USecureD

USecureD-Checklisten

Deliverable AP 4.1

Projekt	USecureD – Usable Security by Design
Förderinitiative	Einfach intuitiv – Usability für den Mittelstand
Förderkennzeichen	01MU14002
Arbeitspaket	AP 4.1
Fälligkeit	30.04.2017
Autor	Hartmut Schmitt (HK Business Solutions)
Status	Final
Klassifikation	Öffentlich

HKBS

HK Business Solutions GmbH
Hartmut Schmitt
Mellinweg 20
66280 Sulzbach
schmitt@hk-bs.de

KMU
(Konsortialführer)

Technology
Arts Sciences
TH Köln

Technische Hochschule Köln
Prof. Dr.-Ing. Luigi Lo Iacono
Betzdorfer Straße 2
50679 Köln
luigi.lo_iacono@th-koeln.de

Hochschule
(Konsortialpartner)

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abstract

Im Projekt USecureD werden Musterlösungen und praxistaugliche Werkzeuge entwickelt, die kleine und mittlere Unternehmen (KMU) bei der Entwicklung bzw. bei der Auswahl betrieblicher Anwendungssoftware mit dem Qualitätsmerkmal „Usable Security“ unterstützen.

Im Rahmen von Arbeitspaket 4 (USecureD-Entscheidungshilfen) wurden Checklisten entwickelt, die Anwenderunternehmen der IKT-Branche bei einer objektiven Auswahl und Evaluierung bedarfsgerechter Softwareprodukte unterstützen. Grundlage dieser Checklisten bildeten die in Arbeitspaket 2 entwickelten Entwurfs- und Gestaltungswerkzeuge.

Schlagworte

Checkliste, Fragenkatalog, Prüfung, Evaluation, Usability, Usable Security, IT-Sicherheit

Inhaltsverzeichnis

1 Aufgabenstellung und Vorgehensweise 4
2 Checklisten 5
2.1 Benutzeroberfläche und Layout 5
2.2 Terminologie 6
2.3 Aufgabenorientierung und mentale Belastung 7
2.4 Steuerbarkeit 9
2.5 Erlernbarkeit und Hilfe 10
2.6 Fehlerprävention und Fehlerbehandlung 11
2.7 Systemhinweise und -feedback 13
2.8 Sicherheitswarnungen 15
2.9 E-Mails und Datenübertragung 17
2.10 Verschlüsselung und Signatur 18
2.11 Zugangs- und Zugriffskontrolle 19
2.12 Datenschutz und Datenlöschung 20
2.13 Formulare 21
2.14 Systementwicklung 22
3 Quellenverzeichnis 23

1 Aufgabenstellung und Vorgehensweise

Checklisten können als Arbeitshilfe verwendet werden, um sich wiederholende Abläufe zu strukturieren, zu kontrollieren und zu dokumentieren. Checklisten enthalten hierzu in korrekter Reihenfolge die Handlungsanweisungen bzw. Abfrageparameter, die zum Durchführen einer bestimmten Maßnahme erforderlich sind.

Die USecureD-Checklisten sollten zu zwei Zwecken herangezogen werden können: zum einen, um den Anwender bei einer zielgerichteten Auswahl von Softwareprodukten mit dem Qualitätsmerkmal Usable Security zu unterstützen, zum anderen, um eine Evaluation von Produkten (Prototypen oder lauffähigen Softwaresystemen) hinsichtlich bestimmter Qualitätskriterien zu ermöglichen. Die USecureD-Checklisten sollten so konzipiert sein, dass sie auch ohne tiefergehende Kenntnisse genutzt werden können.

Grundlage für die Erstellung der Checklisten bildeten die im USecureD-Projekt entwickelten Entwicklungsrichtlinien [1] und Patterns [2]. Sämtliche Richtlinien- und Patternbeschreibungen wurden eingehend analysiert, welche Aspekte der Beschreibungen als Prüfpunkte von Checklisten geeignet sind. Im Anschluss an die Sammlung dieser Punkte wurden inhaltliche Bereiche gebildet, z. B. Punkte, die die Benutzeroberfläche und das Layout betreffen, Punkte, die die Terminologie betreffen, usw. Insgesamt wurden 14 Bereiche definiert; diese entsprechen den Überschriften der Checklisten (vgl. unten).

