 Tagen aufbewahrt werden.
(Diese Anforderung gilt nur, falls auf dem System keine zusätzliche Weiterleitung an einen separaten Log Server umgesetzt ist und Protokollierungsdaten daher ausschließlich lokal erfasst werden.)
- Nach Ablauf von 90 Tagen muss eine umgehende Löschung von gespeicherten Protokollierungsdaten erfolgen.

Abweichungen

Abweichende Aufbewahrungszeiträume und Löschfristen können durch gesetzliche oder regulatorische Anforderungen (insbesondere im Zusammenhang mit personenbezogenen Daten) bestehen oder durch vertragliche Vereinbarungen definiert sein. In diesen Fällen sind die geltenden Zeiträume individuell mit einem Project Security Manager (PSM) bzw. Datenschutzberater (DSB) abzustimmen oder werden durch diesen vorgegeben.

Motivation: Protokollierungsdaten sind ein immens wichtiges Werkzeug der IT-Sicherheit zur Abwendung, Detektierung und Aufklärung von Systemstörungen, Sicherheits- und Datenschutzvorfällen. Auf der anderen Seite unterliegt die Erfassung von Protokollierungsdaten wie jede andere Datenverarbeitung auch gesetzlichen und regulatorischen Auflagen. Entsprechend müssen Richtlinien eingehalten werden, die beides in Einklang bringen.

Umsetzungsbeispiel: Unter Berücksichtigung der gültigen Gesetzeslage und zutreffenden Datenschutz-Regularien werden folgende Löschfristen für lokal erfasste sicherheitsrelevante Protokollierungsdaten auf einem beispielhaften TK-System umgesetzt:

- Standard System Logs: Löschung nach spätestens 90 Tagen
- Protokollierungen von öffentlichen IP-Adressen: Löschung (oder Anonymisierung) nach spätestens 7 Tagen
- Protokollierungen der Vergabe von dynamischen öffentlichen IP-Adressen durch die TK-Lösung: Löschung nach spätestens 7 Tagen
- Protokollierungen nicht abrechnungsrelevanter Call Detail Records: Löschung nach spätestens 7 Tagen
- Protokollierungen der Kommunikations-Inhalte von E-Mail und SMS: Löschung nach spätestens 24 Stunden
- Protokollierungen der behandelten Domain-Abfragen des DNS-Servers der TK-Lösung: Löschung nach spätestens 24 Stunden

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-34/9.0

Req 13	Sicherheitsrelevante Protokollierungsdaten müssen umgehend nach deren Erzeugung an einen separaten Log-Server weitergeleitet werden.
--------	--

Protokollierungsdaten müssen umgehend nach deren Erzeugung an einen separaten Log-Server weitergeleitet werden. Standardisierte Protokolle wie Syslog, HTTPS sollten hierbei bevorzugt zum Einsatz kommen.

Motivation: Werden Protokollierungsdaten nur lokal gespeichert, können diese im Falle einer erfolgreichen Kompromittierung des Systems durch einen Angreifer manipuliert werden, um seinen Angriff und durchgeführte Manipulationen des Systems zu verschleiern. Aus diesem Grund muss die Weiterleitung zeitnah nach dem Auftreten des Ereignisses erfolgen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität

ID: 3.81-13/4.0

Req 14	Für sicherheitsrelevante Protokollierungsdaten, die an den Log Server weitergeleitet werden, muss die Einhaltung geltender Aufbewahrungszeiträume und Löschfristen sichergestellt werden.
--------	---

Folgende Grundregelung ist zu berücksichtigen:

- sicherheitsrelevante Protokollierungsdaten müssen auf dem Log Server für einen Zeitraum von 90 Tagen aufbewahrt werden.
- nach Ablauf von 90 Tagen muss eine umgehende Löschung der auf dem Log Server gespeicherten Protokollierungsdaten erfolgen.

Abweichungen

Abweichende Aufbewahrungszeiträume und Löschfristen können durch gesetzliche oder regulatorische Anforderungen bestehen (insbesondere im Zusammenhang mit personenbezogenen Daten) oder durch vertragliche Vereinbarungen definiert sein. In diesen Fällen sind die geltenden Zeiträume individuell mit einem Project Security Manager (PSM) bzw. Datenschutzberater (DSB) abzustimmen oder werden durch diesen vorgegeben.

Log Server in Verantwortung eines Dritten

Sollte der ausgewählte Log Server nicht innerhalb derselben operativen Verantwortung liegen wie das Quellsystem der Protokollierungsdaten, muss sichergestellt werden, dass dem verantwortlichen Betreiber des Log Servers die gültigen Parameter für die zu empfangenden Protokollierungsdaten bekannt sind und durch diesen im Sinne der hier genannten Regelungen eingehalten werden.

Motivation: Protokollierungsdaten sind ein immens wichtiges Werkzeug der IT-Sicherheit zur Abwendung, Detektierung und Aufklärung von Systemstörungen, Sicherheits- und Datenschutzvorfällen. Auf der anderen Seite unterliegt die Erfassung von Protokollierungsdaten wie jede andere Datenverarbeitung auch gesetzlichen und regulatorischen Auflagen. Entsprechend müssen Richtlinien eingehalten werden, die beides in Einklang bringen.

Umsetzungsbeispiel: Unter Berücksichtigung der gültigen Gesetzeslage und zutreffenden Datenschutz-Regularien werden folgende Löschfristen für ausgeleitete sicherheitsrelevante Protokollierungsdaten eines beispielhaften TK-Systems auf dem separaten Log Server umgesetzt:

- Standard System Logs: Löschung nach spätestens 90 Tagen
- Protokollierungen von öffentlichen IP-Adressen: Löschung (oder Anonymisierung) nach spätestens 7 Tagen
- Protokollierungen der Vergabe von dynamischen öffentlichen IP-Adressen durch die TK-Lösung: Löschung nach spätestens 7 Tagen
- Protokollierungen nicht abrechnungsrelevanter Call Detail Records: Löschung nach spätestens 7 Tagen
- Protokollierungen der Kommunikations-Inhalte von E-Mail und SMS: Löschung nach spätestens 24 Stunden
- Protokollierungen der behandelten Domain-Abfragen des DNS-Servers der TK-Lösung: Löschung spätestens nach 24 Stunden

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-36/9.0

2.4. Zugriffe auf den Machine Learning Algorithmus

Req 15	Der Zugriff für die Verwendung der KI-Komponente darf nicht ohne erfolgreiche Authentifizierung und Autorisierung möglich sein. Das gilt sowohl für API Schnittstellen, als auch für alle weiteren Möglichkeiten, mit dem Machine Learning Algorithmus zu interagieren.
--------	---

Es ist erforderlich, dass eine erfolgreiche Authentifizierung und Autorisierung vorliegt, bevor auf den Machine Learning Algorithmus zugegriffen bzw. dieser genutzt werden kann. Dies gilt für alle Arten von Interaktionen mit dem Algorithmus, einschließlich API-Schnittstellen und anderen Zugriffsmöglichkeiten.

Diese Anforderung gilt für alle Systeme, die in der Verantwortung der Deutschen Telekom liegen. D.h. sollte es sich um einen externen Dienst (Bing Search, Chat-GPT, ...) handeln, so greift dieses Requirement nicht.

Motivation: Bei fehlender Authentifizierung und Autorisierung besteht das Risiko der unbefugten Verwendung des Algorithmus und muss daher unterbunden werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Vertraulichkeit

ID: 3.81-15/4.0

Req 16	In Ausgaben und Meldungen dürfen keine Informationen über interne Strukturen des Systems preisgegeben werden.
--------	---

Informationen über die internen Strukturen eines Systems einschließlich der dort verwendeten Komponenten und entsprechende Implementationsdetails gelten grundsätzlich als schutzbedürftig.

Im Allgemeinen betrifft dies Informationen über

- Produktnamen und Produkt-Identifizier implementierter System-Komponenten
- eingesetzte Betriebssysteme, Middleware, Backend-Software, Software-Bibliotheken und interne Applikationen sowie deren Software-Versionen
- installierte Service-Packs, Patches, Hotfixes
- Seriennummern von Komponenten sowie hinterlegte Produkt-Lizenzen
- Datenbankstrukturen

Typische Beispiele für Ausgaben und Meldungen, in denen eine Preisgabe solcher System-Informationen potenziell auftreten kann:

- Anmelde-Fenster und -dialoge
- Fehlermeldungen
- Statusausgaben
- Banner von aktiven Netzwerk-Diensten
- System-Protokolle und Log Dateien
- Debug-Protokolle, Stack Traces

Soweit es technisch umsetzbar ist, ohne die Funktion und den Betrieb des Systems zu beeinträchtigen, muss die Ausgabe betroffener System-Informationen grundsätzlich deaktiviert sein.

Ein Zugriff auf betroffene System-Informationen darf nur dazu autorisierten Benutzern des Systems möglich sein. In der Regel ist der Kreis autorisierter Benutzer auf Administratoren und Betreiber des Systems zu beschränken. Ebenfalls zulässig ist ein Zugriff für autorisierte Monitoring- und Inventarisierungs-Systeme innerhalb der Einsatzumgebung.

Eine zulässige Ausnahme dieser Einschränkungen besteht für spezifische einzelne System-Informationen, deren Preisgabe für die vorgesehene Funktion des Systems in Verbindung mit dritten Systemen technisch zwingend erforderlich ist; beispielsweise die Präsentation unterstützter Protokolle und deren Versionen während der initialen Parameter-Aushandlung in Sitzungs-Aufbauten zwischen einem Client und einem Server.

Motivation: Informationen über die internen Strukturen eines Systems können von einem Angreifer genutzt werden, um Angriffe auf das System äußerst effektiv vorzubereiten. Beispielsweise kann ein Angreifer aus der Software-Version eventuell bekannte Schwachstellen eines Produktes ableiten, um diese gezielt während des Angriffs auf das System auszunutzen.

Umsetzungsbeispiel: [Beispiel 1]

Deaktivierung der Anzeige des Produktnamens und der installierten Version in den ausgelieferten Fehler-Webseiten eines eingesetzten Web-Servers.

[Beispiel 2]

Entfernung des Produktnamens und des zugehörigen Versions-Strings aus dem Login-Banner eines eingesetzten SSH Servers.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-9/9.0

Req 17	Benutzerkonten müssen mit mindestens zwei Authentisierungsmerkmalen aus unterschiedlichen Faktoren geschützt werden.
--------	--

Sämtliche Benutzerkonten des Systems müssen vor einer unberechtigten Nutzung geschützt werden. Dies ist durch Verwendung von Authentisierungsmerkmalen umzusetzen, die eine eindeutige Identifizierung des legitimen Benutzers ermöglichen.

Authentisierungsmerkmale werden in übergeordneten Gruppen, sogenannten "Faktoren", differenziert:

- Faktor WISSEN: "etwas, das nur der legitime Benutzer weiss"
- Faktor BESITZ: "etwas, das nur der legitime Benutzer besitzt"
- Faktor INHÄRENZ: "etwas, das nur der legitime Benutzer ist"

Es müssen mindestens zwei Authentisierungsmerkmale miteinander kombiniert werden.

Diese müssen aus unterschiedlichen Faktoren stammen ("Multi-Faktor-Authentisierung"; kurz: "MFA").

Eine Kombination von Authentisierungsmerkmalen desselben Faktors (Beispiel: zwei unterschiedliche PINs) ist nicht zulässig.

Beispiele für zulässige Authentisierungsmerkmale

- aus dem Faktor WISSEN: PINs, Passphrases (Passwörter*)
- aus dem Faktor BESITZ: Smartcards, FIDO2 Level 2 Security Keys, Device-bound Passkeys, in einem TPM/ HSM gespeicherte kryptografische Schlüssel, OTPs (One-Time Passwords) generiert in einer zum Einsatz in der Deutschen Telekom freigegebenen Authenticator App
- aus dem Faktor INHÄRENZ: biometrische Merkmale wie Fingerabdruck, Iris- bzw. Retina-Scans, Gesichtserkennung

*) Wichtiger Hinweis zum Einsatz von Passwörtern

Passwörter müssen als Authentisierungsmerkmal strikt vermieden werden.
Sie sind nur dann zulässig, falls sicherere Alternativen nicht umgesetzt werden können.

