Fraunhofer
SIT

IT-Sicherheitsevaluation: fymio-Gesamtlösung

Prüfbericht 17-119717

Fraunhofer-Institut für
Sichere Informationstechnologie SIT

27. Juli 2017

Öffentlich

Management Summary

Die TeamBank AG Nürnberg beauftragte das Fraunhofer-Institut für Sichere Informationstechnologie SIT für eine eingehende IT-Sicherheitsevaluation der fymio Gesamtlösung bestehend aus fymio-Android-, iOS- und Web-App und deren jeweiligen Schnittstellen im fymio-Backend im Security Test Lab des Instituts.

Die Evaluatoren nutzten vertrauliche Designunterlagen der TeamBank AG Nürnberg und den Source Code der fymio-App für Android und iOS und führten gemäß den Richtlinien und Anforderungen des Fraunhofer SIT eine IT-Sicherheitsevaluation mit konzeptioneller und praktischer Analyse durch.

Das Security Test Lab des Fraunhofer SIT untersuchte die technische IT-Sicherheit in Bezug auf Kommunikationssicherheit, Datenhaltung auf den Endgeräten, Nutzer-Authentifikation, Datenein- und -ausgabe und der Absicherung der Schnittstellen des fymio-Backends gegen missbräuchliche Verwendung und machte Vorschläge zur weiteren Verbesserung der fymio-Gesamtsicherheit. Die TeamBank AG Nürnberg hat diese Vorschläge zum Teil in die fymio-Gesamtlösung übernommen.

Das übergeordnete Ziel der bestandenen IT-Sicherheitsevaluation war es, die fymio-Gesamtlösung gegenüber gut akzeptierten Best Practices zu bewerten.

Das Fraunhofer SIT bestätigt die Einhaltung der Sicherheit der Lösung, sofern die Limitierungen und die Empfehlung der Abschnitte 3.1 und 3.2 berücksichtigt werden.

Inhaltsverzeichnis

1 Einleitung

Mit der zunehmenden Verbreitung der Informationstechnologie wächst auch die Bedeutung der IT-Sicherheit. Kunden und Verbraucher wollen deshalb immer häufiger wissen, wie sicher ein IT-Produkt oder eine entsprechende Dienstleistung ist. Das Fraunhofer-Institut für Sichere Informationstechnologie SIT ist nicht nur bestrebt, die allgemeine IT-Sicherheit zu verbessern und neue Sicherheitstechnologien und -anwendungen zu entwickeln, sondern untersucht im Auftrag von Kunden auch die IT-Sicherheitseigenschaften von Software oder softwarebasierten Systemen und Diensten.

Im Falle eines erfolgreichen Testverlaufs, bei dem ein Produkt ausreichende Sicherheitseigenschaften aufweist, vergibt das Institut ein qualifiziertes, produktspezifisches Testat. Das Fraunhofer SIT hat auf der Basis seiner langjährigen Erfahrung in der IT-Sicherheit und des Test-Know-hows hierfür eine Methodik entwickelt. Hierbei wird jeweils der gesamte Nutzungskontext der Dienstleistung oder der Systeme berücksichtigt.

Das Fraunhofer SIT wurde seitens der TeamBank AG Nürnberg kontaktiert, um das fymio-Gesamtsystem bestehend aus fymio-Android-, iOS- und Web-App und deren jeweiligen Schnittstellen im fymio-Backend einer IT-Sicherheitsevaluation zu unterziehen.

Der Testgegenstand ist ein Dienst namens fymio, der Liquiditäts- und Umsatzdaten in unterschiedlichen Formen auswertet und dem Nutzer darstellt. Dies geschieht im fymio-Backend durch Abruf und Klassifizierung der Umsatzdaten der durch den Nutzer eingerichteten Kontoverbindungen. Die Umsatzdaten werden dabei über einen Dienstleister aus den angeschlossenen Kundenkonten abgeholt und Backend-seitig auf Seite von fymio gespeichert.

Der Nutzer interagiert mit der fymio-Gesamtlösung über zwei Schnittstellen, um die aus den Umsatzdaten gewonnenen Zusatzinformationen anzuzeigen oder den Dienst zu verwalten. Zum einen existiert eine iOS- und Android-App, über welche die gesamte Funktionalität des Nutzungsszenarios ausgelöst und genutzt werden kann. Weiterhin besteht eine Web-App, bei der über einen Webbrowser die Dienste mit entsprechendem Funktionsumfang, wie in der App, genutzt und eingerichtet werden können.

Das Fraunhofer SIT führte gemäß seinen eigenen Richtlinien und Anforderungen eine IT-Sicherheitsevaluation mit konzeptioneller und praktischer Analyse durch. Diese kann mit einer Vergabe eines Fraunhofer SIT-Testats beendet werden, weil die vorgefundenen Sicherheitseigenschaften und Schutzmaßnahmen den Anforderungen entsprachen.

2 Ergebnis

Das Security Test Lab des Fraunhofer SIT bescheinigt, dass die fymio-Gesamtlösung bestehend aus fymio-Android-, iOS- und Web-App und deren jeweiligen Schnittstellen im fymio-Backend der

TeamBank AG Nürnberg
Beuthener Str. 25
90471 Nürnberg

erfolgreich die IT-Sicherheitsevaluation bestanden hat.

Das Security Test Lab des Fraunhofer SIT führte eine konzeptionelle Überprüfung der fymio-Gesamtarchitektur und einen angewandten Penetrationstest der fymio-Gesamtlösung (unterstützt durch die Quelltexte der fymio-Android- und iOS-Apps) durch.

Das Fraunhofer SIT bescheinigt, dass die fymio-Gesamtlösung Best-Practices der technischen IT-Sicherheit in Bezug auf Kommunikationssicherheit, Datenhaltung auf den Endgeräten, Nutzer-Authentifikation, Datenein- und -ausgabe und der Absicherung der Schnittstellen des fymio-Backends Schutz gegen missbräuchliche Verwendung einhält.

Hierbei sind die Limitierungen und die Empfehlung der Abschnitte 3.1 und 3.2 zu berücksichtigen.