Anschließend wurde innerhalb der Bereiche jeweils eine logische Reihenfolge für die einzelnen Prüfpunkte definiert, z. B. vom Allgemeinen zum Besonderen oder entsprechend der Abfolge, in der Prüfpunkte inhaltlich aufeinander aufbauen. Bei der Ausarbeitung der Checklisten wurde eine Reihe von Empfehlungen aus der Literatur ([3], [4], [5], [6]) genutzt.

Die in Kapitel 2 aufgeführten Checklisten sind in erster Linie für die Softwareauswahl gedacht: der Anwender kann pro Prüfpunkt erfassen, wie wichtig dieses Kriterium für ihn ist, und er kann bei Bedarf eine Bemerkung notieren. Um die Checklisten für die Evaluation zu nutzen, können diese entsprechend angepasst werden, z. B. mit einer Spalte, in der erfasst wird, ob Prüfpunkte erfüllt sind oder nicht und einer Spalte für Anmerkungen.

2 Checklisten

2.1 Benutzeroberfläche und Layout

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Das visuelle Layout der Benutzeroberfläche ist konsistent gehalten.					
Die Sicherheitsfunktionen des Systems sind für den Nutzer sichtbar und zugänglich.					
Das System zeigt an, welche Elemente der Benutzeroberfläche zur Systemsicherheit gehören (z. B. durch Änderung der Mauszeigerform, Hinweistext).					
Das System bietet einen angemessenen Zugang zu allen Elementen der Benutzeroberfläche, die zur Systemsicherheit gehören.					
Alle Sicherheitselemente, die in der Benutzeroberfläche sichtbar sind, sind mit kurzen Beschreibungstexten versehen (z. B. Tooltips, Schnellinfos).					
Die Benutzeroberfläche ermöglicht dem Nutzer einen schnellen und einfachen Zugang zu allen sicherheitsrelevanten Elementen (inklusive der deaktivierten Elemente).					
Alle systemgenutzten Sicherheitsfunktionen werden an einer zentralen Stelle angezeigt.					
Alle nutzeraktivierten Sicherheitsfunktionen werden an einer zentralen Stelle angezeigt.					
Das System ermöglicht einen schnellen, zentralen Zugriff auf alle internen Sicherheitsfunktionalitäten sowie auf die vom System genutzten externen Sicherheitsfunktionalitäten.					

2.2 Terminologie

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Das System verwendet die Sprache des Nutzers.					
Wichtige Begriffe werden im System möglichst konsistent verwendet.					
Es wird systemweit eine Sprache verwendet, die an den Aufgaben der Nutzer ausgerichtet ist. Sicherheitsspezifische Fachbegriffe werden möglichst allgemeinverständlich erklärt.					
Es gibt eine zentrale Quelle, in der systemübergreifend alle sicherheitsrelevanten Begriffe definiert sind.					
Alle Fehlermeldungen sind in einfacher, verständlicher Sprache gehalten; diese ist möglichst beschreibend, aber trotzdem unmissverständlich und prägnant.					
Die Fehlermeldungen verwenden Begrifflichkeiten, die zu den Aufgaben der Nutzer passen; sie vermeiden Fehlercodes und kryptische Abkürzungen.					