Grundsätzlich nicht zulässig sind Authentisierungsmerkmale, die leicht gefälscht oder manipuliert werden können.
Dazu gehören:

- Rufnummern und Anrufer-IDs
- IP-Adressen
- geografische Standorte
- VPN-Zugehörigkeiten und Netzwerkinformationen
- Status von Clients, etwa von Arbeitsplatzsystemen oder mobilen Endgeräten

Hinweis zu technischen Benutzerkonten

Für den maschinellen Zugriff eingesetzte technische Benutzerkonten (auch unter dem Begriff "Machine-to-Machine" bzw. "M2M"-Konten bekannt) sind von der Verpflichtung zur Multi-Faktor-Authentisierung ausgenommen, da eine solche dort i.d.R. nicht umsetzbar ist.

Motivation: Benutzerkonten, die nicht über angemessene Authentisierungsmerkmale geschützt sind, können von einem Angreifer missbraucht werden, um unberechtigt auf ein System und die darauf gespeicherten Daten und Anwendungen zuzugreifen. Aufgrund vielfältiger gängiger Angriffsmethoden ist der Schutz von Benutzerkonten durch ein einzelnes Authentisierungsmerkmal mittlerweile als schwach zu bewerten, insbesondere, falls hier das klassische Passwort zum Einsatz kommt. Eine Kombination von Authentisierungsmerkmalen aus unterschiedlichen Faktoren erhöht die Sicherheit für Benutzerkonten signifikant.

Umsetzungsbeispiel: Beispiele für MFA

MFA Kombination	Beschreibung	Anmerkung zur Anwendung
Telekom "myCard" plus PIN-Eingabe	1. Faktor: in Hardware implementiertes Zertifikat ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)
FIDO2 Level 2 Security Key plus Fingerabdruck	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: Biometrisches Merkmal ("Inhärenz")	Die Biometrie-Funktion muss vorab konfiguriert werden, da der Biometrie-Sensor sonst nur als "Taste" funktioniert und somit der 2. Faktor ("Inhärenz") nicht gegeben wäre.
Device-bound Passkey in WH4B* auf Nucleus PC plus PIN	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)
Device-bound Passkey in Secure Enclave auf iOS Device plus FaceID	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: Biometrisches Merkmal ("Inhärenz")	(keine)

Passwort plus freigegebene OTP App (z. B. MS Authenticator)	1. Faktor: Passwort ("Wissen") 2. Faktor: spezifisch generiertes One Time Password ("Besitz")	Passwörter sind nur dann zulässig, falls sicherere Alternativen nicht umgesetzt werden können. Die Synchronisation der Authenticator App über einen Clouddienst sowie das Teilen (z. B. über einen Passwortmanager) des OTP ist nicht zulässig.
--	--	--

*) WH4B: "Windows Hello for Business"

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: 3.01-20/9.0

Req 18	Privilegierte Benutzerkonten müssen mit mindestens zwei Authentisierungsmerkmalen geschützt werden, die aus unterschiedlichen Faktoren stammen und erhöhte Resilienz gegen Phishing-Angriffe bieten.
--------	--

Ein privilegiertes Benutzerkonto ist ein Benutzerkonto, welches über erweiterte Berechtigungen innerhalb eines Systems verfügt. Erweiterte Berechtigungen ermöglichen einen Zugriff auf Konfigurationseinstellungen, Funktionen oder Datenbestände, der regulären Benutzern des Systems nicht zu Verfügung steht. In direkter Abhängigkeit zu den besonderen Aufgaben, die mittels eines privilegierten Benutzerkontos innerhalb eines Systems wahrgenommen werden, können die zugewiesenen erweiterten Berechtigungen spezifisch limitiert sein oder einen vollständig uneingeschränkten Systemzugriff umfassen.

Beispiele für privilegierte Benutzerkonten:

- Konten für Administrations-, Wartungs- oder Entstörungsaufgaben
- Konten für Benutzer-Verwaltungsaufgaben (z. B. Anlegen/Löschen von Benutzern; Zuweisen von Berechtigungen; Passwort-Rücksetzungen)
- Konten, die zur Freigabe, Auslösung oder Unterbindung von geschäftskritischen Vorgängen berechtigt sind
- Konten mit Zugriff auf Daten, die im Interesse des DTAG-Konzerns, dessen Kunden oder der Öffentlichkeit als SCD (Sensitive Customer Data) eingestuft sind
- Konten, die in hohem Umfang auf lt. EU-DSGVO als „personenbezogen“ definierte Daten zugreifen können (z. B. Massenabruf von größeren Teilen oder des vollständigen Datenbestands)

Zum Schutz privilegierter Konten müssen mindestens zwei Authentisierungsmerkmale miteinander kombiniert werden.

Diese müssen aus unterschiedlichen Faktoren ("WISSEN", "BESITZ" oder "INHÄRENZ") stammen.

Eine Kombination von Authentisierungsmerkmalen desselben Faktors ist nicht zulässig.

Mindestens eines der Authentisierungsmerkmale darf nicht anfällig gegenüber Phishing-Angriffen sein.

Bei einem Phishing-Angriff wird der legitime Nutzer trickreich manipuliert, um seine Anmeldedaten dem Angreifer offenzulegen, beispielsweise mittels gefälschter Anmelde-Seiten. Ein Phishing-Angriff kann auch gegen eine Kombination aus mehreren Authentisierungsmerkmalen erfolgen.

Phishing-resiliente Authentisierungsmerkmale verhindern Angriffe anhand ihrer technischen Umsetzung. Diese Authentisierungsmerkmale nutzen kryptographische Verfahren und stellen eine starke Bindung zwischen dem Nutzer, dem Gerät und dem Dienst her. Sie erfordern während der Authentisierung zusätzlich eine manuelle Nutzerinteraktion.

on, die nicht automatisiert werden kann; beispielsweise, einen Fingerabdruck-Scan an einem Hardware Token abzugeben.

Als nicht anfällig gegenüber Phishing-Angriffen gelten

- FIDO2 Level 2 Security Keys
- in Hardware implementierte Zertifikate

Wichtiger Hinweis zum Einsatz von Passwörtern

Passwörter müssen als Authentisierungsmerkmal strikt vermieden werden.

Sie sind nur dann zulässig, falls sicherere Alternativen nicht umgesetzt werden können.

Hinweis zu technischen Benutzerkonten

Für den maschinellen Zugriff eingesetzte technische Benutzerkonten (auch unter dem Begriff "Machine-to-Machine" bzw. "M2M"-Konten bekannt) sind von der Verpflichtung zur Multi-Faktor-Authentisierung ausgenommen, da eine solche dort i.d.R. nicht umsetzbar ist.

Motivation: Privilegierte Benutzerkonten stellen ein erhöhtes Risiko für die Sicherheit eines Systems dar. Kompromittiert ein Angreifer erfolgreich ein solches Benutzerkonto, erhält er weitreichende Berechtigungen, mit denen er das System oder Systemanteile unter seine Kontrolle bringen, die Systemfunktionen stören, verarbeitete Daten einsehen/manipulieren oder geschäftskritische Vorgänge beeinflussen kann. Die Kombination von mehreren Authentisierungsmerkmalen unterschiedlicher Art minimiert das Risiko der Kompromittierung eines Benutzerkontos bereits signifikant, jedoch muss für privilegierte Benutzerkonten in besonderem Maße auf Resilienz gegen Phishing-Angriffe geachtet werden. Die zu beobachtenden Phishing-Angriffe werden zunehmend trickreicher und für Nutzer schwerer zu erkennen, so dass eine Multifaktor-Authentifizierung ohne erhöhte Resilienz gegen Phishing nicht mehr als ausreichend für privilegierte Benutzerkonten zu bewerten ist.

Umsetzungsbeispiel: Beispiele für MFA mit erhöhter Resilienz gegen Phishing-Angriffe

MFA Kombination	Beschreibung	Anmerkung zur Anwendung
Telekom "myCard" plus PIN-Eingabe	1. Faktor: in Hardware implementiertes Zertifikat ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)
FIDO2 Level 2 Security Key plus Fingerabdruck	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: Biometrisches Merkmal ("Inhärenz")	Die Biometrie-Funktion muss vorab konfiguriert werden, da der Biometrie-Sensor sonst nur als "Taste" funktioniert und somit der 2. Faktor ("Inhärenz") nicht gegeben wäre.
FIDO2 Level 2 Security Key plus PIN-Eingabe	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)

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: 3.01-21/9.0

Req 19	Es muss gewährleistet werden, dass maschinelle Nutzer keine hart kodierten Geheimnisse wie Passwörter oder Token verwenden, um sich gegenüber dem KI-Algorithmus zu authentifizieren oder autorisieren.
--------	---

Um die Sicherheit und Integrität des Systems zu gewährleisten, ist es wichtig sicherzustellen, dass maschinelle Nutzer keine fest codierten Geheimnisse wie Passwörter oder Token verwenden, um sich gegenüber dem KI-Algorithmus zu authentifizieren oder zu autorisieren. Stattdessen sollten alternative Methoden der Authentifizierung und Autorisierung implementiert werden, um potenzielle Offenlegungen zu vermeiden.

Motivation: Geheimnisse wie Passwörter, Zertifikate und geheime Schlüssel stellen ein hohes Risiko dar, wenn sie an Unbefugte weitergegeben werden. Insbesondere in Code oder Bildern, die in Repositories gespeichert sind, kann es zu einer ungewollten Offenlegung kommen.

Umsetzungsbeispiel: Zur Umsetzung können z. B. folgende Secret Management Systeme verwendet werden:

- HashiCorp. Vault
- CyberArk Conjur
- AWS KMS
- Azure Key Vault
- Google Cloud KMS
- GitLab Protected Variables

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität
- Transparenz

ID: 3.81-19/4.0

Req 20	Benutzerkonten müssen die eindeutige Identifizierung des Benutzers sicherstellen.
--------	---

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, die sich dadurch auszeichnen, dass sie von mehreren Personen gemeinsam genutzt werden, dürfen nicht verwendet werden. Dies gilt uneingeschränkt auch für privilegierte Benutzerkonten. Die meisten Systeme verfügen nach der Grundinstallation zunächst nur über ein einzelnes Benutzerkonto mit administrativen Berechtigungen. Soll das System von mehreren Personen administriert werden, muss jede dieser Personen ein persönliches, individuelles Benutzerkonto verwenden, dem entsprechende administrative Berechtigungen bzw. Rollen zugewiesen sind.

Eine Besonderheit stellen sogenannte technische Benutzerkonten dar. Diese werden für Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt und können damit nicht einer konkreten 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 entsprechenden Passwortes, dass nur einem kleinstmöglichen Kreis von Administratoren bekannt ist.

- Konfiguration des entsprechenden Benutzerkontos, so dass dieses 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.

Weitere Lösungen sind im Einzelfall auf ihre Verwendbarkeit zu prüfen.

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

ID: 3.01-22/9.0

Req 21	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss deren Speicherung unter Einsatz eines für diesen Zweck als ausreichend sicher anerkannten "Password Hashing"-Verfahrens erfolgen, um Offline-Angriffe wie Wörterbuch- und Brute-Force-Attacken stark zu erschweren.
--------	---

Diese Anforderung bezieht sich auf die Speicherung von Passwörtern in sämtlichen Arten von Benutzerdatenbanken, die im vorliegenden System eingesetzt werden, um darüber eingehende Zugriffe (lokal oder aus der Ferne) von Benutzern oder anderen Systemen zu authentisieren.

Gelingt es einem Angreifer, die Kopie einer Benutzerdatenbank des Systems in seinen Besitz zu bringen, kann er diese in einer unabhängigen Umgebung einem automatisierten Wörterbuch- oder Brute-Force-Angriff aussetzen, um enthaltene Passwörter zu ermitteln. Durch Einsatz spezialisierter Werkzeuge in Kombination mit hoher Rechenleistung können bei unzureichenden Schutzmaßnahmen hierbei hohe Erkennungsraten in verhältnismäßig kurzer Zeit erreicht werden. Aufgrund der Unabhängigkeit vom Quellsystem bleibt ein solcher Offline-Angriff auf eine Benutzerdatenbank zudem unbemerkt.

