

Leistungsbeschreibung Rahmenvertrag Sicherheitsanalysen

Anlage 1 zum Rahmenvertrag
(Vergabe-Nr. 2026-0040)

Version: 1
Stand: 19.05.2026

Inhaltsverzeichnis

| | |
|--|-----------|
| Inhaltsverzeichnis | 2 |
| 1 Rahmenbedingungen und Überblick..... | 3 |
| 1.1 Überblick über die Telematikinfrastruktur | 3 |
| 1.2 Ausgangssituation | 3 |
| 2 Leistungsumfang | 4 |
| 2.1 Leistungsportfolio..... | 4 |
| 2.2 Ad-hoc-Sicherheitsanalysen | 4 |
| 2.3 Anforderungen | 5 |
| 2.4 Vorgaben für Einzelaabrufe..... | 6 |
| 2.5 Mengengerüst | 7 |
| 2.6 Schätz- und Höchstwert..... | 7 |
| 3 Beistellungen/Mitwirkungen..... | 8 |
| 4 Rahmenbedingungen der Leistungserbringung | 9 |
| 4.1 Zeitplanung | 9 |
| 4.2 Technische Rahmenbedingungen | 9 |
| 4.3 Organisatorische und räumliche Rahmenbedingungen | 9 |
| Anhang A – Verzeichnisse..... | 10 |
| A1 – Abbildungsverzeichnis | 10 |
| A2 – Tabellenverzeichnis | 10 |
| A3 – Referenzierte Dokumente | 10 |
| Anhang B Anforderungskatalog | 11 |
| A4 – Definition Senioritätsstufen der Analysten | 11 |
| A5 – Felder CSV-Datei..... | 12 |
| A6 – Feststellungskategorie | 13 |

1 Rahmenbedingungen und Überblick

1.1 Überblick über die Telematikinfrastruktur

Die Digitalisierung wird das Gesundheitswesen künftig weiter und nachhaltig verändern.

Die Erfassung, Verarbeitung und Nutzung medizinischer Daten beflügelt die Forschung, revolutioniert Therapien und sorgt dafür, dass wir individueller und besser versorgt werden können. Diesen Prozess in Deutschland entschlossen voranzutreiben und konstruktiv mitzugestalten, ist Ziel, Aufgabe und Mission der gematik.

Die gematik trägt die Gesamtverantwortung für die Telematikinfrastruktur (TI), die zentrale Plattform für digitale Anwendungen im deutschen Gesundheitswesen. Mit der Definition und Durchsetzung verbindlicher Standards für Dienste, Komponenten und Anwendungen in der TI gewährleistet die gematik, dass diese zentrale Infrastruktur sicher, leistungsfähig und nutzerfreundlich ist und bleibt.

Die Arbeit der gematik als Digitalagentur Gesundheit reicht weit über Landesgrenzen hinaus – für die beste medizinische Versorgung der Menschen kooperiert sie international mit e-Health-Kompetenzzentren anderer Länder. Sie ist Kompetenzzentrum für Interoperabilität im Gesundheitswesen (KIG) und versteht sich dabei nicht nur als Prüferin und Standardgeberin, sondern auch als Vermittlerin, Moderatorin und Beraterin.

Gemäß § 311 Abs. 1 SGB V hat die gematik Vorgaben für den sicheren Betrieb der Telematikinfrastruktur zu erstellen und ihre Umsetzung zu überwachen, um ein hohes Sicherheitsniveau für die Telematikinfrastruktur (TI) im laufenden Betrieb zu gewährleisten. Außerdem hat die gematik nach den §§ 329 ff. SGB V umfangreiche Pflichten zur Überwachung der Funktionsfähigkeit und Sicherheit der TI.

1.2 Ausgangssituation

Im Rahmen dieser gesetzlichen Verantwortung lässt die gematik seit Jahren regelmäßig sogenannte Sicherheitsanalysen durch externe Dienstleister in Form von Penetrationstests durchführen, um die Sicherheit von Komponenten der TI bei Anbietern und Herstellern aus Angreifersicht zu überprüfen, potenzielle Schwachstellen zu ermitteln und damit kontinuierlich die Sicherheit in der TI zu verbessern.