2.3 Aufgabenorientierung und mentale Belastung

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Das System macht nur Sicherheitsvorgaben, deren Einhaltung praktikabel ist.					
Alle Sicherheitsmaßnahmen, die besonders tief in die gewohnte Arbeitsweise der Nutzer eingreifen, wurden vorher mit den Betroffenen abgesprochen.					
Es wird die technische und organisatorische Infrastruktur bereitgestellt, die zur Umsetzung der Sicherheitsvorgaben und -maßnahmen notwendig ist.					
Die Gestaltung der Abläufe in dem System entspricht den Fähigkeiten der Nutzer. Häufig ausgeführte Aktionen erfolgen einfach und beiläufig, potentiell gefährliche Aktionen erfordern die Aufmerksamkeit des Nutzers.					
Die Abläufe, Vorgehensweisen und Aufgabenschritte bei der Erledigung ähnlicher oder logisch zusammengehörender Aufgaben und Benutzeraktionen sind standardisiert.					
Der kritische Pfad durch die Anwendung ist für den Nutzer klar erkennbar und ohne Ablenkungen.					
Die Interaktion mit dem System findet in derselben logischen Reihenfolge statt wie die Arbeitsabläufe des Nutzers.					
Das System verdeutlicht die Abfolge der Nutzeraktionen und antizipiert nach Möglichkeit den nächsten Schritt.					
Daten, die der Nutzer benötigt, werden vom System in der korrekten Reihenfolge und ggf. logisch gruppiert ausgegeben.					
Die Anzahl und Komplexität der Aktionen, die der Nutzer zum Erledigen einer Aufgabe ausführen muss (z. B. Klicks, Tastatureingaben, Aufgabenschritte, Seitenaufrufe), beschränken sich auf ein Minimum.					
Die Wechsel der Interaktionsmethode beim Erledigen von Aufgaben (z. B. zwischen Maus und Tastatur) beschränken sich auf ein Minimum.					
Das System unterstützt den Nutzer mit Funktionen, die seine Eingabe sinnvoll ergänzen.					
Bei einfachen Standardaufgaben muss der Nutzer nur die wichtigsten Informationen eingeben; das System blendet die restlichen Informationen in Form von Defaultwerten vor.					
Ein und dieselben Informationen für dieselben oder andere Aufgaben des Nutzers werden vom System nur einmal abgefragt.					
Das System informiert den Nutzer rechtzeitig, falls externe Informationen wie z. B. eine Aus-					

weisnummer benötigt werden.					
Der Nutzer kann Elemente, die logisch zusammengehören, am Ende einer Aufgabe bzw. eines Bearbeitungsschritts mit einer einzigen Aktion abschicken bzw. weiterverarbeiten.					
Der Nutzer kann Aufgaben unterbrechen und abbrechen, sofern die Aufgabe dies zulässt. Er selbst wird beim Erledigen der Aufgaben nicht vom System gestört oder unterbrochen (Ausnahme: Aktive Warnungen).					
Unterbricht der Nutzer die Erledigung einer Aufgabe, so kann er diese später an derselben Stelle fortsetzen.					

2.4 Steuerbarkeit

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Der Nutzer kann in einem logischen und kontinuierlichen Ablauf leicht zwischen den verschiedenen Bereichen der Benutzeroberfläche hin und her navigieren.					
Der Nutzer kann Aktionen einfach rückgängig machen, abbrechen bzw. erneut durchführen, insbesondere wenn eine Aktion zu einem unbeabsichtigten Datenverlust führen kann.					
Das System führt unwiderrufliche Aktionen zeitverzögert aus, sodass diese vom Nutzer noch abgebrochen werden können.					
Das System unterscheidet zwischen Benutzeraktionen zum Öffnen eines Dokuments und zum Starten eines Programms.					
Das System unterbindet das Starten von allen Programmen, die vorher nicht ordnungsgemäß installiert wurden.					
Das System aktiviert nicht automatisch Services, Server oder andere potentiell unsichere Funktionalitäten, es sei denn, es gibt einen Grund dafür.					
Services, die dem System durch eine Softwareinstallation oder ein Upgrade hinzugefügt werden, sind standardmäßig deaktiviert.					
Bei Timeouts stellt das System dem Nutzer eine Möglichkeit zur Verfügung, um angemessen zu reagieren (z. B. steht dem Nutzer beim Ausführen einer Aufgabe mehr Zeit zur Verfügung, damit seine Eingaben nicht verloren gehen).					
Alle E-Mail-Empfänger haben die Möglichkeit, ihre E-Mail-Präferenzen selbst zu ändern.					
Der Nutzer kann Sicherheitsfunktionen deaktivieren, wenn sich diese negativ auf die Geschwindigkeit von Datenübermittlungen auswirken.					