Folgende Maßnahme ist umzusetzen, da diese den größtmöglichen Schutz bei Offline-Angriffen gewährleistet:

- Passwörter müssen unter Verwendung einer für diesen Zweck anerkannt wirksamen, zum aktuellen Stand der Technik als sicher eingestuften, kryptografischen Einwegfunktion gespeichert werden (bekannt als "Password-Hashing" Verfahren)

Hinweis: Zulässige Passwort-Hashing-Verfahren sind im Sicherheitsanforderungsdokument "3.50 / Kryptographische Algorithmen und Sicherheitsprotokolle" beschrieben.

In expliziter Deutlichkeit ist als NICHT ZULÄSSIG hervorzuheben:

- jegliche Speicherung von Passwörtern im Klartext
- jegliche Speicherung von Passwörtern in direkt rückrechenbaren Formaten
- jegliche Speicherung von Passwörtern mittels umkehrbarer Verschlüsselung

Hinweis:

"direkt rückrechenbare Formate" bezieht sich in diesem Kontext auf Formate, die ein Passwort lediglich kodieren, also ohne Einbeziehung eines geheimen Schlüssels transformieren. Da ein Passwort bei Anwendung eines solchen Formats nicht mehr in seinem originalen Klartext lesbar bleibt, werden diese Formate leicht als Schutzmaßnahme

missverstanden. Effektiv bieten sie jedoch keinen Schutz, da die dahinterliegende Kodierung fest definiert ist und von einem Angreifer sehr leicht für die Rückrechnung der Inhalte in den ursprünglichen Klartext genutzt werden kann.

Beispiele für direkt rückrechenbare Formate sind: "base64", "rot13"

"Umkehrbar" sind alle Verfahren der Verschlüsselung, die unter Verwendung des passenden Schlüssels ermöglichen, einen verschlüsselten Inhalt zurück in den originalen Inhalt zu transformieren. Entsprechend stellt sich bei umkehrbarer Verschlüsselung stets die Herausforderung, den Schlüssel sicher aufzubewahren und vor unberechtigtem Zugriff zu schützen. Die Umkehrbarkeit ist auf vielen Einsatzgebieten der Verschlüsselung, z. B. für den Transport von vertraulichen Nachrichten, eine benötigte Grundeigenschaft, für das Speichern von Passwörtern jedoch kontraproduktiv: ein gespeichertes Passwort muss zwar mittels technischer Methoden vergleichbar bleiben, aber darf nicht mehr in seinen Klartext rückwandelbar sein, um es vor unberechtigter Einsicht bestmöglich zu schützen.

Beispiele für umkehrbare Verschlüsselung sind: "AES", "CHACHA20", "3DES", "RSA"

Motivation: Ohne entsprechenden Schutz kann ein Angreifer im Besitz der Benutzerdatenbank durch bloßes Durchprobieren von Wörterbuchlisten oder automatisch erzeugten Zeichenkombinationen versuchen, massenhaft Passwörter zu ermitteln, um so entsprechende Benutzerkonten missbräuchlich zu nutzen. Passwörter, die im Klartext oder direkt rückrechenbaren Formaten gespeichert werden, sind bei einem Offline-Angriff vollkommen schutzlos.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-24/9.0

Req 22	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss ein Schutz gegen Online-Angriffe wie Wörterbuch- und Brute-Force-Attacken vorhanden sein, der das Erraten von Passwörtern stark erschwert.
--------	--

Online Wörterbuch- und Brute-Force Angriffe haben zum Ziel, durch automatisiertes Ausprobieren an einer regulären Zugangsschnittstelle des Systems die Passwörter von Benutzerkonten zu erraten.

Um dies zu verhindern, muss eine der folgenden Maßnahmen oder eine Kombination aus diesen umgesetzt werden:

- mittels technischer Maßnahmen abgebildete Erzwingung einer Wartezeit nach einem fehlgeschlagenen Anmeldeversuch, bevor eine erneute Anmeldung ermöglicht wird. Die Wartezeit sollte sich zudem mit jedem weiteren fehlgeschlagenen Anmeldeversuch automatisch deutlich erhöhen (z. B. durch Verdopplung).
- automatisiertes Sperren des Benutzerkontos nach einer vorgegebenen Anzahl von aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen (typischerweise 5). Allerdings ist bei dieser Lösung zu bedenken, dass diese einen Entsperrungs-Prozess erforderlich macht und ein Angreifer dies gezielt nutzen kann, um Konten zu sperren und somit vorübergehend unbrauchbar zu machen.
- Verwendung von CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart"), um automatisierte Anmeldeversuche von Maschinen ("Robots" oder "Bots") bestmöglich zu unterbinden. Ein CAPTCHA stellt dazu eine kleine Aufgabe, i. d. R. basierend auf grafischen oder akustischen Elementen, die von einer Maschine nur schwer zu lösen ist. Es ist entsprechend zu berücksichtigen, dass CAPTCHA problematisch bzgl. der Barrierefreiheit sein können.

Um eine höhere Sicherheit zu erreichen, ist es oftmals sinnvoll, zwei oder mehrere der genannten Maßnahmen miteinander zu kombinieren. Dies ist abhängig vom Einzelfall zu prüfen und entsprechend umzusetzen.

Motivation: Ohne entsprechenden Schutz kann ein Angreifer durch bloßes Durchprobieren von Wörterbuchlisten oder automatisch erzeugten Zeichenkombinationen versuchen ein Passwort zu ermitteln, um so das entsprechende Benutzerkonto missbräuchlich zu nutzen.

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: 3.01-25/9.0

Req 23	Falls Passwörter als Authentisierungsmerkmal genutzt werden, müssen diese mindestens 12 Zeichen lang sein und drei der folgenden Zeichenkategorien beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.
--------	--

Ein System darf nur Passwörter akzeptieren, welche die folgende Komplexität erfüllen:

- Mindestlänge 12 Zeichen
- Bestehend aus mindestens drei der folgenden vier Zeichenkategorien:
 - Kleinbuchstaben
 - Großbuchstaben
 - Ziffern
 - Sonderzeichen

Die maximal mögliche Länge für Passwörter sollte 25 Zeichen oder mehr betragen. Dies unterstützt Endbenutzer bei Bedarf mit mehr Freiraum, um individuelle merkbare Passwörter bilden zu können, und hilft so, unerwünschte Verhaltensweisen im Umgang mit Passwörtern zu vermeiden, welche durch stark eingeschränkte maximale Passwortlängen provoziert werden können.

Das System muss bei der Vergabe eines Passwortes sicherstellen, dass das Passwort diesen Bildungsregeln entspricht; vorzugsweise mittels technischer Maßnahmen, falls solche aber nicht umsetzbar sein sollten, ersatzweise mittels organisatorischer Maßnahmen.

Bei Verwendung eines zentralen Systems für die Authentisierung der Benutzer [vgl. Wurzel-Anforderungsdokument "[i]3.69 IAM (Identity Access Management) - Framework"] darf diese Aufgabe an das zentrale System weitergereicht bzw. dorthin ausgelagert werden.

Zulässige Abweichung in der Passwort-Mindestlänge

Unter sicherheitsbezogenen Kriterien lassen sich für ein System potenziell Bedingungen identifizieren, die eine Reduzierung der Passwort-Mindestlänge ermöglichen:

- Allgemein zulässig ist eine Reduzierung der Passwort-Mindestlänge für Systeme, die innerhalb des Authentisierungsprozess zusätzlich zum Passwort weitere unabhängige Authentisierungsmerkmale verwenden (Umsetzung von 2-Faktor oder Multi-Faktor Authentisierung).
- Eine Reduzierung der Passwort-Mindestlänge muss grundsätzlich durch einen fachlichen Sicherheitsberater (z. B. ein PSM der Telekom Security) individuell bewertet und als zulässig bestätigt werden. In der Bewertung müssen umgebende technische, organisatorische und gesetzliche Rahmenparameter berücksichtigt sowie der systemspezifische Schutzbedarf und die potenzielle Schadenshöhe bei Sicherheitsvorfällen einbezogen werden.
- Der absolute Mindestwert von 8 Zeichen Länge darf für Passwörter grundsätzlich nicht unterschritten werden.

Motivation: Passwörter mit der genannten Komplexität bieten eine zeitgemäße Robustheit gegen Angriffe bei gleichzeitig akzeptabler Benutzerfreundlichkeit. In der Praxis haben sich Passwörter mit dieser Komplexität bewährt. Triviale und zu kurze Passwörter sind anfällig für Brute-Force- und Wörterbuch-Angriffe und von einem Angreifer leicht zu ermitteln. Ein ermitteltes Passwort kann dann von einem Angreifer für den unautorisierten Zugriff auf das System und dessen Daten genutzt 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
- Abstreiten von durchgeführten Aktionen

ID: 3.01-26/9.0

Req 24	Falls Passwörter als Authentisierungsmerkmal für technische Benutzerkonten genutzt werden, müssen diese mindestens 30 Zeichen lang sein und drei der folgenden Zeichenkategorien beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.
--------	--

Technische Benutzerkonten zeichnen sich dadurch aus, dass sie nicht von Personen verwendet werden. Stattdessen werden sie für die Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt.

Ein System darf für technische Benutzerkonten nur Passwörter verwenden, welche die folgende Komplexität erfüllen:

- Mindestlänge 30 Zeichen
- Bestehend aus mindestens drei der folgenden vier Zeichenkategorien:
 - Kleinbuchstaben
 - Großbuchstaben
 - Ziffern
 - Sonderzeichen

Motivation: Technische Benutzerkonten sind aufgrund ihrer Verwendung in Machine-to-Machine (M2M) Kommunikations-Szenarien oft mit Berechtigungen ausgestattet, die für einen Angreifer von hohem Interesse sein können, um Infrastrukturen zu kompromittieren. Ohne Mechanismen einer umfassenden Kompromittierungserkennung kann dann das Risiko, dass ein Passwort von einem Angreifer ermittelt oder gebrochen wird, über die Zeit deutlich ansteigen. Eine signifikante Erhöhung der Passwort-Länge wirkt diesen Risiken entgegen und lässt sich zudem in M2M Szenarien besonders leicht umsetzen, da die Handhabung eines sehr langen Passworts für eine Maschine (im Gegensatz zu einer Person) keine besondere Herausforderung darstellt.

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: 3.01-27/9.0

Req 25	Falls Passwörter als Authentisierungsmerkmal verwendet werden, muss die Wiederverwendung bereits eingesetzter Passwörter unterbunden werden.
--------	--

Für jedes Benutzerkonto muss eine Historie der bisher genutzten Passwörter aufgezeichnet werden. Wird eine Passwort-Änderung für ein Benutzerkonto initiiert, ist das neue Passwort gegen diese Passwort-Historie abzugleichen. Bei erkannter Wiederverwendung eines Passworts muss die Passwort-Änderung abgelehnt werden. Die Umsetzung dieses Validierungsvorgangs muss im System auf Basis von technischen Maßnahmen erfolgen. Bei Verwendung eines zentralen IAM Systems für die Authentisierung der Benutzer darf die Umsetzung an das zentrale IAM System weitergereicht bzw. dorthin ausgelagert werden [vgl. Wurzel-Anforderungsdokument "3.69 IAM (Identity Access Management) - Framework"].

Generell soll mittels der Passwort-Historie sichergestellt werden, dass ein schon einmal verwendetes Passwort niemals erneut einsetzbar ist.

Aufgrund technischer Limitierungen kann eine Passwort-Historie jedoch in vielen IT/NT-Produkten nicht unbe-

schränkt aufgezeichnet werden. In diesem Fall ist die folgende Grundregelung zu berücksichtigen:

- ein bereits genutztes Passwort darf für den Zeitraum von mindestens 60 Tagen nicht erneut einsetzbar sein (gemessen ab dem Zeitpunkt, an dem das betroffene Passwort durch ein anderes ersetzt wurde)
- in Systemen, in denen der Zeitraum von mindestens 60 Tagen nicht abgebildet werden kann, muss der längst mögliche Zeitraum konfiguriert werden. Zusätzlich muss durch einen Project Security Manager (PSM) bestätigt werden, dass der konfigurierte Zeitraum im Gesamtkontext des Systems noch ausreichend im Sinne der Sicherheitsanforderung ist.