Ziel ist es, weiterhin regelmäßig Sicherheitsanalysen von TI-Anwendungen, TI-Diensten und gematik-Plattformen in Form von Penetrationstests (die den überwiegenden Anteil darstellen) und Konzeptanalysen (die den geringeren Anteil darstellen) durch externe Experten durchführen zu lassen. Dabei sollen Produkte wie beispielsweise die Frontends der Versicherten (FdV) der elektronischen Patientenakte (ePA) und des E-Rezepts, die ePA- und E-Rezept-Fachdienste, der TI-Messenger, der Proof of Patient Presence (PoPP) und die Zero-Trust-Architektur der TI 2.0 auf potentielle Angriffs- und Manipulationsmöglichkeiten hin geprüft werden.

Aufgrund der Vielzahl an Sicherheitsanalysen sowie der damit verbundenen regelmäßigen Leistungen ist der Abschluss eines Rahmenvertrags erforderlich, über den die Sicherheitsanalysen per Einzelabruf beauftragt werden können.

2 Leistungsumfang

2.1 Leistungsportfolio

Die Durchführung der Sicherheitsanalysen umfasst grundsätzlich folgende Leistungen:

- Nach Abruf/Ankündigung einer Sicherheitsanalyse, i. d. R. mit einem Vorlauf von mindestens vier Wochen, Teilnahme an Vorbereitungsgesprächen (mit der gematik) und Kick-off-Meetings (mit der gematik sowie Anbietern/Herstellern) zur Konkretisierung des jeweiligen Prüfumfangs,
- Konzeption der jeweiligen Sicherheitsanalyse,
 - unter Berücksichtigung geeigneter Analyse-Werkzeuge sowie bei Bedarf inkl. Toolentwicklung und Übergabe und Übereignung des Tools an den Auftraggeber,
- Durchführung von Sicherheitsanalysen in Form von Penetrationstests (White-, Grey- und Blackbox) und/oder konzeptionellen Analysen von TI-Anwendungen, TI-Diensten und gematik-Plattformen, die grundsätzlich folgenden Testumfang vorsehen:
 - Überprüfung durch sinnvolle und geeignete Tests, ob die Sicherheit der TI-Komponenten und der darüber bereitgestellten Leistungen den an die Implementierung gestellten Sicherheits- und Datenschutzanforderungen entsprechen,
 - Versuch des unbefugten Zugriffs und der Manipulation von Daten der TI-Komponenten (inkl. aller erreichbaren Schnittstellen) sowie der Darstellung, über welche Ressourcen ein Angreifer verfügen muss, um eine mögliche Schwachstelle ausnutzen zu können und welche Auswirkungen der Angriff haben kann,
 - Feststellung des Sicherheitsniveaus sowie der Abweichungen von Spezifikationen, BSI-Prüfvorschriften, OWASP Mobile App Security Checkliste inkl. Anti-Resiliency und OWASP-Top-10- Mobile-Risiken in den jeweils aktuellen Versionen (siehe Abschnitt A3 – Referenzierte Dokumente),
- umgehende Meldung von gravierenden Schwachstellen/Auffälligkeiten an die gematik,
- Durchführung von Ergebnispräsentationen und im Einzelfall von Workshops, z. B. zur Vorstellung eines eigens entwickelten Tools und
- Erstellung des Analyseberichts mit den nachvollziehbaren und reproduzierbaren Ergebnissen inkl. Eintrittsmöglichkeit/-wahrscheinlichkeit und Maßnahmenempfehlungen gemäß Ziffer 2.3 (Anforderungen)

2.2 Ad-hoc-Sicherheitsanalysen

Optional muss für den Auftraggeber die Möglichkeit bestehen, jährlich bis zu zwei Ad-hoc-Penetrationstests zu beauftragen. Ad-hoc-Penetrationstests unterscheiden sich von den regulären Sicherheitsanalysen lediglich im zeitlichen Vorlauf. Dieser liegt im Ad-hoc-Fall bei einer Woche, anstelle der üblichen vier Wochen und kann mit einem Preisaufschlag von 10 % durch den Auftragnehmer angeboten werden.