2.1 Testierte Versionen

- fymio-Android-App: Version 3.0.0 (aus dem Google Play Store)
- fymio-iOS-App: Version 3.0.1 (aus dem Apple App Store)

Laut Auftraggeber wurden die folgenden Versionen der fymio-Web-App bzw. des fymio-Backends untersucht:

- fymio-Web-App: Version 3.0.1
- fymio-Backend: Stand Juni 2017

3 Rahmenbedingungen der IT-Sicherheitsevaluation

3.1 Limitierungen

Ausführungsplattformen

Die im Abschnitt 2 genannte Beurteilung der IT-Sicherheitseigenschaften der fymio-Gesamtarchitektur bezieht sich ausschließlich auf den Einsatz der fymio-Apps auf nicht kompromittierten Endgeräten, da die fymio-Gesamtlösung keine Schutzmechanismen (beispielsweise App-Härtung oder -Obfuskierung) gegen Angriffe mit erweiterten Rechten aufweist.

Vertrauen in externen Dienstleister

Das fymio-Nutzungsszenario und dessen Sicherheit hängt in Teilaspekten von einer Interaktion zwischen dem fymio-Backend und einem externen Dienstleister zum Abruf der Umsatzdaten ab.

Insgesamt geht das fymio-Nutzungsszenario und dessen Sicherheit von einer Vertrauensbeziehung zwischen dem fymio-Nutzer und diesem Anbieter aus.

Datenschutzaspekte und Schutz der Nutzerdaten im fymio-Backend

In der IT-Sicherheitsevaluation wurden Datenschutzaspekte des Gesamtdienstes und der Schutz der Nutzerdaten innerhalb der fymio-Backend-Infrastruktur bei den beteiligten Dienstleistern nicht betrachtet.

3.2 Empfehlung

Nutzerauthentisierung mit Nutzername und Passwort

Sicherheitsaffinen fymio-Nutzern wird in der Android und iOS fymio-App empfohlen, den Mechanismus des Einloggens mittels Nutzernamen (E-Mail-Adresse) und Passwort zu verwenden. Ein Einloggen mittels Code wird diesen Nutzern nicht empfohlen.

3.3 Annahmen

Genereller Fokus und Ausschlüsse

Um die Grenzen für diese Sicherheitsanalyse festzulegen, wurden die folgenden Überlegungen ausgeschlossen, wenn sie nicht für den Testgegenstand spezifisch waren und unabhängig auch für andere Ziele überprüft werden mussten.

Diese IT-Sicherheitsevaluation betrachtete keine Angriffe, die nicht auf bestimmten spezifischen Eigenschaften des Testgegenstands basierten, wie physischer Schaden, Vandalismus oder Social Engineering.

Wir definieren Angriffe als gezielte Aktionen, um ein bestimmtes Ziel zu erreichen. Bedrohungen durch unbeabsichtigte Handlungen oder mangelnde Kenntnisse wurden nicht betrachtet.

Darüber hinaus wurden keine Anfälligkeiten der zugrunde liegenden Ressourcen, Mechanismen oder verwendeten Technologien explizit untersucht. Diese waren jedoch für die IT-Sicherheitsevaluation dann relevant, wenn bestimmte Eigenschaften des Testgegenstands bestimmte Ressourcen, Mechanismen oder Technologien nutzten, von denen öffentlich bekannt ist, dass sie anfällig oder verwundbar sind.

Die IT-Sicherheitsanalyse konzentrierte sich daher auf Schwachstellen, die die Sicherheit der fymio-Komponenten und ihrer Umgebung innerhalb des Testgegenstands beeinträchtigen.

Ausführung und Betrieb in einem Vertrauensbereich

Die physische und netzwerktechnische Sicherheit des Betriebs des fymio-Backend wurde für garantiert erachtet und daher nicht in der IT-Sicherheitsanalyse getestet. Es wurde weiterhin davon ausgegangen, dass alle im fymio-Kontext verwendeten Backendkomponenten und die TeamBank AG Nürnberg eigenen Komponenten, mit denen das fymio-Backend interagiert, in einem gemeinsamen Vertrauensbereich liegen, in denen die Systeme, Netzwerkkomponenten und -pfade nicht mit Dritten innerhalb des Providers geteilt werden, geteilt werden könnten oder Dritte darauf Zugriff erhalten könnten.

Es wird sicherstellt, dass der physische Zugriff auf die verwendeten Systeme nur autorisiertem Personal genehmigt wird.

Angriffe und Gefährdungen ausschließlich von außerhalb des Vertrauensbereiches

Diese IT-Sicherheitsevaluation berücksichtigte ausschließlich Angriffe oder Gefährdungen außerhalb des fymio-Vertrauensbereiches. Dieser besteht aus dem fymio-Backend und anderen TeamBank AG Nürnberg eigenen Komponenten, mit denen das fymio-Backend interagiert.

Daher war die Untersuchung auf die exponierten Schnittstellen des fymio-Backends, neben den beiden fymio-Apps für Android und iOS und dem fymio-Web-Frontend beschränkt.

3.4 Sicherheitsanforderungen

Die aufgestellten Sicherheitsanforderungen für die durchgeführte IT-Sicherheitsevaluation sind im *Anhang: Sicherheitsanforderungen* beschrieben.

3.5 Angreiferklassen

Die in dieser IT-Sicherheitsevaluation relevanten Angreiferklassen wurden nach den Kategorien des generellen Wissens, des spezifischen Wissens über die fymio-Lösung und dessen Komponenten, der Berechtigungen (legitime oder nicht-legitim erlangten Berechtigungen), dem möglichen Angriffspunkt und seiner Rollenzugehörigkeit und Vorgehensweise / Handlungsrichtung charakterisiert.

Prinzipiell sind im Rahmen der Anforderungen allen denkbaren Angreifertypen der im Projekt definierten Kategorien durch technische und organisatorische Maßnahmen zu begegnen. Es werden ausschließlich interne Angreifer (beispielsweise TeamBank AG Nürnberg Mitarbeiter oder Mitarbeiter des Providers) ausgeschlossen; also diejenigen, die über legitime Berechtigungen verfügen und weiterhin diejenigen, die Zugriff auf interne Systemschnittstellen oder -daten haben.

4 Testat IT-Sicherheit: Konzept, Kriterien und Vorgehensweise

Leitidee der in diesem Projekt durchgeführten IT-Sicherheitsevaluation ist, dass ein sicheres IT-System in seinem typischen Anwendungskontext keine relevanten Sicherheitsmängel aufweist. Als relevant werden dabei alle nach dem Stand der Kunst bekannten Sicherheitslücken und durchführbare Angriffsmethoden betrachtet, welche die allgemeinen Schutzziele der Integrität, Vertraulichkeit, Verfügbarkeit und Verbindlichkeit gefährden. Dabei wird der Testgegenstand mit allen Teilkomponenten evaluiert, die typischerweise im Nutzungskontext verwendet werden. Dies umfasst in diesem Projekt die fymio-Gesamtlösung bestehend aus fymio-Android-, iOS- und Web-App und deren jeweiligen Schnittstellen im fymio-Backend.