2.5 Erlernbarkeit und Hilfe

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Alle Sicherheitsmechanismen des Systems sind so konzipiert, dass sie das Lernen des Nutzers fördern.					
Das System ermöglicht dem Nutzer eine einfache Unterscheidung zwischen verschiedenen Sicherheitsebenen (z. B. durch visuelle Hinweise wie Icons).					
Das System ermöglicht dem Nutzer eine einfache Unterscheidung zwischen mehr bzw. weniger sicheren Optionen (z. B. durch visuelle Hinweise wie Icons).					
Der Nutzer kann schnell und einfach feststellen, ob ein Sicherheitsmechanismus aktiviert ist oder nicht.					
Der Nutzer kann Detailinformationen über spezifische und generelle Sicherheitsthemen einsehen.					
Detailinformationen über spezifische und generelle Sicherheitsthemen sind nicht Teil der Hinweis- und Warnungstexte, sondern mit diesen verknüpft.					
Der Nutzer kann deutlich erkennen, welche Daten innerhalb des Systems er wegen fehlender Berechtigung nicht bearbeiten darf.					
Alle Bedienelemente, die der Ablaufsteuerung dienen, sind klar als solche zu erkennen.					
Design und Funktionalität der Interaktionselemente sind über das gesamte System hinweg konsistent (standardisiert).					
Die Funktionalität von Controls, Buttons und Links geht aus dem Design bzw. der Beschriftung der Elemente klar hervor.					
Die Namen von Bedienelementen, Funktionen und Benutzeraktionen werden im System konsistent verwendet.					
Die Bedienung bzw. das Resultat einer Eingabe entspricht den Erwartungen des Nutzers und erfolgt in gewohnter Form.					
Die Hilfefunktion ist an den Aufgaben und Zielen des Nutzers ausgerichtet und der Nutzer hat einen schnellen Zugriff auf die Hilfe.					
Alle Hilfetexte sind vollständig, akkurat und dem Kenntnisstand der Zielgruppe angemessen.					
Für wichtige Rückfragen des Nutzers zu Transaktionen führt das System an zentraler Stelle alle notwendigen Kontaktinformationen auf.					

2.6 Fehlerprävention und Fehlerbehandlung

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Das System enthält keine fehleranfälligen Interaktionselemente und antizipiert nach Möglichkeit Fehler bei Benutzereingaben.					
Immer dann, wenn eine Aktion ausführt werden soll, die potentiell gefährlich ist (z. B. Löschen von Daten), muss der Nutzer diese Aktion bestätigen.					
Das System kann mit allen erdenklichen Benutzerfehlern und Falscheingaben angemessen umgehen.					
Das System ist in der Lage, Fehler zu erkennen, dem Nutzer eine konstruktive Lösung aufzuzeigen und einfache, nachvollziehbare Mechanismen für die Fehlerbehandlung anzubieten.					
Stellt das System einen Fehler fest, so kann der Nutzer diesen sofort und mit möglichst wenig Aufwand korrigieren.					
Fehlerhafte Aktionen des Nutzers lassen den Systemstatus unverändert.					
Alle Bedienelemente, die der Nutzer aktuell nicht benötigt (insbesondere solche, deren Benutzung ungewünschte Auswirkungen haben können), sind in dem System deaktiviert.					
Interaktionselemente wie Radio-Buttons, Check-Boxes u. ä. werden in der dafür vorgesehenen Weise verwendet.					
Die Beschriftungen aller Buttons geben dem Nutzer einen deutlichen Hinweis, was passiert, wenn er die Buttons anklickt.					
Das System führt Fehlerprüfungen im jeweiligen Aufgabenkontext durch, ohne den Nutzer in seiner Arbeit zu unterbrechen.					
Entdeckt das System einen Eingabefehler, so bleiben Eingaben, die der Nutzer bisher gemacht hat, erhalten und können von ihm weiterbearbeitet werden.					
Entdeckt das System einen Eingabefehler, so unterstützt es den Nutzer nach Möglichkeit mit Vorschlägen. Wenn dies zur Aufgabe des Nutzers passt, kann er mit der Fehlerbehebung bis zu einem späteren Zeitpunkt warten.					
Alle Fehlermeldungen sind für den Nutzer gut bemerkbar.					
Alle Fehlermeldungen identifizieren das jeweilige Problem und beschreiben die Ursache, die zu dem jeweiligen Fehler geführt hat.					
Alle Fehlermeldungen erklären dem Nutzer, was er verkehrt gemacht hat, und geben ihm klare Anweisungen, was er als nächstes tun					

muss (z. B. schlagen sie ihm eine oder mehrere richtige Lösungen vor).					
Komplexere Anweisungen in den Fehlermeldungen sind Schritt für Schritt in der richtigen Reihenfolge beschrieben.					
Alle Fehlermeldungen sind so gestaltet, dass der Nutzer leicht wieder zum Problemkontext zurückkehren kann.					

