USecureD

Schlussbericht des Vorhabens

„USecureD – Usable Security by Design“

Autoren:

Hartmut Schmitt, HK Business Solutions

Prof. Dr.-Ing. Luigi Lo Iacono, Technische Hochschule Köln

HKBS

Technology
Arts Sciences
TH Köln

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie unter dem Förderkennzeichen 01MU14002 gefördert.

Projektträger:
Deutsches Zentrum für Luft- und Raumfahrt
DLR Projektträger, Digitale Anwendungen - Mittelstand-Digital

Schlussbericht des Vorhabens
„USecureD – Usable Security by Design“

Web: www.usecured.de

Ansprechpartner:
Hartmut Schmitt
HK Business Solutions GmbH
Mellinweg 20
66280 Sulzbach
Tel.: +49 (0)6897 99904-24
E-Mail: hartmut.schmitt@hk-bs.de

Abstract

Dieses Dokument ist der Schlussbericht (gemäß Nr. 8.2 NKBF 98) des Projekts „USecureD – Usable Security by Design“, BMWi-Förderkennzeichen 01MU14002. Das Projekt USecureD ist Teil der Förderinitiative „Einfach intuitiv – Usability für den Mittelstand“, die im Rahmen des Förderschwerpunkts „Mittelstand-Digital – Strategien zur digitalen Transformation der Unternehmensprozesse“ vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert wird. Das USecureD-Konsortium bestand aus den Partnern HK Business Solutions GmbH (Konsortialführer, 01MU14002A) und Technische Hochschule Köln (Projektpartner, 01MU14002B). Der Bericht stellt die Ziele, den Ablauf, die Ergebnisse und die zukünftige Verwertung der Resultate des Projekts vor.

Schlagworte

Usability, Gebrauchstauglichkeit, Benutzerfreundlichkeit, Security, IT-Sicherheit, Software Engineering, Softwareentwicklung, Anwendungssoftware, betriebliche Software

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlechter.

Inhalt

1 Aufgabenstellung

Das Projekt „USecureD – Usable Security by Design“ wurde mit dem Ziel gestartet, das innovative Qualitätsmerkmal *Usable Security* (gebrauchstaugliche Informationssicherheit) stärker im deutschen IKT-Sektor und in dessen Anwendungsbranchen zu verankern. Usable Security bedeutet für Anwender einen Mehrgewinn an Benutzerfreundlichkeit und an Informationssicherheit. Kleine und mittlere Unternehmen (KMU), die sich für betriebliche Anwendungssoftware mit diesem Qualitätsmerkmal entscheiden, haben also ein Werkzeug an der Hand, mit dem sie ihre Geschäftsprozesse effizienter, effektiver, zufriedenstellender und zugleich sicherer gestalten können.

Um das USecureD-Gesamtziel zu erreichen, sollte das Projekt zum einen die Herstellerseite stärken, indem es kleine und mittlere Unternehmen der Softwareindustrie in die Lage versetzt, E-Business-Produkte mit dem Qualitätsmerkmal Usable Security auf eine möglichst systematische sowie durchgängige Art und Weise herzustellen (by Design). Hierzu sollten im Rahmen des Projekts geeignete Methoden und Werkzeuge des Software-Engineerings identifiziert bzw. neu entwickelt werden. Diese sollten in Pilotprojekten evaluiert und auf einer USecureD-Plattform veröffentlicht werden, so dass sie auch für IKT-Firmen außerhalb des Konsortiums für den diskriminierungsfreien Zugang und kostenlosen Gebrauch zur Verfügung stehen.

Zum anderen strebte das Konsortium an, durch Maßnahmen auf der Anwenderseite den Markt für neuartige Softwareprodukte mit dem Qualitätsmerkmal Usable Security vorzubereiten: Die Partner planten, ein Kompetenzzentrum aufzubauen, das ein stärkeres Bewusstsein für das noch junge Thema Usable Security schafft und das gezielt die Nachfrage nach innovativen Produkten mit den entsprechenden Qualitätseigenschaften weckt. Schlüssige Entscheidungshilfen sollten Anwenderunternehmen in die Lage versetzen, Softwareprodukte in Bezug auf Usable Security zu bewerten und passende Produkte für das eigene Unternehmen auszuwählen.