Ausgehend von den allgemeinen Schutzzielen zur IT-Sicherheit (Integrität, Vertraulichkeit, Verfügbarkeit und Verbindlichkeit) wird der Testgegenstand an folgenden Leitfragen evaluiert:

- Welche Sicherheitsfunktionen sind vorhanden?
- Sind diese Sicherheitsfunktionen ausreichend?
- Arbeiten die Sicherheitsfunktionen korrekt?
- Bieten die Sicherheitsfunktionen einen wirksamen Schutz?

4.1 Evaluationsprinzipien

Die durchgeführte IT-Sicherheitsevaluation war abhängig von Aufwand und Zeit, die für die Evaluierung zur Verfügung steht. Um verlässliche und ausreichend qualifizierte Aussagen über den Testgegenstand zu gewährleisten, wurde deshalb das Angemessenheitsprinzip zur Selektion der Aufwände angewandt.

Dementsprechend wurden der Aufwand und die Zeit einer Evaluation dem Sicherheitsbedarf des Testgegenstands und dessen Anwendungskontext angemessen angepasst. Hierbei wurde das Konzept der mehrseitigen Sicherheit angewandt. Dies sieht eine ausgewogene Balance zwischen Schutzbedarf und Ansprüchen aller Beteiligten im vollständigen Nutzungskontext des Testgegenstands vor.

Ausgehend von diesen Konzepten untersuchte das Fraunhofer SIT die Wirksamkeit der Schutzvorrichtungen anhand folgender Fragestellungen:

- Sind die sicherheitsspezifischen Funktionen des Testgegenstands dazu geeignet, den in den Sicherheitsvorgaben aufgezählten Bedrohungen zu widerstehen?
- Wirken die sicherheitsspezifischen Funktionen und Mechanismen synergetisch zusammen, sodass sie sich gegenseitig unterstützen und ein integriertes wirksames Ganzes bilden?
- Können die Sicherheitsmechanismen des Testgegenstands einem direkten Angriff widerstehen?
- Gibt es bekannte Schwachstellen in der Konstruktion des Testgegenstands, die in der Praxis eine Sicherheitkompromittierung des Testgegenstands erlauben?
- Schützt die Konstruktion des Testgegenstands vor Sicherheitskompromittierung durch Ausnutzung bekannter Schwachstellen?
- Erlaubt der Testgegenstand eine unsichere Konfiguration, die für Nutzer, Systemverwalter oder Betreiber nicht als unsicher zu erkennen ist?

4.2 Evaluationstiefe

Die Evaluationstiefe ist von entscheidender Bedeutung für die zu erwartenden Aussagen über die Sicherheitseigenschaften eines Produkts oder Dienstes.

Dieses Projekt führte sowohl eine Evaluierung des Sicherheitsdesigns des Testgegenstands als auch der Implementierungsaspekte der betrachteten Testgegenstand-Komponenten durch.

Die Tiefe der Prüfung der Komponenten richtete sich nach den zu erwartenden Auswirkungen beim Fund von Schwachstellen sowie nach den skizzierten Bedrohungen.

Die Untersuchungen wurden dazu in einem White Box Verfahren (d.h. mit Kenntnis des internen Aufbaus des Testgegenstands und des Source Codes der Apps) durchgeführt.

4.3 Evaluationsprozess

Die IT-Sicherheitsevaluation des Testgegenstands erfolgte in Kooperation und Abstimmung mit dem Auftraggeber.

Zentraler Bestandteil der durchgeführten IT-Sicherheitsevaluation war die Festlegung der produkt- bzw. dienstspezifischen Sicherheitsanforderungen. Diese bildeten den allgemeinen Erwartungshorizont für die nachfolgenden Untersuchungen und die abschließende Bewertung. Im Zentrum der Betrachtung stand eine Bewertung des potentiellen Ausmaßes möglicher Schäden im Hinblick auf

realistische Szenarien. Das heißt, es wurde bewertet, wie sicher der Testgegenstand im Hinblick auf die Bedrohungen ist, die nach aktuellem Forschungs- und Entwicklungsstand zu erwarten sind.

Ausgangspunkt der Sicherheitsuntersuchung war eine umfassende Bedrohungsanalyse. Diese ermittelte, unter welchen Bedingungen Gefahren entstehen können und welche Bereiche des Testgegenstands diese Gefahren betreffen. Darauf folgte eine Risikoanalyse, die aus den identifizierten Gefahren mögliche Folgen ableitet. Ob ein Risiko akzeptabel ist oder nicht, spielt hierbei noch keine Rolle – die Gefahren werden zu diesem Zeitpunkt lediglich aufgenommen und priorisiert.

Mit Hilfe dieser Vorüberlegungen wurden durch struktur- und prozessorientierte Analyse des Testgegenstands konkrete Bedrohungsszenarien ausgearbeitet. Die darin festgestellten kausalen Zusammenhänge zwischen vermeintlichen Schwachstellen und möglichen Schadenspotentialen wurden durch praktische Analyse überprüft.

Das Evaluationsschema gestaltete sich dementsprechend wie folgt:

- Phase 1: IST-Analyse
  - Kategorisierung der Software-Architektur, Komponenten, Kommunikationsprotokolle und Schnittstellen
  - Identifikation potentieller Schwachstellen
  - Vor-Analyse der eingesetzten Architektur, Komponenten und Protokolle
- Phase 2: Sicherheitsanforderungen und Bedrohungsanalyse
  - Feststellung der Sicherheitsanforderungen
  - Ermittlung potentieller Bedrohungen
  - Bestimmung allgemeiner und spezifischer Risiken
  - Identifizierung möglicher Sicherheitslücken Bewertung der Sicherheitsanforderungen
- Phase 3: Sicherheitstests
  - Durchführung der Angriffsszenarien für alle relevanten Komponenten, Kommunikationsprotokolle und Schnittstellen
  - Analyse der Sicherheitsauswirkungen auf den Testgegenstand und seine Umgebung
  - Automatischer und manueller Einsatz von Werkzeugen zum Auffinden von Schwächen
  - Ergebnisdokumentation der Erkenntnisse

- Phase 4: IST/Soll-Vergleich
  - Entwicklung von Empfehlungen für Verbesserungsvorschläge zur Steigerung der Sicherheit und / oder Schließung gefundener Sicherheitslücken
  - Bei Nichterfüllung der notwendigen Sicherheitsanforderungen und Sicherheitseigenschaften kann der Testgegenstand (mehrere) Re-Evaluationen durchlaufen, bevor alle notwendigen Sicherheitsanforderungen und Sicherheitseigenschaften erfüllt werden und dadurch das Testat ausgestellt werden kann. Innerhalb dieser Re-Evaluationen werden (bei geringen Änderungen des Testgegenstands) die Phasen 3 und 4 erneut durchgeführt.