2.3 Anforderungen

☒ Anforderungskatalog für diese Leistungen im Anhang zu diesem Dokument

☒ Es bestehen folgende Anforderungen an die Leistungen (Leistungskatalog)

- Einsatz eines Analystenteams je Sicherheitsanalyse bestehend aus mindestens zwei Analysten (aus dem angebotenen Analysten-Pool), davon mindestens ein/e Senior-Analyst/in (eine Definition der Senioritätsstufen der Analysten ist im Anhang B aufgeführt),
- Koordination von Terminen mit den jeweils Beteiligten im Rahmen der Analyse-Durchführung, z. B. bei Rückfragen, ausstehenden Bereitstellungen (z. B. Referenzumgebung inkl. Zugänge) und kritischen Findings,
- Nutzung eigener Test-Hardware für alle gängigen Plattformen, wie Android und iOS bzw. für die Betriebssysteme Windows, MacOS und Linux,
- Ansprechbarkeit bei Rückfragen zu Analyseergebnissen – auch nach Analyse-Abschluss,
- Inhalte des Analyseberichts:
 - Projektüberblick und Analysezeitraum,
 - Nennung der Analysten,
 - Beschreibung der Vorgehensweise, eingesetzten Prüfmethoden und Werkzeuge sowie der Bewertungsmethodik,
 - Managementzusammenfassung mit
 - Aussage zum Sicherheitsniveau,
 - Fazit und
 - generelle Empfehlung,
 - Diagramm der identifizierten Schwachstellen dargestellt nach Schweregrad,
 - Übersicht aller geprüften Bereiche, d. h. inkl. Status über keine Befunde (Prozess-Evaluation ohne Feststellung),
 - Ergebnisse/Schwachstellen:
 - vollständige Beschreibung der einzelnen Schwachstellen inkl. Auswirkungen, Empfehlungen zur Behebung, Referenzen und Nachweisen kategorisiert nach Schweregrad und
 - tabellarische Zusammenfassung als CSV-Datei mit Feldern gemäß Tabelle 3 im Anhang B
- Bereitstellung des Analyseberichts in deutscher Sprache als Draftversion im MS-Word-Format und nach Freigabe durch den Auftraggeber im PDF-Format,
- Einverständnis des Auftragnehmers mit einer potenziellen Veröffentlichung des Prüfberichts und/oder von Teilen daraus einschließlich der Nennung der Firma des Auftragnehmers.

2.4 Vorgaben für Einzelabrufe

Der Auftraggeber wird über die Vertragslaufzeit die zu erbringenden Leistungen in Form von einzelnen, zeitlich abgegrenzten Aufträgen (Einzelabrufe) abrufen.

Grundsätzlich wird die gematik den jeweiligen Testbeginn mit einem Vorlauf von i. d. R. vier Wochen ankündigen.

Im darauffolgenden Kick-off-Meeting – werden der Testumfang, technische Prüfungsdetails und erforderliche Voraussetzungen besprochen. Vereinzelt findet im Bedarfsfall vor dem Kick-off-Meeting zwischen gematik und Auftragnehmer ein Vorbereitungsgespräch statt. Im Anschluss erstellt der Auftragnehmer eine konkrete Zeit- und Aufwandsplanung inkl. Kostenschätzung, die nach entsprechender Prüfung durch die gematik beauftragt werden kann.

Innerhalb der Woche vor dem eigentlichen Analysebeginn prüft der Auftragnehmer die erforderlichen Voraussetzungen, wie z. B. bereitgestellte Zugänge, um sicherzustellen, dass mit dem Analysebeginn die eigentliche Prüfung durchgeführt werden kann.

Sollten während der Analysedurchführung Probleme auftreten, die die Analysedurchführung behindern, oder gravierende Schwachstellen ermittelt werden, kümmert sich der Auftragnehmer um eine entsprechende Kommunikation mit den Beteiligten.

I. d. R. innerhalb einer Woche nach der Analysedurchführung stellt der Auftragnehmer die gefundenen Schwachstellen in einer Ergebnispräsentation vor.