Anmerkung:

Einige IT/NT-Produkte bieten keinen technischen Konfigurationsparameter an, mit dem die Passwort-Historie direkt an einen Zeitraum gebunden werden kann, sondern ermöglichen nur, die Anzahl der aufzuzeichnenden Passwörter zu definieren. In solchen Fällen darf der Zeitraum alternativ durch eine Verknüpfung der folgend beschriebenen, i. d. R. breit verfügbaren Konfigurationsparameter sichergestellt werden. Innerhalb der resultierenden Policy kann ein Benutzer nur einmal pro Tag sein Passwort ändern und aufgrund der Anzahl der aufgezeichneten Passwörter effektiv nach frühestens 60 Tagen ein altes Passwort erneut einsetzen.

- Minimum Passwort-Alter: 1 Tag
- Passwort-Historie: Aufzeichnung der letzten 60 benutzten Passwörter

In dieser Umsetzungsvariante ist zu beachten, dass das Minimum Passwort-Alter nicht mehr als einen Tag betragen sollte, um den Benutzer nicht unangemessen hinsichtlich der grundsätzlichen Notwendigkeit einzuschränken, das Passwort jederzeit selbstständig ändern zu können.

Motivation: Benutzer favorisieren in der Regel Passwörter, die sie sich gut merken können und verwenden diese in Folge oft wiederkehrend über lange Zeiträume, falls das System dies zulässt. Aus Sicht des Benutzers ist das Verhalten nachvollziehbar, führt aber effektiv zu einer erheblichen Reduzierung der Schutzwirkung dieses Authentisierungsparameters. Mit etwa entsprechenden Kenntnissen über den Benutzer oder erbeuteten Informationen aus zurückliegenden System-Kompromittierungen kann ein Angreifer so Zugriff auf vermeintlich geschützte Benutzerkonten erlangen. Insbesondere auch in Situationen, in denen im Rahmen einer akuten Risikobehandlung zentral neue Initialpasswörter vergeben werden, die Benutzer diese jedoch unmittelbar aus Bequemlichkeit auf ein vorheriges Passwort zurückändern, bestünde hohe Gefahr, dass ein Angreifer seinen illegalen Zugriff erneut aufnehmen kann. Es ist daher wichtig zu vermeiden, dass Benutzer alte Passwörter erneut einsetzen.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-28/9.0

Req 26	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss eine Änderung des eigenen Passwortes jederzeit durch den Benutzer möglich sein.
--------	---

Das System muss eine Funktion bieten, die es einem Benutzer ermöglicht, sein Passwort jederzeit zu ändern.

Bei der Verwendung eines zentralen Systems darf die Funktion auf dieses System weitergereicht oder ausgelagert werden.

Motivation: Nur durch die Möglichkeit, dass ein Benutzer sein Authentisierungsmerkmal jederzeit selbsttätig ändern kann, ist ein zeitnahe Änderung möglich, wenn der Benutzer den Verdacht hat, dass dieses in den Besitz Dritter gelangt sein könnte.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-29/9.0

Req 27	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss nach spätestens 12 Monaten ein Passwort-Wechsel erfolgen.
--------	---

Die maximal zulässige Nutzungsdauer für Passwörter beträgt 12 Monate.
Erreicht ein Passwort die maximal zulässige Nutzungsdauer, muss es geändert werden.

Das System muss hierzu den Benutzer automatisch bei dessen nächster Systemanmeldung auf die abgelaufene Nutzungsdauer hinweisen und ihn unmittelbar durch einen Passwort-Änderungsdialog führen. Der Zugriff auf das System darf ohne eine erfolgreich abgeschlossene Passwort-Änderung nicht weiter zugelassen werden.
Für technische Benutzerkonten (M2M bzw. Machine-2-Machine), die für die Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt werden, müssen ebenfalls automatisierte Lösungen zur Einhaltung der zulässigen Nutzungsdauer für Passwörter implementiert werden.

Falls eine automatisierte Abbildung des Prozesses zur Passwort-Änderung nicht umsetzbar ist, muss ersatzweise eine wirksame organisatorische Maßnahme angewendet werden, die eine verbindliche manuelle Passwort-Änderung bei Ablauf der zulässigen Nutzungsdauer sicherstellt.

Motivation: Passwörter sind im Gegensatz zu moderneren Authentisierungsmerkmalen leichter angreifbar. Ohne spezifische Maßnahmen einer verlässlichen technisch automatisierten Kompromittierungserkennung kann das Risiko, dass ein Passwort von einem Angreifer ermittelt oder gebrochen wird, über die Zeit deutlich steigen.

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: 3.01-30/9.0

Req 28	Falls Passwörter als Authentisierungsmerkmal genutzt werden, darf deren Darstellung während der Eingabe nicht im Klartext erfolgen.
--------	---

Passwörter dürfen während deren Eingabe nicht in lesbarem Klartext auf Bildschirmen oder sonstigen Ausgabegeräten dargestellt werden. Eine Darstellung während der Eingabe darf keine Rückschlüsse auf die tatsächlich im Passwort verwendeten Zeichen ermöglichen.

Diese Anforderung gilt für jegliche Arten von Eingabemasken und -feldern für Passwörter.
Beispiele hierfür sind Dialoge zur Passwort-Vergabe, zur Passwort-basierenden Anmeldung an Systemen oder zur Änderung von bestehenden Passwörtern.

Ausnahmeregelungen:

- Innerhalb eines Eingabefelds ist eine optionale Klartext-Darstellung eines Passworts zulässig, sofern diese Klartext-Darstellung einem validen Zweck dient, nur temporär anhält, dazu fallbezogen durch den legitimen Benutzer explizit zu aktivieren ist und von diesem umgehend auch wieder deaktiviert werden kann.
Ein valider Zweck wäre beispielsweise, dem legitimen Benutzer bei Bedarf eine unkomplizierte visuelle Überprüfung zu ermöglichen, sein Passwort in einem Anmelde-Dialog korrekt eingegeben zu haben, bevor er die Anmeldung letztendlich final vollzieht.

Eine solche optionale Klartext-Darstellung eines Passworts muss vollständig in der Kontrolle des legitimen Benutzers verbleiben, damit er über deren Aktivierung/Deaktivierung situationsgerecht entscheiden kann. In der Standard-Einstellung des Systems muss die Klartext-Darstellung deaktiviert sein.

- Das auf vielen mobilen Endgeräten (Smartphones) typische Verhalten, jedes einzelne Zeichen bei der Eingabe eines Passworts sehr kurz im Klartext anzuzeigen, um dem Benutzer die Eingabekontrolle zu erleichtern, ist dort grundlegend zulässig. Allerdings darf dabei niemals das vollständige Passwort im Klartext auf dem Bildschirm dargestellt werden.

Motivation: Im Fall einer Klartext-Darstellung besteht das Risiko, dass dritte Personen ein Passwort während der Eingabe zufällig oder gezielt über die Bildschirm-Ausgabe ausspähen können.

Umsetzungsbeispiel: In der Darstellung auf dem Bildschirm wird während der Eingabe eines Passworts jedes einzelne Zeichen einheitlich durch ein "*" ersetzt.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-31/9.0

2.5. Zugriffe des Machine Learning Algorithmus auf andere Systeme

Req 29	Die Ergebnisse und Entscheidungen des Machine Learning Algorithmus dürfen nicht ohne vorherige Prüfung auf produktive Systeme übertragen werden.
--------	--

Es ist von entscheidender Bedeutung, dass die Ergebnisse und Entscheidungen, die von einem Machine Learning Algorithmus generiert werden, sorgfältig geprüft und validiert werden, bevor sie auf produktive Systeme übertragen werden. Obwohl Machine Learning Algorithmen in der Lage sind, komplexe Muster und Zusammenhänge in großen Datenmengen zu erkennen, sind sie dennoch nicht perfekt und können fehlerhaft sein. Wenn diese Fehler nicht erkannt und korrigiert werden, können sie schwerwiegende Auswirkungen auf das betroffene System haben. Daher ist es wichtig, dass die Ergebnisse und Entscheidungen des Algorithmus überprüft und validiert werden, um sicherzustellen, dass sie korrekt und zuverlässig sind. Diese Überprüfung muss nicht zwangsläufig von einem Menschen durchgeführt werden.

Motivation: Ohne vorherige Überprüfung der Ergebnisse des Machine Learning Algorithmus, können getroffene Entscheidung zu Systemausfällen führen. Dies gilt es grundsätzlich zu vermeiden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Verfügbarkeit
- Transparenz

ID: 3.81-29/4.0

3. KI-Komponenten Nutzende Systeme

Req 30	Die KI-Komponente muss jederzeit vollständig durch einen Systemadministrator gestoppt und deaktiviert werden können, wenn dies erforderlich ist.
--------	--

Falls ein System über die Funktionalität einer KI-Komponente verfügt, muss ein Systemadministrator jederzeit dazu in der Lage sein, die KI-Komponente sofort vollständig stoppen und deaktivieren zu können.

Motivation: Um die vollständige Kontrolle und Aufsicht über eine KI-Komponente gewährleisten zu können, muss eine unkomplizierte und schnelle Lösung zur sofortigen Beendigung der KI-Komponente existieren. So wird sichergestellt, dass im Falle einer Kompromittierung oder unvorhersehbarem bzw. fehlerhaften Verhalten der KI-Komponente weiterer Schaden abgewendet werden kann.

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: 3.81-30/4.0

Req 31	Die KI-Komponente muss jederzeit durch den Nutzer deaktiviert werden können. Dies beinhaltet auch einzelne Sessions oder Userinteraktionen.
--------	---

Falls ein System über die Funktionalität einer KI-Komponente verfügt, muss diese durch den Nutzer deaktivierbar sein. Entscheidend ist auch, dass der Nutzer einzelne Interaktionen mit der KI-Komponente beenden kann und über die Beendigung informiert wird. Darüber hinaus muss eine Dokumentation vorliegen, wie der Nutzer die KI-Komponente aktivieren, deaktivieren und ggf. einzelne Sessions wiederherstellen kann.

Motivation: Eine KI-Komponente, die nicht deaktiviert werden kann, birgt das Risiko, Einfluss auf das System zu haben, ohne, dass dies beabsichtigt ist. Es könnten sensible Daten übertragen werden, ohne, dass der Nutzer Kenntnis davon hat. Im Falle einer Fehlfunktion muss der Nutzer außerdem die Möglichkeit haben, die KI-Komponente zu beenden, auch wenn dies eine erhebliche Beeinträchtigung der Funktion zur Folge hätte.

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: 3.81-31/4.0

Req 32	Die KI-Komponente darf sich nicht selbstständig wieder einschalten können, nachdem sie ausgeschaltet bzw. deaktiviert worden ist.
--------	---

Sollte die KI-Komponente durch das System oder den Nutzer ausgeschaltet oder deaktiviert worden sein, darf die KI-Komponente nicht dazu in der Lage sein, sich selbstständig wieder zu aktivieren. Sofern die KI-Komponente deaktiviert worden ist, muss auch sichergestellt werden, dass diese bei einem kompletten Neustart des gesamten Systems nicht automatisch aktiviert wird, wenn diese Funktion vorher deaktiviert worden ist.

Motivation: Ein Nutzer, der die KI-Komponente bewusst deaktiviert hat, muss sich darauf verlassen können, dass dies so bleibt. Sollte eine kompromittierte KI-Komponente sich selbst wieder aktivieren können, birgt dies die Gefahr, dass ein Angreifer Informationen oder Daten abgreift, ohne, dass der Nutzer dies bemerkt. Es könnten außerdem Handlungen und Änderungen am System durch die KI-Komponente vorgenommen werden, die vom Nutzer nicht beabsichtigt 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

ID: 3.81-32/4.0

Req 33	Eine KI-Komponente darf ausschließlich als Assistenzsystem genutzt werden und darf keine eigenständigen Entscheidungen treffen.
--------	---

Falls ein System über die Funktionalität einer KI-Komponente verfügt, muss sichergestellt werden, dass diese keine eigenständigen Entscheidungen trifft, sondern ausschließlich als Assistenzsystem genutzt werden darf. Wird eine KI-Komponente eingesetzt, müssen Prozessentscheidungen immer bei einer realen Person liegen, die über die benötigten Berechtigungen verfügt. Eine KI-Komponente darf nicht dahingehend verändert werden, Entscheidungen zu treffen.