4.4 Fraunhofer-Institut für Sichere Informationstechnologie SIT

Das Fraunhofer-Institut für Sichere Informationstechnologie SIT zählt zu den weltweit führenden Forschungseinrichtungen für Cybersicherheit und Privatsphärenschutz. Das Institut beschäftigt sich mit den zentralen Sicherheitsherausforderungen in Wirtschaft, Verwaltung und Gesellschaft und betreibt praxisorientierte Spitzenforschung und Innovationsentwicklung. Zahlreiche Preise und Auszeichnungen belegen die hohe Qualität der Ergebnisse und Entwicklungen.

Die rund 180 Wissenschaftlerinnen und Wissenschaftler des Instituts beschäftigen sich mit aktuellen Fragestellungen zu Cybersicherheit und Datenschutz und entwickeln in diesem Bereich neue Technologien und konkrete Lösungen für reale Herausforderungen. Das Institut unterstützt seine Partner etwa bei der Konzeption neuer IT-Systeme, der Absicherung bestehender IT-Infrastrukturen sowie der Entwicklung neuer Produkte und Dienstleistungen. Gleichzeitig berät das Institut in wichtigen IT-Sicherheitsfragen und engagiert sich in der nationalen und internationalen Standardisierung. Als Spezialist für anwendungsnahe IT-Sicherheit entwickelt das Fraunhofer SIT unmittelbar einsetzbare Lösungen, die vollständig auf die Bedürfnisse der Auftraggeber ausgerichtet sind.

Das Fraunhofer SIT gehört zu den Impulsgebern der internationalen IT-Sicherheitslandschaft und ist Teil des Centers for Research in Security and Privacy (CRISP) in Darmstadt, dem größten Forschungszentrum zur Cybersicherheit in Deutschland und Europa. Ein Großteil der Forschung am Institut erfolgt in Kooperation mit führenden akademischen und industriellen Cybersicherheitseinrichtungen in aller Welt, insbesondere mit den führenden Cybernationen Israel und den USA.

Zudem bilden die Fraunhofer-Institute für Sichere Informationstechnologie SIT und für Graphische Datenverarbeitung IGD das Leistungszentrum für „Sicherheit und Datenschutz in der digitalen Welt“, ein Beleg für den Exzellenzstatus in der Fraunhofer-Gesellschaft e.V. Zur Erhöhung der Cybersicherheit entwickeln und verbessern die Partner gemeinsam Methoden, Werkzeuge und Prozesse.

Das Fraunhofer SIT, als ein auf IT-Sicherheit spezialisiertes Fraunhofer-Institut, beschäftigt sich u.a. mit der Analyse von gängigen Sicherheitssystemen, Sicherheitsrisiken, Schwachstellenanalyse von Produkten und Lösungen, Penetrationstests sowie sicherheitskritischen System- und Anwendungsanalysen. Es verfügt über langjähriges Know-how in der Schwachstellenanalyse und betreibt seit 2004 das Security Test Lab, das im Auftrag von Herstellern, Anwendern und Dritten IT-Systeme auf ihre Sicherheitseigenschaften untersucht.

Das Testlabor Mobile Sicherheit als Teil des Security Test Lab, in dem diese IT-Sicherheitsevaluation durchgeführt wurde, verfügt über einschlägige Erfahrung bei der Konzeption und Verifikation von Sicherheitskonzepten für mobile Umgebungen und hat fundierte Erfahrung bezüglich der Sicherheitseigenschaften mobiler Endgeräten. Zudem besteht Erfahrung mit ergänzenden Schutzmaßnahmen aus praktischen Tests und Entwicklungsprojekten. Die Kompetenzen des Testlabor Mobile Sicherheit liegen im Bereich der iOS, Android, BlackBerry und Windows Sicherheit, einschließlich der mobilen Anwendungen, der Anwendungs-Frameworks und der zugehörigen Ökosysteme. Die Erfahrung und das starke Verständnis für IT-Sicherheitsrisiken, Mobilfunksicherheit und der Anforderungen bzw. Implementierungen in Unternehmen ermöglicht es, effizient IT-Sicherheitsuntersuchungen und -bewertungen durchzuführen; mit Ergebnissen, die direkt für die Weiterentwicklung und Wartung verwendet werden können.

Das Institut besitzt mehrere Standorte, der Hauptsitz befindet sich in Darmstadt, darüber hinaus unterhält das Institut eine Zweigstelle in St. Augustin bei Bonn und ein Büro in Berlin. Außerdem kooperiert das Fraunhofer SIT mit der Hebrew University of Jerusalem in einem gemeinsamen Projekt Center in Israel. Eine weitere Zweigstelle des Instituts in Singapur befindet sich im Aufbau.

5 Disclaimer

Die Fraunhofer-Gesellschaft e.V. übernimmt keinerlei Gewähr oder Garantie für die inhaltliche Richtigkeit, Vollständigkeit oder Eignung der in dem Bericht enthaltenen Informationen für einen bestimmten Zweck, die Sicherheit des fymio-Dienstes sowie der darauf bezogenen prognostischen Aussagen. Die Nutzung der in dem Bericht enthaltenen Informationen erfolgt ausschließlich auf eigene Gefahr. Jeder Nutzer wird darauf hingewiesen unabhängige professionelle Unterstützung beim Einsatz der im Bericht behandelten Technologien in Anspruch zu nehmen. Es können hieraus weder Ansprüche gegen die Fraunhofer-Gesellschaft e.V. noch die Berechtigung zur Nutzung des fymio-Dienst hergeleitet werden.

A Anhang: Sicherheitsanforderungen

Es ist üblich, als Grundwerte der Informationssicherheit die drei Schutzziele Vertraulichkeit, Integrität und Authentizität zu unterscheiden. Daneben lassen sich weitere, zum Teil aus diesen drei Grundwerten abgeleitete, zum Teil diese ergänzende Schutzziele formulieren, um einem gegebenen Anwendungskontext gerecht zu werden. In diesem Test werden zusätzlich zu den drei genannten Grundwerten die Aspekte Zugriffskontrolle sowie Nachvollziehbarkeit berücksichtigt.

