Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie TR-03174: Anforderungen an Anwendungen im Finanzwesen

Teil 3: Hintergrundsysteme

Version 3.0

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	18.05.2022	Referat DI 24	Erste Version
2.0	25.03.2024	Referat DI 24	Überarbeitung Kapitel 3 Überarbeitung Kapitel 4
3.0	16.09.2024	Referat D24	Finalisierung

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: referat-d24@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

Tabellenverzeichnis

1 Einleitung

1.1 Gegenstand der Technischen Richtlinie

Nicht erst seit dem Inkrafttreten der Payment Service Directive 2 **Fehler! Verweisquelle konnte nicht gefunden werden.** ist es für Fintechs und ähnliche Akteure möglich, Dienstleistungen im Bezahl- und Paymentumfeld anzubieten. Es ist jedoch ein konkretes Ziel der PSD2/3 den Wettbewerb im Bereich der Paymentdienstleistungen europaweit zu fördern. Zu diesen Dienstleistungen zählen insbesondere die Möglichkeit, Zugriffe auf Konten oder spezielle Kontoinformationen oder die Initiierung von Zahlungen mittels digitaler Anwendungen zu ermöglichen. Mit den Regulatory Technical Standards for Strong Customer Authentication [RTS] gibt die EU einen groben Rahmen vor, wie diese Dienstleistungen sicher gestaltet werden können. Dieser grobe Rahmen soll durch die Verwendung der hier vorliegenden Technischen Richtlinie konkretisiert werden.

Die TR richtet sich an Hersteller von Anwendungen im Finanzwesen für Hintergrundsysteme. Zusätzlich kann sie als Richtlinie für Hintergrundsysteme betrachtet werden, welche sensible Daten verarbeiten oder speichern.

1.2 Zielsetzung der Technischen Richtlinie

Die Digitalisierung aller Lebensbereiche, sei es im Beruf, in Heimumgebungen, im Individual- oder im öffentlichen Personenverkehr, schreitet stetig voran. Bereits im Jahr 2018 überschritt die Anzahl der Internetnutzer die Grenze von vier Milliarden Menschen. Zwei Drittel der zurzeit 8,2 Milliarden Menschen zählenden Weltbevölkerung nutzen ein Mobiltelefon. Mehr als drei Milliarden Menschen nutzen soziale Netzwerke und tun dies in neun von zehn Fällen über ihr Smartphone (vgl. [GDR18]). Diese Entwicklung lässt sich auch im Finanzwesen beobachten. So überprüfen Nutzer ihren Kontostand während Sie unterwegs sind, lösen Überweisungen aus oder Zahlen am Point of Sale ganz intuitiv mit dem Smartphone oder einer Smartwatch. Dabei sind Daten zur finanziellen Situation eines Menschen besonders schützenswert. Ein kompromittiertes Smartphone kann somit das gesamte digitale Leben des Nutzers ungewollt offenlegen und zu hohem finanziellen Schaden führen. Das Einhalten von geeigneten Sicherheitsstandards, gerade im Bereich der Hintergrundsysteme, kann dies wesentlich erschweren und möglicherweise sogar verhindern. Schon während der Entwicklungsphase sollten Hersteller sehr verantwortungsvoll planen, wie ein Hintergrundsystem personenbezogene und andere sensible Daten verarbeitet, speichert und schützt.

Die IT-Sicherheit verfolgt im Wesentlichen drei Schutzziele: Vertraulichkeit, Integrität und Verfügbarkeit.

Gerade bei Anwendungen im Finanzwesen ist die Einhaltung dieser Anforderungen von besonderer Wichtigkeit. Der Verlust der Vertraulichkeit von Finanzdaten kann für das Opfer negative Auswirkungen sowohl im privaten, wie auch im beruflichen Kontext haben.

Sollte ein Angreifer in der Lage sein, sensible Daten eines Dritten zu manipulieren und damit deren Integrität zu verletzen, könnte er wesentlichen Einfluss auf das Leben des Betroffenen haben. Im Bereich der Finanzanwendungen könnte die Verletzung der Integrität dazu führen, dass Zahlungen, die zwar der rechtmäßige Kontoinhaber auslöst, auf ein Konto überwiesen werden, welches jedoch nicht dem beabsichtigten Zahlungsempfänger zugeordnet ist. Daher können unsichere Finanzanwendungen großen wirtschaftlichen Schaden bei natürlichen und juristischen Personen anrichten.

Eine Verletzung der Verfügbarkeit kann bei Betroffenen dazu führen, dass notwendige Zahlungen oder Überweisungen nicht durchgeführt werden können. Dies kann dann die Grundlage für weitere Probleme sein, wenn zum Beispiel der getätigte Einkauf nicht bezahlt oder eine fällige Rechnung nicht beglichen werden kann.

Diese Technische Richtlinie soll daher als Leitfaden dienen, um Entwickler von Hintergrundsystemen bei der Erstellung und dem Betrieb sicherer Hintergrundsysteme zu unterstützen.

1.3 Übersicht der Technischen Richtlinie

1.3.1 Methodik

Anwendungen im Sinne dieser TR sind Applikationen auf (mobilen) Endgeräten. Dies schließt insbesondere digitale Finanzanwendungen. Der Betrieb kann autonom durch die Anwendung auf dem Endgerät oder in Kombination mit einem sicheren Hintergrundsystem umgesetzt werden. Wird im Folgenden der Begriff Hintergrundsystem verwendet, ist insbesondere auch der Einsatz von Cloud Computing gemeint. Auf Grund des rasanten technischen Fortschritts und der Diversität der Architekturen und Tools von Hintergrundsystemen, erhebt die Technische Richtlinie keinen Anspruch auf Vollständigkeit. Sie kann als Mindestanforderung für den sicheren Betrieb einer Anwendung betrachtet werden.

Die Technische Richtlinie formuliert eine Security Problem Definition (SPD), welche potentielle Bedrohungsszenarien aufweist. Aus der SPD werden Prüfaspekte für Hintergrundsysteme und deren Plattformen bzw. Einsatzumgebungen abgeleitet, um vor Bedrohungen zu schützen.

Die in dieser Technischen Richtlinie formulierten Bedrohungsszenarien und Prüfaspekte basieren auf Erfahrungen, die das BSI bei bisherigen Untersuchungen von Hintergrundsystemen im Finanzwesen gesammelt hat. Darüber hinaus orientiert sie sich an allgemeinen Empfehlungen des BSI zur Absicherung von Hintergrundsystemen (Absicherung eines Servers [[ISi-Server]], Sichere Anbindung von lokalen Netzen an das Internet [[ISi-LANA]]) sowie internationalen Standards wie der OWASP Top 10 [[OWASP_Top10]], mit dem dazugehörigen OWASP Testing Guide [OWASP_TG].

Eine Grundanforderung an Anwendungen im Sinne der Technischen Richtlinie ist die Orientierung an Best-Practice-Empfehlungen und anderen allgemeinen Anforderungen an sichere, verteilte Anwendungen. Dazu zählen die Durchführung intensiver funktionaler Tests, Integrationstests sowie insbesondere Positiv-/Negativ-Tests von Sicherheitsleistungen der Anwendung. Die TR stellt darüber hinaus zusätzliche, spezifische Anforderungen.

1.3.2 Begriffe

Diese Technische Richtlinie verwendet folgende Begriffe:

Tabelle 1: Begriffe der Technischen Richtlinie

Begriff	Beschreibung
MUSS	Der Hersteller muss eine bestimmte Eigenschaft zwingend implementieren.
DARF NICHT / DARF KEIN(E)	Das Hintergrundsystem darf eine bestimmte Eigenschaft unter keinen Umständen aufweisen.
SOLL	Das Hintergrundsystem muss eine bestimmte Eigenschaft aufweisen, außer es wird dargelegt, dass durch ein Nicht-Umsetzen kein Risiko für den sicheren Betrieb besteht, bzw. eine Umsetzung, aufgrund von technischen Einschränkungen, derzeit nicht möglich ist.
KANN	Das Hintergrundsystem kann eine bestimmte Eigenschaft aufweisen, wobei ein Umsetzen dieser Eigenschaft vom Lösungsanbieter anzuzeigen ist.

Begriff	Beschreibung
primärer Zweck	Der primäre Zweck des Hintergrundsystems im Sinne der Technischen Richtlinie ist ein Zweck des bestimmungsgemäßen Gebrauchs sowie alle Zwecke, die unmittelbar auf die Verankerung des Hintergrundsystems im geltenden Rechtsrahmen abzielen.
rechtmäßiger Zweck	Der rechtmäßige Zweck eines Hintergrundsystems im Sinne der Technischen Richtlinie ist ein Zweck, der durch geltendes Recht als Grundlage zur Verarbeitung personenbezogener Daten zulässig ist.

2 Überblick der Sicherheitsanforderungen an Anwendungen im Finanzwesen

2.1 Anwendungskonzepte auf mobilen Endgeräten

Der Begriff „mobile Anwendung“ bezeichnet ein Programm, das auf einer mobilen Plattform ausgeführt wird. Grundsätzlich lassen sich solche Anwendungen in drei Kategorien unterteilen. Die erste Kategorie bilden die nativen Applikationen (Kapitel 2.1.1), welche direkt auf die Plattform, auf der sie ausgeführt werden, zugeschnitten sind, ab. Dem gegenüber stehen die Web-Anwendungen (Kapitel 2.2). Ihre Implementierung ist völlig unabhängig von der Plattform und sie laufen innerhalb des Web-Browsers des Endgeräts. In die dritte Kategorie fallen die hybriden Ansätze (Kapitel 2.1.2). Sie spiegeln alle möglichen Kombinationen aus nativen Applikationen und Web-Anwendungen wider.

Unabhängig davon, ob die Anwendung selber einen nativen, Web- oder Hybridansatz verfolgt, benötigt sie je nach Anwendungsfall ein Hintergrundsystem, das die weitere Verarbeitung der Daten realisiert und evtl. zusätzliche Funktionalitäten bereitstellt. Da der Fokus dieser Publikation auf Hintergrundsystemen liegt, beziehen sich die nachfolgenden Bedrohungsanalysen und die Prüfaspekte auf den Schutz von Hintergrundsystemen. Für weiterführende Hinweise zum sicheren Betrieb und der sicheren Entwicklung von Mobilen Anwendungen wird auf „TR-03174 Anforderungen an Anwendungen im Finanzwesen Teil 1 Mobile-Anwendungen“ verwiesen [TR03174-1].

2.1.1 Native-Applikationen

Eine native Applikation ist passend auf eine Plattform und deren Betriebssystem zugeschnitten. Sie basiert auf den von der Plattform (beispielsweise Android oder iOS) bereitgestellten Programmierwerkzeugen (Software Development Kits - SDKs). Diese ermöglichen einen direkten Zugriff auf Gerätekomponenten, wie beispielsweise GPS, Kamera oder Mikrofon. Aufgrund ihrer Nähe zum Betriebssystem können sie eine sehr gute Performanz, eine hohe Zuverlässigkeit und eine intuitive Bedienbarkeit erreichen. Die Applikationen werden beispielsweise über den plattformeigenen App-Store installiert und können oft auch offline betrieben werden.

Mit der Nähe zum Betriebssystem sind allerdings auch Nachteile verbunden. Änderungen am Betriebssystem, beispielsweise durch Updates, können dazu führen, dass Anpassungen an der Applikation vorgenommen werden müssen. Sollte dies nicht erfolgen, kann es zu Beeinträchtigungen der Funktionsfähigkeit der Applikation kommen. Darüber hinaus ist es nicht möglich sie auf anderen Betriebssystemen zu installieren. Soll die gleiche Applikation auf mehreren Betriebssystemen publiziert werden, so muss jeweils eine eigene Codebasis[1] existieren. Dies ist häufig mit einem hohen Aufwand und somit auch hohen Kosten verbunden.

2.1.2 Hybride Ansätze

Hybride Anwendungen verbinden sowohl die Vor-, als auch die Nachteile von nativen Anwendungen sowie Web-Anwendungen und Web-Services. Mit Hilfe des SDKs wird eine Rahmen-Applikation geschaffen, welche alle Vor- und Nachteile von nativen Anwendungen aufweist. Sie kann auf Gerätekomponenten zugreifen und über einen App-Store bezogen werden, jedoch nicht auf anderen Plattformen installiert werden, ohne Anpassungen am Quellcode vorzunehmen. Darüber hinaus beinhalten die Rahmen-Applikationen einen eingebetteten Web-Browser, mit dessen Hilfe Web-Anwendungen in native

[1] Es existieren auch plattformübergreifende Implementierungsansätze, welche die Entwicklung einer Anwendung für verschiedene Plattformen gleichzeitig unterstützen. Allerdings verschiebt sich dadurch die Abhängigkeit lediglich in diese sehr umfangreiche Middleware, die alle Zielplattformen abdecken muss.

Applikationen eingebunden werden können. Dadurch ist es auch Web-Anwendungen möglich auf die sonst nur den nativen Applikationen vorbehaltenen Gerätekomponenten zuzugreifen. Darüber hinaus kann es durch den Einsatz unterschiedlicher Benutzerschnittstellen zu einer negativen Beeinträchtigung der User-Experience kommen. Die Plattformabhängigkeit der Anwendung bezieht sich nun lediglich auf die Rahmen-Applikation, womit der Aufwand für eine Migration auf andere Plattformen deutlich reduziert wird.

2.2 Web-Anwendungen

Web-Anwendungen sind Anwendungsprogramme, meist Webseiten, die in Kombination mit einem Hintergrundsystem (Kapitel 2.3) ohne Installation auf einem lokalen System betrieben werden können. Solche Webseiten sind oft so programmiert, dass sie wie eine native Anwendung für klassische Desktop-Systeme oder mobile Endgeräte aussehen und sich vergleichbar verhalten. Im Gegensatz zu nativen Anwendungen basieren sie nicht auf einem SDK der zugrundeliegenden Plattformen, sondern auf klassischen Programmierwerkzeugen der Web-Entwicklung. In den meisten Fällen kommen HTML5 und JavaScript zum Einsatz. Aus diesem Grund ist mit ihnen nur ein sehr eingeschränkter Zugriff auf Gerätekomponenten möglich. Ihr größter Vorteil besteht darin, dass sie unabhängig vom Betriebssystem sind. Da die Anwendungen innerhalb eines Web-Browsers laufen, können sie auf jeder Plattform gleichermaßen eingesetzt werden, ohne Anpassungen an der Codebasis vornehmen zu müssen.