2.7 Systemhinweise und -feedback

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Das System informiert den Nutzer schnell und einfach über den internen Zustand des Systems.					
Der aktuelle Sicherheitszustand des Systems ist für den Nutzer sichtbar (in einer nicht aufdringlichen Weise).					
Das System informiert den Nutzer schnell und effizient über den (geänderten) momentanen Zustand des Systems.					
Wenn technische Probleme vorliegen, versorgt das System den Nutzer mit aktuellen Informationen, z. B. ab wann das betroffene (Teil-)System wieder zur Verfügung stehen wird und welche Alternativen es gibt, um Aufgaben zu erledigen bzw. Ziele zu erreichen.					
Immer dann, wenn ein Objekt sich wesentlich anders verhält als erwartet, informiert das System den Nutzer.					
Das System weist den Nutzer auf eingeschränkte Elemente in der Benutzeroberfläche hin (z. B. durch Änderung der Mauszeigerform).					
Das System informiert den Nutzer über Sicherheitsfunktionen, die vom System aktiviert wurden, z. B. um vertrauliche Informationen bei Datenübertragungen zu schützen.					
Das System informiert den Nutzer über Sicherheitsfunktionen, die von ihm selbst ausgewählt und aktiviert wurden, z. B. um vertrauliche Informationen bei Datenübertragungen zu schützen.					
Das System gibt dem Nutzer informatives und möglichst konkretes Feedback.					
Bei erfolgreich durchgeführten Transaktionen wie z. B. Anmeldungen, Anfragen und Bestellungen gibt das System eine klare Bestätigung an den Nutzer aus.					
Bei häufig ausgeführten, weniger kritischen Aktion gibt das System dem Nutzer ein dezentes (passives) Feedback.					
Bei selten ausgeführten, kritischen Aktionen gibt das System dem Nutzer ein deutlich wahrnehmbares (aktives) Feedback.					
Alle kontextabhängigen Hinweise, die der Nutzer für eine Entscheidung benötigt, werden im Aufmerksamkeitsbereich des Nutzers platziert.					
Alle kontextabhängigen Hinweise, die der Nutzer für Entscheidung benötigt, sind zum Zeitpunkt der Entscheidung verfügbar.					
Alle kritischen Inhalte sind im System hervorgehoben, z. B. mittels Schriftfarbe, Schriftgröße oder durch eine entsprechende Anmerkung.					
Alle Elemente, auf denen der Nutzer eine Operation ausführt, sind in der Benutzeroberfläche					

optisch hervorgehoben.					
Das System warnt den Nutzer vor Timeouts.					

2.8 Sicherheitswarnungen

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Wann immer die Datensicherheit bedroht ist, gibt das System eine Sicherheitswarnung an den Nutzer (oder Systemadministrator) aus.					
Das System informiert den Nutzer schnell und effizient über alle neuen Gefahren (z. B. durch auditives und visuelles Feedback).					
Immer dann, wenn das System eine Gefahr identifiziert hat, gibt es eine Sicherheitswarnung an den Nutzer (oder Systemadministrator) aus.					
Immer dann, wenn das System eine Gefahr identifiziert hat, schlägt es dem Nutzer alle Aktionen vor, die notwendig sind, um mögliche Schäden zu minimieren.					
Immer dann, wenn das System eine Gefahr erkennt, präsentiert es dem Nutzer eine klare Empfehlung zum sicheren Fortfahren und zeigt eine Liste mit anderen möglichen Optionen an.					
In dem System sind Grenzen für Gefahrenstufen definiert, um Sicherheitswarnungen verschiedener Stufen voneinander unterscheidbar zu machen.					
Alle Sicherheitswarnungen sind in einer Weise gestaltet, die ihrer Gefahrenstufe entspricht.					
Alle Sicherheitswarnungen folgen einem gebräuchlichen visuellen Layout.					
Damit der Nutzer kritische Sicherheitswarnungen wahrnimmt und darauf reagiert, reißen ihn diese Warnungen aus seiner Primäraufgabe heraus und ziehen die Aufmerksamkeit auf sich.					
Kritische Sicherheitswarnungen können vom Nutzer nicht ohne weiteres ignoriert werden. Die Option zum Verwerfen einer kritischen Warnung wird nicht direkt angezeigt. Der Nutzer benötigt mehrere Schritte, um die Warnung zu verwerfen.					
Die Sicherheitswarnungen weisen den Nutzer auf alle notwendigen Aktionen hin. Sie erläutern, warum Aktionen notwendig sind, und liefern alle Informationen, die benötigt werden, um eine Entscheidung zu treffen.					
Alle Sicherheitswarnungen enthalten einen kurzen und präzisen Hinweis, warum der Nutzer die Warnung erhält und was die möglichen Konsequenzen sind, falls er diese ignoriert.					
Alle Sicherheitswarnungen beschreiben in verständlicher Weise die drohenden Gefahren.					
Alle Warnhinweise sind prägnant und präzise formuliert.					
Alle Sicherheitswarnungen sind kurz und fokussiert, enthalten aber trotzdem alle notwendigen Informationen, wie schwer die Auswirkungen eines (möglichen) Vorfalls sind und was zu					