1.1 Motivation

Bei der Anschaffung von Geschäftsanwendungen ist deren Sicherheit eines der zentralen Auswahlkriterien. Dennoch entpuppt sich vermeintlich sichere Software im alltäglichen Gebrauch oft als Risikofaktor, wenn z.B. Sicherheitselemente aufgrund mangelnder Usability von den Nutzern falsch oder gar nicht bedient werden. Daraus folgt, dass IT-Systeme mit Sicherheitsfunktionen und Sicherheitsmechanismen ausgestattet werden müssen, die nicht nur für Security-Experten und Poweruser, sondern auch für Laien und Gelegenheitsnutzer verständlich sind. Denn auch Nichtexperten müssen die Sicherheitsmechanismen und deren Notwendigkeit zumindest grundlegend verstehen, damit sie diese annehmen und ordnungsgemäß verwenden können.

Dies wiederum bedeutet, dass eine Verschmelzung des Usability-Engineerings mit dem Security-Engineering eine fundamentale Voraussetzung zur Schaffung einer effektiven Sicherheit von IT-Systemen darstellt. Die Wahrnehmung der User über den Einsatz und ihr Mitwirken an der Sicherheit des Systems ist hierbei ein wichtiger Aspekt. In besonderem Maße gelten diese Schlüsse für Anwendungen im Unternehmensumfeld. Denn oft sind hier die Sicherheitsmechanismen nur unzureichend auf die primären (betrieblichen) Aufgaben der Anwender ausgerichtet oder es wird in Bezug auf die Endbenutzer schlicht von falschen Annahmen ausgegangen.

1.2 Wissenschaftliche und technische Arbeitsziele des Vorhabens

Vom Gesamtziel des USecureD-Vorhabens wurden die wissenschaftlichen und technischen Arbeitsziele abgeleitet, die sich nach den beiden Hauptadressaten des Projekts, IKT-Herstellern (vgl. Kapitel 1.2.1) und IKT-Anwendern (vgl. Kapitel 1.2.2) unterteilen lassen. Viele dieser Ziele waren unmittelbar mit dem Erreichen bestimmter Projektergebnisse/Deliverables verknüpft.

Die im Folgenden beschriebenen Arbeitsziele sollten in geeigneter Form veröffentlicht und kostenlos zur Verfügung gestellt werden, so dass sie eine möglichst gute Breitenwirkung bei Anwenderunternehmen, Entwicklergemeinde und wissenschaftlicher Community entfalten können. Abbildung 1 am Ende dieses Kapitels stellt diese Ergebnisse in einer Übersicht dar. Daneben gab es eine Reihe von Ergebnissen, mit denen der Projektfortschritt gegenüber dem Projektträger dokumentiert wurde und die nicht zur Veröffentlichung bestimmt waren.

Um die Übertragbarkeit und angestrebte Allgemeingültigkeit aller veröffentlichten Ergebnisse auf beliebige Anwendungsdomänen sicherzustellen, war eine enge Zusammenarbeit mit mehreren Anwendungspartnern vorgesehen. Zudem war vorgesehen, während der Projektlaufzeit über die Aktivitäten des USecureD-Kompetenzzentrums weitere potentielle Anwendungspartner zu gewinnen.

1.2.1 Arbeitsziele mit der Zielgruppe IKT-Hersteller

Auf Herstellerseite standen Arbeitsziele im Vordergrund, die kleine und mittelgroße Softwareunternehmen dazu befähigen werden, gebrauchstaugliche und sichere betriebswirtschaftliche Anwendungssysteme mit möglichst kurzen Produkteinführungszeiten zu entwickeln. Ausgangspunkt hierfür sollte eine umfassende Untersuchung sein, welche konkreten Anforderungen an Usable Security auf Anwenderseite bestehen und welches die aktuellen Sicherheitsschwachstellen der Benutzerinteraktion im Bereich (webbasierter) Geschäftsanwendungen sind. Die darauf aufbauenden Ergebnisse waren im Einzelnen:

Entwicklung eines USecureD-Qualitätsmodells

Eine Verschmelzung des Usability-Engineerings mit dem Security-Engineering erfordert ein ganzheitliches, konsolidiertes Qualitätsverständnis. Dieses Qualitätsverständnis sollte im USecureD-Projekt in Form eines Qualitätsmodells dokumentiert werden. Ziel bei der Entwicklung des USecureD-Qualitätsmodell war es, einen möglichst guten Trade-off zwischen den Qualitätsmerkmalen Usability, User Experience und Security zu finden, insbesondere zwischen denjenigen Teilmerkmalen, die miteinander konkurrieren oder die sich gegenseitig verstärken. Das USecureD-Qualitätsmodell sollte von IKT-Herstellern herangezogen werden können, um die relevanten Qualitätseigenschaften der eigenen Softwareprodukte zu ermitteln und zu beurteilen. Bei der Erstellung des Qualitätsmodells sollte auf bestehende Softwarequalitätsmodelle wie z. B. den ISO-Standard 25010, auf Vorarbeiten der Projektpartner und auf Vorarbeiten außerhalb des Projekts zurückgegriffen werden.

Aufbau einer USecureD-Patternsammlung

Für jeden Softwarearchitekten und -entwickler ist es hilfreich, wenn er beim Lösen von Entwurfsproblemen auf bewährte, gut dokumentierte und wiederverwendbare Musterlösungen, sog. Patterns, zurückgreifen kann. Beispiele für bereits dokumentierte Lösungsmuster aus dem Bereich Usable Security sind etwa das „Verzögerte Ausführen nicht wiederherstellbarer Löschungen“ oder das „Warnen vor unsicheren Konfigurationen“. Vor Beginn des USecureD-Projekts gab es noch keine umfassende Patternsammlung für den Bereich Usable Security – insbesondere keine deutschsprachige Patternsammlung. Daher sollte im USecureD-Projekt eine entsprechende Patternsammlung aufgebaut und veröffentlicht werden. Hierfür sollten bestehende Ansätze aus der Literatur zusammengeführt und weitere erfolgversprechende Gestaltungslösungen identifiziert und dokumentiert werden. Für die Dokumentation der Usable-Security-Patterns sollte im Projekt ein geeignetes Beschreibungstemplate entwickelt werden. Hierdurch sollte sichergestellt werden, dass alle dokumentierten Patterns möglichst einfach auf unterschiedliche Geschäftsdomänen übertragen und nahtlos in beliebige Softwareentwicklungsprozesse integriert werden können. Den Schwerpunkt der frei zugänglichen USecureD-Patternsammlung sollten die im Projekt implementierten und validierten Patterns bilden, die mit konkreten Implementierungsbeispielen versehen werden sollten.

Aufbau einer Use-Case-Sammlung

Oftmals ist die Verwendung eines Design- oder Interaktionspatterns an ein bestimmtes Szenario gebunden oder die Verwendung eines bestimmten Patterns ist in einem bestimmten Anwendungskontext naheliegend. Die Verwendung des Usable-Security-Patterns „Verzögertes Ausführen nicht wiederherstellbarer Löschungen“ kann beispielsweise sinnvoll sein bei Benutzeraktionen wie dem Löschen von Profilen, Dokumenten, Nutzungsprotokollen usw. Eine Dokumentation solcher Zusammenhänge stellt für die praktische Arbeit von Softwareingenieuren und Entwicklern eine große Hilfe dar. Die Informationen zu bekannten Anwendungsfällen aus dem Bereich Usable Security sollten daher strukturiert in Form von Use Cases dokumentiert werden. Ziel dieser Dokumentation war es, eine Verknüpfung der Use Cases mit entsprechend geeigneten USecureD-Patterns herzustellen. Hierdurch sollte erreicht werden, dass ein Softwareingenieur, der einen bestimmten Use Case wie z. B. „Benutzerprofil löschen“ als Softwareentwurf oder als technische Implementierung umsetzen möchte, mit der Use-Case-Beschreibung zugleich passende Pattern-Empfehlungen mitsamt Implementierungsbeispielen erhält. Für die Dokumentation der identifizierten Use Cases sollte in USecureD ein geeignetes Beschreibungstemplate entwickelt werden. Sämtliche im Projekt dokumentierten Use Cases sollten der Entwicklergemeinde als frei zugängliche Use-Case-Sammlung zur Verfügung gestellt werden.