Da der Fokus dieser Publikation auf Hintergrundsystemen liegt, beziehen sich die nachfolgenden Bedrohungsanalysen und die Prüfaspekte auf den Schutz von Hintergrundsystemen. Für weiterführende Hinweise zum sicheren Betrieb und der sicheren Entwicklung von Web-Anwendungen wird auf „TR-03161 Anforderungen an Anwendungen im Finanzwesen Teil 2: Web-Anwendungen“ verwiesen [TR03174-2].

2.3 Hintergrundsysteme

Die meisten Anwendungen verlassen sich für die Verarbeitung und Speicherung von Daten nicht ausschließlich auf die von der Laufzeitumgebung bereitgestellten Ressourcen. Sie lagern diese Aufgaben auf ein Server-System aus. Weil diese Server aus Nutzerperspektive nicht sichtbar sind, werden sie auch Hintergrundsysteme oder Backend-Services genannt (als Abgrenzung zu der Anwendung, die der Nutzer sieht, welche Frontend genannt wird). Neben der fachspezifischen Verarbeitung und Speicherung von Daten übernehmen diese Systeme oft Aufgaben zur Authentifizierung und Autorisierung von Nutzern oder andere zentrale Tätigkeiten. Dies erlaubt, dass nicht alle Funktionalitäten der Applikationen auf den Endgeräten umgesetzt werden müssen. Oft beschränken sie sich lediglich auf eine grafische Nutzerführung. Eine generelle Aussage darüber, wie viel Funktionalität in der Applikation selbst umgesetzt und wie viel auf einen Server ausgelagert wird, kann nicht getroffen werden. Die Ausprägungen können von Anwendung zu Anwendung variieren. Daher ist bei einer vollumfänglichen sicherheitstechnischen Betrachtung der gesamten Anwendung die Sicherheit des Hintergrundsystems ein essentieller Teil.

. Für die Nutzung von Anwendungen, die an ein Hintergrundsystem angeschlossen sind, ist eine aktive Internetverbindung meistens zwingend erforderlich. Dabei wird für die Kommunikation zwischen Vorder- und Hintergrundsystem meist eine über TLS gesicherte Transportverbindung eingesetzt. Der Einsatz von Hintergrundsystemen beschränkt sich nicht nur auf den Bereich der mobilen Anwendungen, sondern spiegelt den aktuellen Stand der Technik für fast alle Anwendungen wider. Hierbei werden im wesentlichen drei Szenarien unterschieden:

- Der Hersteller der Anwendung verwaltet die Infrastruktur des Hintergrundsystems selbst (Kapitel 2.3.1).
- Der Hersteller der Anwendung lässt die Infrastruktur von einem externen Dienstleister verwalten (Kapitel 2.3.2).
- Die gesamte Hintergrundsystem-Komponente der Anwendung wird bei einem Cloud-Dienstleister gehostet (Kapitel 2.3.3).

Abhängig von der Art des Betriebs und den damit verbundenen unterschiedlichen Angriffsvektoren stehen dem Hersteller unterschiedliche Möglichkeiten zur Verfügung, die Sicherheit der Gesamtlösung und der gespeicherten und verarbeiteten Daten zu gewährleisten. Einen guten Einstieg bieten die „Top 10 Web Application Security Risks“ der OWASP Foundation [T10WASR].

2.3.1 Selbst gehostete Systeme

Bei selbst gehosteten Systemen agiert der Hersteller der Anwendung selber als Betreiber der Hintergrundsysteme. Damit hat er den direkten Zugriff auf die Systeme und deren Umgebung. Die Server, auf denen die Lösung läuft, ist innerhalb der Betriebsumgebung des Herstellers untergebracht und die physische, technische und organisatorische Absicherung der Systeme erfolgt durch ihn alleine. Der größte Vorteil dieser Lösung besteht darin, dass der Hersteller die alleinige Hoheit über die Systeme hat und schnell und direkt auf jegliche Vorgänge reagieren kann. Da er die Systeme selbst verwaltet und die Softwarekomponenten auswählt bzw. entwickelt, hat er am meisten Wissen über die mögliche Verwundbarkeit dieser Systeme. Allerdings lastet in diesem Fall auch die alleinige Verantwortung auf dem Hersteller, so dass er z.B. dauerhaft Personal bereitstellen muss, um den Betrieb, die Wartung und auftretende Sicherheitsvorfälle zu überwachen und angemessen darauf zu reagieren. Je nach geschäftlicher Ausrichtung des Herstellers besitzt dieser möglicherweise zwar viel Wissen in dem fachlichen Bereich seiner jeweiligen Anwendung, aber weniger im Bereich der IT-Sicherheit.

2.3.2 Extern gehostete Systeme

Bei dieser Variante werden die Server in einem Datacenter eines externen Dienstleisters gehostet, der sich üblicherweise auf Hosting spezialisiert hat. Die sicherheitstechnischen Vorteile bei dieser Lösung bestehen darin, dass der Dienstleister in der Regel mehr Erfahrung mit dem Betrieb solcher Systeme hat. Dies hat vor allem einen positiven Einfluss auf die Verfügbarkeit. Je nach Ausgestaltung der Dienstleitung übernimmt der externe Hoster auch weitergehende Aufgaben, wie z.B. die Versorgung der Betriebssysteme mit Sicherheitsupdates, Datensicherung und Backups, sowie Überwachung und Monitoring, um rechtzeitig auf verdächtige Aktivitäten reagieren zu können.

Der Betreiber muss dem Hoster ein gewisses Maß an Vertrauen entgegenbringen. So kann er selber z.B. die Integrität der Hardware nicht überwachen, weil mit einem direkten physischen Zugang Software-Überwachungsmaßnahmen immer umgangen werden können. Außerdem besitzt der Hoster in der Regel viele Kunden, die alle auf technischer Ebene voneinander separiert werden müssen um unbeabsichtigten Informationsabfluss, etwa zu Konkurrenten oder an die Öffentlichkeit, zu verhindern. Nicht zuletzt können durch die Aufteilung der Zuständigkeitsberichte Reibungsverluste entstehen, die gerade bei kritischen Situationen wertvolle Zeit kosten können.

2.3.3 Cloud Computing

Cloud Computing beschreibt ein Modell, das bei Bedarf – meist über das Internet und geräteunabhängig – zeitnah und mit wenig Aufwand geteilte Computerressourcen als Dienstleistung, etwa in Form von Servern, Datenspeicher oder Applikationen, bereitstellt und nach Nutzung abrechnet. Je nach Bedarf des Kunden können Ressourcen flexibel erweitert werden. Dadurch hat der Hersteller des Dienstes noch weniger Einfluss auf die Umgebung der Ausführung als bei einem einfachen Hosting. Es ist. z.B. nicht mehr möglich, zu erkennen, auf welchem Gerät genau eine bestimmte Operation vorgenommen wird. Der Betreiber muss sich hier voll und ganz auf den Anbieter der Cloud-Lösung verlassen können. Deswegen ist beim Einsatz von Cloud Computing für Anwendungen im Sinne der TR auf Anbieter zurückzugreifen, welche die Anforderungen aus dem „Kriterienkatalog Cloud Computing“ des BSI ([KCC-C5]) erfüllen. Der Betreiber muss auf Basis des vorgelegten C5-Testats prüfen, ob die Anforderungen der TR durch die genutzten Cloud-Dienste erfüllt werden. Alternativ zum C5-Testat sind auch Anbieter mit vergleichbaren Testaten oder Zertifikaten zulässig (vgl. O.Org_2).

2.4 Security Problem Definition

Die Security Problem Definition beschreibt Annahmen, Bedrohungen und organisatorische Sicherheitspolitiken, die für Anwendungen im Finanzwesen zur Erbringung der Sicherheitsleistung relevant sind.

2.4.1 Annahmen

A.Hardware Die Hardware ist sicher. Es gibt keine unveröffentlichten Angriffe auf die Hardware.

A.UserCredentials Der Nutzer gibt sein Passwort nicht bewusst oder freiwillig weiter.

A.PasswordReset Der für das Gesamtsystem genutzte Dienst des Nutzers oder der Account zum Zurücksetzen des Passwortes ist nicht kompromittiert.

A.Admin Der Administrator, der für die Wartung des Systems Zugriff auf die Server-Komponenten hat, ist kompetent und vertrauenswürdig, sodass vorsätzlich böswillige oder grob fahrlässige Handlungen auszuschließen sind.

2.4.2 Bedrohungen

T.EavesdropCom Angreifer können die Kommunikation zwischen Hintergrundsystem und Applikation abhören und damit sensible Daten mitlesen oder die Kommunikation abfangen und durch manipulierte Pakete ersetzen. Es können sensible Daten ausgelesen und auf dem Transportweg manipuliert werden.

T.ReadAssets Angreifer können Daten auf dem Server auslesen. Dies können entweder sensible Daten der Nutzer, oder deren Authentifizierungsinformationen sein. Außerdem ist es möglich, durch die gewonnenen Informationen eine Grundlage für weitere Angriffe wie insbesondere T.HijackBackend zu schaffen.

T.ManipulateAssets Angreifer können Daten auf dem Server unbemerkt manipulieren. Dadurch können Nutzer getäuscht und zu ungewollten Aktionen verleitet werden. Sicherheitsmaßnahmen können umgangen werden. Außerdem ist es möglich, durch die Manipulation einiger Daten eine Grundlage für weitere Angriffe wie insbesondere T.HijackBackend zu schaffen.

T.HijackBackend Der Angreifer bringt einen oder mehrere Dienste des Hintergrundsystems unter seine Kontrolle. Dadurch können Nutzerdaten in großem Umfang abgefangen werden.

T.SensitiveDataExport Sensible Daten werden unverschlüsselt in Log- oder Backup-Dateien außerhalb des gesicherten Hintergrundsystems vorgehalten. Ein Angreifer kann mit reduziertem Aufwand auf diese Daten zugreifen.

T.Expense Die Anwendung verursacht unvorhergesehene, zusätzliche Kosten für den Nutzer oder Betreiber.

2.4.3 Organisatorische Sicherheitspolitiken

OSP.Authorization Der Hersteller entwickelt ein Autorisierungskonzept, welches sowohl den lesenden, als auch den schreibenden Zugriff auf sensible Daten steuert. Die Zugriffsberechtigungen müssen so gewählt werden, dass ausschließlich für die Erfüllung des primären bzw. rechtmäßigen Zwecks erforderliche Rechte erteilt werden. Das Autorisierungskonzept muss unabhängig von der Authentifizierung implementiert werden.

OSP.SecurityLog Alle Logs zu sicherheitsrelevanten Ereignissen werden auf dem Hintergrundsystem gespeichert.

OSP.CriticalUpdates Der Hersteller überprüft und überwacht die Server-Betriebssysteme sowie die genutzte Drittanbieter-Software [2] dauerhaft auf ausnutzbare Schwachstellen und Updates. Der Hersteller muss bei bekannt werden von Schwachstellen kurzfristig ein Update einspielen und weiterhin ein hohes Patchlevel verfolgen.

OSP.ServicesIn Von externen Diensten eingehende Daten sollen vor einer Verarbeitung im Hintergrundsystem validiert werden (z. B. XML-Schemavalidierung, Prüfung auf ungültiges Encoding, etc.). Ziel ist es, die Anwendung vor Angriffen durch bösartige Eingaben zu schützen.
Anwendungshinweis: Wird eine potentiell schädliche Eingabe erkannt, muss sie entweder bereinigt/maskiert oder abgelehnt/verworfen werden. Das Verwerfen sollte dem Bereinigen vorgezogen werden.

OSP.ServicesOut Das Hintergrundsystem soll sensible Daten nicht im Klartext an externe Dienste weitergeben.
Anwendungshinweis: Sofern vorher maskierte oder bereinigte Eingaben weitergegeben werden, müssen diese so maskiert oder enkodiert werden, dass sie im Kontext der Weitergabe keine schädlichen Effekte haben.

OSP.Libraries Im Hintergrundsystem verwendete Frameworks bzw. Libraries dürfen keine eigenständigen Verbindungen zu externen Diensten aufbauen, die nicht explizit vom Hintergrundsystem-Betreiber freigegeben wurden.

OSP.Purpose Jegliche Datenerhebung, -verarbeitung, -speicherung und -weitergabe darf nur mit einer Zweckbindung erfolgen. Der Hersteller veröffentlicht dafür den rechtmäßigen Zweck der Anwendung und darüber hinaus welche Daten wie verarbeitet werden und wo und wie lange sie gespeichert werden.

OSP.SecurityLifeCycle Der Hersteller realisiert einen Entwicklungszyklus, dessen Teilschritte darauf ausgelegt sind, die Sicherheit des Hintergrundsystems zu stärken. Darunter fallen Maßnahmen, mit denen bösartige Aktivitäten erkannt werden und der Betreiber angemessene Gegenmaßnahmen einleiten kann.

2.4.4 Restrisiken

Der Betrieb eines Hintergrundsystems für Anwendungen im Finanzwesen hat besonders hohe Anforderungen an die Vertraulichkeit der gespeicherten und verarbeiteten Daten. Daher weist die Technische Richtlinie auf bestehende Restrisiken hin.

Persönliche Daten, wie Informationen über den Finanzstatus, die in großer Menge auf aus dem Internet erreichbaren Servern verarbeitet bzw. gespeichert werden, ziehen erfahrungsgemäß das Interesse unterschiedlicher Angreifertypen auf sich. Auch wenn ein einzelnes Datum (etwa ein Puls zu einem bestimmten Zeitpunkt) i.d.R. keinen großen Wert für potentielle Angreifer hat, so ist doch die Menge der Daten ein durchaus verlockendes Ziel, um etwa Nutzerverhalten oder Bewegungsprofile zu erstellen, die dann verkauft, veröffentlicht oder für z.B. Erpressungen verwendet werden können. Deshalb ist der Datensatz, der in einem Hintergrundsystem für Anwendungen im Finanzwesen gespeichert bzw. verarbeitet wird, in der Regel ein weitaus lohnenderes Ziel als nur die Daten einzelner Nutzer.

Regelmäßig werden große Datensätze personenbezogener Daten in Leaks veröffentlicht, sodass davon auszugehen ist, dass es noch eine erhebliche Menge weiterer Diebstähle gibt, die nicht an die Öffentlichkeit kommen.

[2] Unter einer Drittanbieter-Software soll die Zusammenfassung von Funktionalität verstanden werden, die nicht in der Hoheit des Entwicklers des Hintergrundsystems entstanden ist und die auch nicht Teil der Funktionalität der verwendeten Betriebssystemplattform ist.