In diesen Abschnitt werden zu erreichende, für eine Testatsvergabe notwendige umzusetzende Schutzziele der fymio-App, der fymio-Web-App und des fymio-Backends im Kontext von Finanzdienstleistungen oder im Kontext sensibler Kundendaten beschrieben.

A.1 Sicherheitsanforderungen bezüglich der fymio-App

A.1.1 Authentizität

Authentizität des User-Interfaces zwischen der App und dem Nutzer (Req A 1.1)

Der Nutzer sollte durch geeignete Maßnahmen innerhalb der App in die Lage versetzt werden sicherzustellen, dass er eine Interaktion mit der realen fymio-App auf Android und iOS durchführt. Externe Apps, welche die Interaktion des Nutzers mit der realen fymio-App auf Android und iOS auf unterschiedlichen Wegen übernehmen, sind daher zu detektieren oder diese Vorgehensweise ist durch geeignete Maßnahmen abzuwehren.

Authentizität des Nutzers gegenüber der App (lokale Authentifizierung des Nutzers) (Req A 1.2)

Die fymio-App auf Android und iOS ist durch geeignete Maßnahmen in die Lage zu versetzen, selbst zweifelsfrei beurteilen zu können, dass der legitime Nutzer die Interaktionen mit ihr durchführt. Hierzu muss sich der Nutzer gegenüber der App authentifizieren.

Authentizität der Interaktion zwischen der fymio-App und Kommunikationspartnern (Req A 1.3)

Die fymio-App auf Android und iOS hat die Identität von Kommunikationspartnern, mit denen sie interagiert, zu prüfen bevor ein Austausch (vertraulicher) Daten oder eine Ressourcenzuweisung beginnt. In allen Fällen, in denen (vertrauliche) Daten übertragen werden, muss gewährleistet sein, dass die Gegenstelle authentisch ist.

Authentizität der App (Req A 1.4)[1]

Die fymio-App auf Android und iOS muss durch geeignete Maßnahmen innerhalb der App zur Laufzeit selbst zweifelsfrei beurteilen können, ob sie vom ursprünglichen Herausgeber erzeugt wurde und noch authentisch ist.

Authentizität der Interaktion zwischen Nutzer und Backend (Req A 1.5)

Der Nutzer muss sich vor jeder Aktion mittels der fymio-App gegenüber dem Dienst authentisieren, um vom Backend authentifiziert werden zu können.

Keine ausschließlich lokale Authentifizierung (Req A1.6)

Um eine Aktion auszuführen genügt es nicht, den Nutzer lediglich durch die App zu authentifizieren. Die Authentifizierung des Nutzers muss immer durch das fymio-Backend erfolgen.

A.1.2 Zugriffskontrolle

Zugriffsschutz der Nutzerdaten (Req A 2.1)

Die fymio-App auf Android und iOS hat den Zugang zu persönlichen Nutzerdaten auf autorisierte Entitäten zu beschränken. Jeder unberechtigte Zugang und jede unbefugte Offenlegung von Benutzerdaten über die fymio-App auf Android und iOS als eine Art Tunnel unter Umgehung der Sicherheitszonen ist daher zu verhindern.

Zugriffskontrolle auf Schnittstellen (Req A 2.2)

Die fymio-App auf Android und iOS nutzt unterschiedliche Schnittstellen zur Kommunikation mit anderen Entitäten innerhalb des Nutzungskontexts. Es besteht das Schutzziel, dass der Zugang zu diesen Schnittstellen stets mittels dezidierter Zugriffskontrollmechanismen durchgesetzt wird. Die fymio-App auf Android und iOS hat für jeden Kommunikationspartner zu bestimmen, ob dieser die Rechte zum Ausführen eines bestimmten Kommunikationsprozesses oder zur Nutzung einer bestimmten Schnittstelle hat.

[1] nicht erfüllt, daher Limitierung in Abschnitt 3.1

Brute-Force-Schutz der App (Req A 2.3)

Die fymio-App sollte Maßnahmen ergreifen, die einen Brute-Force-Angriff auf die App internen Schnittstellen nur unter hohem Aufwand und/oder Kosten ermöglicht.

A.1.3 Vertraulichkeit

Vertrauliche Speicherung sensibler Daten (Req A 3.1)

Es muss sichergestellt werden, dass sensible Daten vor, während und nach ihrer Verarbeitung in der fymio-App auf sichere Art und Weise gespeichert, archiviert oder gelöscht werden. Die fymio-App auf Android und iOS muss Zugangsdaten, zwischengespeicherte Daten, Protokolldaten, Laufzeitdaten und temporäre Daten mit sensiblen Inhalt vor unbefugter Informationsgewinnung schützen und für diese Daten eine sichere Datenverarbeitung gemäß o.g. Definition umsetzen.

Korrekte Nutzung kryptografischer Funktionen (Req A 3.2)

Die kryptografischen Algorithmen, die innerhalb der fymio-App auf Android und iOS verwendet werden, müssen korrekt umgesetzt werden und den entsprechenden Standardalgorithmen entsprechen.

Vertraulichkeit der Interaktion zwischen dem Nutzer und der App (Req A 3.3)

Alle Daten und Informationen, die in der Interaktion zwischen der App und dem Nutzer erzeugt werden, sind von der fymio-App gegenüber Dritten vor unberechtigter Informationsgewinnung zu schützen.

Vertraulichkeit der Interaktion zwischen der fymio-App und Kommunikationspartnern (Req A 3.4)

Alle Daten und Informationen, die in der Interaktion zwischen der fymio-App und Kommunikationspartnern übermittelt werden, sind von der fymio-App gegenüber Dritten vor unberechtigter Informationsgewinnung zu schützen.

Keine versteckten Funktionen (Req A 3.5)

Es darf keine Möglichkeit in der App bestehen, die es Dritten ermöglicht, undokumentierte Funktionen auszuführen, die einen negativen Einfluss auf die Sicherheit der Nutzerdaten haben.

Keine fest einkodierten Passwörter und kryptografischen Schlüssel (Req A 3.6)

Innerhalb der fymio-App sollten keine Passwörter, sonstige Credentials oder kryptografische Schlüssel im Quelltext der App fest einkodiert oder in Dateien des App-Bundles abgelegt werden, wenn diese als alleiniges Merkmal für Authentifikation oder Autorisation verwendet werden.

Sensible Daten unmittelbar nach Verwendung löschen (Req A 3.7)

Um ein nachträgliches Auslesen zu vermeiden, sollten sensible Informationen (z.B. Cookies, Token, o.ä.) umgehend nach der Verwendung im Arbeitsspeicher gelöscht werden und nicht im Dateisystem abgelegt werden. Sollte eine Speicherung unbedingt funktional notwendig sein, sollten diese Dateien direkt nach der Verwendung ebenfalls gelöscht werden.