Motivation: Eine KI-Komponente, die eingeständig Entscheidungen trifft, stellt eine Gefahr für das gesamte System dar. Verfügt eine KI-Komponente über die gleichen Berechtigungen, die bspw. ein Systemadministrator oder Nutzer mit erweiterten Berechtigungen hat, könnte ein Angreifer die KI-Komponente für maliziöse Zwecke 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

ID: 3.81-33/4.0

Req 34	Es muss sichergestellt werden, dass eine KI-Komponente keinen Zugriff auf sicherheitskritische Informationen hat.
--------	---

Falls ein System über die Funktionalität einer KI-Komponente verfügt, muss sichergestellt sein, dass diese keinen Zugriff auf sicherheitskritische Informationen und Aktionen hat. Auf Sicherheitskritische Informationen, wie bspw. Passwörter oder Zertifikate dürfen ausschließlich berechtigte Nutzer oder Administratoren zugreifen.

Motivation: Eine KI-Komponente, die Zugriff auf sicherheitskritische Informationen oder Aktionen, wie Benutzerdaten, Passwörter oder Zertifikate hat birgt ein erhebliches Sicherheitsrisiko. Sollte eine KI-Komponente durch einen Angreifer übernommen worden sein, hätte dieser auch automatisch Zugriff auf sensible Informationen und Daten der Benutzer und Administratoren.

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: 3.81-34/4.0

Req 35	Interaktionen mit der KI-Komponente müssen an einen zentralen Logserver weitergeleitet werden.
--------	--

Falls ein System über die Funktionalität einer KI-Komponente verfügt, muss es sicherstellen, dass sämtliche Protokollierungsdaten mit der KI-Komponente an einen zentralen Logserver weitergeleitet werden. So kann gewährleistet werden, dass die Systemadministratoren genau nachvollziehen können, wie die KI-Komponente arbeitet.

Motivation: Eine KI-Komponente kann Ziel von Angreifern werden oder Systemabstürze erleiden. Damit genau nachvollzogen werden kann, wann genau bestimmte Events stattgefunden haben, muss ein zentraler Logserver eingesetzt

werden, um diese Events forensisch aufarbeiten zu können und ggf. geeignete Maßnahmen zur zukünftigen Vermeidung einzuleiten.

Folgende Grundregelung ist zu berücksichtigen:

- sicherheitsrelevante Protokollierungsdaten müssen auf dem separaten Log Server für einen Zeitraum von 90 Tagen aufbewahrt werden.
- nach Ablauf von 90 Tagen muss eine umgehende Löschung der auf dem separaten Log Server gespeicherten Protokollierungsdaten erfolgen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.81-35/4.0

Req 36	Die KI-Komponente muss über eine Missbrauchserkennung verfügen, die bspw. unethische und bössartige Aktionen oder Ausgaben verhindert. Diese Missbrauchserkennung muss ausreichend beschrieben sein.
--------	--

Falls ein System über die Funktionalität einer KI-Komponente verfügt, muss diese über eine Missbrauchserkennung verfügen. So wird sichergestellt, dass die KI-Komponente nicht für bössartige und maliziöse Absichten missbraucht wird. Über die Funktionsweise und Zugriffe dieser Missbrauchserkennung muss eine Dokumentation vorliegen. Die Missbrauchserkennung darf durch den Nutzer nicht deaktiviert werden können.

Motivation: KI-Komponente wie bspw. Large Language Model können in der Lage dazu sein, maliziösen und unethischen Content zu generieren, der vom Nutzer missbraucht werden könnte. Dazu zählen bspw. Codegenerierungen für Ransomware oder Anleitungen zum Durchführen von Denial of Service Attacks. In aller Regel können solche Ausgaben durch Filter verhindert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.81-36/4.0

Req 37	Interaktionen mit der KI-Komponente dürfen keine Rückschlüsse auf verwendete Trainingsdaten zulassen.
--------	---

Falls ein System über die Funktionalität einer KI-Komponente verfügt, darf ein Nutzer von der KI-Komponente keine Auskunft darüber erhalten, welche Trainingsdaten für das Training des KI-Modells verwendet worden sind. Die für das Training des Modells verwendeten Daten dürfen nicht öffentlich zugänglich sein. Eine Extraktion der Trainingsdaten muss durch festgelegte Verhaltensregeln der KI-Komponente verhindert werden.

Motivation: Jede KI-Komponente durchläuft vor der Inbetriebnahme einen Trainingsprozess, um die Komponente auf ihren Einsatzzweck vorbereiten zu können. Dafür werden Trainingsdatensätze verwendet, die von den Systemadministratoren als geeignet eingestuft worden sind. Es ist möglich, dass Trainingsdaten sensible Informationen enthalten, die Datenschutzrechtliche- oder sicherheitskritische Relevanz haben, weshalb dem Nutzer keine Auskunft über die Trainingsdaten erteilt werden darf.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Req 38 KI generierter Inhalt muss immer klar als solcher gekennzeichnet sein.

Falls ein System über die Funktionalität einer generativen KI-Komponente verfügt, muss Inhalt, der durch diese erzeugt wird, klar als KI-generiert gekennzeichnet werden. Insbesondere bei eingebetteten KI-Assistenten muss klar zwischen KI- und nicht-KI generierten Inhalte unterschieden werden können. Bei Texten und Wörtern muss dies ein Zusatz im erstellten Inhalt sein. Bei Bild- und Videomaterial ist ein Wasserzeichen zu verwenden.

Motivation: Generative KI ist in der Lage, Texte, Bilder oder Videomaterial zu erzeugen, die anschließend vom Nutzer verwendet werden können. Sollten E-Mails automatisiert generiert werden oder Texte über eine generative KI ergänzt werden, muss der Empfänger darauf hingewiesen werden, dass Teile der E-Mail nicht vom eigentlichen Absender selbst geschrieben worden sind.

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität
- Transparenz

Req 39 Bei einer Interaktion mit einer KI-Komponente muss dem Nutzer mitgeteilt werden, dass er mit keiner natürlichen Person interagiert, sondern mit einer künstlichen Intelligenz.

Falls ein System über die Funktionalität einer KI-Komponente in Form eines Large Language Models (bspw. ein Chat Bot) verfügt und dieser mit einem Nutzer interagiert, muss diesem mitgeteilt werden, dass es sich um keine natürliche Person handelt, sondern eine künstliche Intelligenz und die Antworten unpräzise sein könnten.

Motivation: Einem Nutzer eines Large Language Models muss zu jeder Zeit klar sein, dass er mit einer künstlichen Intelligenz interagiert und nicht mit einem realen Menschen. Das kann dazu führen, dass Antworten des Modells unpräzise oder unlogisch sein könnten. Sog. „Halluzinationen“ können jederzeit auftreten und die Unterhaltung mit dem Nutzer beeinflussen. Deswegen ist es wichtig, den Nutzer zu Beginn der Interaktion auf etwaige Ungenauigkeiten hinzuweisen.

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität
- Transparenz

Req 40 Daten, die an eine KI-Komponente übermittelt werden, müssen vor der Übertragung vorverarbeitet werden. Das beinhaltet u. A. Entrauschungsalgorithmen für Bilder, Videos und Sprache, als auch vergleichbare Vorverarbeitung für Eingaben in andere KI-Komponenten, wie textbasierte Algorithmen.

Diese Vorverarbeitung umfasst verschiedene Schritte die an die Art der Eingabedaten (Bilder, Video, Sprache, Text, etc.) angepasst sein müssen. Durch diese Vorverarbeitung wird sichergestellt, dass die Daten in einer für die KI-Komponente optimal analysierbaren Form vorliegen und somit manipulationsbasierte Angriffe erschwert werden.

Beispiele für Vorverarbeitungen:

1. Bilder und Video

- Entrauschungsalgorithmen
- Skalierung auf einheitliche Größe
- Kontrastanpassung
- Farbkorrektur

- Ausschneiden von relevanten Bereichen
2. Sprache
- Entfernung von Störgeräuschen
 - Normalisierung der Sprachlautstärke
 - Einschränkung der Frequenzbereiche
3. Text
- Entfernung von potentiell maliziösen Zeichenfolgen (einzelne Worte oder ganze Wortgruppen bzw. Sätze)

Motivation: Durch Vorverarbeitung der Daten können potentielle maliziöse Benutzereingaben herausgefiltert werden, bevor sie die KI-Komponente erreichen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Verfügbarkeit
- Vertraulichkeit
- Integrität

ID: 3.81-40/4.0

Req 41 Es muss gewährleistet werden, dass keine vertraulichen Daten durch das System oder den Nutzenden an die KI-Komponenten übertragen werden, wenn dies nicht explizit vorgesehen ist.

Es ist sicherzustellen, dass keine schutzbedürftige Daten durch das System oder den Nutzenden an KI-Komponenten übertragen werden, es sei denn, dies ist ausdrücklich vorgesehen. Dies erfordert eine sorgfältige Überprüfung und Kontrolle der Datenflüsse innerhalb des Systems, um sicherzustellen, dass die Vertraulichkeit und Integrität der Daten jederzeit gewahrt bleibt. In jedem Fall sollten vertrauliche Daten anonymisiert werden, bevor sie an eine KI-Komponente übertragen werden.

Regelung zur Klassifikation von Informationen: <https://informationsdrehscheibe.telekom.de>

Motivation: Alle Informationen, die an KI-Komponenten übergeben werden, könnten vom Betreiber oder Dritten eingesehen und auch außerhalb des vereinbarten Verarbeitungsvertrags verwendet werden.

Der beste Schutz vor unerwünschter Verwendung von vertraulichen Daten ist es, solche Daten nur an Systeme zu übergeben die explizit zu deren Verarbeitung konzipiert sind.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Vertraulichkeit

ID: 3.81-41/4.0

Req 42 Das System muss gewährleisten, dass ausschließlich Daten an die KI-Komponenten übertragen werden, die deren Anforderungen gerecht werden. Somit dürfen z. B. keine .exe-Programme als Benutzereingabe für einen Bilderkennungsalgorithmus akzeptiert werden.

Damit die KI-Komponente effektiv und sicher arbeitet, dürfen nur Daten an sie übertragen werden, die den Anforderungen an einen sicheren Betrieb dieser Komponente entsprechen. Es ist wichtig, bestimmte Dateiformate oder Datenarten zu vermeiden, um eine fehlerhafte oder ungenaue Verarbeitung zu verhindern. Zum Beispiel sollten keine

.exe-Programme als Eingabe für einen Bilderkennungsalgorithmus akzeptiert werden, da diese Art von Daten nicht mit der Funktionsweise des Algorithmus kompatibel ist und zu unerwünschten Ergebnissen führen kann.

Motivation: Unzulängliche Eingangsdaten können bei Ihrer Verarbeitung weitreichende Folgen haben. Durch Input-Validierung soll vermieden werden, dass es in der KI-Komponente zu einem undefinierten Verhalten kommt.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität

ID: 3.81-42/4.0

Req 43	Es muss eine verantwortliche Person benannt sein, die Verantwortung für die Entscheidungen des Machine Learning Algorithmus trägt, sodass im Falle von Fehlern oder Schäden eine klare Zuordnung möglich ist.
--------	---

KI-Komponenten können bei Missbrauch oder im Fehlerfall große Schäden für ein Unternehmen verursachen. Daher ist es wichtig eine klare Zuordnung der Verantwortung sicherzustellen.

Handlungsanweisungen und Prozesse für alle denkbaren Fehlerszenarien müssen vorab festgelegt werden. Auch ethische und rechtliche Fragen müssen von einer zuständigen Person oder einem verantwortlichen Bereich bereits vor Inbetriebnahme geklärt sein und dann laufend aktualisiert werden.