tun ist.					
Alle Warnhinweise bieten dem Nutzer verständliche Auswahlmöglichkeiten an.					
Alle Sicherheitswarnungen verdeutlichen dem Nutzer, welche Folgen und Risiken eine Aktion hat, bevor er diese ausführt.					
Alle Sicherheitswarnungen versorgen den Nutzer mit den benötigten kontextrelevanten Informationen, um eine fundierte Entscheidung zwischen den Auswahlmöglichkeiten treffen zu können.					
Hat der Nutzer in der Vergangenheit Aktionen ausgeführt hat, die ihm dabei helfen können, die mit einer aktuellen Entscheidung verbundenen Risiken zu verstehen, so zeigen ihm Warnhinweise alle relevanten Informationen an.					
Bei allen Sicherheitswarnungen ist die empfohlene Option unmittelbar erkennbar und hervorgehoben, z. B. farblich oder durch größere Schrift.					
Bei Sicherheitswarnungen ist die empfohlene Option immer markanter gestaltet als alle anderen Optionen.					
Bei Sicherheitswarnungen verhilft die empfohlene Option dem Nutzer immer beim Vervollständigen seiner Primäraufgabe.					
Bei allen Sicherheitswarnungen ist das Ausführen der empfohlenen Option die schnellste Methode, um auf die Warnung zu reagieren.					
Um den Nutzer über vorhandene Gefahren zu informieren, zeigt das System in zurückhaltender Weise redundante Hinweise an, z. B. Mitteilungen, Bilder oder Metaphern aus der realen Welt.					
Das System warnt den Nutzer regelmäßig (aber nicht zu häufig) vor unsicheren Systemzuständen und Operationen.					
Zeigt das System eine Sicherheitswarnung an, die sich auf eine Webseite bezieht, so bleibt diese Webseite zunächst verborgen oder wird ausgegraut.					

2.9 E-Mails und Datenübertragung

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Während einer Datenübertragung zeigt das System dem Nutzer in einfacher Weise alle nötigen Informationen über den aktuellen Sicherheitszustand des Systems an.					
Das System informiert den Nutzer über Sicherheitsmaßnahmen, wenn vertrauliche Informationen übertragen werden (z. B. durch eine einfach verständliche Textmitteilung oder einen visuellen Hinweis).					
Wichtige Informationen zu Transaktionen werden dem Nutzer in Form einer Bestätigungsmail, eines PDF-Downloads o. ä. zur Verfügung gestellt.					
Immer dann, wenn eine Datenübertragung fehlgeschlagen ist, benachrichtigt das System den Nutzer und erläutert das Problem.					
Übertragungsfehler führen nicht dazu, dass Daten verloren gehen oder zerstört werden.					
Übertragungsfehler führen nicht dazu, dass der Nutzer in seiner Arbeit gestört oder behindert wird.					
Das System ermöglicht dem Nutzer eine Unterscheidung von E-Mails, die von innerhalb eines Systems stammen, und solchen E-Mails, die von außerhalb kommen und behaupten, von einer internen Adresse zu stammen.					
Das System kennzeichnet E-Mails, die innerhalb des Systems versendet wurden, in einer Weise, die nicht von Außenstehenden gefälscht werden kann.					