Der Ergebnisbericht wird i. d. R. innerhalb von zehn (10) Werktagen nach der Ergebnispräsentation der gematik ausgehändigt.

Der Auftraggeber prüft den Bericht und gibt ihn frei, sofern die jeweiligen Anforderungen ausreichend betrachtet worden sind. Potenzielle Anpassungen/Nacharbeiten müssen zeitnah erfolgen.

Sobald der finale Bericht und ein Leistungsnachweis für die erbrachte Analyse vorliegen, erfolgt die Abnahmeerklärung der Leistung, so dass der Auftragnehmer die Rechnung stellen kann.

Die folgende Abbildung skizziert den Prozessablauf sowie die zeitlichen Vorgaben für den Einzelabruf einer Sicherheitsanalyse.

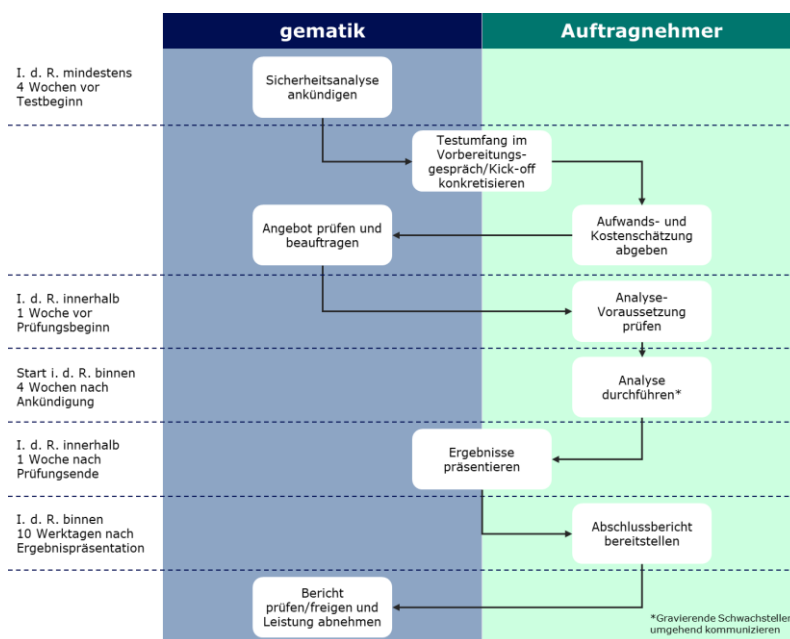


Abbildung 1 Prozess-Skizze Einzelabruf

2.5 Mengengerüst

Die folgende Tabelle gibt einen Überblick über das geschätzte Mengengerüst über die gesamte Vertragslaufzeit inkl. Verlängerungsoption:

Tabelle 1 Geschätztes Mengengerüst Sicherheitsanalysen

| Bezeichnung | 2026 | 2027 | 2028 | 2029 | 2030 | Gesamtanzahl |
|---------------------------|-----------|-----------|-----------|-----------|----------|--------------|
| Sicherheitsanalyse | 13 | 21 | 21 | 21 | 7 | 83 |
| Ad-hoc-Sicherheitsanalyse | | 2 | 2 | 2 | 1 | 7 |
| Summe | 13 | 23 | 23 | 23 | 8 | 90 |

Die Schätzmenge der Einzelabrufe aus dem Rahmenvertrag beträgt insgesamt voraussichtlich 90 Sicherheitsanalysen.

2.6 Schätz- und Höchstwert

Der Schätzwert liegt bei 2.270.000 EUR und der Höchstwert bei 2.497.000 EUR jeweils bezogen auf eine Gesamtvertragslaufzeit von vier Jahren (inkl. Verlängerungsoption).

- Beim Schätzwert handelt es sich um das von der gematik geschätzte, wertmäßige Gesamtvolumen der Einzelabrufe für diesen Rahmenvertrag gemäß § 3 VgV (Auftragswertschätzung).
- Beim Höchstwert handelt es sich um das von der gematik festgelegte, wertmäßige Gesamtvolumen der Einzelabrufe für diesen Rahmenvertrag, bei dessen Erreichen der Rahmenvertrag – unabhängig vom Erreichen einer bestimmten Laufzeit oder von einer Kündigung – keine weiteren Abrufe mehr getätigt werden können.