Die Benennung einer verantwortlichen Person, oder eines Bereichs, mit klarer Angabe der Kontaktdaten, ist daher erforderlich.

Motivation: Eine klare Verantwortlichkeit für den Einsatz von KI-Komponenten ist wichtig, um sicherzustellen, dass im Falle von Fehlern oder Schäden eine klare Zuordnung möglich ist und damit schnelles Handeln den eintretenden Schaden reduzieren kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Transparenz

ID: 3.81-43/4.0

Req 44	Vordefinierte Authentisierungsmerkmale müssen geändert werden.
--------	--

Nach der Übernahme oder Erstinstallation eines Systems existieren üblicherweise vordefinierte Authentisierungsmerkmale (z. B. Passwörter, SSH Keys, SSL/TLS Zertifikate) im System, wie sie durch Hersteller, Entwickler, Lieferanten oder automatisierte Installationsroutinen vergeben wurden.

Solche vordefinierten Authentisierungsmerkmale müssen unmittelbar nach der Übernahme bzw. Installation des Systems auf neue, individuelle Werte geändert werden.

Motivation: Von Dritten vordefinierte Werte in Authentisierungsmerkmalen können nicht als vertrauenswürdig angesehen werden, da sie kein kontrolliertes Geheimnis darstellen. Betroffene Authentisierungsmerkmale können von Unbefugten dafür missbraucht werden, um auf Systeme zuzugreifen und diese zu kompromittieren. Dieses Risiko ist signifikant erhöht, falls für Authentisierungsmerkmale allgemein bekannte Standard-Werte verwendet werden (z. B. ein Standardpasswort für das Administrator-Benutzerkonto in einem bestimmten Software-Produkt).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

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

ID: 3.01-8/9.0

4. Technischer Basisschutz von IT-/NT-Systemen

4.1. Technisch-organisatorische Voraussetzungen für den Einsatz von Komponenten im System

Req 45	Software und Hardware des Systems müssen von einem Sicherheitsschwachstellen-Support seitens des Herstellers abgedeckt werden.
--------	--

In einem System dürfen nur Software- und Hardware-Produkte eingesetzt werden, für die ein Sicherheitsschwachstellen-Support durch den Hersteller besteht.

Ein solcher Support muss umfassen, dass der Hersteller

- das Produkt kontinuierlich auf eine Betroffenheit von Sicherheitsschwachstellen beobachtet und analysiert,
- über Art, Schweregrad und Ausnutzbarkeit von im Produkt entdeckten Schwachstellen umgehend informiert
- zeitnah Produktaktualisierungen oder wirksame Workarounds zur Behebung der Schwachstellen bereitstellt.

Der Sicherheitsschwachstellen-Support muss für die gesamte Dauer bestehen, in der das betroffene Produkt im Einsatz verbleibt.

Support-Phasen mit eingeschränktem Leistungsumfang

Viele Hersteller bieten für ihre Produkte als Option einen zeitlich ausgedehnten Support an, welcher über die für den allgemeinen Markt vorgesehene Support-Phase hinausgeht, aber oftmals mit Einschränkungen verbunden ist. Einige Hersteller definieren ihren Support grundlegend in Abstufungen, die Einschränkungen schon während der letzten Phase vor dem absoluten Endtermin des regulären Supports enthalten können.

Wird ein Produkt innerhalb von Support-Phasen eingesetzt, die Einschränkungen unterliegen, muss explizit sichergestellt werden, dass diese Einschränkungen die Verfügbarkeit des Sicherheitsschwachstellen-Support nicht beeinträchtigen.

Open Source Software und Hardware

Open Source Produkte werden häufig von freien Organisationen oder Communities entwickelt; entsprechend ist ein vertraglich vereinbarter Sicherheitsschwachstellen-Support unter Umständen nicht verfügbar. Grundsätzlich muss auch hier sichergestellt werden, dass von der Organisation/Community (oder einem offiziell durch diese eingesetzten Dritten) für das betroffene Produkt ein umfassendes Sicherheitsschwachstellen-Management betrieben wird, welches die oben genannten Kriterien erfüllt und als zuverlässig etabliert gilt.

Motivation: Hardware- und Software-Produkte, für die kein vollumfassender Sicherheitsschwachstellen-Support durch den Hersteller besteht, stellen ein Risiko dar. Dies bedeutet, dass ein Produkt nicht ausreichend auf eine Betroffenheit durch weiterentwickelte Angriffsformen oder neu entdeckte Schwächen technischer Umsetzungen geprüft wird. Analog werden bei vorhandenen Sicherheitsschwachstellen in einem Produkt keine Nachbesserungen (z. B. Updates, Patches) bereitgestellt. Hieraus resultiert ein System, dessen Schwachstellen nicht behoben werden können, so dass sie für einen Angreifer ausnutzbar bleiben, um das System zu kompromittieren oder es negativ zu beeinträchtigen.

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: 3.01-1/9.0

4.2. Grundlegende Systemhärtung

Req 46	Auf dem System darf ausschließlich nur benötigte Software eingesetzt werden.
--------	--

In den Hersteller-seitig bereitgestellten Installationsroutinen für Software sind oftmals Komponenten oder einzelne Bestandteile der Software als Standard-Installation vorausgewählt, die für den Betrieb und die Funktion eines spezifischen Systems nicht notwendig sind. Hierzu zählen auch Teile einer Software, die als Anwendungsbeispiele (z. B. Default-Web-Seiten, Beispieldatenbanken, Testdaten) mit installiert, aber typischerweise im Anschluss nicht verwendet werden.

Solche Komponenten müssen bei der Installation des Systems gezielt abgewählt (nicht mit installiert) werden oder - falls eine Abwahl während der Installation nicht möglich ist - unmittelbar im Anschluss entfernt werden.

Des Weiteren darf grundsätzlich keine Software auf einem System eingesetzt sein, die für den Betrieb, die Wartung oder die Funktion des Systems nicht erforderlich ist.

Motivation: Schwachstellen in der Software eines Systems sind Einfallstore für Angreifer. Durch die Deinstallation nicht benötigter Komponenten können die potentiellen Angriffsflächen deutlich reduziert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-3/9.0

Req 47 Nicht benötigte Funktionen in der eingesetzten Software und Hardware müssen deaktiviert werden.

Während der initialen Installation von Software können zunächst Funktionen standardmäßig aktiviert worden sein, die für den Betrieb und die Funktionalität des konkreten Systems nicht notwendig sind. Funktionen sind meistens ein fester Bestandteil der Software, der nicht einzeln gelöscht oder deinstalliert werden kann.

Solche Funktionen müssen unmittelbar nach der initialen Installation über die Konfigurationseinstellungen der Software deaktiviert werden, so dass sie auch nach einem Neustart des Systems dauerhaft deaktiviert bleiben.

Bereits vor der Auslieferung oder während der initialen Inbetriebnahme sind möglicherweise auch in der Hardware zunächst Funktionen standardmäßig aktiviert worden, die für den Einsatz des konkreten Systems nicht benötigt werden. Solche Funktionen, wie beispielsweise nicht benötigte Schnittstellen, müssen ebenfalls unmittelbar nach der initialen Inbetriebnahme dauerhaft deaktiviert werden.

Motivation: Die Hardware oder Software eines Systems enthält oft aktivierte Funktionen, die nicht genutzt werden. Solche Funktionen können eine unnötige Angriffsfläche für Manipulationen darstellen. Des Weiteren entsteht darüber ein Potential, dass unautorisiert auf Bereiche oder Daten des Systems zugegriffen werden kann.

Umsetzungsbeispiel: [Beispiel 1]

Deaktivierung von Debugging-Funktionen in einer Software, die im Falle der Entstörung genutzt werden, aber während des normalen Betriebs nicht aktiv sein müssen.

[Beispiel 2]

Deaktivierung von ungenutzten Netzwerk-Schnittstellen eines Servers.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-4/9.0

Req 48 Nicht benötigte Dienste müssen deaktiviert werden.

Nach der Installation von Systemen und Softwareprodukten sind häufig herstellerseitig voreingestellte, lokale oder aus dem Netz erreichbare Dienste aktiv, die für den Betrieb und die Funktionalität des konkreten Systems im vorgesehenen Einsatzumfeld nicht erforderlich sind.

Auf einem System dürfen jedoch grundsätzlich nur die tatsächlich benötigten Dienste aktiv sein.

Entsprechend müssen unmittelbar nach der Installation sämtliche auf einem System nicht erforderliche Dienste vollständig deaktiviert werden. Es muss sichergestellt werden, dass diese Dienste auch nach einem Neustart des Systems weiterhin deaktiviert bleiben.

Motivation: Aktive Dienste, die nicht benötigt werden, vergrößern unnötig die Angriffsfläche eines Systems und in unmittelbarer Folge das Risiko einer erfolgreichen Kompromittierung. Dieses Risiko kann zusätzlich nochmals erhöht sein, falls - wie bei nicht benötigten Diensten häufig beobachtet - eine gezielte Betrachtung und Optimierung der Konfiguration hinsichtlich Sicherheit nicht ausreichend stattfindet.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-5/9.0

Req 49 Die Erreichbarkeit von aktivierten Diensten muss eingeschränkt werden.

Ein bereitgestellter Dienst muss grundsätzlich auf allen Schnittstellen des Systems vollständig deaktiviert werden, über die eine Erreichbarkeit des Dienstes für den ordnungsgemäßen Betrieb des Systems nicht erforderlich ist. Die Deaktivierung ist primär durch eine entsprechende Konfiguration des Dienstes bzw. Betriebssystems umzusetzen. In Fällen, in denen die zu Verfügung stehenden Konfigurationsoptionen eine Deaktivierung auf einzelnen Schnittstellen nicht ermöglichen, darf stattdessen auch ein lokaler Filter ("Host Firewall") auf dem System eingesetzt werden, um Zugriffe auf den Dienst über nicht erforderliche Schnittstellen zu blockieren.

Die Erreichbarkeit eines Dienstes über die erforderlichen Schnittstellen muss zudem auf legitime Kommunikationspartner eingeschränkt werden. Die Einschränkung ist durch eine entsprechende Konfiguration des Dienstes bzw. Betriebssystems oder mittels eines lokalen Filters ("Host Firewall") umzusetzen. Alternativ darf diese Aufgabe an ein netzseitiges Filterelement ausgelagert werden, sofern sich das System in einem separaten Netzwerk-Segment befindet und die Kommunikation mit diesem Segment ausschließlich über das netzseitige Filterelement möglich ist.

Motivation: Mittels Deaktivierung von Diensten auf Schnittstellen, über die eine Erreichbarkeit nicht notwendig ist, sowie durch die Einschränkung möglicher Kommunikationspartner, kann die Angriffsfläche, die ein System bietet, stark reduziert werden.

Umsetzungsbeispiel: Ein SNMP-Dienst, über den ein System gemonitort wird, ist ausschließlich auf der dedizierten Management-Netzwerk-Schnittstelle des Systems aktiviert. Über eine Firewall ist zusätzlich reglementiert, dass einzig das legitime Monitoring System der Infrastruktur-Umgebung diesen Dienst erreichen kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-6/9.0

Req 50 Vordefinierte, nicht benötigte Benutzerkonten müssen gelöscht oder zumindest deaktiviert werden.

Auf vielen Systemen existieren nach der initialen Installation vordefinierte, aber nicht genutzte Benutzerkonten (z. B. "Gast").

Diese vordefinierten Benutzerkonten müssen unmittelbar nach der initialen Installation gelöscht oder zumindest deaktiviert werden; sollten diese Maßnahmen nicht umsetzbar sein, muss das entsprechende Benutzerkonto für einen Fernzugriff gesperrt werden. In jedem Fall müssen auch deaktivierte oder gesperrte Benutzerkonten mit einem Authentisierungsmerkmal (z. B. einem Passwort oder einem SSH Key) versehen werden, so dass im Fall einer Fehlkonfiguration die unberechtigte Nutzung eines solchen Benutzerkontos verhindert wird.