In der Regel werden Einbrüche, die zu solchen Leaks führen durch bekannte Schwachstellen der verwendeten Software ermöglicht. Aber auch bei einem aktuellen Software-Stand besteht das Risiko, für sogenannte 0-Day-Exploits, also Angriffe, bei denen bisher unveröffentlichte Schwachstellen zum Diebstahl von Daten ausgenutzt werden. Darüber hinaus kann sich ein Angreifer durch Verwendung geeigneter Schwachstellen in den Systemen des Betreibers verankern und somit über einen längeren Zeitraum Zugriff auf sensible Daten erlangen.

Ein weiteres Restrisiko besteht bei extern gehosteten Hintergrundsystemen und insbesondere bei Cloud-Anbietern. Der jeweilige Betreiber hat i.d.R. mehrere Kunden und muss die Zugriffsberechtigungen strikt voneinander trennen. Im Rahmen einer kurzfristigen Fehlkonfiguration kann es zu ungewollten Zugriffsmöglichkeiten auf das System kommen, welche es ermöglichen können, z.B. ein vollständiges Datenbankabbild zu ziehen. Eine unzureichende Mandantentrennung kann ebenfalls durch eine unzureichende Sicherheit in dem Hintergrundsystem selbst entstehen, sofern dieses Hintergrundsystem von mehreren Kunden genutzt werden kann.

Das Schadenspotential eines Daten-Leaks wird zusätzlich erhöht, sofern die zur Verschlüsselung verwendeten Schlüssel nicht selbst geschützt werden. Darüber hinaus erhöht die Verwendung des gleichen Schlüssels für mehrere Operationen das Restrisiko, da bei Erlangen eines Schlüssels ein Zugriff auf mehrere Daten erfolgen kann.

3 Prüfaspekte für Anwendungen im Finanzwesen

3.1 Prüfaspekte

Die Prüfung nach der Technischen Richtlinie deckt die minimalen Sicherheitseigenschaften von Anwendungen in Hintergrundsystemen ab. Die zu prüfende Sicherheitsfunktionalität lässt sich in folgende Prüfaspekte gliedern:

(1) Prüfung des Anwendungszwecks

(2) Prüfung der Architektur

(3) Prüfung des Quellcodes

(4) Prüfung der Drittanbieter-Software

(5) Prüfung der kryptographischen Umsetzung

(6) Prüfung der Authentifizierung

(7) Prüfung der Datenspeicherung und des Datenschutzes

(8) Prüfung der kostenpflichtigen Ressourcen

(9) Prüfung der Netzwerkkommunikation

(10) Prüfung der Organisatorischen Sicherheit

Der Hersteller dokumentiert für jeden Prüfaspekt, sofern die zu schützende Funktionalität verwendet wird, wie dessen Anforderung durch die Implementierung sichergestellt wird.

3.1.1 Prüfaspekt (1): Anwendungszweck

O.Purp_1	Das Hintergrundsystem DARF KEINE Daten erheben und verarbeiten, die nicht dem rechtmäßigen Zweck der Anwendung dienen.
O.Purp_2	Das Hintergrundsystem MUSS vor jeglicher Erfassung oder Verarbeitung personenbezogener Daten eine aktive und eindeutige Einwilligungserklärung des Nutzers einholen.
O.Purp_3	Daten, deren Verarbeitung der Nutzer nicht ausdrücklich zugestimmt hat, DÜRFEN NICHT von dem Hintergrundsystem verarbeitet werden.
O.Purp_4	Das Hintergrundsystem MUSS ermöglichen, dass der Nutzer eine bereits erteilte Einwilligung wieder entziehen kann. Der Nutzer MUSS vor der Einwilligung über die Möglichkeit des Widerrufs und die sich daraus ergebenden Veränderungen im Verhalten der Anwendung informiert werden.
O.Purp_5	Der Anbieter[3] MUSS ein Verzeichnis führen, welches erkennen lässt, welche Nutzereinwilligungen vorliegen. Der nutzerspezifische Teil des Verzeichnisses MUSS für den Nutzer automatisiert einsehbar sein. Es SOLL eine Historie dieses Verzeichnisses angefordert werden können.
O.Purp_6	Setzt das Hintergrundsystem Drittanbieter-Software ein, SOLLEN alle verwendeten Funktionen für den rechtmäßigen Zweck des Gesamtsystems erforderlich sein. Anderweitige Funktionen SOLLEN sicher deaktiviert sein. Wird nur eine einzige oder sehr wenige Funktionen der Drittanbieter-Software benötigt, SOLL abgewogen werden,

[3] Anbieter beschreibt die für die Inhalte des Produktes verantwortliche juristische Person. Hosting-Anbieter bei extern gehosteten Systemen oder Cloud-Lösungen sind hier explizit nicht gemeint.

ob die Einbindung der gesamten Drittanbieter-Software im Verhältnis zur Vergrößerung der Angriffsoberfläche durch die verwendete Drittanbieter-Software steht.

O.Purp_7 Sofern es nicht für den vorgesehenen primären oder rechtmäßigen Zweck einer Anwendung erforderlich ist, DÜRFEN sensible Daten NICHT mit Dritten geteilt werden. Dies betrifft auch die Ablage dieser Daten in Teilen des Dateisystems, auf die auch andere Anwendungen Zugriff haben. Die Anwendung MUSS den Nutzer über die Konsequenzen einer eventuellen Weitergabe von Anwendungsdaten, die dem primären oder rechtmäßigen Zweck dienen, vollumfänglich informieren und sein Einverständnis einholen (OPT-IN).

3.1.2 Prüfaspekt (2): Architektur

O.Arch_1 „Security“ MUSS ein fester Bestandteil des Softwareentwicklungs- und Lebenszyklus für die gesamte Anwendung sein.

O.Arch_2 Bereits in der Designphase des Hintergrundsystems MUSS berücksichtigt werden, dass das Hintergrundsystem der Anwendung in der Produktivphase sensible Daten verarbeiten wird. Die Architektur des Hintergrundsystems MUSS dafür die sichere Erhebung, Verarbeitung, Speicherung und Löschung der sensiblen Daten in einem Datenlebenszyklus gewährleisten.

O.Arch_3 Der Lebenszyklus von kryptographischem Schlüsselmaterial MUSS einer ausgearbeiteten Richtlinie folgen, die Eigenschaften wie die Zufallszahlenquelle, detaillierte Angaben zur Aufgabentrennung von Schlüsseln, Ablauf von Schlüsselzertifikaten, Integritätssicherung durch Hash-Algorithmen etc., umfasst. Die Richtlinie SOLL auf anerkannten Standards wie [TR02102-2] und [NIST80057] basieren.

O.Arch_4 In Backups gespeicherte sensible Daten MÜSSEN gemäß dem Stand der Technik verschlüsselt sein.

O.Arch_5 Sicherheitsfunktionen MÜSSEN immer auf allen Außenschnittstellen und API-Endpunkten implementiert werden.

O.Arch_6 Nutzt das Hintergrundsystem Drittanbieter-Software (etwa für Datenbanken, Authentifizierung oder Logging), MUSS der Hersteller sicherstellen[4], dass nur solche Drittanbieter-Software zum Einsatz kommt, deren zu nutzende Funktionen sicher genutzt werden können und dem Nutzer Informationen über den Nutzungsumfang und die eingesetzten Sicherheitsmechanismen klar darstellt. Das Hintergrundsystem MUSS diese Funktionen sicher nutzen. Der Hersteller MUSS darüber hinaus sicherstellen[4], dass ungenutzte Funktionen durch Dritte nicht aktiviert werden können.

O.Arch_7 Das Hintergrundsystem MUSS alle Anfragen der Anwendung über eine vollständig dokumentierte API entgegennehmen. Es DARF KEINE nicht dokumentierten Zugriffsmöglichkeiten enthalten.

O.Arch_8 Der Hersteller MUSS dem Nutzer eine barrierearme Möglichkeit bereitstellen, um Sicherheitsprobleme zu melden. Die Kommunikation SOLL über einen verschlüsselten Kanal stattfinden.

O.Arch_9 Das Hintergrundsystem MUSS so implementiert sein, dass ungewollte Zugriffe über eventuelle Management-Schnittstellen effektiv unterbunden werden. Insbesondere bei externem Hosting (s. Kapitel 2.3.2) und Cloud-Diensten (s. Kapitel 2.3.3) MUSS

[4] Sicherstellen meint das Abfragen einer Eigenschaft oder eines Zustands und anschließende Prüfen der Abfrage auf ein positives Ergebnis.

sichergestellt werden, dass der Betreiber Zugriffsmöglichkeiten zwischen verschiedenen Kunden unterbindet.

O.Arch_10 Dienste, die das Hintergrundsystem zur Verfügung stellt, SOLLEN nur mit den notwendigen Rechten ausgeführt werden. Dienste, die von außen erreichbar sind, DÜRFEN NICHT mit Administrator-, System- bzw. Root-Rechten laufen.

O.Arch_11 Das Hintergrundsystem MUSS über ein zentrales Protokollierungssystem verfügen, in dem alle Log-Nachrichten der verschiedenen Dienste zusammenlaufen. Protokolle SOLLEN auf einem dedizierten System (sog. Logserver) gesammelt werden, um einem Löschen und Manipulieren auf den Quellsystemen entgegenzuwirken.

O.Arch_12 Das Hintergrundsystem MUSS die Anwendung über sicherheitsrelevante Updates informieren und nach einer Übergangsfrist (Grace Period) die Benutzung einer veralteten Anwendung unterbinden.

3.1.3 Prüfaspekt (3): Quellcode

O.Source_1 Das Hintergrundsystem MUSS alle Eingaben vor deren Verarbeitung prüfen, um potenziell bösartige Werte vor der Verarbeitung herauszufiltern.

O.Source_2 Das Hintergrundsystem MUSS eingehende und ausgehende Daten maskieren beziehungsweise von potenziell schadhaften Zeichen bereinigen oder deren Verarbeitung ablehnen.

O.Source_3 Potenzielle Ausnahmen im Programmablauf (Exceptions) MÜSSEN abgefangen, kontrolliert behandelt und dokumentiert werden. Technische Fehlerbeschreibungen (z.B. Stack Traces) DÜRFEN dem Nutzer NICHT angezeigt werden.

O.Source_4 Bei Ausnahmen im Programmablauf (Exceptions SOLL das Hintergrundsystem Zugriffe auf sensible Daten abbrechen und die Anwendung anweisen, diese im Speicher sicher zu löschen.

O.Source_5 Sofern das Hintergrundsystem oder Teile davon über eine manuelle Speicherverwaltung verfügen (d.h., das entsprechende Programm kann selbst exakt festlegen, wann und wo Speicher gelesen und beschrieben wird), MUSS für lesende und schreibende Zugriffe auf Speichersegmente auf sichere Funktionsalternativen (z. B. sprintf_s statt printf) zurückgegriffen werden.

O.Source_6 Alle Optionen zur Unterstützung der Entwicklung (z. B. Entwickler-URLs, Testmethoden, Überreste von Debugmechanismen etc.) MÜSSEN in der Produktiv-Version vollständig entfernt sein.

O.Source_7 Das Hintergrundsystem MUSS sicherstellen, dass alle sensiblen Daten unverzüglich nach der Erfüllung ihres Verarbeitungszwecks sicher gelöscht werden.

O.Source_8 Der Hersteller MUSS einen Deployment-Prozess für die Inbetriebnahme, Aktualisierungen und Abschaltung des Hintergrundsystems etablieren, der sicherstellt, dass zu keinem Zeitpunkt die Veröffentlichung oder das Kompromittieren sensibler Daten möglich ist.

O.Source_9 Der Hersteller SOLL automatische Tools zur Identifikation von Programmfehlern und Best-Practice Violations im Build Process verwenden. Jegliche Warnungen MÜSSEN von dem Hersteller vor dem Produktivbetrieb mitigiert werden.

O.Source_10 Für den Bau des Hintergrundsystem SOLLEN moderne Sicherheitsmechanismen, wie beispielsweise Obfuskation und Stack-Protection aktiviert werden.

O.Source_11 Für die Entwicklung des Hintergrundsystems SOLLEN Werkzeuge zur statischen Codeanalyse eingesetzt werden.

3.1.4 Prüfaspekt (4): Drittanbieter-Software

O.TrdP_1 Der Anbieter[5] MUSS eine zentrale und vollständige Liste von Abhängigkeiten durch Drittanbieter-Software führen.

O.TrdP_2 Drittanbieter-Software MUSS in der neusten oder der ihr vorhergehenden, für die Veröffentlichung vorgesehenen Version verwendet werden.

O.TrdP_3 Drittanbieter-Software MUSS durch den Hersteller regelmäßig (durch Auswertung öffentlich verfügbarer Informationen oder durch statische/dynamische Testmethoden) auf Schwachstellen überprüft werden. Überreste von Optionen zur Unterstützung der Entwicklung (vgl. O.Source_6) sind hierbei als Schwachstelle zu werten. Der Hersteller MUSS für alle öffentlich bekannten Schwachstellen analysieren, inwieweit die Schwachstelle die Sicherheit des Gesamtsystems beeinträchtigt. Software, bzw. Funktionen aus Drittanbieter-Software DÜRFEN bei bekannten Schwachstellen, die die Sicherheit des Gesamtsystems betreffen NICHT eingesetzt werden.

O.TrdP_4 Sicherheitsupdates für Drittanbieter-Software sowie Betriebssysteme MÜSSEN zeitnah eingespielt werden. Der Hersteller MUSS ein Sicherheitskonzept vorlegen, das anhand der Kritikalität ausnutzbarer Schwachstellen die geduldete Weiternutzung für das Hintergrundsystem festlegt. Nachdem die Übergangsfrist (Grace Period) abgelaufen ist, MUSS das Hintergrundsystem bis zur Behebung der Schwachstelle deaktiviert werden.

O.TrdP_5 Vor der Verwendung von Drittanbieter-Software MUSS deren Quelle auf Vertrauenswürdigkeit geprüft werden.

O.TrdP_6 Die Anwendung SOLL sensible Daten NICHT an Drittanbieter-Software weitergeben.

O.TrdP_7 Über Drittanbieter-Software eingehende Daten MÜSSEN validiert werden.

O.TrdP_8 Drittanbieter-Software die nicht mehr gewartet wird, DARF NICHT verwendet werden.

O.TrdP_9 Wenn das Hintergrundsystem externe Dienste verwendet, die nicht unter der Kontrolle des Herstellers stehen MUSS der Nutzer über die mit den Diensten geteilten Daten informiert werden. Dies gilt auch, wenn das Hintergrundsystem oder Teile davon als Cloud-Lösung realisiert sind.

O.TrdP_10 Schnittstellen zwischen Hintergrundsystemen des Herstellers und externen Diensten müssen gemäß O.Arch_5 geschützt werden.