2.10 Verschlüsselung und Signatur

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Alle Systeme, die kryptographische Keys benötigen, können direkt und ohne das Beziehen von Drittanbieter-Zertifikaten benutzt werden.					
Falls für das System keine SSL- und S/MIME-Zertifikate einer bekannten Zertifizierungsstelle verwendet werden können, werden selbstsignierte Zertifikate verwendet oder Zertifikate, die von einer unbekannten Zertifizierungsstelle herausgegeben wurden.					
Das System versendet S/MIME-signierte E-Mails.					
In einer Datenbank mit den E-Mail-Präferenzen der Empfänger ist hinterlegt, welche Verschlüsselungstechnologien die E-Mail-Clients nutzen.					
Das System gewährleistet, dass alle verschlüsselten bzw. signierten E-Mails von den vorgesehenen Empfängern erfolgreich verarbeitet werden können.					
Das System unterstützt den Nutzer dabei, Schlüssel auf andere Geräte zu übertragen und zu sichern.					
Das System zeigt dem Nutzer an, welche der von ihm empfangenen E-Mails signiert sind.					
In einer Datenbank mit Schlüsseln und Zertifikaten ist hinterlegt, ob bzw. wie oft diese bereits verwendet wurden.					
Die Nutzer des Systems können überprüfen, ob sie einen bestimmten Schlüssel erstmals erhalten, ob dieser bereits mehrfach benutzt wurde oder ob der Schlüssel sehr häufig in Gebrauch ist.					

2.11 Zugangs- und Zugriffskontrolle

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Die vom System verwendeten Verfahren zur Benutzeridentifikation sind so einfach wie möglich (in Einklang mit dem angestrebten Schutz).					
Mit dem System können Identifikationsmethoden, die in der Organisation bereits existieren, weiter genutzt werden.					
Das System verwendet für die Zugangs- und Zugriffskontrolle technische Lösungen, die die mentale Belastung des Nutzers minimieren; z. B. erlaubt es dem Nutzer, seine Passwörter sicher zu speichern.					
In dem System werden nur dann Passwörter verwendet, wenn dies wirklich notwendig ist.					
Das System erlaubt dem Nutzer, sein Passwort schnell und einfach zu ändern und ein eigenes Passwort zu wählen.					
Dem Nutzer steht eine einfache Möglichkeit zur Verfügung, mit der er Zugangsdaten zurücksetzen oder wiederherstellen kann.					
Das System nutzt beim Ändern von Zugangsdaten eine vordefinierte E-Mail-Adresse, um den Nutzer zu identifizieren und zu autorisieren.					
Der Nutzer wird nur dann aufgefordert, sein Passwort zu ändern, wenn es einen Hinweis oder einen Verdacht auf eine Gefährdung gibt.					
Die Autorisierung des Nutzers erfolgt mit dem (ersten) Log-in; anschließend ist keine weitere Authentifizierung notwendig, wenn der Nutzer bestimmte Daten anfordert.					
Bei einer bestimmten Anzahl oder Rate von Fehlversuchen sperrt das System automatisch das betroffene Benutzerkonto.					

2.12 Datenschutz und Datenlöschung

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Das System unterscheidet zwischen dem Grundsystem, Anwendungen, die nicht Teil dieses Grundsystems sind, und den von den Nutzern generierten Daten.					
Das System bietet dem Nutzer eine Möglichkeit, alle persönlichen oder privaten Informationen mittels einer einzigen Operation zu löschen.					
Der Nutzer hat die Möglichkeit, einzusehen, welche Daten über ihn erhoben und gespeichert werden und wie diese verwendet werden.					
Das System hat keinen versteckten Bereich, in dem automatisch Nutzer- oder Nutzungsdaten aufzeichnet werden.					
Vom Nutzer gelöschte Informationen können nicht wiederhergestellt werden. Es bleiben keine versteckten Informationen erhalten.					
Es werden nur solche Informationen abgefragt, die vom System tatsächlich benötigt werden.					
Die Sensibilität der abgefragten Daten und die Dauer der Datenhaltung sind auf ein Minimum beschränkt.					
Der Nutzer kann sensible Daten (z. B. persönliche Informationen oder bestimmte Finanzdaten), die das System nicht länger benötigt, einfach wieder löschen.					
Werden dem Nutzer persönliche Information in der Benutzeroberfläche angezeigt, so hat er die Möglichkeit, diese zu löschen. Ist der Nutzer in Ausnahmefällen nicht autorisiert ist, bestimmte Informationen zu löschen, zeigt das System Kontaktinformationen der verantwortlichen Instanz an, die dazu berechtigt ist.					
Der Nutzer kann deutlich erkennen, welche Daten innerhalb des Systems vertraulich zu behandeln sind.					