Erarbeitung von USecureD-Entwicklungsrichtlinien

Entwicklungsrichtlinien (Design Guidelines) sind wichtig, um bereits bei der Entwicklung von Systemen möglichst viele Ursachen für spätere Schwachstellen zu eliminieren. Im USecureD-Projekt sollten daher

praxisgerechte Entwicklungsrichtlinien definiert werden, die Softwarehersteller in die Lage versetzen, strukturiert betriebliche Anwendungssysteme mit dem Qualitätsmerkmal gebrauchstauglicher Informationssicherheit zu entwickeln. Diese sollten somit zur Gewährleistung einer besseren Softwarequalität beitragen und gleichzeitig die Komplexität von Software-Entwicklungsprojekten verringern. Die USecureD-Entwicklungsrichtlinien sollten so konzipiert werden, dass sie als Arbeitsgrundlage für Softwareingenieure und Systementwickler, als Kommunikationsbasis im Team und zugleich als Vertragsgrundlage zwischen Auftraggeber und Auftragnehmer dienen können. Die Richtlinien sollten mit besonderem Augenmerk auf webbasierte betriebliche Anwendungssysteme entwickelt und ausgestaltet werden, jedoch auch auf andere Anwendungsdomänen übertragbar sein.

Entwicklung eines Guideline-Tools

Ein Guideline-Tool sollte sämtliche USecureD-Entwicklungsrichtlinien beinhalten und diese mit zusätzlichen Ressourcen und weiterführenden Informationen anreichern z. B. mit Umsetzungsbeispielen, Tipps für geeignete Entwicklungswerkzeuge, Hinweisen zur Wirkungsweise und zu vertiefender Literatur. Ziel des Guideline-Tools war es, dem Softwareingenieur bzw. -entwickler bei der Dialog- und Interaktionsgestaltung nachvollziehbare Entscheidungshilfen zur Verwendung einzelner bzw. zur sinnvollen Kombination mehrerer USecureD-Patterns zu geben. Diese Unterstützung sollte in einer Form erfolgen, die für Softwareingenieure bzw. -entwickler möglichst geeignet ist, etwa als Wiki, Fragenkatalog, Checklistensammlung o. ä. Herstellerunternehmen der IKT-Branche sollte das Guideline-Tool außerdem die Generierung individueller Entwicklungsrichtlinien ermöglichen. Um bestimmten Qualitätszielen oder technischen Aspekten besser Rechnung zu tragen, sollte mit dem Guideline-Tool z. B. eine Auswahl aus den universalen Entwicklungsrichtlinien getroffen werden können, die dann bei Bedarf individuell angepasst werden kann.

Definition geeigneter Usable-Security-Metriken

Im Rahmen des Projekts sollte ein Set von USecureD-Metriken definiert werden, zum einen, um die im Projekt entwickelten Lösungen hinsichtlich des Qualitätsmerkmals Usable Security zu evaluieren. Zum anderen sollten die Metriken über das USecureD-Projekt hinaus genutzt werden können, um dieses Qualitätsmerkmal bzw. die Teilmerkmale Usability, User Experience und Security im Rahmen beliebiger Anwendungssoftware zu bewerten. Ziel war es, für IKT-Anwender- und -Herstellerunternehmen eine zuverlässige Bewertungs- und Vergleichsmöglichkeit für eines oder mehrere Softwareprodukte zur Verfügung zu stellen. Bei der Auswahl bzw. Definition der Usable-Security-Metriken sollte die Praxisrelevanz für KMU und die einfache Interpretation der gewonnenen Messergebnisse im Vordergrund stehen. Soweit möglich sollte bei der Auswahl der USecureD-Metriken auf bekannte und etablierte Kenngrößen zurückgegriffen werden.