3.1.5 Prüfaspekt (5): Kryptographische Umsetzung

O.Cryp_1 Beim Einsatz von Verschlüsselung in der Anwendung DÜRFEN KEINE fest einprogrammierten geheimen, bzw. privaten Schlüssel eingesetzt werden.

O.Cryp_2 Die Anwendung MUSS auf bewährte Implementierungen zur Umsetzung kryptographischer Primitive und Protokolle zurückgreifen (vgl. [TR02102-2]).

O.Cryp_3 Die Wahl kryptographischer Primitive MUSS passend zum Anwendungsfall sein und dem aktuellen Stand der Technik (siehe [TR02102-1]) entsprechen.

[5] Anbieter beschreibt die für die Inhalte des Produktes verantwortliche juristische Person. Hosting-Anbieter bei extern gehosteten Systemen oder Cloud-Lösungen sind hier explizit nicht gemeint.

O.Cryp_4 Kryptographische Schlüssel DÜRFEN NICHT für mehr als genau einen Zweck eingesetzt werden. Der Hersteller des Hintergrundsystems MUSS ein Verschlüsselungskonzept vorlegen, aus dem alle verwendeten Schlüssel und deren Hierarchien hervorgehen.

O.Cryp_5 Die Stärke der kryptographischen Schlüssel MUSS dem aktuellen Stand der Technik entsprechen (siehe [TR02102-1]).

O.Cryp_6 Alle kryptographischen Schlüssel SOLLEN in einer vor Manipulation und Offenlegung geschützten Umgebung liegen.

O.Cryp_7 Alle kryptographischen Operationen SOLLEN in einer vor Manipulation und Offenlegung geschützten Umgebung stattfinden.

O.Cryp_8 Bei TLS-Verbindungen MUSS eine der in [TR02102-2], Kapitel 3.3.1 empfohlenen Cipher-Suiten verwendet werden. Verbindungen, die diese Cipher-Suiten nicht unterstützen DÜRFEN NICHT aufgebaut werden.

3.1.5.1 Zufallszahlen

O.Rand_1 Alle Zufallswerte MÜSSEN über einen starken kryptographischen Zufallszahlengenerator erzeugt werden, welcher mit ausreichend Entropie geseedet wurde (vgl. [TR02102-1]).

3.1.6 Prüfaspekt (6): Authentisierung und Authentifizierung

O.Auth_1 Der Hersteller MUSS ein Konzept zur Authentisierung auf angemessenem Vertrauensniveau (vgl. [TR03107-1]), zur Autorisierung (Rollenkonzept) und zum Beenden von Sitzungen dokumentieren. Das Konzept MUSS hierbei auch Kommunikationsverbindungen innerhalb eines Hintergrundsystem-Netzwerkes berücksichtigen.

O.Auth_2 Das Hintergrundsystem MUSS für die Anbindung einer Anwendung eine geeignete Authentisierung unterstützen.

O.Auth_3 Das Hintergrundsystem SOLL Authentisierungsmechanismen und Autorisierungsfunktionen separat realisieren. Sind für den Zugriff auf das Hintergrundsystem verschiedene Rollen notwendig, MUSS eine Autorisierung bei jedem Datenzugriff separat realisiert werden.

O.Auth_4 Jeder Authentifizierungsvorgang des Nutzers MUSS in Form einer Zwei Faktor Authentisierung umgesetzt werden.

O.Auth_5 Für die Bewertung eines Authentisierungsvorgangs SOLLEN zusätzliche Informationen (z. B. das verwendete Endgerät, die verwendete IP-Adresse oder die Zeit des Zugriffs) mit einbezogen werden.

O.Auth_6 Das Hintergrundsystem MUSS jede Anfrage gemäß des Rechte- und Rollenkonzeptes (vgl.O.Auth_1) authentifizieren und autorisieren.

O.Auth_7 Dem Nutzer SOLL eine Möglichkeit gegeben werden, sich über ungewöhnliche Anmeldevorgänge informieren zu lassen.

O.Auth_8 Das Hintergrundsystem MUSS Maßnahmen umsetzen, die ein Ausprobieren von Login-Parametern (z. B. Passwörter) erschweren.

O.Auth_9 Das Hintergrundsystem MUSS die Anwendungssitzung nach einer angemessenen Zeit, in der sie nicht aktiv verwendet wurde (idle time) beenden und eine erneute Authentisierung fordern.

O.Auth_10 Das Hintergrundsystem MUSS für die Anwendungssitzung nach einer angemessenen Zeit, in der sie aktiv verwendet wurde (active time) eine erneute Authentisierung fordern.

O.Auth_11 Die Authentisierungsdaten DÜRFEN NICHT ohne eine erneute Authentifizierung des Nutzers geändert werden.

O.Auth_12 Bei Änderung der Zugangsparameter SOLL der Nutzer über die zuletzt hinterlegten, gültigen Kontaktdaten über die Änderung informiert werden. Dem Nutzer SOLL über diesem Weg eine Möglichkeit geboten werden, die gemeldete Änderung zu sperren und nach entsprechender Authentifizierung neue Zugangsparameter zu setzen.

O.Auth_13 Der Hersteller MUSS ein Konzept zur Rechteverwaltung (z.B. Benutzerrollen) vorlegen.

O.Auth_14 Alle einem Nutzer oder einer Sitzung zugeordneten Identifier MÜSSEN mit einem Zufallszahlengenerator gemäß O.Rand_1 erzeugt werden und eine geeignete Länge aufweisen.

O.Auth_15 Das Hintergrundsystem MUSS es dem Nutzer ermöglichen ein oder alle zuvor ausgestellten Authentifizierungstoken bzw. Session-Identifier ungültig zu machen.

O.Auth_16 Wird eine Anwendungssitzung beendet, MUSS das Hintergrundsystem den Authentifizierungstoken bzw. Session-Identifier sicher löschen. Dies gilt sowohl für das aktive Beenden durch den Benutzer (log-out), als auch für das automatische Beenden durch die Anwendung (vgl. O.Auth_8und O.Auth_9).

O.Auth_17 Session-Identifier MÜSSEN als sensible Daten geschützt werden.

O.Auth_18 Es DÜRFEN KEINE sensiblen Daten in ein Authentisierungstoken eingebettet werden.

O.Auth_19 Ein Authentisierungstoken MUSS ausschließlich die erwarteten Felder enthalten.

O.Auth_20 Authentisierungstoken MÜSSEN mit einem geeigneten Verfahren signiert werden (vgl. [TR02102-1]). Das Hintergrundsystem MUSS die Signatur des Authentisierungstokens prüfen. Dabei ist darauf zu achten, dass der Signaturtyp nicht none sein darf und das Hintergrundsystem Anfragen mit einem ungültigen oder abgelaufenen Authentifizierungstoken ablehnt.

3.1.6.1 Authentifizierung über Passwort

O.Pass_1 Bei einer Authentifizierung mittels Benutzername und Passwort MÜSSEN starke Passwortrichtlinien existieren. Diese SOLLEN sich am aktuellen Stand gängiger Best-Practices orientieren.

O.Pass_2 Für die Einrichtung einer Authentisierung mittels Benutzername und Passwort KANN die Stärke des verwendeten Passworts dem Nutzer angezeigt werden. Informationen über die Stärke des gewählten Passworts DÜRFEN NICHT gespeichert werden.

O.Pass_3 Der Nutzer MUSS die Möglichkeit haben, sein Passwort zu ändern.

O.Pass_4 Das Ändern und Zurücksetzen von Passwörtern MUSS protokolliert werden ohne das Passwort selbst zu protokollieren.

O.Pass_5 Werden Passwörtergespeichert, MÜSSEN diese mit einer den aktuellen Sicherheitsstandards entsprechenden Hash-Funktion und unter Verwendung geeigneter Salts gehasht werden.

3.1.7 Prüfaspekt (7): Datensicherheit

O.Data_1 Sensible Daten MÜSSEN verschlüsselt gespeichert werden. Das Hintergrundsystem SOLL sensible Daten, verschlüsselt speichern, so dass sie nur von dem Nutzer selber wieder entschlüsselt werden können.

O.Data_2 Alle erhobenen sensiblen Daten DÜRFEN NICHT über die Dauer ihrer jeweiligen Verarbeitung hinaus im Hintergrundsystem gehalten werden.

O.Data_3 Das Hintergrundsystem MUSS die Grundsätze der Datensparsamkeit und Zweckbindung berücksichtigen.

O.Data_4 Das Hintergrundsystem MUSS sämtliche Metadaten mit Datenschutz-Relevanz, wie etwa Rückschlüsse auf den GPS-Koordinaten des Aufnahmeorts, eingesetzte Hardware etc., entfernen, wenn diese Daten nicht für den rechtmäßigen Zweck der Anwendung benötigt werden.

O.Data_5 Sensible Daten wie private Schlüssel DÜRFEN NICHT aus der Komponente, auf der sie erzeugt wurden, exportiert werden, außer es ist für den rechtmäßigen Zweck der Anwendung notwendig (s. Tabelle 15).

O.Data_6 Das Hintergrundsystem DARF KEINE sensiblen Daten in Meldungen oder Benachrichtigungen, die nicht vom Benutzer explizit eingeschaltet wurden, schreiben.

O.Data_7 Das Hintergrundsystem MUSS dem Nutzer die Möglichkeit geben, dass bei Deinstallation der Anwendung alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen vollständig vom Hintergrundsystem gelöscht bzw. unzugänglich gemacht werden. Entscheidet sich der Nutzer, die Daten im Hintergrundsystem nicht zu löschen, MUSS eine für den Zweck angemessene maximale Verweildauer definiert sein. Der Nutzer MUSS über die Verweildauer informiert werden. Nach Ablauf der maximalen Verweildauer MÜSSEN alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen vollständig gelöscht werden. Dem Nutzer MUSS die Möglichkeit gegeben werden alle Daten auch vor Ablauf der Verweildauer vollständig zu löschen oder unzugänglich zu machen.

O.Data_8 Um dem Missbrauch von sensiblen Daten nach einem Geräteverlust entgegenzuwirken, KANN die Anwendung einen Kill-Switch realisieren, d.h. ein absichtliches, sicheres Überschreiben von Nutzerdaten im Gerät auf Applikationsebene, ausgelöst durch das Hintergrundsystem. Der Hersteller MUSS die Auslösung des Kill-Switches durch den Anwender über das Hintergrundsystem durch erneute Authentifizierung vor missbräuchlicher Nutzung schützen.

3.1.8 Prüfaspekt (8): Kostenpflichtige Ressourcen

O.Paid_1 Wenn die Anwendung kostenpflichtige Leistungen anbietet, MUSS das Hintergrundsystem die durch den Nutzer erbrachten Einverständnisse sicher speichern. Das Hintergrundsystem MUSS der Anwendung die Möglichkeit geben, die erteilten Einverständnisse anzuzeigen.

O.Paid_2 Das Hintergrundsystem MUSS der Anwendung die Möglichkeit geben, die erteilten Einverständnisse zurückzuziehen.

O.Paid_3 Das Hintergrundsystem SOLL die Transaktionshistorie von zahlungspflichtigen Ressourcen und Funktionen sicher speichern. Die Transaktionshistorie, einschließlich der Metadaten, MUSS als sensibles Datum gemäß O.Purp_7 behandelt werden.

O.Paid_4 Falls die Anwendung kostenpflichtige Funktionen anbietet, MUSS der Hersteller ein Konzept vorlegen, welches vorbeugt, dass Dritte die Zahlungsströme zur Nutzung von Anwendungsfunktionen zurückverfolgen können.

O.Paid_5 Das Hintergrundsystem MUSS der Anwendung eine Möglichkeit geben, dem Nutzer eine Übersicht der entstandenen Kosten anzuzeigen. Falls die Kosten aufgrund einzelner Zugriffe erfolgt sind, MUSS die Anwendung einen Überblick der Zugriffe aufführen.

O.Paid_6 Die Validierung von getätigten Bezahlvorgängen MUSS im Hintergrundsystem vorgenommen werden.

O.Paid_7 Zahlverfahren von Drittanbietern MÜSSEN die Anforderungen an Drittanbieter-Software erfüllen (vgl. Kapitel 3.1.4).

3.1.9 Prüfaspekt (9): Netzwerkkommunikation

O.Ntwk_1 Jegliche Netzwerkkommunikation des Hintergrundsystems MUSS durchgängig verschlüsselt (zum Beispiel TLS) werden. Dies schließt auch die Kommunikation innerhalb des Hintergrundsystem-Netzwerks mit ein.

O.Ntwk_2 Jedes System eines Hintergrundsystem-Netzwerks MUSS über ein von einer beglaubigten Certification Authority ausgestelltes Zertifikat verfügen.

O.Ntwk_3 Jedes System MUSS, bei Kommunikationsverbindungen in denen es als Client fungiert, die gesamte Zertifikatskette prüfen.

O.Ntwk_4 Die Konfiguration der verschlüsselten Verbindungen MUSS dem aktuellen Stand der Technik entsprechen (vgl. [TR02102-2]).

O.Ntwk_5 Die Anwendung MUSS sicherheitsüberprüfte Drittanbieter-Software verwenden, um sichere Kommunikationskanäle aufzubauen. Dies schließt die im Betriebssystem mitgelieferte Bibliothek mit ein.

O.Ntwk_6 Das Hintergrundsystem MUSS die Integrität und Authentizität der Antworten der Anwendung validieren.

O.Ntwk_7 Das Hintergrundsystem MUSS für alle aufgebauten Verbindungen sowie Verbindungsversuche Log-Dateien vorhalten.

O.Ntwk_8 Ein abgebrochener Verbindungsaufbau MUSS als Sicherheitsereignis im Hintergrundsystem protokolliert werden.

O.Ntwk_9 Wenn das Hintergrundsystem aus mehreren Systemen besteht, die ein Netzwerk bilden, so MUSS dieses Netzwerk durch Firewalls an allen Schnittstellen nach außen geschützt werden.

O.Ntwk_10 Die Firewalls, die das Hintergrundsystem-Netzwerk schützen, MÜSSEN auf dem DENY-ALL Ansatz basieren, also explizit alle nicht erlaubten Verbindungen verwerfen.

3.1.10 Prüfaspekt (10): Organisatorische Sicherheit

O.Org_1 Der Betreiber der Hintergrundsysteme MUSS eine Zertifizierung nach [ISO27001], auf der Basis von IT-Grundschutz [BSI27001] oder einem vergleichbaren Standard nachweisen.