3 Beistellungen/Mitwirkungen

Der Auftraggeber benennt einen festen Ansprechpartner zur Koordination der Sicherheitsanalysen. Außerdem benennt der Auftraggeber interne fachlich qualifizierte Ansprechpartner, die dem Auftragnehmer für die Beantwortung von Fragen und für fachliche Erörterungen zur Verfügung stehen.

Die Ansprechpartner der gematik stehen dem Auftragnehmer in der Regel zu folgenden Zeiten zur Verfügung: Montag bis Donnerstag von 09:00 Uhr bis 16:00 Uhr und Freitag von 09:00 Uhr bis 13:00 Uhr; davon ausgenommen sind Feiertage im Land Berlin.

Im Vorfeld wird der Auftraggeber alle relevanten Beteiligten zur geplanten Durchführung der Analyse einbinden.

Die darüber hinaus erforderlichen Mitwirkungspflichten der gematik muss der Auftragnehmer in seinem Angebot beschreiben.

4 Rahmenbedingungen der Leistungserbringung

4.1 Zeitplanung

| | |
|--|--|
| Leistungsbeginn: | spätestens mit Zuschlag, vsl. Juli 2026 |
| Laufzeit des Vertrages: | 3 Jahre + optional 1 Verlängerungsjahr |
| Fertigstellung der Leistung/Leistungsende: | Vertragsende nach Laufzeit oder bei Erreichen des Höchstwertes |

Nach Erteilung des Zuschlags soll ein Kick-off-Meeting (per Videokonferenz oder vor Ort) zum gegenseitigen Kennenlernen sowie zur Besprechung der Zusammenarbeit und der ersten geplanten Sicherheitsanalysen bis Ende 2026 stattfinden.

Der erste Abruf aus der Rahmenvereinbarung bzw. die erste Ankündigung ist zeitnah nach dem Zuschlag geplant.

4.2 Technische Rahmenbedingungen

Die Sicherheitsanalysen finden größtenteils in einer Referenzumgebung (RU) statt. Viele erforderliche Bereitstellungen, wie z. B. Zugänge, Testdaten etc., erfolgen abhängig vom jeweiligen Prüfobjekt durch die für die TI-Komponente verantwortlichen Anbieter/Hersteller. Bereitstellungen können aber auch etwaige vom Auftragnehmer entwickelte Tools sein. Darüber hinaus können auch bedarfsbezogene Bereitstellungen durch die gematik erfolgen.

4.3 Organisatorische und räumliche Rahmenbedingungen

Der Auftragnehmer benennt dem Auftraggeber einen Projektleiter, der als fester, primärer Ansprechpartner über die gesamte Vertragslaufzeit für alle Belange des Rahmenvertrags zuständig ist, wie z. B. die Koordination aller Sicherheitsanalysen, die Erstellung einer Aufwands-/Kostenschätzung in Form eines Angebots nach Abruf/Ankündigung einer Sicherheitsanalyse, Teilnahme an Regelmeetings (alle zwei Wochen jeweils eine halbe Stunde). Eine kurzfristige Vertretung ist bei Bedarf sicherzustellen.

In seiner Ressourcenplanung muss der Auftragnehmer ein Analystenteam bestehend aus mindestens sechs Analysten einplanen, um den Abruf der Leistungen – auch kurzfristig – zu gewährleisten.

Der Auftragnehmer muss alle frei zugänglichen Informationsquellen für einen umfassenden Überblick über die Dienste und Produkte der TI nutzen, um eine effiziente Analyse durchführen zu können. Informationsquellen sind insbesondere frei zugängliche Spezifikationen, die über die gematik-Plattform gemSpecPages (<https://gemspec.gematik.de/>) bereitgestellt werden (siehe auch Abschnitt A3 Referenzierte Dokumente). Als Prüfungsgrundlage dienen jeweils die aktuellsten, veröffentlichten Versionen dieser Dokumente.