Sammlung von USecureD-Evaluationswerkzeugen

Eine Reihe von USecureD-Evaluationswerkzeugen sollte die zuvor beschriebenen Usable-Security-Metriken operationalisieren: Sie sollten dazu dienen, die Usable-Security-Eigenschaften beliebiger Anwendungssoftware zu überprüfen, zu bewerten und vergleichbar zu machen, z. B. um einen Vergleichstest zwischen einem herkömmlichen Produkt und einem nach der USecureD-Methode hergestellten Produkt durchzuführen. Es sollte eine Werkzeug-Sammlung inklusive Toolbox-Handbuch erstellt werden, die so „leichtgewichtig“ konzipiert ist, dass sie auch von kleinen Herstellern im eigenen Kontext selbständig angewendet werden kann – also ohne Laborumgebung, ohne eigenen Usability- bzw. Security-Stab und ohne besondere Spezial- oder Expertenkenntnisse. Soweit möglich sollte bei der Zusammenstellung der Toolbox auf etablierte Instrumente zurückgegriffen werden, die sich durch gute Praxistauglichkeit und Effizienz auszeichnen.

Aufbau einer USecureD-Plattform

Eine USecureD-Plattform sollte auf den oben genannten Projektergebnissen aufbauen und diese in einer zentralen Umgebung bündeln. Dadurch sollte die Plattform mittelständischen Softwareunternehmen eine Hilfestellung bei der Entwicklung eigener Produkte geben und zudem eine günstige Möglichkeit bieten, um fundierte und umfangreiche Evaluationen von Softwareprodukten durchzuführen. Geplant war, dass Hersteller ihre Produkte registrieren und in konkreten Usable-Security-Tests bewerten lassen können – entweder durch eigene Nutzer oder durch externe Probanden, zu denen über die Plattform Kontakt hergestellt werden kann. Mit einem USecureD-Fragebogeneditor zum Erstellen von Testaufgaben und Fragebögen sollte die Plattform Hilfestellung für Testleiter beim Design individueller Tests

liefern Außerdem sollte sie mit einem Umfragetool und einem Auswertungstool Unterstützung bei der Durchführung und Auswertung bzw. Interpretation von Testergebnissen leisten.

Erstellung eines Seminarkonzepts

Alle Projektergebnisse sollten so konzipiert werden, dass sie von Unternehmen der IKT-Branche auch ohne Trainings oder Spezialkenntnisse angewendet werden können. Für Softwarefirmen, die ihre Kenntnisse vertiefen möchten oder die eine größere Sicherheit bei der Anwendung der Gestaltungs- und Evaluierungswerkzeuge erwerben möchten, sollte zusätzlich ein entsprechendes Seminarkonzept entwickelt und individuelle USecureD-Schulungen und -Tutorials angeboten werden.

1.2.2 Arbeitsziele mit der Zielgruppe IKT-Anwender

Auf Anwenderseite ging es primär um Arbeitsziele, die kleine und mittlere Unternehmen zum Einsatz von IKT-Produkten mit dem Qualitätsmerkmal Usable Security motivieren sollten und die diesen Unternehmen eine gezielte Produktauswahl ermöglichen sollten. Im Einzelnen waren dies:

Aufbau einer Projektwebsite

Die USecureD-Projektwebsite sollte ein breites Download- und Serviceangebot für interessierte Anwenderunternehmen bieten. Insbesondere sollten hier alle veröffentlichten Projektergebnisse zur Verfügung stehen. Die Bekanntheit der Projektwebsite sollte mit Maßnahmen in den Bereichen Online-PR, Online-Marketing und Social-Media-Marketing unterstützt werden.

Entwicklung eines Demonstrators

Der USecureD-Demonstrator war geplant als konkrete Implementierung der im Projekt erarbeiteten Methoden und Konzepte, insbesondere der validierten Usable-Security-Patterns. Mit dem USecureD-Demonstrator sollten die Projektergebnisse auf anschauliche Weise bei Messen, Konferenzen und ähnlichen Veranstaltungen der interessierten Fachöffentlichkeit präsentiert und vorgeführt werden können. Hierfür sollten User Stories bzw. Epics entwickelt werden, also konkrete Geschichten zum Erleben des Demonstrators, die das Ziel haben, dass die Besucher die Tragkraft ihrer Entscheidungen als Anwender besser einschätzen können. Der Demonstrator sollte durch einen begleitenden Leitfaden unterstützt werden, der seine Bedienung erläutert und die verwendeten Patterns sowie die zugrundeliegenden USecureD-Konzepte anschaulich erklärt. In erster Linie sollte der Demonstrator die Evaluation von außerfachlichen Aspekten unterstützen, die in der Einschätzung von Praktikern und späteren Anwendern in Bezug auf die Einsatzmöglichkeiten der entwickelten Patterns und Werkzeuge sichtbar werden.