Ausgenommen von der Anforderung, vordefinierte Benutzerkonten zu löschen oder zu deaktivieren, sind Benutzerkonten, die ausschließlich der internen Nutzung auf dem entsprechenden System dienen und die für die Funktionali-

tät einer oder mehrerer Anwendungen des Systems notwendig sind. Auch für ein solches Benutzerkonto muss sichergestellt werden, dass ein Fernzugriff oder eine lokale Anmeldung nicht möglich ist und dass ein Benutzer des Systems ein solches Benutzerkonto nicht missbräuchlich nutzen kann.

Motivation: In einem Produkt standardmäßig vordefinierte Benutzerkonten sind typischerweise allgemein bekannt und können von einem Angreifer sehr gezielt für Brute-Force- und Wörterbuchangriffe ausgewählt werden. Werden diese Benutzerkonten in einem konkreten System gar nicht benötigt, stellt deren Existenz dann eine unnötige Angriffsfläche dar. Ein besonderes Risiko stellen vordefinierte Benutzerkonten dar, die ohne Passwort oder mit einem weithin bekannten Standardpasswort vorkonfiguriert sind. Solche Benutzerkonten können unmittelbar von einem Angreifer missbraucht werden, falls ihre Absicherung aufgrund der nicht weiter vorgesehenen Nutzung im konkreten System versäumt wurde.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-7/9.0

Req 51	Bekannte Schwachstellen in der Software oder Hardware des Systems müssen behoben oder gegen Missbrauch abgesichert werden.
--------	--

Bekannte Schwachstellen in Software- und Hardware Komponenten müssen mittels Installation von verfügbaren Systemaktualisierungen des Herstellers (z. B. Patches, Updates/Upgrades) behoben werden. Alternativ ist der Einsatz von Workarounds (Akut-Lösungen, welche die Schwachstelle nicht beheben, aber die Ausnutzung wirksam verhindern) zulässig. Workarounds sollten grundlegend nur temporär Verwendung finden und sobald möglich durch eine reguläre Systemaktualisierung ersetzt werden, um die Schwachstellen vollständig zu schließen.

Komponenten, die bekannte, nicht behebbare Schwachstellen enthalten, dürfen in einem System nicht eingesetzt werden.

Die Behandlung von neu bekannt werdenden Schwachstellen muss zudem für die gesamte Einsatzphase des Systems fortlaufend sichergestellt und in den kontinuierlichen Betriebsprozessen eines Security Patch Managements umgesetzt werden.

Motivation: Der Einsatz von Komponenten ohne eine Behebung enthaltener Schwachstellen erhöht deutlich das Risiko einer erfolgreichen Kompromittierung. Der Angreifer wird zusätzlich dadurch begünstigt, dass i. d. R. nicht nur detaillierte Informationen zu bereits bekannt gewordenen Schwachstellen offen verfügbar sind, sondern oft auch bereits angepasste Angriffswerkzeuge, die eine aktive Ausnutzung erleichtern.

Umsetzungsbeispiel: Im Anschluss an die initiale Installation eines Betriebssystems von einem offiziellen Installationsmedium werden alle aktuell verfügbaren Patches und Sicherheits-Updates eingespielt.

Zusätzliche Informationen:

Primäre Quellen für bereits bekannt gewordene Schwachstellen in einer Software/Hardware sind Auflistungen in den Versionshinweisen sowie die Sicherheitshinweise aus den offiziellen Meldekanälen des Herstellers oder unabhängiger CERTs. Insbesondere die Meldekanäle werden sinnvollerweise fest in kontinuierliche Prozesse des Security Patch Managements für ein System eingebunden, damit neu bekanntwerdende Schwachstellen zeitnah registriert und in operative Behebungsmaßnahmen geführt werden können.

Als ergänzende Maßnahme zur Aufdeckung von potenziell noch enthaltenen, grundsätzlich bereits bekannt gewordenen Arten von Schwachstellen können gezielte Schwachstellenuntersuchungen des Systems durchgeführt werden. Zu diesem Zweck eignen sich besonders spezialisierte Werkzeuge wie automatisierte Schwachstellen-Scanner. Beispiele hierfür sind: Tenable Nessus, Qualys Scanner Appliance.

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: 3.01-10/9.0

4.3. Schutz der Verfügbarkeit und Integrität

Req 52 Das System muss vor Überlastsituationen geschützt werden.

Ein System muss über Schutzmechanismen verfügen, die Überlastsituationen so weit wie möglich verhindern. Insbesondere ist eine partielle oder komplette Beeinträchtigung der Verfügbarkeit des Systems zu vermeiden.

Beispiele für mögliche Schutzmaßnahmen sind:

- Begrenzung des pro Anwendung verfügbaren Arbeitsspeichers (RAM)
- Begrenzung der maximalen Sessions einer Web-Anwendung
- Begrenzung der maximalen Größe eines Datensatzes
- Begrenzung von CPU-Ressourcen pro Prozess
- Priorisieren von Prozessen
- Begrenzung der Anzahl oder der Größe von Transaktionen eines Benutzers oder von einer IP-Adresse in einem bestimmten Zeitraum

Anmerkung:

vor Netzwerk-basierenden Angriffen mit extrem hohen Daten- oder Paketraten, den sogenannten "Distributed Denial of Service" (DDoS) Angriffen, kann ein System sich i. d. R. selbst nicht mehr schützen. Zur Abwehr von DDoS Angriffen wird eine vorgelagerte Lösung in der Netzwerk-Schicht benötigt.

Motivation: Angreifer können mit gezielten ressourcenlastigen oder großvolumigen Anfragen versuchen, die Ressourcen eines Systems aufzubrauchen, so dass das System seine regulären Aufgaben bzw. vorgesehenen Aufgabenvolumen nicht mehr erfüllen kann und die Verfügbarkeit der angebotenen Dienste effektiv gestört ist. Die Begrenzung der Ressourcen, die je gestellter Anfrage an das System maximal in Anspruch genommen werden können, ist eine grundlegende Maßnahme, um die Auswirkungen solcher Denial-of-Service (DoS) Angriffe zu reduzieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.01-12/9.0

Req 53 In Überlastsituationen muss sich das System berechenbar verhalten.

Selbst umfassende systemeigene Schutzmaßnahmen können in extremen Situationen möglicherweise nicht mehr verhindern, dass ein System in eine Überlastsituation gerät.

Es muss daher sichergestellt sein, dass das System in Überlastsituationen nicht in einen Zustand überwechselt, der sicherheitsrelevante Funktionen oder Eigenschaften des Systems außer Kraft setzt. Leistungseinbußen (bspw. die Verringerung des Durchsatzes von legitimen Netzwerk-Paketen oder der Anzahl beantworteter Server-Anfragen pro Zeitraum) sind in Überlastsituationen i. d. R. nicht vermeidbar, das reguläre funktionale Verhalten des Systems muss jedoch grundlegend erhalten bleiben.

Dies kann im Extremfall bedeuten, dass ein kontrolliertes Herunterfahren des Systems eher hinnehmbar ist, als ein Weiterbetrieb bei unkontrolliertem Versagen der Sicherheitsfunktionen und somit dem Verlust des Systemschutzes.

Motivation: Mittels eines Denial-of-Service-Angriffs kann ein Angreifer versuchen, ein System gezielt zu überlasten. Reagiert ein solches System dann unberechenbar oder versagt sein reguläres Verhalten, insbesondere hinsichtlich dessen Sicherheitsfunktionen, kann dies dem Angreifer eine erweiterte Angriffsfläche auf Funktionen und Daten des

Systems eröffnen sowie potentiell weitere verknüpfte Systeme gefährden.

Umsetzungsbeispiel: Eine Firewall, die in Überlastsituationen ihr Filter-Regelwerk verwirft und sämtliche Pakete ohne Prüfung weiterleitet, würde die Anforderung nicht erfüllen. In diesem Fall wäre das Blockieren sämtlicher Pakete durch die Abschaltung der Firewall eher hinnehmbar als das Versagen ihrer regulär vorgesehenen Schutzaufgabe für nachgelagerte Systeme.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-13/9.0

4.4. Schutz von Daten und Informationen

Req 54	Schutzbedürftige Daten müssen während der Übertragung vor nicht autorisierter Einsichtnahme und Veränderung geschützt werden.
--------	---

Der Schutzbedarf von zu übertragenden Daten ist abhängig von deren Einstufung (beispielsweise nach geltenden gesetzlichen Datenschutzvorgaben, regulatorischen Auflagen, vertraglichen Verpflichtungen), dem Schadenspotential bei deren Missbrauch, sowie weiteren relevanten Faktoren (beispielsweise der Übertragung über öffentliche Netze). Art und Umfang der Schutzmaßnahmen müssen entsprechend angemessen gewählt werden.

Authentisierungsmerkmale wie beispielsweise Passwörter oder Tokens gelten grundsätzlich als schutzbedürftige Daten. Ebenfalls grundsätzlich als schutzbedürftig gelten Daten, die Funktionalität und sicherheitsrelevantes Verhalten eines Systems bestimmen (z. B. Updates & Patches, Konfigurationsparameter, Fernwartungen, Steuerung über APIs).

Die Einhaltung der Schutzziele Vertraulichkeit und Integrität muss während der Übertragung von schutzbedürftigen Daten durchgängig gewährleistet werden.

I.d.R. erfordert dies eine Implementation von kryptografischen Verfahren (z. B. Verschlüsselung, Signaturen, Hashes). Kryptografische Verfahren können

- vor der Übertragung direkt auf die Daten angewendet werden, was eine anschließende Übertragung der Daten auch über unsichere Kanäle vertretbar machen kann
- auf dem Übertragungs-Kanal eingesetzt sein, um einen sicheren Kanal zu schaffen und beliebige Daten, die durch diesen geleitet werden, zu schützen
- oder auch als Kombination aus beidem umgesetzt sein.

Bei der Übertragung von Daten eingesetzte kryptografische Verfahren müssen für diesen Zweck anerkannt wirksam sein und dürfen keine bekannten Schwachstellen aufweisen.

Motivation: Die Übertragung von Daten ohne einen adäquaten Schutz ermöglicht es einem Angreifer, diese unberechtigt abzufangen, zu nutzen, zu verbreiten, zu verändern oder aus der Übertragung zu entfernen. Dies eröffnet potenziell weitere Angriffsvektoren auf die unmittelbaren Zielsysteme sowie angeschlossene weitere Systeme und kann zu erheblichen Ausfällen, Kontrollverlusten und Schäden sowie resultierenden Strafzahlungsforderungen und Reputationsverlusten gegenüber Kunden und Geschäftspartnern führen.

Umsetzungsbeispiel: [Beispiel 1]

Vertrauliche Dokumente werden vor dem Versand per E-Mail an den Kunden verschlüsselt.

[Beispiel 2]

Ein Administrator konfiguriert eine neue Cloud-Anwendung über das Internet. Der Zugriff erfolgt über eine TLS-verschlüsselte Verbindung ("https").

[Beispiel 3]

Ein System bezieht automatische Software-Updates von einem Update-Server. Der Update-Server liefert die Software Updates kryptografisch signiert aus. Das System kann die empfangenen Software-Updates somit validieren und sicher ausschließen, dass diese während der Übertragung manipuliert wurden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-15/9.0

4.5. Schutz von Sitzungen

Req 55 Sitzungen müssen gegen eine unautorisierte Übernahme ("Session Hijacking") geschützt werden.

In Schnittstellen, die Funktionen für Sitzungen zum System bereitstellen, müssen technische Maßnahmen implementiert werden, die verhindern, dass die Sitzung eines legitimen Benutzers von einem nicht autorisierten Dritten übernommen und weitergeführt werden kann.

Ein derartiger Schutz kann beispielsweise durch die Umsetzung einer für das spezifische System sinnvollen Kombination aus den folgenden Optionen erreicht werden:

- Auf der Transportschicht: Verwendung des TCP-Protokolls (mit dessen Sequenz-Nummern) und entsprechenden Filterlisten
- Auf der Sitzungsschicht: Verwendung des TLS-Protokolls
- Auf der Applikationsschicht: Aushandlung eines zufälligen geheimen Sitzungsschlüssels zwischen Sender und Empfänger zwecks Autorisierung allen Sitzungsverkehrs (z. B. Session-ID, Session Cookie, Session Token)
- Nutzung kryptographischer Verfahren zum Schutz von Sitzungsschlüsseln vor Ausspähung oder Veränderung

Motivation: Ungeschützte Sitzungen können potenziell von einem Angreifer gekapert und weitergeführt werden, um darüber im Kontext des betroffenen Benutzers unberechtigte Zugriffe auf das System auszuüben.