2.13 Formulare

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Alle Formulare sind so gestaltet, dass der Nutzer sie möglichst einfach und effizient benutzen kann.					
In allen Formularen gibt es eine sinnvolle Reihenfolge der Felder (inklusive der Tab-Reihenfolge).					
In den Formularen werden soweit möglich Defaultwerte verwendet, die der Nutzer einfach übernehmen und bei Bedarf ändern kann.					
In den Formularen gibt es eine klare Unterscheidung zwischen Pflichtfeldern und optionalen Feldern.					
Alle Labels, Anweisungstexte und Fragen in den Formularen sind knapp, präzise und möglichst konsistent (auch formularübergreifend) formuliert.					
Die Labels aller Formularfelder sind so eindeutig, dass der Nutzer die Felder klar voneinander unterscheiden kann.					

2.14 Systementwicklung

Kriterium	sehr wichtig	wichtig	weniger wichtig	nicht wichtig	Bemerkung
Die verwendete API erfüllt sicherheitsrelevante und nicht-sicherheitsrelevante Anforderungen.					
In die verwendete (Standard-)API sind kryptographische Funktionalitäten integriert.					
Die verwendete API ist auch ohne kryptographisches Fachwissen leicht erlernbar.					
Die verwendete API bricht nicht mit dem Entwickler-Paradigma der Nutzergruppe.					
Die verwendete API kann auch ohne Dokumentation einfach genutzt werden.					
Die verwendete API beugt einer falschen Nutzung vor und macht Fehler sichtbar.					
Die verwendete API bietet sichere und unzweideutige Standards.					
Die verwendete API verfügt über einen Test-Modus mit reduzierten bzw. ohne Sicherheitsmechanismen.					
Die verwendete API generiert einfach lesbaren bzw. wartbaren Code, der problemlos up-to-date gehalten werden kann.					
Die verwendete API bietet geeignete Hilfestellungen für Endnutzer-Interaktionen.					

3 Quellenverzeichnis

[1] USecureD-Konsortium (2016): USecureD-Entwicklungsrichtlinien: Entwicklungsrichtlinien, die das Qualitätsmerkmal Usable Security fördern und auf verschiedene Einsatzgebiete, Nutzungskontexte und Sicherheitsbedürfnisse abgestimmt sind. Verfügbar unter: https://das.th-koeln.de/usecured/guidelines [15.03.2017]

[2] USecureD-Konsortium (2016): USecureD-Patternsammlung: Sammlung von bewährten, wiederverwendbaren und übertragbaren Gestaltungsmustern mit dem Qualitätsmerkmal Usable Security. Verfügbar unter: https://das.th-koeln.de/usecured/patterns [15.03.2017]

[3] Schmitt, Hartmut (2015): Checklisten verwenden. Verfügbar unter: http://www.pq4agile.de/PQ4WP/wp-content/uploads/2015/02/PQ4Agile-AP-2.2-Checklisten-verwenden-V.2.pdf [15.03.2017]

[4] Mangold, Thomas (2013): Warum du unbedingt mit Checklisten arbeiten solltest. Verfügbar unter: http://selbst-management.biz/warum-du-unbedingt-mit-checklisten-arbeiten-solltest/ [15.03.2017]

[5] Wenk, Oliver (2011): Mit Checklisten Zeit sparen und Nerven schonen – Wie funktioniert das? Verfügbar unter: http://www.gruenderhelden.de/mit-checklisten-zeit-sparen-und-nerven-schonen-wie-funktioniert-das/ [15.03.2017]

[6] Wikipedia (2017): Fragenkatalog. Verfügbar unter: https://de.wikipedia.org/wiki/Fragenkatalog [15.03.2017]