Entwicklung von Entscheidungshilfen für die Produktauswahl

Die vorgesehenen Entscheidungshilfen sollten potentiellen Anwenderunternehmen eine einfache und zielgerichtete Evaluation von E-Business-Anwendungen ermöglichen. Vorgesehen waren USecureD-Checklisten und ein Auswahlwerkzeug, das den Anwender entlang geeigneter Usable-Security-Metriken zu einer objektiven, bedarfsgerechten Produktauswahl führt. Die Entscheidungshilfen sollten so aufgebaut sein, dass sie von Anwenderunternehmen der IKT-Branche selbständig und ohne weitere Spezialkenntnisse im Rahmen einer Produktauswahl bzw. -evaluation verwendet werden können.

Verbesserung der (Public) Awareness und Sensibilisierung der Zielgruppe

Das Konsortium sah zahlreiche Transferaktivitäten vor, um eine positive öffentliche Wahrnehmung des Themas Usable Security und eine möglichst gute Breitenwirkung des USecureD-Projekts zu erreichen. Vorgesehen waren z. B. Messebesuche, Beiträge zu Tagungen und Fachkonferenzen, die Publikation von Fach- und Forschungsartikeln und die Verbreitung in (universitären) Lehrveranstaltungen. Hierbei sollte mit regionalen und bundesweiten Multiplikatoren in Industrie und Handel sowie in Forschung und Lehre zusammengearbeitet werden. Die genannten Maßnahmen sollten nicht nur für eine verbesserte Awareness des Themas Usable Security und für eine höhere Nachhaltigkeit des Projekts sorgen, sondern auch unmittelbar zu einer stärkeren Verankerung von Usability im Allgemeinen beitragen.

Etablierung eines Kompetenzzentrums

Das USecureD-Konsortium plante, gemeinsam mit assoziierten Partnern und anderen Multiplikatoren ein Kompetenzzentrum aufzubauen, das das Thema Usable Security in Praxis und Forschung vorantreibt und das auch nach Projektende langfristig als Serviceanbieter und als zentraler Ansprechpartner für gebrauchstaugliche Informationssicherheit zur Verfügung steht. Das Kompetenzzentrum sollte alle Personengruppen ansprechen, die vom Thema Usable Security betroffen sind, also insbesondere Anwender-, Hersteller- und Dienstleistungsunternehmen der IKT-Branche, aber auch Vertreter aus Wissenschaft und Forschung sowie die allgemeine Öffentlichkeit.