Die Sicherheitsanalysen finden i. d. R. vor Ort beim Auftragnehmer bzw. Analysten statt. In Abhängigkeit von der zu prüfenden TI-Komponente kann es erforderlich sein, die Prüfungen vor Ort beim Auftraggeber durchzuführen. Die Geschäftsräume der gematik befinden sich in der Rosenthaler Straße 30 in 10178 Berlin. Abstimmungen mit Vertretern der gematik können per Telefon-/Videokonferenz oder vor Ort beim Auftraggeber stattfinden.

Sofern die Verarbeitung personenbezogener Daten Bestandteil der Leistung wird, erfolgt der Abschluss eines Auftragsvertrages nach Vorgaben der gematik.

Anhang A – Verzeichnisse

A1 – Abbildungsverzeichnis

| | |
|--|---|
| Abbildung 1 Prozess-Skizze Einzelabruf | 7 |
|--|---|

A2 – Tabellenverzeichnis

| | |
|--|----|
| Tabelle 1 Geschätztes Mengengerüst Sicherheitsanalysen | 7 |
| Tabelle 2 Definition Senioritätsstufen der Analysten | 11 |
| Tabelle 3 Spaltentitel sowie Inhalt CSV-Datei | 12 |
| Tabelle 4 Feststellungskategorie inkl. Beschreibung | 13 |

A3 – Referenzierte Dokumente

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt.

| [Quelle] | Herausgeber: Titel |
|---|---|
| https://gemspec.gematik.de/ | gematik: gemSpecPages |
| [BSI Prüfvorschrift] | BSI: Prüfvorschrift für den Produktgutachter des „ePA-Frontend des Versicherten“ und des „E-Rezept-Frontend des Versicherten“ |
| [BSI TR-03161] | BSI: Anforderungen an Anwendungen im Gesundheitswesen |
| https://owasp.org/www-project-mobile-security-testing-guide/ | OWASP Mobile Application Security |
| https://owasp.org/www-project-mobile-top-10 | OWASP Mobile Top 10 |

Anhang B Anforderungskatalog

A4 – Definition Senioritätsstufen der Analysten

Die folgende Tabelle gibt eine Übersicht, wie aus Auftraggebersicht die Senioritätsstufen der Analysten definiert sind:

Tabelle 2 Definition Senioritätsstufen der Analysten

| Seniorität | Definition |
|-------------------|---|
| Junior-Analyst | <ul style="list-style-type: none">• Die Berufserfahrung in der Durchführung von Penetrations-tests liegt typischerweise unter zwei Jahren.• Die Arbeit erfolgt unter fachlicher Anleitung. Vorgehensweisen und Arbeitspakete werden überwiegend vorgegeben.• Bekannte Testmethoden werden nach Anleitung angewendet.• Die Kommunikation beschränkt sich überwiegend auf interne technische Abstimmungen.• Die Verantwortung liegt in der zuverlässigen operativen Umsetzung definierter Aufgaben. |
| Mid-Level-Analyst | <ul style="list-style-type: none">• Die Berufserfahrung in der Durchführung von Penetrations-tests liegt typischerweise zwischen zwei und fünf Jahren.• Die Arbeitsumsetzung erfolgt eigenständig mit hohem fachlichem Gestaltungsspielraum.• Geeignete Testmethoden und Vorgehensweisen werden selbstständig ausgewählt und angewendet.• Die Kommunikation umfasst die direkte Abstimmung mit Kunden und Stakeholdern.• Die Verantwortung liegt in der fachlich korrekten Umsetzung sowie der eigenständigen Bewertung von Schwachstellen und Risiken. |
| Senior-Analyst | <ul style="list-style-type: none">• Die Berufserfahrung in der Durchführung von Penetrations-tests liegt typischerweise über fünf Jahren.• Arbeitspakete werden eigenverantwortlich geplant, strukturiert und koordiniert. Die Arbeitsumsetzung erfolgt selbstbestimmt und methodisch souverän.• Teststrategien werden eigenverantwortlich entwickelt.• Die Kommunikation umfasst Beratung, Moderation, Managementkommunikation sowie die Begleitung kritischer Abstimmungen und Eskalationen.• Verantwortung wird für Qualität, Sicherheit, methodisches Vorgehen und fachliche Ergebnisse übernommen. Komplexe Projekte werden begleitet, Arbeitsergebnisse gereviewt und fachliche Weiterentwicklung anderer Teammitglieder unterstützt. |