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: 3.01-16/9.0

Req 56 Das System muss es Benutzern ermöglichen, sich von ihrer laufenden Sitzung abzumelden.

Das System muss über eine Funktion verfügen, die es dem angemeldeten Benutzer ermöglicht, sich jederzeit abzumelden. Die Wiederaufnahme einer abgemeldeten Sitzung darf nicht ohne erneute und erfolgreiche Authentifizierung des Benutzers möglich sein.

Motivation: Ein Benutzer muss die vollständige Kontrolle über von ihm aufgebaute Sitzungen behalten, um jederzeit situationsgerecht seinen Zugriff auf ein System zu beenden und damit über diesen Zugriff exponierte Daten und Funktionen schützen zu können. Zudem muss der Benutzer davon ausgehen können, dass durch ihn gezielt beendete Sitzungen nicht im Anschluss durch unberechtigte Dritte wieder aufgenommen und weitergeführt 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

ID: 3.01-17/9.0

Req 57	Sitzungen müssen nach einer dem Verwendungszweck angepassten Zeit der Inaktivität automatisch beendet werden.
--------	---

Es ist notwendig, dass Sitzungen auf einem System nach einer vorgegebenen Zeit der Inaktivität automatisch beendet werden.

Aus diesem Grund muss ein Time-Out für Sitzungen gesetzt werden. Der hier zu wählende Zeitraum richtet sich nach der Verwendung des Systems und ggf. nach der physischen Umgebung. So ist beispielsweise der Time-Out für eine Anwendung, die in einer ungesicherten Umgebung genutzt wird, kürzer (wenige Minuten) zu wählen als der Time-Out für eine Anwendung, die von Betriebsmitarbeitern für System-Monitoring-Aufgaben in einem zugangsgeschützten Bereich genutzt wird (60 Minuten und länger).

Motivation: Für eine offene, aber ungenutzte Sitzung besteht ein Risiko, dass ein nicht legitimer Benutzer diese unbemerkt übernimmt und weiterführt, um im Namen des betroffenen Benutzers einen nicht autorisierten Zugriff auf das System und enthaltene Daten auszuüben.

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: 3.01-18/9.0

4.6. Authentifizierung und Autorisierung

Req 58	Die Berechtigungen von Benutzern und Anwendungen müssen auf den zur Erfüllung ihrer Aufgaben benötigten Umfang beschränkt werden.
--------	---

Die Berechtigungen auf einem System müssen so weit eingeschränkt werden, dass ein Benutzer nur auf Daten zugreifen und Funktionen nutzen kann, die er im Rahmen seiner Arbeit benötigt. Entsprechende Berechtigungen sind auch für den Zugriff auf Dateien zu vergeben, die Bestandteil des Betriebssystems oder von Anwendungen sind oder von diesen erzeugt werden (z. B. Konfigurations- und Protokollierungsdateien).

Neben dem Zugriff auf Daten muss auch die Ausführung von Anwendungen und deren Bestandteilen mit möglichst niedrigen Berechtigungen erfolgen. Anwendungen sollten nicht mit Administrator- oder Systemberechtigungen ausgeführt werden.

Motivation: Werden einem Benutzer zu weitreichende Berechtigungen auf einem System gewährt, kann er in einem Umfang auf Daten und Anwendungen zugreifen, der zur Erfüllung der zugewiesenen Aufgaben nicht erforderlich ist. Dies erzeugt ein unnötig erhöhtes Risiko im Falle eines Missbrauchs, insbesondere auch, falls der Benutzer oder dessen Benutzerkonto durch einen Angreifer kompromittiert werden.

Anwendungen, die über zu weitreichende Berechtigungen verfügen, können von einem Angreifer missbraucht werden, um unbefugte Zugänge zu erhalten oder zu erweitern und damit einen Zugriff auf schutzbedürftige Daten und Systembereiche zu erlangen.

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

4.7. Protokollierung

Req 59 Die Systemzeit muss zu einer exakten Referenzzeit (Zeitnormal) synchronisiert werden.

Als Zeitnormal ist eine Zeitgeber-Quelle heranzuziehen, die ein Zeitsignal auf Basis der koordinierten Weltzeit ("UTC" = "Universal Time Coordinated") liefert.

Anmerkung: die anhand der Zeitgeber-Quelle zu UTC synchronisierte Systemzeit darf auf dem lokalen System mittels entsprechender Zeitzone-Konfiguration bei der Ausgabe von Zeitinformationen in die Ortszeit transformiert werden, sofern die so stattfindende Zeitzoneanpassung eindeutig erkennbar und nachvollziehbar ist.

Systeme, die zu einer gemeinsamen Sicherheits-Domäne gehören, müssen sich einheitlich an derselben Zeitgeber-Quelle synchronisieren.

Motivation: Zeitsynchronisation kann auf einem System eine technische Voraussetzung sein, um zeitkritische Abhängigkeiten in beispielsweise der Nutzung von Zertifikaten oder Authentisierungsmechanismen korrekt bedienen zu können. Dringend erforderlich sind außerdem exakte Zeitstempel in Protokollierungseinträgen, damit diese bei Sicherheitsvorfällen oder Problemanalysen in eindeutiger zeitlicher Relation auswertbar sind.

Umsetzungsbeispiel: Einige zulässige Zeitgeber-Quellen:

- vertrauenswürdige eingestufte NTP ("NetworkTimeProtocol") Server im IP-Netzwerk
- DCF77-Funksignal über physisch angebundenes Empfängermodul
- GPS-Funksignal über physisch angebundenes Empfängermodul

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-32/9.0

Req 60 Sicherheitsrelevante Protokollierungsdaten müssen echtzeitnah an eine Erkennungs- und Reaktionslösung für Sicherheitsvorfälle bereitgestellt werden.

Eine zulässige Erkennungs- und Reaktionslösung im Sinne dieser Anforderung muss die folgenden Kriterien erfüllen:

- Es erfolgt eine kontinuierliche Analyse bzw. Korrelation der aus angebundenen IT/NT-Systemen bereitgestellten Protokollierungsdaten.
- Die Identifizierung bedrohlicher Aktivitäten und laufender Angriffe findet auf Basis einer fortlaufend aktuell gehaltenen Erkennungsmuster-Datenbank statt.
- Integrierte Alarmierungsprozesse lösen im Fall eines Fundes die Einleitung von Gegenmaßnahmen aus.
- Sicherheitsexperten sind aktiv involviert in den Betrieb der Lösung sowie die Auswertung von Alarmen.

Eine solche Lösung ist in ihrer Funktion nicht mit einem Log Server gleichzusetzen. Entsprechend muss die Bereitstellung an eine Erkennungs- und Reaktionslösung stets zusätzlich zu einer vorhandenen Weiterleitung an einen Log Server erfolgen. Eine Ausnahme besteht, falls der genutzte Log Server seinerseits die Protokollierungsdaten umgehend nach Erhalt zusätzlich an eine Erkennungs- und Reaktionslösung bereitstellt. In diesem Fall ist es ausreichend, dass das System die Protokollierungsdaten nur an den Log Server weiterleitet.

Die Protokollierungsdaten müssen ab dem Zeitpunkt ihrer Erzeugung im System innerhalb von 5 Minuten an die Erkennungs- und Reaktionslösung bereitgestellt werden ("echtzeitnah").

Die konkret zu unterstützenden technischen Schnittstellen und Protokolle für die Bereitstellung werden durch die im Einsatzumfeld des Systems verfügbare Erkennungs- und Reaktionslösung sowie die technische Basis des Systems

bestimmt.

Motivation: IT/NT-Systeme sind permanent sicherheitstechnischen Bedrohungen und Angriffen ausgesetzt. Mittels einer zentralen Analyse und der Korrelation erfasster System-Ereignisse ganzer IT-Landschaften in nahezu Echtzeit können aktuelle Bedrohungen und laufende Angriffe auch über Systemgrenzen hinaus erkannt und zeitnah passende Gegenmaßnahmen eingeleitet werden. Die unverzügerte Bereitstellung von Protokollierungsdaten an die Erkennungs- und Reaktionslösung ist essenziell für deren Effektivität.

Umsetzungsbeispiel: **Beispiel 1:** Ein System auf Basis eines klassischen Servers erfasst sicherheitsrelevante Protokollierungsdaten im lokalen Syslog oder Windows Event Log des Betriebssystems. Die Protokollierungsdaten werden kontinuierlich zur weiteren Analyse, Angriffserkennung und Alarmbehandlung an ein SIEM (Security Information and Event Management) weitergeleitet.

Beispiel 2: Auf einem System wird ein EDR ("Endpoint Detection and Response") Agent ausgeführt. Der EDR-Agent leitet die von ihm auf dem System erfassten sicherheitsrelevanten Protokollierungsdaten kontinuierlich an das zentrale Backend der EDR-Lösung aus, auf dem die weitere Analyse, Angriffserkennung und Alarmbehandlung erfolgt.

Beispiel 3: Netzwerk-Komponenten stellen Ereignisse an ein SIEM bereit, die es ermöglichen, verdächtiges Kommunikationsverhalten wie Netzwerk-Scans, unzulässige Datenflüsse zwischen Netz-Segmenten oder aktive Verbindungen bzw. Verbindungsversuche zu verdächtigen Zielen im Internet zu entdecken. Im speziellen liefern Gateway Router aus dem CNDTAG "Netflow" Logs, während Forward Proxies Zugriffe auf Domänen und/oder IP-Adressen melden und Firewalls blockierte Verbindungsversuche loggen.

Beispiel 4: Auf Basis von Cloud-nativen Funktionen entwickelte Systeme erzeugen Protokollierungsdaten mittels der Cloud-eigenen Protokollierungs- und Überwachungsinfrastruktur direkt aus diesen Funktionen heraus. In einem solchen System wird die Erzeugung sicherheitsrelevanter Protokollierungsdaten in den entsprechenden Konfigurationsoptionen der eingesetzten Cloud-nativen Funktionen gezielt aktiviert. Die entstehenden Protokollierungsdaten werden kontinuierlich zur weiteren Analyse, Angriffserkennung und Alarmbehandlung an ein SIEM (Security Information and Event Management) übertragen. Einige Cloud-Anbieter leisten eine gewisse Angriffsmustererkennung bereits in der Cloud-eigenen Überwachungsinfrastruktur und erzeugen daraus spezifische Cloud-Alarme. Diese werden zusätzlich an das SIEM übertragen.

Beispiel 5: Ein System basiert auf einer SaaS ("Software as a Service") Applikation eines Cloud-Anbieters. Typischerweise verantwortet im SaaS Modell der Cloud-Anbieter alle operativen Aspekte der Applikation, inkl. des Sicherheitsmanagements. Der Cloud-Kunde selbst hat keinen Einfluss auf die zugrunde liegende technische Infrastruktur oder den Betrieb der Applikation. Anhand von Vertragsvereinbarungen, anerkannten Zertifikaten und dokumentierten Selbstauskünften des Cloud-Anbieters wird formell überprüft, dass der Cloud-Anbieter eine Erkennungs- und Reaktionslösung für Sicherheitsvorfälle implementiert hat. Einige Cloud-Anbieter erzeugen zusätzlich dedizierte Protokollierungsdaten über sicherheitsrelevante Aktivitäten innerhalb der separaten Kunden-Mandanten ihrer SaaS Applikation (beispielsweise zu Änderungen von Konfigurationseinstellungen, Berechtigungsvergaben oder Benutzer-Konten innerhalb der Mandanten) und stellen diese den Cloud-Kunden zu Verfügung. Diese sogenannten Audit-Logs werden kontinuierlich zur weiteren Analyse, Angriffserkennung und Alarmbehandlung an ein SIEM (Security Information and Event Management) übertragen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

ID: 3.01-37/9.0