Kein Logging sensibler Daten (Req A 3.8)

Sensible Daten (z.B. Passwörter, PIN o. Bankdaten) sollten nicht von der App geloggt werden. Ausgaben auf der Konsole sollten vermieden werden.

Anwendung des Minimalitätsprinzips (Req A 3.9)

Es sollten innerhalb der fymio-App die für den jeweiligen Nutzungskontext *minimal* notwendigen Daten erfasst, verarbeitet oder erzeugt werden.

Keine direkte Speicherung von App-spezifischen Nutzergeheimnissen (Req A 3.10)

Nutzergeheimnisse innerhalb der fymio-App dürfen nicht auf dem Gerät gespeichert werden.

Durchführung einer Schlüsselableitung aus dem App-spezifischen Nutzergeheimnis (Req A 3.11)

Es muss ein Schlüsselableitungsverfahren verwendet werden, um aus dem App-spezifischen Nutzergeheimnis einen Schlüssel zur Sicherung bzw. Entschlüsselung von sensiblen App-Daten abzuleiten.

A.1.4 Integrität

Schutz vor Manipulation der App (Req A 4.1)[2]

Die fymio-App auf Android und iOS muss durch geeignete Maßnahmen innerhalb der App zur Laufzeit beurteilen können, ob ein Dritter sie manipuliert hat.

[2] nicht erfüllt, daher Limitierung in Abschnitt 3.1

Überprüfung der Integrität der Ausführungsplattform (Req A 4.2)[3]

Die fymio-App auf Android und iOS muss durch geeignete Maßnahmen innerhalb der App zur Laufzeit beurteilen können, ob ein Dritter die Ausführungsplattform (beispielsweise durch Jailbreaking oder Rooting) manipuliert hat.

Eingabe- und Ausgabevalidierung (Req A 4.3)

Alle Daten, die von außen über eine Schnittstelle in die fymio-App gelangen, sollten validiert werden, bevor sie verarbeitet oder angezeigt werden. Neben der Korrektheit der Datenstruktur sollte auch die Plausibilität der Eingaben überprüft werden. Dabei ist zu gewährleisten, dass durch Manipulationen keine negativen Auswirkungen im Hinblick auf die Sicherheit des Gesamtsystems verursacht werden. (Bewusst) fehlerhafte, unterdrückte oder duplizierte Nachrichten, Daten oder Aktivitäten sind zu detektieren und in allen Fällen ist Störungssicherheit zu gewährleisten.

A.1.5 Nachvollziehbarkeit

Kein Sicherheitsverlust durch falsche GUI Nutzer-Interpretation (Req A 5.1)

Die Grafische Nutzeroberfläche (GUI) der fymio-App auf Android und iOS darf keine unklaren Optionen beinhalten, die den Benutzer auf Basis dieser unklaren Definition dazu führen können, versehentlich eine Einstellung mit negativem Einfluss auf die Gesamtsicherheit zu tätigen. Jede Beschreibung der sicherheitsrelevanten Einstellungen sollte deutlich ihre Wirkung darstellen und sollte keinen Auslegungsspielraum lassen.

A.1.6 Sonstige Anforderungen

Hinführen zu ausreichend langen und komplexen Passwörtern (Req A 6.1)

Die fymio-App sollte den Nutzer dazu auffordern, ein ausreichend langes und komplexes Passwort zu definieren. Es sollte erschwert werden kurze Passwörter oder Passwörter mit eingeschränktem Schlüsselraum zu verwenden.

App Härtung (Req A 6.2)[4]

Die fymio-App sollte Maßnahmen gegen Reverse Engineering und Laufzeitmodifikationen enthalten. Diese sollten dem State-of-the-Art entsprechen.

[3] nicht erfüllt, daher Limitierung in Abschnitt 3.1
[4] nicht erfüllt, daher Limitierung in Abschnitt 3.1

A.2 Sicherheitsanforderungen bezüglich der fymio-Web-App

A.2.1 Authentizität

Authentizität der Interaktion zwischen der fymio-Web-App und dem Nutzer (Req W 1.1)

Der Nutzer sollte durch geeignete Maßnahmen innerhalb der fymio-Web-App in die Lage versetzt werden, stets überprüfen zu können, ob er eine Interaktion mit der realen fymio-Web-App durchführt. Angriffe innerhalb des Webbrowsers, die die Interaktion des Nutzers mit der realen fymio-Web-App auf unterschiedlichen Wegen übernehmen, sind daher zu detektieren oder diese Vorgehensweise ist durch geeignete Maßnahmen abzuwehren.

Authentizität der Interaktion zwischen der fymio-Web-App und dem fymio-Backend (Req W 1.2)

Die fymio-Web-App hat die Identität des fymio-Backend, mit dem sie und deren Prozesse interagiert, zu prüfen, bevor ein Austausch (vertraulicher) Daten oder eine Ressourcenzuweisung beginnt. In allen Fällen, in denen (vertrauliche) Daten übertragen werden, muss gewährleistet sein, dass die Gegenstelle authentisch ist.

A.2.2 Zugriffskontrolle

Zugriffsschutz der Nutzerdaten (Req W 2.1)

Die fymio-Web-App hat den Zugang zu persönlichen Nutzerdaten auf autorisierte Entitäten zu beschränken. Jeder unberechtigte Zugang und jede unbefugte Offenlegung von Benutzerdaten über die fymio-Web-App als eine Art Tunnel unter Umgehung der Sicherheitszonen ist daher zu verhindern.

Zugriffskontrolle auf Schnittstellen (Req W 2.2)

Die fymio-Web-App nutzt unterschiedliche Schnittstellen zur Kommunikation mit anderen Entitäten innerhalb des Nutzungskontexts. Es besteht das Schutzziel, dass der Zugang zu diesen Schnittstellen stets mittels dezidierter Zugriffskontrollmechanismen durchgesetzt wird. Die fymio-Web-App hat für jeden Kommunikationspartner zu bestimmen, ob dieser die Rechte zum Ausführen eines bestimmten Kommunikationsprozesses oder zur Nutzung einer bestimmten Schnittstelle hat.