A5 – Felder CSV-Datei

Tabelle 3 Spaltentitel sowie Inhalt CSV-Datei

| Spaltentitel | Inhalt der Spalte |
|---------------------|---|
| Title | ID sowie Titel/Name der Feststellungen |
| Description | Beschreibung der Feststellungen |
| Vulnerability | Beschreibung, wie die Feststellungen ausgenutzt werden können, um Systeme zu kompromittieren und/oder die Vertraulichkeit, Integrität, Verfügbarkeit und Verwertbarkeit von sensiblen Daten zu schaden. |
| Impact | Beschreibung welche Auswirkung die Ausnutzung dieser Feststellung auf das betrachtete System und/oder die Vertraulichkeit, Integrität, Verfügbarkeit und Verwertbarkeit von sensiblen Daten hat. |
| Fix | Handlungsempfehlung zur Behebung der Schwachstelle und/oder Vorschläge zur Verbesserung der Sicherheit des betrachteten Systems. |
| CVSS Basis Score | CVSS Basis Score |
| CVSSv3.Vec-tor | CVSS Vektor |
| Tag | Einstufung Kritikalität der Feststellung: [Critical, High, Medium, Low, Info, None] |
| Kategorisierung | Feststellungskategorie gemäß Tabelle 4 |
| References | Referenz |

A6 – Feststellungskategorie

Tabelle 4 Feststellungskategorie inkl. Beschreibung

| Kategorie | Beschreibung Kategorie |
|----------------------------|--|
| Veraltete Software | <p>Einsatz veralteter Software bzw. Einsatz von Software mit bekannten Sicherheitslücken:</p> <ul style="list-style-type: none"> - Es wird veraltete Software eingesetzt - Es wird Software mit bekannten Sicherheitslücken eingesetzt. |
| Konfiguration & Deployment | <p>Konfiguration & Deployment:</p> <ul style="list-style-type: none"> - Konfigurationsschwäche feststellen in Applikationen, Betriebssysteme und Hardware → ein nicht gehärtetes System liegt vor. <p>Darunter fallen unter anderem:</p> <ul style="list-style-type: none"> - Verwendung von werkseitigen Standardpasswörtern oder -einstellungen (Unsichere Standardkonfigurationen) - Unsichere Netzwerkeinstellungen wie offene Ports oder schwache Firewall-Regeln (Fehlhafter Netzwerkconfiguration) - Fehlende Verschlüsselung oder Authentifizierung für Datenbankzugriffe (Ungesicherte Datenbanken) |
| Authentifizierung | <p>Authentifizierung:</p> <ul style="list-style-type: none"> - Betrachtung des Login-Prozesses während des Pentests <p>Darunter fallen unter anderem:</p> <ul style="list-style-type: none"> - Weak or stolen credentials Schwache/gestohlene Zugangsinformationen - Fehlerhafte Authentifizierung (Login, bypass login) |
| Autorisierung | <p>Autorisierung:</p> <ul style="list-style-type: none"> - Betrachtung der Berechtigung während des Pentests <p>Darunter fallen unter anderem:</p> <ul style="list-style-type: none"> - Missing authorization (Priv Esc) Fehlende Berechtigungen. - Access Control Zugangskontrolle (inkl. Session-Man.) |
| Session-Management | <p>Session-Management</p> <p>Darunter fallen unter anderem:</p> <ul style="list-style-type: none"> - Cookies, Session-fixation - Session-invalidation - Session-timeouts |
| Web-Schwachstellen | <p>Web-typische Schwachstellen</p> <p>Darunter fallen unter anderem:</p> <ul style="list-style-type: none"> - XSS (reflected, stored, DOM) - Server-side-request-forgery (hybride-Schwachstelle) (SSRF) - Falsch gesetzter oder fehlender Wert im HTTP-Security-Header |