O.Org_2 Ist das Hintergrundsystem komplett oder teilweise als Cloud-Lösung realisiert, MUSS der Cloud-Anbieter über den gesamten Nutzungszeitraum für die genutzten Cloud-Dienste aus der genutzten Region über ein C5 Testat vom Typ 2 oder ein vergleichbares Testat oder Zertifikat verfügen. Sofern Abweichungen oder Mängel im Testat oder Zertifikat

aufgeführt werden, muss der Anbieter des Hintergrundsystems die daraus entstehenden Risiken analysieren und angemessen auf diese Risiken reagieren.

O.Org_3 Der Betreiber des Hintergrundsystems MUSS über ein Monitoring-System verfügen, das bei verdächtigen Operationen einen Alarm auslöst. Darüber hinaus KANN er zusätzlich ein Intrusion Detection/Prevention System einsetzen.

O.Org_4 Der Anbieter MUSS Prozesse für den Umgang mit jedem möglichen Alarmtyp des Monitoring-Systems definieren. Nicht definierte Alarmtypen MÜSSEN manuell bewertet werden.

O.Org_5 Der Anbieter MUSS ein Notfallvorsorgekonzept vorlegen, das beschreibt, wie die Versorgung bei Notfällen sichergestellt wird.

4 Prüfschritte einer Anwendung im Finanzwesen

4.1 Anforderungen an die Prüfung

Die TR-Prüfung von Anwendungen im Finanzwesen orientiert sich an den Prüfaspekten, die in Kapitel 3.1 aufgeführt sind. Kapitel 4.3 leitet aus den Prüfaspekten Testcharakteristika ab, welche die Anforderungen um eine Prüftiefe und Hinweise für TR-Prüfer erweitert. Unterstützend kann der Hersteller Aussagen tätigen, in denen er die betreffende Umsetzung skizziert und eine Referenz auf die jeweilige Implementierung angibt. Bei komplexen Testcharakteristika stellt der Hersteller eine umfassende Liste der Vorkommen zur Verfügung. Abhängig von der umgesetzten Prüftiefe unterstützen diese Herstelleraussagen die TR-Prüfung. Die untenstehende Tabelle legt dar, welche Prüfschritte mindestens für die jeweilige Prüftiefe gefordert sind.

Tabelle 2: Prüftiefen und Mindestanforderungen

Prüftiefe	Mindestanforderungen an die Prüfung
CHECK	Der Evaluator validiert (englisch „check“, analog zu Begriffsverwendung in der Common Criteria Evaluation Methodology) die vom Hersteller beschriebene Maßnahme im Hinblick auf ihre Wirksamkeit und räumt bestehende Zweifel (Plausibilitätsprüfung) aus, ob die Sicherheitsproblematik umfassend durch die beschriebenen Maßnahmen verhindert wird. Hierbei MUSS der Evaluator den aktuellen Stand der Technik für die jeweilige Plattform mitberücksichtigen. Die Validierung KANN weitergehende Schritte, wie z.B. eine Quelltextanalyse, umfassen, falls der Evaluator diese für eine umfassende Einschätzung benötigt.
EXAMINE	Der Evaluator untersucht (englisch „examine“, analog zu Begriffsverwendung in der Common Criteria Evaluation Methodology) die betreffende Testcharakteristik. Der Evaluator MUSS in seiner Prüfung über die Mindestanforderungen für „CHECK“ hinausgehen: In der Regel wird dies durch umfassende Quelltextanalyse der relevanten Implementierungsanteile und Penetrationstests geschehen. Die Unterstützung durch den Hersteller kann genutzt werden. „EXAMINE“ erfordert in jedem Fall eine eigenständige Beurteilung durch den Evaluator.

Aus den Prüftiefen folgt auch der Einsatz einer Quelltextanalyse bei der Begutachtung. Bei „CHECK“ wählt der TR-Prüfer aus, wie hoch die Abdeckung der Analyse für seine Einschätzung notwendig ist. Für „EXAMINE“ muss der TR-Prüfer erläutern, inwiefern sämtliche relevanten Codezeilen in Betracht gezogen wurden.

4.2 Protokollierung der Ergebnisse

Die Protokollierung der Testergebnisse ist so zu gestalten, dass unbeteiligte Dritte in die Lage versetzt werden, anhand der Angaben aus dem Prüfbericht die vorgenommen Prüfschritte zu wiederholen und dabei das gleiche Ergebnis zu erzielen. Hierzu ist es neben der Beschreibung der einzelnen Prüfschritte notwendig, dass die verwendeten Prüfwerkzeuge in den verwendeten Versionen in dem Prüfbericht ersichtlich sind. Die untenstehende Tabelle definiert die zulässigen Prüfergebnisse, welche sich aus der Prüfung einer Charakteristik ergeben können. Der TR-Prüfer begründet, wie er zu einem entsprechenden Ergebnis gekommen ist.

Tabelle 3: Mögliche Prüfergebnisse

Ergebnis	Notwendige Angaben
PASS	Der Prüfer erläutert sein Verständnis, warum die Hersteller-Implementierung das geforderte Sicherheitsziel erfüllt. Der Prüfbericht führt die durchgeführten Prüfschritte sowie das Prüfergebnis aus.
INCONCLUSIVE	Der Prüfbericht spezifiziert/referenziert die fehlenden oder inkonsistenten Informationen, damit der Hersteller die Nicht-Konformität zu dem betreffenden Aspekt des Sicherheitsziel bereinigen kann.
FAIL	Das geprüfte Hintergrundsystem verfehlt das betreffende Sicherheitsziel. Der Prüfer dokumentiert, inwiefern Angriffe durch Sicherheitsmaßnahmen in der Umgebung der Anwendung (z.B. operative Maßnahmen) verhindert werden können. Der Prüfer nimmt eine Evidenz der Verletzung der Prüfcharakteristik in die Protokollierung auf. Der Prüfer nimmt das durch die Verletzung der Testcharakteristik entstehende Risiko in die Risikoabschätzung mit auf.
NOT APPLICABLE (N/A)	Das geprüfte Hintergrundsystem verfügt über keinerlei Implementierung der durch den Prüfaspekt zu schützenden Funktionalitäten. Daher kann die betreffende Testcharakteristik nicht auf das zu prüfende Hintergrundsystem angewandt werden.

Die TR-Prüfer identifizieren bestehende Restrisiken beim Einsatz des Hintergrundsystems im Finanzwesen. Mit der Aufdeckung bestehender Restrisiken wird dem Umstand Rechnung getragen, dass der Verlust von Finanzdaten sofort zu einem Schaden für den Nutzer führt und ausreichende Schutzmaßnahmen zum Zeitpunkt der TR-Prüfung nicht identifiziert werden konnten. Die Risikobewertung muss mindestens folgende Aspekte umfassen:

- Identifikation von Risiken aus der unterlassenen oder unzureichenden Umsetzung von „SOLL"-Anforderungen in Sicherheitszielen.
- Implementierungsspezifische Risiken.
- Risiken durch Integration in der geplanten Betriebsumgebung.
- Die Eignung des Monitorings sowie im Produkt vorgesehene Reaktionsmöglichkeiten für den Betreiber in der Produktprüfung berücksichtigen.

4.3 Testcharakteristika

Die Testcharakteristiken erweitern die Prüfaspekte aus Kapitel 3 um ihre Prüftiefe und ergänzende Informationen für Evaluatoren. Der Evaluator soll über die einzelnen Prüfschritte hinaus sicherstellen, dass das betreffende Sicherheitsziel insgesamt erfüllt wird. Dies umfasst möglicherweise weitere, hier nicht aufgeführte Testcharakteristika.

4.3.1 Testcharakteristik zu Prüfaspekt (1): Anwendungszweck

Tabelle 4: Testcharakteristik: Anwendungszweck

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Purp_1	Zweckgebundene Erhebung und Verarbeitung der Daten.	CHECK	Der Evaluator prüft, ob eine Beschreibung vorhanden ist und diese den rechtmäßigen Zwecken der Anwendung entspricht. Dabei werden die vom Hersteller definierten rechtmäßige Zwecke als Grundlage genutzt. Eine juristische Prüfung der Rechtmäßigkeit ist nicht erforderlich.
O.Purp_2	Einholung einer Einwilligungserklärung des Nutzers.	CHECK	Der Evaluator prüft, ob ohne Zustimmung des Nutzers personenbezogene Daten verarbeitet werden können.
O.Purp_3	Verarbeitung ausschließlich zugestimmter Daten.	CHECK	Der Evaluator prüft, welche Daten das Hintergrundsystem verarbeitet und ob der Nutzer der Anwendung der Verarbeitung dieser Daten zugestimmt hat.
O.Purp_4	Entzug der Einwilligung ermöglichen.	CHECK	Der Evaluator prüft, ob dem Nutzer die Möglichkeit gegeben wird erteilte Einwilligungen wieder zu entziehen. Darüber hinaus validiert er, dass der Nutzer beim Entzug von Einwilligungen auf die daraus resultierenden Konsequenzen hingewiesen wird.
O.Purp_5	Führen eines Verzeichnisses der Nutzereinwilligungen.	CHECK	Der Evaluator prüft das Vorhandensein, die Aktualität und die Vollständigkeit des Verzeichnisses.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Purp_5	Nutzung nur erforderlicher Drittanbieter-Software.	CHECK	Der Evaluator prüft die Abwägungen des Herstellers bei Funktionen, die nicht dem rechtmäßigen Zweck für die Anwendung dienen. So dürfte beispielsweise eine API für soziale Netzwerke nur verwendet werden, wenn dies mit dem rechtmäßigen Zweck der Anwendung vereinbar ist. Die Risikobewertung erfasst die Auswirkungen auf den Schutz der Finanzdaten, beispielsweise bei dem für Dritte erkennbaren Nutzungsverhalten in Logging Frameworks.
O.Purp_6	Weitergabe von sensiblen Daten nur für den primären oder rechtmäßigen Zweck.	CHECK	Der Evaluator prüft die Abwägungen des Herstellers, ob die Weitergabe von sensiblen Daten an Dritte dem primären oder rechtmäßigen Zweck für die Anwendung dient. Darüber hinaus prüft er, ob die Weitergabe immer explizit durch den Nutzer erlaubt werden muss (Opt-In). Die Weitergabe an Dienste, deren primärer Zweck die Verarbeitung von Daten für Werbezwecke ist, ist generell verboten. Die Risikobewertung berücksichtigt, wie die Weitergabe von Daten an Dritte im Verhältnis zum Schutzbedarf der weitergeleiteten Informationen (Daten) und der daraus resultierenden Gefahr der Preisgabe von Informationen steht.

4.3.2 Testcharakteristik zu Prüfaspekt (2): Architektur

Tabelle 5: Testcharakteristik: Architektur

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Arch_1	„Security“ ist Bestandteil des Softwareentwicklungs- und Lebenszyklus.	CHECK	Der Evaluator prüft, ob der Quelltext und die Design-Dokumente auf die Verwendung aktueller „Best-Practices“ bei der Entwicklung schließen lassen.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Arch_2	Berücksichtigung der Verarbeitung sensibler Daten in der Design-Phase.	CHECK	Der Evaluator prüft Design- und Architektur-Dokumente auf die Berücksichtigung der Verarbeitung sensibler Daten inkl. des Datenlebenszyklus.
O.Arch_3	Dokumentation des Lebenszyklus von kryptographischem Material.	CHECK	Der Evaluator bewertet die ausgearbeitete Richtlinie des Herstellers und deren Berücksichtigung in der Risikobewertung.
O.Arch_5	Keine unverschlüsselten sensiblen Daten in Backups.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests, ob sensible Daten unverschlüsselt in Backups vorhanden sind.
O.Arch_5	Verteilte Implementierung von Sicherheitsfunktionen.	EXAMINE	Der Evaluator prüft das Vorhandensein und die Güte von Sicherheitsfunktionen durch Quelltextanalyse und praktische Tests. Als Sicherheitsfunktionen sind unter anderem Authentifizierung, Autorisierung, Input-Validierung und die Verwendung von Escape-Syntaxen zu verstehen.
O.Arch_6	Sichere Nutzung der Funktionen von Drittanbieter-Software.	EXAMINE	Der Evaluator prüft, durch Quelltextanalyse und praktische Tests, dass Funktionalitäten sicher verwendet werden und ungenutzte Funktionalitäten nicht zugänglich sind. Darüber hinaus prüft er, ob der Nutzer ausreichend über die Verwendung von Drittanbieter-Software informiert wird.
O.Arch_7	Vollständig dokumentierte API.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests, ob die Dokumentation der API die tatsächliche Funktionalität vollständig abdeckt.
O.Arch_8	Barrierearme Möglichkeit zum Melden von Sicherheitsproblemen.	CHECK	Der Evaluator prüft, ob eine entsprechende Möglichkeit vorhanden ist. Falls kein verschlüsselter Kanal bereitgestellt wird, ist dies in der Risikobewertung zu berücksichtigen.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Arch_9	Unterbindung von ungewollten Zugriffen über Management-Schnittstellen.	EXAMINE	Der Evaluator prüft die API-Dokumentation und das Sicherheitskonzept der Management-Schnittstellen. Er prüft durch Quelltextanalyse und praktische Tests die Effektivität der umgesetzten Maßnahmen.
O.Arch_10	Dienste mit minimalen Rechten.	CHECK	Der Evaluator prüft die von dem Hersteller bereitgestellte Liste aller in den Hintergrundsystemen laufenden Dienste, die Beschreibung des Zwecks des entsprechenden Dienstes und welche Rechte für diesen Zweck notwendig sind. Anschließend verifiziert der Evaluator auf den Hintergrundsystemen, ob tatsächlich nur die notwenigen Rechte erteilt werden.
O.Arch_11	Zentrales Protokollierungssystem.	CHECK	Der Evaluator prüft durch Quelltextanalyse und praktische Tests, ob alle Log-Nachrichten in einem zentralen und dafür vorgesehenen System zusammenlaufen.
O.Arch_12	Informieren der Anwendung über sicherheitsrelevante Updates.	CHECK	Der Evaluator prüft, ob das Hintergrundsystem die Anwendung über sicherheitsrelevante Updates informiert und die Benutzung einer veralteten Anwendung wirksam unterbindet.