A.2.3 Vertraulichkeit

Vertrauliche Speicherung sensibler Daten (Req W 3.1)

Es muss sichergestellt werden, dass sensible Daten vor, während und nach ihrer Verarbeitung in der fymio-Web-App auf sichere Art und Weise gespeichert, archiviert oder gelöscht werden. Die fymio-Web-App muss Zugangsdaten, zwischengespeicherte Daten, Protokolldaten, Laufzeitdaten und temporäre Daten mit sensiblen Inhalt vor unbefugter Informationsgewinnung schützen und für diese Daten eine sichere Datenverarbeitung gemäß o.g. Definition umsetzen.

Korrekte Nutzung kryptografischer Funktionen (Req W 3.2)

Die kryptografischen Algorithmen, die innerhalb der fymio-Web-App verwendet werden, müssen ordnungsgemäß umgesetzt werden und den entsprechenden Standardalgorithmen entsprechen.

Vertraulichkeit der Interaktion zwischen der fymio-Web-App und dem Nutzer (Req W 3.3)

Alle Daten, die in der Interaktion zwischen der fymio-Web-App und dem Nutzer erzeugt werden, sind von der fymio-Web-App gegenüber Dritten vor unberechtigter Informationsgewinnung zu schützen.

Vertraulichkeit der Interaktion zwischen der fymio-Web-App und dem fymio-Backend (Req W 3.4)

Alle Daten, die in der Interaktion zwischen der fymio-Web-App und dem fymio-Backend erzeugt werden, sind von der fymio-Web-App gegenüber Dritten vor unberechtigter Informationsgewinnung zu schützen.

Keine versteckten Funktionen (Req W 3.5)

Es darf keine Möglichkeit in der fymio-Web-App bestehen, die es Dritten ermöglicht, undokumentierte Funktionen auszuführen, die einen negativen Einfluss auf die Sicherheit der Nutzerdaten haben.

A.2.4 Integrität

Eingabe- und Ausgabevalidierung (Req W 4.1)[5]

Alle Daten, die von außen über eine Schnittstelle in die fymio-Web-App gelangen, sollten validiert werden, bevor sie verarbeitet oder angezeigt werden. Neben der Korrektheit der Datenstruktur sollte auch die Plausibilität der Eingaben überprüft werden. Dabei ist zu gewährleisten, dass durch Manipulationen

[5] für eine Schnittstelle mit dem externen Dienstleister zum Abruf der Umsatzdaten nicht vollständig erfüllt, daher Limitierung in Abschnitt 3.1

keine negativen Auswirkungen im Hinblick auf die Sicherheit des Gesamtsystems verursacht werden. (Bewusst) fehlerhafte, unterdrückte oder duplizierte Nachrichten, Daten oder Aktivitäten sind zu detektieren und in allen Fällen ist Störungssicherheit zu gewährleisten.

Verhinderung von Manipulationen in der Interaktion zwischen der fymio-Web-App und dem Nutzer (Req W 4.2)

Die fymio-Web-App sollte vorhandenen Schutzmaßnahmen im Webbrowser anwenden, die Angriffe auf die Interaktion zwischen der fymio-Web-App und dem Nutzer zielen.

A.2.5 Sonstige Anforderungen

Hinführen zu ausreichend langen und komplexen Passwörtern (Req W 5.1)

Die fymio-App sollte den Nutzer dazu auffordern, ein ausreichend langes und komplexes Passwort zu definieren. Es sollte erschwert werden kurze Passwörter oder Passwörter mit eingeschränktem Schlüsselraum zu verwenden.

Überprüfen verwendeter Bibliotheken auf bekannte Verwundbarkeiten (Req W 5.2)

Alle in der fymio-Web-App verwendeten Drittanbieter Bibliotheken sollten keine bekannten, in Verwundbarkeitsbibliotheken gelisteten, Schwachstellen enthalten.

WebApp Härtung (Req W 5.3)

Die fymio-Web-App sollte Maßnahmen gegen Reverse Engineering enthalten.

A.3 Sicherheitsanforderungen bezüglich des fymio-Backend

A.3.1 Authentizität

Authentizität der Interaktion mit externen Entitäten (Req B 1.1)

Jede fymio-interne Backendkomponente hat die Identität der anderen externen Entitäten, mit denen sie und deren Prozesse interagiert, zu prüfen, bevor ein Austausch sensibler Daten beginnt. Dies betrifft alle Kommunikationsprozesse, in denen der Vertrauensbereich des fymio-Backend (Bereich des fymio-Backend, in dem alle im fymio-Kontext verwendeten Backendkomponenten und die TeamBank AG Nürnberg eigenen Komponenten, mit denen das fymio-Backend interagiert, verortet sind in denen die Systeme, Netzwerkkomponenten

und -pfade nicht mit Dritten innerhalb des Providers geteilt werden, geteilt werden könnten oder Dritte darauf Zugriff erhalten könnten) oder der TeamBank AG Nürnberg verlassen wird. In allen Fällen, in denen sensible Daten an externer Entitäten übertragen werden, muss gewährleistet sein, dass die Gegenstelle authentisch ist.

A.3.2 Zugriffskontrolle

Zugriffsschutz auf sensible Nutzerdaten (Req B 2.1)

Der Zugang zu sensiblen Daten von Nutzern ist auf autorisierte und legitimierte Nutzer zu beschränken. Jeglicher unbefugte Zugriff auf Daten mit Hilfe des fymio Gesamtsystems als eine Art Tunnel unter Umgehung der Sicherheitszonen ist zu verhindern.

Schutz vor systematischem Ausprobieren von Zugangsdaten (Req B 2.2)[6]

Ein übliches Angriffsschema zur Überwindung einer Zugriffskontrolle ist das systematische Ausprobieren von Zugangsdaten (Passwort, Token, ...) so lange, bis eine gültiges Datum gefunden wurde. Es sollte daher serverseitig eine Überwachung umgesetzt sein, die solche Angriffe erkennt und entsprechende Gegenmaßnahmen einleitet, um den Angriff zu unterbinden oder so weit zu verlangsamen, dass dieser für den Angreifer uninteressant wird.

Keine fest einkodierten Zugangsdaten (Req B 2.3)

Zur Authentifikation an den öffentlich erreichbaren Schnittstellen sollten ausschließlich benutzerspezifische Credentials verwendet werden. Statische Passwörter oder sonstige Credentials dürfen nicht als alleiniges Authentifikationsmerkmal verwendet werden.

A.3.3 Vertraulichkeit

Vertraulichkeit der Interaktion mit externen Entitäten (Req B 3.1)

Sollten sensible, durch das fymio-Backend erhobene oder erzeugte Daten an externe (auch TeamBank AG Nürnberg-interne) Komponenten weitergegeben werden, so ist sicherzustellen, dass stets durch Verschlüsselung geschützte Kommunikationskanäle (beispielsweise HTTPS oder VPN) verwendet werden.