| Kategorie | Beschreibung Kategorie |
|-------------------------------------|--|
| | <ul style="list-style-type: none"> - Injections, wie SQL injection, LDAP injection, Command-injection, XXE - Unrestricted Upload - Remote Code Execution (RCE) Ausführung von Schadcode - Insufficient Validate user Input Unzureichende Validierung von Nutzereingaben - Version Disclosure Preisgabe von Software-Versionen |
| Technologische Schwachstellen | <p>Technologische Schwachstellen</p> <ul style="list-style-type: none"> - Falsche semantische Nutzung eines Technologiekomplexes. <p>Darunter fallen unter anderem:</p> <ul style="list-style-type: none"> - Falsche Verwendung von Kryptographie, Missing data encryption Fehlende Datenverschlüsselung - Falsche Konfiguration von TLS, Missing / weak TLS encryption Fehlende/schwache Transportverschlüsselung - Konfiguration/Härtung von Cloud-Diensten - Nicht passende Nutzung von KI bezüglich der Businesslogik - Angriffe, die darauf abzielen, Dienste unzugänglich zu machen (Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS)) |
| Plattformspezifische Schwachstellen | <p>Plattformspezifische Schwachstellen</p> <ul style="list-style-type: none"> - Inadäquate Wahl der zugrunde liegenden Plattform - API falsch benutzt <p>Darunter fallen unter anderem:</p> <ul style="list-style-type: none"> - Vulnerable API Anfällige Programmierschnittstelle - Mobile Betriebssysteme <ul style="list-style-type: none"> o Android API o iOS API - Desktop/Server Betriebssysteme <ul style="list-style-type: none"> o Windows API o Linux API - Windows API wurde mit einem unzureichend geprüften Wert aufgerufen. |
| Menschliche Schwachstellen | <p>Social Engineering Menschliche Manipulation</p> <p>Darunter fallen unter anderem:</p> <ul style="list-style-type: none"> - Social Engineering - Täuschungsversuche per E-Mail oder anderer Kommunikationsmittel, um vertrauliche Daten zu erhalten (Phishing-Angriffe) - Fehlendes Wissen oder Bewusstsein der Mitarbeiter für Sicherheitsrisiken und -verfahren (Mangelndes Sicherheitsbewusstsein) |
| Netzwerk-Schwachstellen | <p>Network vulnerabilities Netzwerk-Schwachstellen</p> <p>Darunter fallen unter anderem:</p> |

| Kategorie | Beschreibung Kategorie |
|-------------------------|---|
| | <ul style="list-style-type: none"> - Unzureichende Trennung von Daten und Ressourcen verschiedener Benutzer (Fehlende Isolation) - Fehlende Netzwerksegmentierung |
| Unzureichendes Logging | Insufficient monitoring and Logging Unzureichende Überwachung und Loggen |
| Physische Sicherheit | <p>Schwachstellen in der physischen Sicherheit</p> <p>Darunter fallen unter anderem:</p> <ul style="list-style-type: none"> - Mangelnde Zugangskontrollen zu Serverräumen oder Büros (Unzureichender physischer Schutz). - Keine oder unzureichende Videoüberwachung oder Sicherheitspersonal (Fehlende Überwachung). |
| Software-Schwachstellen | <p>Software-Schwachstelle</p> <ul style="list-style-type: none"> - Schwachstellen aus Source Code Analyse <p>Darunter fallen unter anderem:</p> <ul style="list-style-type: none"> - Vulnerabilities in Source Code - Programmiersprachenspezifische Schwachstellen, wie Type-confusions in Java und - undefined behaviour in C/C++ |
| Datenschutzverstoß | <p>Data Protection Violation Datenschutzverstoß</p> <ul style="list-style-type: none"> - Fahrlässige Veröffentlichung von sensiblen Informationen, z.B. bei persönlichen Daten → EU DSGVO. |
| Informationspreisgabe | <p>Informationspreisgabe</p> <ul style="list-style-type: none"> - Preisgabe von technischen Details, z. B. durch Stack Traces, Exceptions (NPEs) für OS, eingesetzte Komponenten, Aufbau Software etc. |