4.3.3 Testcharakteristik zu Prüfaspekt (3): Quellcode

Tabelle 6: Testcharakteristik: Quellcode

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Source_1	Prüfung von Eingaben vor Verarbeitung.	CHECK	Der Evaluator prüft, ob für alle Eingaben Sicherheitsfunktionen gemäß O.Arch_5 vorhanden sind. Eingaben meinen jegliche Art von Daten, die in die Anwendung hineinfließen. Das sind zum Beispiel Nutzereingaben, Eingaben aus Drittanbieterkomponenten etc.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Source_2	Nutzung einer Escape-Syntax bei strukturierten Daten.	CHECK	Der Evaluator prüft, ob eine Escape-Syntax von strukturierten Daten für alle Daten gemäß O.Arch_5 vorhanden ist. Schadhafte Zeichen sind kontextabhängig zu betrachten. Im Datenbank-Kontext sind beispielsweise Hochkommata oder Prozentzeichen gegebenenfalls schadhaft, während im Web/HTML Kontext eher Tag-Klammern (<) schadhaft sind. Grundsätzlich muss die Input-Validierung daher kontextbezogen stattfinden. Wird eine potenziell schädliche Eingabe erkannt, muss sie entweder bereinigt/maskiert oder abgelehnt/verworfen werden. Das Verwerfen sollte dem Bereinigen vorgezogen werden. Sofern vorher maskierte oder bereinigte Eingaben weitergegeben werden, müssen diese so maskiert oder enkodiert werden, dass sie im Kontext der Weitergabe keine schädlichen Effekte haben.
O.Source_3	Kontrollierte Behandlung und Dokumentation von Ausnahmen („Exceptions“).	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests die kontrollierte Behandlung und Dokumentation von Exceptions.
O.Source_4	Abbruch des Zugriffs auf sensible Daten bei Exceptions.	EXAMINE	Der Evaluator prüft den Zugriff auf sensible Daten bei Ausnahmen im Programmablauf. Jeglicher identifizierte Zugriff muss in der Risikobewertung betrachtet werden.
O.Source_5	Nutzung von sicheren Funktionsalternativen beim Zugriff auf Speichersegmente.	EXAMINE	Der Evaluator prüft durch eine Quelltextanalyse, ob die Dienste des Hintergrundsystems auf unsichere Funktionen zum Zugriff auf den Speicher zurückgreift. Die Prüfung umfasst sämtlichen vom Hersteller implementierten Quelltext. Drittanbieter-Software wird in den O.TrdP Testcharakteristiken behandelt.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Source_6	Vollständige Entfernung von unterstützenden Entwicklungsoptionen und Debugmechanismen in der Produktiv-Version.	EXAMINE	Der Evaluator überprüft die produktive Version des Hintergrundsystems auf Rückstände von Optionen zur Unterstützung der Entwicklung sowie Rückstände von Zeichenketten, Debugmechanismen und Debuginformationen.
O.Source_7	Sicheres Löschen von sensiblen Daten nach ihrer Verarbeitung.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests, ob alle sensiblen Daten, welche nicht durch O.Data_1 geschützt sind, unverzüglich nach ihrer Verarbeitung sicher gelöscht werden. „Sicheres Löschen“ erfordert ein Überschreiben der Daten im Speicher. Hier ist auch auf eventuelle Kopien der Daten zu achten. Dies beinhaltet bei Programmiersprachen ohne manuelle Speicherverwaltung unter anderem das Ersetzen von Strings durch Byte-Arrays.
O.Source_8	Sicherer Deployment-Prozess.	CHECK	Der Evaluator prüft, ob der Hersteller den Deployment-Prozess vollständig dokumentiert hat und ob die getroffenen Maßnahmen und Abläufe dem Schutzniveau entsprechen.
O.Source_9	Automatische Erkennung von Programmfehlern und Best-Practice Violations	CHECK	Der Evaluator überprüft die verwendeten Tools und deren Konfiguration zur Identifikation von Programmfehlern und Best-Practice Violations hinsichtlich des Stand der Technik und der Effektivität.
O.Source_10	Aktivierung von modernen Sicherheitsmechanismen der Entwicklungsumgebung.	CHECK	Der Evaluator prüft, ob auf moderne Sicherheitsmechanismen der Entwicklungsumgebungen zurückgegriffen wurde. Sollten entsprechende Sicherheitsmechanismen nicht umgesetzt werden können, muss dies in der Risikobewertung betrachtet werden.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Source_11	Verwendung von Werkzeugen zur statischen Codeanalyse.	CHECK	Der Evaluator prüft durch Quelltextanalyse und Befragung des Herstellers, ob bei der Entwicklung Werkzeuge zur statischen Codeanalyse eingesetzt wurden. Wurden keine Werkzeuge zur statischen Codeanalyse verwendet, muss dies in der Risikobewertung betrachtet werden.

4.3.4 Testcharakteristik zu Prüfaspekt (4): Drittanbieter-Software

Tabelle 7: Testcharakteristik: Drittanbieter-Software

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.TrdP_1	Abhängigkeiten durch Drittanbieter-Software.	CHECK	Der Anbieter stellt eine Liste der eingesetzten Drittanbieter-Software inkl. der verwendeten Versionen bereit. Der Evaluator prüft die bereitgestellte Liste auf Vollständigkeit.
O.TrdP_2	Verwendung der aktuellen Version bei Drittanbieter-Software.	CHECK	Der Evaluator prüft die in O.TrdP_1 bereitgestellte Liste auf Aktualität der verwendeten Drittanbieter-Software-Versionen. Diese Abwägungen zu den gewählten Versionen werden in der Risikobewertung berücksichtigt.
O.TrdP_3	Herstellerprüfung von Drittanbieter-Software auf Schwachstellen.	CHECK	Der Anbieter stellt eine Übersicht der letzten Schwachstellenanalyse, der eingesetzten Drittanbieter-Software bereit. Diese wird vom Evaluator geprüft und in der Risikobewertung berücksichtigt. Zusätzlich prüft der Evaluator, ob der Hersteller bei Auftreten von Schwachstellen eine Mitigationsstrategie im Rahmen einer angemessenen Grace-Period bereitstellt.
O.TrdP_4	Sicherheitskonzept für zeitnahes Einspielen von Sicherheitsupdates für Drittanbieter-Software und Betriebssysteme.	CHECK	Der Evaluator prüft das Vorhandensein eines solchen Konzeptes. Eine inhaltliche Prüfung ist im Rahmen der TR nicht erforderlich. Zusätzlich prüft der Evaluator, ob der Hersteller eine Mitigationsstrategie bereitstellt.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.TrdP_5	Prüfung auf Vertrauenswürdigkeit der Quelle von Drittanbieter-Software.	CHECK	Der Evaluator prüft die Maßnahmen des Herstellers zur Verifikation der Vertrauenswürdigkeit von Drittanbietern.
O.TrdP_6	Keine Weitergabe von sensiblen Daten an Drittanbieter-Software.	EXAMINE	Der Evaluator prüft durch eine Quelltextanalyse und praktische Tests, dass keine Weitergabe von sensiblen Daten an Drittanbieter-Software vorgenommen wird. Eine Ausnahme hierzu bietet die Weitergabe von Daten, die für den primären bzw. rechtmäßigen Zweck der Anwendung erforderlich ist (beispielsweise Drittanbieter-Software zur Transportverschlüsselung). Risiken, die aus einer Nichteinhaltung resultieren, sind in der Risikobewertung zu berücksichtigen.
O.TrdP_7	Validierung eingehender Daten über Drittanbieter-Software.	CHECK	Der Evaluator prüft, ob eingehende Daten über Drittanbieter-Software gemäß O.Source_1 behandelt werden und dem Stand der Technik entsprechende Sicherheitsfunktionen gemäß vorhanden sind.
O.TrdP_8	Prüfung der Wartung von verwendeter Drittanbieter-Software.	CHECK	Der Evaluator prüft, ob die verwendete Drittanbieter-Software aktiv gepflegt wird. Eine Software gilt als nicht mehr gewartet, sofern sicherheitskritische Verwundbarkeiten bekannt sind, jedoch nicht innerhalb einer angemessenen Frist mitigiert worden sind.
O.TrdP_9	Benachrichtigung über die Verwendung externer Dienste.	CHECK	Der Evaluator prüft, welche externen Dienste verwendet werden und ob die für den Nutzer bereitgestellten Informationen durch den Hersteller vollständig sind.
O.TrdP_10	Schutzfunktionen an Schnittstellen für externe Dienste	CHECK	Der Evaluator prüft, welche externen Dienste verwendet werden und ob für alle Dienste die Anforderungen nach O.Arch_5 erfolgreich umgesetzt wurden.

4.3.5 Testcharakteristik zu Prüfaspekt (5): Kryptographische Umsetzung

Tabelle 8: Testcharakteristik: Kryptographische Umsetzung

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Cryp_1	Keine fest einprogrammierten Schlüssel oder anderweitige Geheimnisse.	EXAMINE	Der Evaluator prüft, ob fest einprogrammierte geheime, bzw. private Schlüssel eingesetzt werden. Wird ein Asset durch eine kaskadierte Verschlüsselung geschützt, soll mindestens eine Verschlüsselungsebene stark gegen Reverse Engineering geschützt sein und mindestens ein nicht-statischer Schlüssel eingesetzt werden.
O.Cryp_2	Nur bewährte Implementierungen bei kryptographischen Primitiven.	EXAMINE	Der Evaluator prüft die Liste der verwendeten Krypto-Implementierungen gegen den aktuellen Stand der Technik (vgl. [TR02102-1]).
O.Cryp_3	Passende Wahl der kryptographischen Primitive.	EXAMINE	Der Evaluator prüft die Abwägungen des Herstellers zur Wahl der kryptographischen Primitive und prüft, ob diese dem aktuellen Stand der Technik entsprechen (vgl. [TR02102-1])
O.Cryp_4	Zweckbindung kryptographischer Schlüssel.	EXAMINE	Der Evaluator prüft die verwendeten kryptographischen Schlüssel auf ihre Zweckgebundenheit. Es wird der Zweck nach Schutz durch Verschlüsselung und Authentisierung unterschieden.
O.Cryp_5	Nutzung von starken kryptographischen Schlüsseln.	EXAMINE	Der Evaluator prüft die Stärke der verwendeten Schlüssel gegen den aktuellen Stand der Technik (vgl. [TR02102-1]).
O.Cryp_6	Manipulationsschutz kryptographischer Schlüssel durch Umgebung.	EXAMINE	Der Evaluator prüft die Umgebung für die Ablage kryptographischer Schlüssel. Als sichere Umgebung gilt beispielsweise ein Hardware Sicherheitsmodul (HSM). Bei Nichteinhaltung prüft der Evaluator die Abwägungen des Herstellers zu den Auswirkungen auf die Sicherheit der Anwendungen bzw. diskutiert einen fehlenden Schutz in der Risikobewertung.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Cryp_7	Manipulationsschutz kryptographischer Operationen durch Umgebung.	EXAMINE	Der Evaluator prüft die Umgebung für die Durchführung kryptographischer Operationen analog zu O.Cryp_6.
O.Cryp_8	Empfohlene TLS-Cipher-Suiten	CHECK	Bei TLS-Verbindungen MUSS eine der in [TR02102-2], Kapitel 3.3.1 empfohlenen Cipher-Suiten verwendet werden. Verbindungen, die diese Cipher-Suiten nicht unterstützen DÜRFEN NICHT aufgebaut werden.
O.Rand_1	Erzeugung von Zufallswerten durch sicheren Zufallszahlengenerator.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests die Güte des kryptographischen Zufallszahlengenerators. Informationen zu ausreichend sicheren Zufallszahlengeneratoren sind [TR02102-1] Kapitel 10 zu entnehmen. Für die Nachbearbeitung der Zufallszahlen sind die vom BSI als ausreichend sicher angesehen Algorithmen (s.[AIS20], [TR03107-1] und [TR03116-4]) zu verwenden.

4.3.6 Testcharakteristik zu Prüfaspekt (6): Authentifizierung

Tabelle 9: Testcharakteristik: Authentisierung, Authentifizierung und Autorisierung