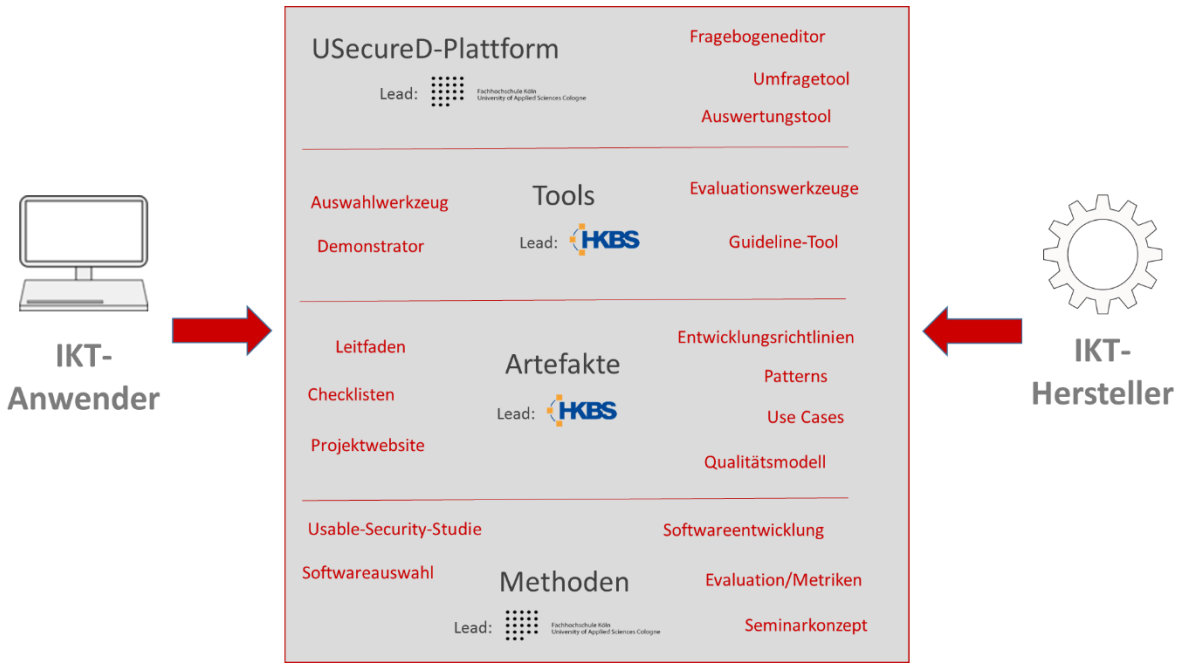


Abbildung 1: Übersicht der wissenschaftlichen und technischen Arbeitsziele (Stand: 10/2014)

1.3 Bezug des Vorhabens zu den förderpolitischen Zielen

Das Konsortium strebte an, mit dem Verbundvorhaben USecureD substanzielle Beiträge zu den förderpolitischen Zielen der Ausschreibung „Einfach intuitiv – Usability für den Mittelstand“ zu leisten. Die Beiträge zu den einzelnen Förderzielen sind im Folgenden kurz beschrieben:

Stärkung der Wettbewerbsfähigkeit deutscher KMU

Das USecureD-Projekt sollte kleinen und mittleren Herstellerunternehmen einen zügigen Markteintritt mit IT-Produkten ermöglichen, die gleichermaßen sicher und benutzerfreundlich sind. Dadurch sollten diese KMU ein Alleinstellungsmerkmal und einen Wettbewerbsvorteil gegenüber ihren Mitbewerbern haben, insbesondere gegenüber großen, internationalen IT-Herstellern, und sie sollten sich besser am Markt behaupten können. Mittelständische Unternehmen aus den Anwenderbranchen der IKT sollten durch USecureD bzw. durch die nach der USecureD-Methode hergestellten Softwareprodukte gleich mehrfach profitieren: Aus Sicht der Endanwender ist die verbesserte Gebrauchstauglichkeit wünschenswert, da sie ein leichteres und komfortableres Arbeiten ermöglicht. Die Software fördert somit zum einen die Motivation der Mitarbeiter, zum anderen trägt sie unmittelbar zur Effizienzsteigerung der softwarebasierten Geschäftsprozesse und damit zum Unternehmenserfolg bei. Zudem sollten die Unternehmen von einer erhöhten Sicherheit ihrer betrieblichen IT-Systeme profitieren.

Entwicklung von Vorgehensmodellen zur verstärkten Einbeziehung von Usability in den Auswahl- und Entwicklungsprozess betrieblicher Software

Mit dem USecureD-Projekt sollten für mittelständische Unternehmen die Voraussetzungen geschaffen werden, Usable Security (und somit auch Usability) als wichtiges Qualitätskriterium in den Auswahl-

bzw. Entwicklungsprozess ihrer betrieblichen Anwendungssoftware einzubeziehen. Für Anwenderunternehmen der IKT-Branche sollten Evaluationswerkzeuge und ein Vorgehen entwickelt werden, mit denen diese betriebliche Software gezielt nach dem Gesichtspunkt Usable Security bewerten und auswählen können. IKT-Hersteller sollten durch die Veröffentlichung der USecureD-Toolbox eine breite Unterstützung beim Design, der Entwicklung und der Qualitätsüberprüfung ihrer Software erhalten. Geplant war, dass die USecureD-Toolbox u. a. eine Patternsammlung mit bewährten Lösungsmustern, Entwicklungsrichtlinien inklusive eines Guideline-Tools sowie Auswertungs-, Interpretations- und Berichtsinstrumente für die Evaluation der Softwareprodukte enthält. Für Herstellerunternehmen sollte zudem eine USecureD-Plattform eingerichtet werden, auf der umfangreiche Usable-Security-Studien mit Softwareprodukten durchgeführt werden können.