Dies betrifft alle Kommunikationsprozesse, in denen der Vertrauensbereich des fymio-Backend (Bereich des fymio-Backend, in dem alle im fymio-Kontext verwendeten Backendkomponenten und die TeamBank AG Nürnberg eigenen Komponenten, mit denen das fymio-Backend interagiert, verortet sind in denen die Systeme, Netzwerkkomponenten und -pfade nicht mit Dritten innerhalb

[6] nicht vollständig erfüllt, daher Empfehlung in Abschnitt 3.2

des Providers geteilt werden, geteilt werden könnten oder Dritte darauf Zugriff erhalten könnten) oder der TeamBank AG Nürnberg verlassen wird.

Korrekte Nutzung kryptografischer Funktionen (Req B 3.2)

Die kryptografischen Algorithmen, die innerhalb des fymio-Backend verwendet werden, müssen ordnungsgemäß umgesetzt werden und den entsprechenden Standardalgorithmen entsprechen.

Vertraulichkeit der Interaktion zwischen der fymio-App und dem fymio-Backend (Req B 3.3)

Alle sensiblen Daten, die in der Interaktion zwischen der fymio-App und dem fymio-Backend erzeugt werden, sind von dem fymio-Backend gegenüber Dritten vor unberechtigter Informationsgewinnung zu schützen.

Vertraulichkeit der Interaktion zwischen dem fymio-Web-App und dem fymio-Backend (Req B 3.4)

Alle sensiblen Daten, die in der Interaktion zwischen dem fymio-Web-App und dem fymio-Backend erzeugt werden, sind von dem fymio-Backend gegenüber Dritten vor unberechtigter Informationsgewinnung zu schützen.

Vertraulichkeit der vom fymio-Backend versandten E-Mails (Req B 3.5)

Alle E-Mails, welche vom fymio-Backend zu Kunden versendet werden, sollten nicht im Klartext übermittelt werden. Als Minimum wird eine Transportverschlüsselung zwischen den verwendeten SMTP-Server angesehen.

A.3.4 Integrität

Detektion von Manipulationen in der Interaktion mit externen Entitäten (Req B 4.1)

Das fymio-Backend nutzt unterschiedliche externe Schnittstellen zur Kommunikation mit anderen Entitäten innerhalb des Nutzungskontexts. Dies betrifft alle Kommunikationsprozesse, in denen der Vertrauensbereich des fymio-Backend (Bereich des fymio-Backend, in dem alle im fymio-Kontext verwendeten Backendkomponenten und die TeamBank AG Nürnberg eigenen Komponenten, mit denen das fymio-Backend interagiert, verortet sind in denen die Systeme, Netzwerkkomponenten und -pfade nicht mit Dritten innerhalb des Providers geteilt werden, geteilt werden könnten oder Dritte darauf Zugriff erhalten könnten) oder der TeamBank AG Nürnberg verlassen wird. Es besteht das Schutzziel, dass diese externe Kommunikation stets integritätsgesichert durchzuführen ist.

Detektion von Manipulationen in der Interaktion zwischen der fymio-App und dem fymio-Backend (Req B 4.2)

Ein Integritätsschutz hat auf der Schnittstelle zwischen der fymio-App auf Android und iOS und dem fymio-Backend zu gewährleisten, dass durch Manipulationen keine negativen Auswirkungen im Hinblick auf die Sicherheit des Gesamtsystems verursacht werden. (Bewusst) fehlerhafte, unterdrückte oder duplizierte Nachrichten, Daten oder Aktivitäten sind zu detektieren und in allen Fällen ist Störungssicherheit zu gewährleisten.

Detektion von Manipulationen in der Interaktion zwischen der fymio-Web-App und dem fymio-Backend (Req B 4.3)

Ein Integritätsschutz hat auf der Schnittstelle zwischen der fymio-Web-App und dem fymio-Backend zu gewährleisten, dass durch Manipulationen keine negativen Auswirkungen im Hinblick auf die Sicherheit des Gesamtsystems verursacht werden. (Bewusst) fehlerhafte, unterdrückte oder duplizierte Nachrichten, Daten oder Aktivitäten sind zu detektieren und in allen Fällen ist Störungssicherheit zu gewährleisten.

Eingabe- und Ausgabevalidierung (Req B 4.4)[7]

Alle Daten, die von außen über eine Schnittstelle in das fymio-Backend gelangen, sollten validiert werden, bevor sie verarbeitet oder gespeichert werden. Neben der Korrektheit der Datenstruktur sollte auch die Plausibilität der Eingaben überprüft werden. Dabei ist zu gewährleisten, dass durch Manipulationen keine negativen Auswirkungen im Hinblick auf die Sicherheit des Gesamtsystems verursacht werden. (Bewusst) fehlerhafte, unterdrückte oder duplizierte Nachrichten, Daten oder Aktivitäten sind zu detektieren und in allen Fällen ist Störungssicherheit zu gewährleisten.

Minimierung der Angriffsfläche (Req B 4.5)

Das fymio-Backend sollte die nach außen bereitgestellte Angriffsfläche minimieren. Dies betrifft neben nach außen bereitgestellten Diensten, welche auf das unbedingt notwendige Minimum reduziert werden sollten, auch die Preisgabe von Informationen wie zum Beispiel registrierte Benutzernamen.

A.3.5 Verfügbarkeit

Robustheit gegenüber Denial-of-Service Angriffen (Req B 5.1)

Das fymio-Backend muss einen grundlegenden Schutz vor Denial-of-Service Angriffe bieten. Dieser grundlegende Schutz beinhaltet Angriffe, die ausschließlich durch einzelne Angreifer entstanden ist. Sind mehrere Angreifer beteiligt oder

[7] für eine Schnittstelle mit dem externen Dienstleister zum Abruf der Umsatzdaten nicht vollständig erfüllt, daher Limitierung in Abschnitt 3.1

verwendet ein Angreifer viele Ressourcen zur Durchführung des Angriffs, so übersteigt dieser Angriff die Möglichkeiten, die ein grundlegender Schutz vor Denial-of-Service Angriffe bieten kann und muss somit möglicherweise nicht betrachtet werden.

A.3.6 Sonstige Anforderungen

Erzwingen von ausreichend langen und komplexen Passwörtern (Req B 6.1)

Das fymio-Backend sollte die Nutzung von ausreichend langen und komplexen Passwörtern verhindern. Es sollte erschwert werden kurze Passwörter oder Passwörter mit eingeschränktem Schlüsselraum zu verwenden.