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Auth_1	Herstellerkonzept zur Authentisierung von Anwendungssitzungen.	CHECK	Der Evaluator prüft das vom Hersteller bereitgestellt Konzept zur Authentisierung, Autorisierung und Beenden der Anwendungssitzung. Er bewertet die Güte der eingesetzten Verfahren Anhand des aktuellen Standes der Technik.
O.Auth_2	Geeignete Authentisierung für Anwendung.	CHECK	Der Evaluator prüft, ob das Hintergrundsystem eine für die Anbindung einer Anwendung geeignete Authentisierung unterstützt.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Auth_3	Getrennte Realisierung von Authentisierungsmechanismen und Autorisierungsfunktionen.	EXAMINE	Der Evaluator prüft und bewertet die getroffenen Maßnahmen zur Trennung von Autorisierungs- und Authentisierungsmechanismen. Sollte keine Trennung der Mechanismen vorgenommen sein, sind die Abwägungen des Herstellers zu prüfen und in der Risikobewertung zu berücksichtigen.
O.Auth_4	Zwei-Faktor-Authentisierung.	EXAMINE	Der Evaluator prüft durch Quelltextanalyse und praktische Tests das Vorhandensein der Zwei-Faktor-Authentisierung. Insbesondere prüft er, ob die verwendeten Faktoren aus unterschiedlichen Kategorien stammen (Wissen, Besitz, Inhärenz) und mit dem in O.Auth_1 beschriebenem Konzept übereinstimmen.
O.Auth_5	Zusätzliche Informationen bei Bewertung des Authentisierungsvorgangs einbeziehen.	EXAMINE	Der Evaluator prüft das Vorhandensein und die Güte von zusätzlichen Informationen zur Bewertung eines Authentisierungsvorgangs. Solche Informationen können beispielsweise über die Invalidierung/Löschung von Schlüsseln oder Token umgesetzt werden. Eine Prüfung auf Konformität zum Datenschutz der erhobenen Informationen ist im Rahmen der TR nicht erforderlich, eine zusätzliche Prüfung ist daher empfehlenswert. Werden keine zusätzlichen Informationen zur Bewertung verwendet, prüft der Evaluator die Abwägungen des Herstellers. Diese sind in der Risikobewertung zu berücksichtigen.
O.Auth_6	Authentifizierung und Autorisierung von jeder Anfrage.	CHECK	Der Evaluator prüft, ob jede Anfrage an das Hintergrundsystem gemäß dem Rechte- und Rollenkonzept authentifiziert und autorisiert wird.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Auth_7	Information des Benutzers über ungewöhnliche Anmeldeversuche.	CHECK	Der Evaluator prüft, ob dem Nutzer leicht zugänglich die Möglichkeit gegeben wird, Informationen zu Anmeldevorgängen nachzuvollziehen. Ist das nicht der Fall, sind die Abwägungen des Herstellers zu prüfen und in der Risikobewertung zu berücksichtigen.
O.Auth_8	Verhinderung des Ausprobierens von Login-Parametern.	EXAMINE	Der Evaluator validiert, dass ein Ausprobieren von Login-Parametern verhindert wird. Dies kann beispielsweise durch Verzögerung nachfolgender Login-Versuche oder den Einsatz von sogenannten Captchas erreicht werden.
O.Auth_9	Erneute Authentifizierung nach angemessene Zeit in der sie nicht aktiv verwendet wurde.	CHECK	Der Evaluator validiert, dass nach einer der Anwendung angemessenen Zeit, in der sie nicht aktiv verwendet wurde, eine erneute Authentifizierung erfolgen muss. Die Güte der geforderten Authentifizierung muss dem Vertrauensniveau angemessen sein (vgl. O.Auth_4).
O.Auth_10	Erneute Authentifizierung nach angemessener Zeit in der sie dauerhaft aktiv verwendet wurde.	CHECK	Der Evaluator validiert, dass nach einer der Anwendung angemessenen Zeit, in der sie dauerhaft aktiv verwendet wurde, eine erneute Authentifizierung erfolgen muss. Die Güte der geforderten Authentifizierung muss dem Vertrauensniveau angemessen sein (vgl. O.Auth_4). Sollte die Erkennung durch das Hintergrundsystem aufgrund der gewählten Architektur nicht gewährleistet werden können, ist hiermit die Vorbereitung auf entsprechende Meldungen aus dem Vordergrundsystem zu verstehen.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Auth_11	Verhinderung nicht authentisierter Änderungen der Authentisierungsdaten.	CHECK	Der Evaluator prüft die Anforderungen zum Ändern der Authentisierungsdaten auf ihre Güte. Dies betrifft auch einen Ablauf zum Passwort zurücksetzen. Beruht dieser Ablauf bspw. auf Sicherheitsabfragen, darf die Antwort nicht einfach zu erraten oder gar aus möglicherweise öffentlichen Informationen ermittelbar sein (z.B. Mädchenname der Mutter).
O.Auth_12	Information des Benutzers über Änderung der Authentisierungsdaten.	EXAMINE	Der Evaluator prüft, ob dem Nutzer leicht zugänglich die Möglichkeit gegeben wird, Informationen über die Änderung der Authentisierungsdaten nachzuvollziehen. Darüber hinaus prüft der Evaluator durch praktische Tests die Güte des Mechanismus zum Sperren neuer Zugangsparameter. Ein besonderes Augenmerk liegt hierbei auf der Notwendigkeit einer erneuten Authentifizierung des berechtigten Nutzers. Wird durch den Hersteller kein Mechanismus zum Sperren umgesetzt, sind die Abwägungen des Herstellers zu prüfen und in der Risikobewertung zu berücksichtigen.
O.Auth_13	Dokumentation zur Rechteverwaltung	CHECK	Der Evaluator prüft das vom Hersteller bereitgestellte Konzept und bewertet dessen Güte.
O.Auth_14	Erzeugung von Identifiern für Nutzer oder Sitzungen.	EXAMINE	Der Evaluator prüft, ob die verwendeten Identifier kollisionssicher sind und nicht erraten werden können.
O.Auth_15	Invalidierung bereits ausgestellter Authentifizierungstoken bzw. Session-Identifier.	CHECK	Der Evaluator prüft, ob das Hintergrundsystem auf Anfrage des Nutzers, ein oder alle zuvor ausgestellten Authentifizierungstoken bzw. Session-Identifier invalidiert.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Auth_16	Löschen des Authentifizierungstoken bzw. Session-Identifiers nach Ende der Anwendungssitzung.	EXAMINE	Der Evaluator prüft, ob das Authentifizierungstoken bzw. der Session-Identifier nach Ende der Anwendungssitzung invalidiert wird. Hierzu testet er das Hintergrundsystem mit gültigen Abfragen, die den alten Authentifizierungstoken bzw. Session-Identifier enthalten.
O.Auth_17	Session-Identifier sind sensible Daten.	CHECK	Der Evaluator prüft, ob die Session-Identifier als sensible Daten gemäß den Anforderungen der TR behandelt werden.
O.Auth_18	Authentifizierungstoken ohne Einbettung sensibler Daten.	CHECK	Der Evaluator validiert, dass keine sensiblen Daten in ein Authentifizierungstoken eingebettet werden.
O.Auth_19	Prüfung der Inhalte des Authentifizierungstokens.	CHECK	Der Evaluator prüft, ob die Authentifizierungstoken die Standardkonformität einhalten und dass die Authentifizierungstoken ausschließlich vorgesehene Daten beinhalten.
O.Auth_20	Prüfung der Verfahren und Gültigkeit des Authentifizierungstokens.	CHECK	Der Evaluator prüft, ob das Authentifizierungstoken mit einem geeigneten Verfahren signiert wird und ob das Hintergrundsystem die Signatur und Gültigkeit des Tokens prüft.
O.Pass_1	Durchsetzung starker Passwortrichtlinien.	CHECK	Der Evaluator prüft, ob Passwortrichtlinien, welche dem aktuellen Stand der Technik entsprechen, eingesetzt werden. Andernfalls sind die Abwägungen des Herstellers zu prüfen und in der Risikobewertung zu berücksichtigen.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Pass_2	Anzeige der Stärke des verwendeten Passworts.	EXAMINE	Der Evaluator prüft, ob dem Nutzer die Stärke des verwendeten Passworts angezeigt wird. Ist dies der Fall, prüft er durch Quelltextanalyse und praktische Tests, ob dadurch Informationen über das Password oder dessen Güte im Anwendungsspeicher oder Hintergrundsystem verbleiben. Für die Prüfung des Hintergrundsystems ist eine Überwachung der verwendeten Kommunikationskanäle im praktischen Test und eine Quelltextanalyse der Anwendung ausreichend.
O.Pass_3	Möglichkeit zur Änderung des Passwortes.	CHECK	Der Evaluator prüft, ob der Nutzer die Möglichkeit hat, sein Passwort zu ändern und verifiziert, dass diese Funktionalität nicht zweckentfremdet werden kann.
O.Pass_4	Protokollierung und Information über Änderungen und Zurücksetzen von Passwörtern.	CHECK	Der Evaluator prüft das Vorhandensein und die Güte von zusätzlichen Informationen zur Protokollierung von Änderungen und dem Zurücksetzen von Passwörtern.
O.Pass_5	Verwendung von kryptographisch sicheren Hashing-Algorithmen und Salts zur Speicherung der Passwörter.	EXAMINE	Der Evaluator prüft, ob Passwörter im Hintergrundsystem gespeichert werden. Er verifiziert, dass die verwendeten Schutzmechanismen dem aktuellen Stand der Technik und den Anforderungen an Hashing-Funktionen genügen (vgl. [TR02102-1]). In der Risikobewertung werden Maßnahmen, die Brute-Force-Angriffe verlangsamen, berücksichtigt.

4.3.7 Testcharakteristik zu Prüfaspekt (7): Datensicherheit

Tabelle 10: Testcharakteristik: Datenspeicherung und Datenschutz

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Data_1	Verschlüsselung aller sensiblen Daten.	EXAMINE	Der Evaluator validiert, dass sensible Daten (s. Anhang A) im Hintergrundsystem nur verschlüsselt gespeichert werden. Der Evaluator prüft das Verschlüsselungskonzept des Herstellers und berücksichtigt die Abwägungen des Herstellers in der Risikobetrachtung.
O.Data_2	Löschung aller erhobenen sensiblen Daten nach Abschluss der Verarbeitung durch die Anwendung.	CHECK	Der Evaluator prüft, ob Daten über den Zeitraum ihrer Verarbeitung hinaus im Hintergrundsystem gehalten werden. Daten, die nicht mehr genutzt werden, müssen sicher gelöscht werden.
O.Data_3	Verarbeitung von ausschließlich für den rechtmäßigen Zweck der Anwendung notwendigen Daten.	CHECK	Der Evaluator prüft, welche Daten vom Hintergrundsystem verarbeitet werden und stellt diese dem rechtmäßigen Zweck der Anwendung gegenüber.
O.Data_4	Entfernung von Metadaten mit Datenschutzrelevanz.	CHECK	Der Evaluator prüft, ob die Anwendung Daten erheben kann, die Metadaten enthalten. In diesem Fall prüft der Evaluator, ob Metadaten mit Datenschutzrelevanz vor der weiteren Verarbeitung, wie beispielsweise dem Transfer an das Hintergrundsystem, entfernt werden. Idealerweise sollte die Entfernung schon innerhalb der Anwendung geschehen.
O.Data_5	Kein Export sensibler Daten aus der Quelle.	EXAMINE	Der Evaluator prüft, ob sensible Daten aus der Komponente, auf der sie erzeugt wurden, exportiert werden und ob dies für den Zweck notwendig ist.
O.Data_6	Keine sensiblen Daten in Meldungen	CHECK	Das Hintergrundsystem DARF KEINE sensiblen Daten in Meldungen oder Benachrichtigungen, die nicht vom Benutzer explizit eingeschaltet wurden schreiben

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Data_7	Löschen aller Daten im Hintergrundsystem	CHECK	Der Evaluator prüft, ob das Hintergrundsystem dem Nutzer die Möglichkeit gibt, dass bei Deinstallation der Anwendung alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen vollständig vom Hintergrundsystem gelöscht bzw. unzugänglich gemacht werden. Der Evaluator prüft weiterhin, ob die Vorgaben bzgl. der Verweildauer und des vorzeitigen Löschens eingehalten werden.
O.Data_8	Kill-Switch	EXAMINE	Der Evaluator prüft das Vorhandensein und die Effektivität der entsprechenden Funktion. Darüber hinaus prüft der Evaluator die Güte der Authentifizierungsmechanismen zum Schutz vor missbräuchlicher Nutzung.

4.3.8 Testcharakteristik zu Prüfaspekt (8): Kostenpflichtige Ressourcen

Tabelle 11: Testcharakteristik: Kostenpflichtige Ressourcen

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Paid_1	Speichern und Anzeigen der erteilten Einverständnisse.	CHECK	Der Evaluator prüft, ob das Hintergrundsystem die durch den Nutzer erbrachten Einverständnisse sicher speichert und ob es eine Möglichkeit für den Nutzer gibt die erteilten Einverständnisse einzusehen.
O.Paid_2	Entzug des Einverständnisses ermöglichen.	CHECK	Der Evaluator prüft, ob die Einverständnisse des Nutzers wieder zurückgezogen werden können.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Paid_3	Ablage der sensiblen Transaktionshistorie im Hintergrundsystem.	EXAMINE	Der Evaluator prüft über praktische Tests und Quelltextanalyse, ob eine Transaktionshistorie im Hintergrundsystem sicher gespeichert wird und als sensibles Datum behandelt wird. Wenn die Transaktionshistorie in der Anwendung selber gespeichert wird, ist in einer Risikobewertung darzustellen, inwieweit die Sicherheit der gespeicherten Daten gewährleistet werden kann.
O.Paid_4	Profilbildung durch Nachverfolgung der Zahlungsströme durch Dritte.	CHECK	Der Evaluator prüft, ob über die Nachverfolgung von Zahlungsströmen Rückschlüsse auf die Eigenschaften oder das Verhalten des Nutzers möglich sind. Die Abwägungen des Herstellers bei potentiellen Rückschlüssen sind in der Risikobewertung zu berücksichtigen.
O.Paid_5	Anzeige der Übersicht der entstandenen Kosten.	CHECK	Der Evaluator prüft, ob die Anwendung dem Nutzer eine Übersicht der entstandenen Kosten anbietet. Falls die Kosten aufgrund einzelner Zugriffe erfolgt sind, prüft der Evaluator, ob die Anwendung einen Überblick der Zugriffe aufführt.
O.Paid_6	Validierung von getätigten Bezahlvorgängen im Hintergrundsystem.	EXAMINE	Der Evaluator prüft durch Quelltext-analyse und praktische Tests, ob das Hintergrundsystem getätigte Bezahlvorgänge validiert.
O.Paid_7	Anforderungen bei Zahlverfahren von Drittanbietern.	CHECK	Der Evaluator prüft die Zahlverfahren durch Drittanbieter. Sowohl bei Drittanbieter-Software, als auch bei Web-Diensten wird geprüft, dass keine sensiblen Nutzerdaten an den Zahlungsdienstleister abfließen (z.B., dass der Titel der gebuchten Leistung keine sensiblen Informationen enthält).

4.3.9 Testcharakteristik zu Prüfaspekt (9): Netzwerkkommunikation

Tabelle 12: Testcharakteristik: Netzwerkkommunikation

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Ntwk_1	Netzwerkkommunikation durchgängig verschlüsselt.	EXAMINE	Der Evaluator validiert, dass ausschließlich verschlüsselte Kommunikation zwischen der Anwendung und anderen Komponenten möglich ist.
O.Ntwk_2	Zertifikate für jedes System eines Hintergrundsystem-Netzwerks.	EXAMINE	Der Evaluator prüft, ob jedes System, welches zum Hintergrundsystem gehört oder mit diesem kommuniziert, über ein von einer beglaubigten Certification Authority ausgestelltes Zertifikat verfügt.
O.Ntwk_3	Prüfung der gesamten Zertifikatskette für Systeme mit Clientfunktion.	EXAMINE	Der Evaluator prüft, ob Systeme, welche als Client fungieren, bei Kommunikationsverbindungen die gesamte Zertifikatskette prüfen.
O.Ntwk_4	Konfiguration der verschlüsselten Verbindung gemäß aktuellem Stand der Technik.	EXAMINE	Der Evaluator validiert, dass die verwendete Verschlüsselung der Kommunikation dem Stand der Technik (siehe [TR02102-2]) entspricht.
O.Ntwk_5	Sichere Kommunikationskanäle nur mit Betriebssystem-Funktionen oder sicherheitsüberprüfter Drittanbieter-Software.	EXAMINE	Der Evaluator prüft, wie ein sicherer Kommunikationskanal aufgebaut wird. Wenn keine Betriebssystem-Funktionen verwendet werden, validiert der Evaluator, dass die Drittanbieter-Software, welche zum Verbindungsabbau verwendet wird, den in Kapitel 3.1.4 beschriebenen Anforderungen genügt. Eigene Implementierungen zum Aufbau sicherer Kommunikationskanäle sind nicht zulässig.
O.Ntwk_6	Validierung der Integrität und Authentizität der Antworten der Anwendung.	EXAMINE	Der Evaluator bestätigt, dass die Integrität und Authentizität der Nachrichten der Anwendung vom Hintergrundsystem validiert werden.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Ntwk_7	Vorhaltung von vollständigen Log-Dateien für alle aufgebauten Verbindungen.	CHECK	Der Evaluator überprüft die von dem Anbieter bereitgestellten Log-Dateien und validiert, dass die HTTP-Header vollständig miterfasst sind. Wenn kein Logging sicherheitsrelevanter Ereignisse auf dem Hintergrundsystem stattfindet, muss dieser Aspekt in der Risikobewertung berücksichtigt werden.
O.Ntwk_8	Protokollierung bestimmter Sicherheitsereignisse.	CHECK	Der Evaluator validiert, dass ein abgebrochener Start und andere Sicherheitsereignisse der Anwendung protokolliert werden. Die Informationen dienen der Post-Mortem Analyse von Sicherheitsvorfällen und sollten daher Informationen über alle ausgehenden Verbindungen enthalten, unter anderem Metainformationen über verwendete Proxys und überprüfte Server-Zertifikate.
O.Ntwk_9	Schutz des Netzwerks durch Firewalls.	EXAMINE	Der Evaluator prüft, ob das Netzwerk der Hintergrundsysteme Firewalls an allen Außenschnittstellen implementiert hat. Weiterhin prüft er die Güte der Konfiguration der Firewalls.
O.Ntwk_10	Firewalls mit DENY ALL Ansatz.	CHECK	Der Evaluator prüft, ob die Firewalls auf dem DENY-ALL Ansatz basieren, also explizit alle nicht erlaubten Verbindungen verwerfen.

4.3.10 Testcharakteristik zu Prüfaspekt (10): Plattformspezifische Interaktionen

Tabelle 13: Testcharakteristik: Plattformspezifische Interaktionen

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Org_1	Zertifizierung für Hosting durch Betreiber.	CHECK	Der Evaluator prüft, ob der Betreiber eine entsprechende Zertifizierung besitzt.

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Org_2	Zertifizierung für Cloud-Umgebung.	CHECK	Der Evaluator prüft, ob der Cloud-Anbieter ein entsprechendes C5 Testat besitzt. Im Falle von Mängeln oder Auffälligkeiten, die durch das Testat identifiziert wurden, prüft der Evaluator, ob diese die Hintergrundsysteme betreffen. Auffälligkeiten und Mängel die das Hintergrundsystem betreffen sind in der Risikoanalyse zu berücksichtigen. Verfügt der Anbieter über ein zu C5 vergleichbares Testat oder Zertifikat gilt das Vorgehen analog. Ob ein Testat oder Zertifikat als vergleichbar zu C5 gilt, kann beim BSI angefragt werden.
O.Org_3	Monitoring-System.	EXAMINE	Der Evaluator prüft, ob der Betreiber des Hintergrundsystem über ein Monitoring-System verfügt, das bei verdächtigen Operationen einen Alarm auslöst.
O.Org_4	Bewertung der Monitoring-Alarme.	CHECK	Der Evaluator prüft, ob Prozesse für den Umgang mit jedem definierten Alarmtyp vorhanden sind. Nicht definierte Alarmtypen müssen manuell bewertet werden.
O.Org_5	Versorgung im Notfall.	CHECK	Der Evaluator prüft, ob der Anbieter ein Notfallkonzept zur Versorgung in Notfällen erstellt hat. Der Evaluator validiert, dass alle relevanten Szenarien durch das Konzept berücksichtigt werden.

5 Sicherheitsstufen und Risikoanalyse

Grundlage für das Prüfurteil soll ein dokumentiertes Risikomanagementverfahren sein. Als allgemeine Referenz werden BSI Standard 200-3 [BSI200-3], ISO 27005 [ISO27005] und Anhang B der Common Criteria Evaluation Methodology [CEM] genannt. Das Prüflabor darf nach Abstimmung ein vergleichbares, auf eine IT-Sicherheitsanwendung ausgerichtetes Risikomanagementverfahren einsetzen.

Die TR-Prüfer führen eine methodische Risikoanalyse durch, die mindestens folgende Schritte umfassen muss:

1. Sicherheitsproblem vollständig aufarbeiten – Ausgangspunkt der Risikoanalyse sind die Bedrohungen, Annahmen und Policies der Anwendung (Kapitel 2.44). Der TR-Prüfer etabliert eine vollständige Liste aller sensiblen Daten, die in im Hintergrundsystem verarbeitet werden.
2. Schutzbedarf feststellen – die IT-Sicherheit betrachtet generell den Schutzbedarf hinsichtlich Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit. Der TR-Prüfer klassifiziert den jeweiligen Schutzbedarf aller verarbeiteten Daten, vgl. Anhang B in [ISO27005]. Die Daten im Rahmen der TR werden anhand ihrer Kritikalität unterschieden (vgl. Tabelle 14).
3. Risikoszenarien bewerten – Der TR-Prüfer führt unter Berücksichtigung der etablierten Gegenmaßnahmen eine Bewertung von Risikoszenarien durch. Es muss dafür ein dokumentierter, ganzheitlicher Ansatz auf die sensiblen Daten der Anwendung durchgeführt werden, beispielsweise [ISO27005], Abschnitt 8.3 und Anhänge C/D/E.

In die Bewertung durch den TR-Prüfer geht ein, welche Schutzmaßnahmen im Produkt realisiert sind, und deren Effektivität (Beispielsweise Maßnahmen gegen Brute-Force Angriffe auf Login Credentials). Ebenfalls werden Vorgaben für die sichere Nutzung berücksichtigt, sofern diese dem Nutzer ausreichend dargelegt sind. Ob das Sicherheitsproblem angemessen behandelt wird, schätzen die TR-Prüfer anhand der Schwierigkeit ermittelter Angriffspfade ein. (Die Schwierigkeit eines Angriffs ersetzt dabei die in der ISO 27005 referenzierte Eintrittswahrscheinlichkeit eines Risikos.)

Häufig werden für die Angriffsbewertung auf Hintergrundsysteme folgende Bewertungsprinzipien eingesetzt:

1. Zeitbasierter Ansatz – Der Prüfer schätzt den zeitlichen Aufwand eines Angreifers um die bestehenden Gegenmaßnahmen auszuhebeln. Der Hersteller versichert, dass vor Ablauf dieser Zeit eine neue Produktversion mit neuem Schlüsselmaterial bereitgestellt wird (z.B. spätestens monatlich). Die Anwendung ist so beschaffen, dass Angriffe nur an der aktuellsten Produktversion ausgeführt werden können. In diesem Szenario wird eine Ausnutzung des Angriffspfads durch ein rechtzeitiges Update unterbunden.
2. Reaktiver Ansatz – Hier analysiert der Prüfer die effektive Bekämpfung der Risikoszenarien mittels proaktiven Monitorings / Reaktion. Beispielsweise werden Betriebsparameter erfasst und der Zugriff auf sensible Daten wird abgewehrt, sofern diese auf absichtliche Modifikationen hindeuten. Extern vom Hersteller selbst-realisierte Schutzmechanismen müssen im Rahmen der TR-Prüfung mitbetrachtet werden.

Der Prüfer muss aufgrund der ermittelten Restrisiken ein Urteil abgeben, inwiefern das von der TR adressierte Sicherheitsproblem adäquat erfüllt wird. Tabelle 14zeigt die Anforderungen je Datum. Eine Zertifizierung kann nur erteilt werden, falls die TR-Prüfung ergibt, dass die Anforderungen für alle Daten erfüllt werden.

Diese TR dient primär der Bewertung von Anwendungen, wie sie in Kapitel 1.3.1 Tabelle 14.definiert sind. Bei solchen Anwendungen ist der Schaden beim Verlust von Finanzdaten oft nicht zu beziffern, unter anderem weil eine einmal stattgefundene Offenbarung nicht mehr rückgängig gemacht werden kann. Anwendungen, die nach dieser TR evaluiert werden, können allerdings auch andere sensible Daten enthalten, die gegen Offenbarung geschützt werden müssen. Das Sicherheitsniveau dieser Daten kann ggf. unter dem der Finanzdaten liegen (vgl. Tabelle 14). Die Klassifizierung der Sicherheitsstufen für die

einzelnen Daten ist mit dem BSI im Einzelfall abzustimmen. Hierbei kann auf Risikoabschätzungen basierend auf etablierten Standards zurückgegriffen werden.

Tabelle 14: Anforderung anhand der Daten-Kritikalität

Kritikalität	Beschreibung	Anforderung
Sehr hoch	Eine Verletzung des Schutzbedarfs führt zu einem nicht zu beziffernden oder potenziell schwerwiegenden Schaden für den Dateninhaber.	Die realisierten Maßnahmen werden als wirksam erachtet sämtliche Risikoszenarien ohne Restrisiken auszuräumen.
Hoch	Eine Verletzung des Schutzbedarfs führt zu einem hohen oder mittleren Schaden für den Dateninhaber.	Die realisierten Maßnahmen reduzieren die Risikoszenarien erheblich. Der TR-Prüfer muss die Durchführung verbleibender Angriffe bewerten und deren Auswirkungen dokumentieren. Im Einzelfall ist das Restrisiko darzustellen und kann Auflagen in der Nutzung der Zertifizierung verursachen.
Normal	Es kann höchstens ein geringer Schaden eintreten.	Die realisierten Maßnahmen reduzieren die Risikoszenarien. Der TR-Prüfer muss die Durchführung verbleibender Angriffe bewerten und Restrisiken offenlegen.

Anhang A: Schutzbedarf sensibler Datenelemente

Abhängig von der realisierten Anwendung und der Kritikalität der jeweils verarbeiteten Datenelemente kann ein unterschiedlicher Schutzbedarf notwendig sein. Personenbezogene Daten unterliegen dem Datenschutz und dürfen nur bei Zweckbindung und nach Einverständnis verarbeitet werden, vgl. Abschnitt 3.1.1. Die Sensibilität verarbeiteter Datenelemente wird in der folgenden Tabelle bestimmt.

Tabelle 15: Schutzbedarf sensibler Datenelemente

Information	Sensibel	Übertragung an externe Dienste erlaubt	Bemerkungen
Daten	Ja	Nur nach ausdrücklicher Bestätigung durch den Nutzer	-
Meta-Daten	Ja	Nur nach ausdrücklicher Bestätigung durch den Nutzer	Zeit, IP-Adresse, ..
Zugangsdaten	Ja	Ja	Zulässig ist die Übertragung an Dienste zur Authentifizierung (z.B. OAuth)
Private Schlüssel für Session Handling	Ja	Nein	-
Aggregierte Anwendungsdaten z.B. Therapiebericht als PDF	Ja	Nur nach ausdrücklicher Bestätigung durch den Nutzer	-

Abkürzungsverzeichnis

Tabelle 16: Abkürzungsverzeichnis

API	Application Programming Interface (Anwendungs-/Programmierschnittstelle)
App	Applikation
A.*	Assumption (Annahme)
BSI	Bundesamt für Sicherheit in der Informationstechnik
GPS	Global Positioning System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IoT	Internet of Things
IPC	Interprozess Kommunikation
O.*	Objective (Prüfaspekt)
OSP.*	Organizational Security Policies (Organisatorische Sicherheitspolitiken)
SD-Karte	Secure Digital Memory Card
SDK	Software Development Kit
SGB V	Sozialgesetzbuch (SGB) Fünftes Buch (V)
SMS	Short Message Service
SPD	Security Problem Definition
SSID	Service Set Identifier
T.*	Threat (Bedrohung)
TR	Technische Richtlinie
TLS	Transport Layer Security

URL	Uniform Resource Locator
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

Literaturverzeichnis

[AIS20]

Bundesamt für Sicherheit in der Informationstechnik, „AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren“, 15.05.2013, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.pdf?__blob=publicationFile&v=1

[BSI200-3]

Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz“, Version 1.0, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2

[BSI27001]

Bundesamt für Sicherheit in der Informationstechnik, „ISO 27001 Zertifizierung auf Basis von IT-Grundschutz“, verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/iso-27001-basis-it-grundschutz_node.html;jsessionid=2B1D3D293ED1490742AC0E7C1DF454BE.internet482

[CEM]

Common Methodology for Information Technology Security Evaluation – Evaluation methodology, April 2017, Version 3.1, Revision 5, verfügbar unter https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

[GDR18]

we are social, „Global Digital Report 2018“, Version Januar 2018, verfügbar unter https://wearesocial.com/de/blog/2018/01/global-digital-report-2018

[gemSpec_IDP_Sek]

gematik, „Spezifikation Sektoraler Identity Provider“, verfügbar unter https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_Sek/latest/

[ISi-LANA]

Bundesamt für Sicherheit in der Informationstechnik, „Sichere Anbindung von lokalen Netzen an das Internet“, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_studie_pdf.pdf?__blob=publicationFile&v=1

[ISi-Server]

Bundesamt für Sicherheit in der Informationstechnik, „Absicherung eines Servers“, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi-server_pdf.pdf?__blob=publicationFile&v=1

[ISO27001]

ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements

[ISO27005]

BS ISO/IEC 27005:2011, Information technology - Security techniques – Information security risk management

[KCC-C5]

Bundesamt für Sicherheit in der Informationstechnik, „Kriterienkatalog Cloud Computing“, Version 2020, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2

[NIST80057]

National Institute of Standards and Technology, „Recommendation for Key Management“, Revision 5, verfügbar unter https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

[OWASP_TG]

The OWASP Foundation, „Web Security Testing Guide“, verfügbar unter https://owasp.org/www-project-web-security-testing-guide/

[OWASP_Top10]

The OWASP Foundation, „OWASP Top 10:2021“, verfügbar unter https://owasp.org/Top10/

[RTS]

EUR-Lex, „Delegierte Verordnung (EU) 2018/389 der Kommission”, 27. November 2017, verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R0389&from=EN

[T10WASR]

The OWASP Foundation, “Top 10 -2017”, Version 2017, verfügbar unter https://www.owasp.org/images/9/90/OWASP_Top_10-2017_de_V1.0.pdf

[TR02102-1]

Bundesamt für Sicherheit in der Informationstechnik, „ Kryptographische Verfahren: Empfehlungen und Schlüssellängen”, Version 2021-01, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=10

[TR02102-2]

Bundesamt für Sicherheit in der Informationstechnik, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS)”, Version 2021-01, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=2

[TR03107-1]

Bundesamt für Sicherheit in der Informationstechnik, „Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1“, Version 1.1.1, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.html

[TR03116-4]

Bundesamt für Sicherheit in der Informationstechnik, “Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4: Kommunikationsverfahren in Anwendungen”, 10. Januar 2020, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf?__blob=publicationFile&v=1

[TR03174-1]

Bundesamt für Sicherheit in der Informationstechnik, „Anforderungen an Anwendungen im Finanzwesen Teil 1: Mobile Anwendungen”, Version 2.0, verfügbar unter https://www.bsi.bund.de/dok/TR-03161-1

[TR03174-2]

Bundesamt für Sicherheit in der Informationstechnik, „Anforderungen an Anwendungen im Finanzwesen Teil 2: Web-Anwendungen”, Version 1.0, verfügbar unter https://www.bsi.bund.de/dok/TR-03161-2