Etablierung von Kompetenzzentren

Das USecureD-Konsortium bestand aus einem Anbieter für betriebliche Anwendungssoftware und einer entsprechend profilierten Technischen Hochschule. Die Konsortialpartner planten, gemeinsam mit assoziierten Partnern ein Kompetenzzentrum aufzubauen, welches das junge Thema Usable Security gemeinsam mit zusätzlichen Multiplikatoren in Praxis und Forschung vorantreibt. Hierdurch sollte das Vorhaben nicht nur für eine verbesserte Awareness des Themas Usable Security sorgen, sondern auch unmittelbar zu einer stärkeren Verankerung von Usability im Allgemeinen beitragen. Um eine Nachhaltigkeit der Projektergebnisse zu gewährleisten, sollte das Kompetenzzentrum auch langfristig als zentraler Ansprechpartner und Serviceanbieter für gebrauchstaugliche Informationssicherheit zur Verfügung stehen – sowohl für Anwender-, Hersteller- und Dienstleistungsunternehmen der IKT-Branche wie auch für Forscher und Wissenschaftler.

Pilothafte Erprobung der Vorgehensmodelle in Form eines Dienstleistungsangebotes der Kompetenzzentren

Sämtliche Methoden und Gestaltungs- bzw. Evaluationswerkzeuge, die das Konsortium im Rahmen von USecureD zu entwickeln plante, sollten zur Projektlaufzeit in Zusammenarbeit mit assoziierten Partnern in Pilotprojekten erprobt werden. Basierend auf den hierbei gemachten Erfahrungen sollten die Methoden und Werkzeuge für den Praxiseinsatz optimiert, dokumentiert und in geeigneter Form veröffentlicht werden, so dass sie auch von Anwender- und Hersteller-KMU außerhalb des Konsortiums genutzt werden können. Als unterstützende Dienstleistungen planten die Konsortialpartner, Support, Schulungen und Praxisseminare für die Anwendung der USecureD-Methoden und -Werkzeuge anzubieten. Mit dem USecureD-Demonstrator sollte eine konkrete, anschauliche Implementierung der erarbeiteten Usable-Security-Methoden und -Konzepte zur Verfügung stehen die auf Messen, Konferenzen und ähnlichen Veranstaltungen vorgeführt werden kann.

2 Voraussetzungen

2.1 Konsortialpartner und bisherige Arbeiten

2.1.1 HK Business Solutions GmbH

Als Experte für Software- und Hardwarelösungen unterstützt die HK Business Solutions GmbH (kurz: HKBS, http://www.hk-bs.de) kleine und mittelständische Unternehmen bei der Optimierung ihrer Investitionen in strategische Geschäfts- und Technologieinitiativen. Die HKBS stellt diesen Kunden ein innovatives und umfassendes Softwareangebot bereit, bei dem passende Hardware und strukturierte Netzwerktechnik den Rahmen für eine perfekte Office-Lösung bilden. Kompetente Beratung, Planung, Installation und optimale Sicherheitsvorkehrungen gehören ebenso zum Standard wie die Zusammenarbeit mit renommierten Partnerunternehmen. Die HKBS verfügt über mehr als 12 Jahre Erfahrung bei der Entwicklung firmenspezifischer Softwarelösungen für Kunden aus unterschiedlichsten Branchen. Neben der Softwareentwicklung gehört insbesondere die Einführung von ERP-, PPS- und CRM-Software bei kleinen und mittelständischen Unternehmen zum Kerngeschäft der HK Business Solutions.

Hartmut Schmitt, Projektleiter des Gesamtvorhabens USecureD sowie des Teilvorhabens der HKBS, brachte für die inhaltliche Arbeit in USecureD insbesondere Kompetenzen in den Bereichen Requirements Engineering, Usability/User Experience Engineering, intuitive Softwarebenutzung sowie bei der Durchführung von Evaluationen mit Endbenutzern ein. Er ist seit 2006 in Forschungsprojekten auf dem Gebiet Mensch-Computer-Interaktion tätig, u. a. als Projektkoordinator in den BMBF-geförderten Verbundvorhaben „FUN – Fun of Use für Geschäftsanwendungen“, „FUN-NI – Fun of Use with Natural Interactions“, „IBIS - Gestaltung intuitiver Benutzung mit Image Schemata“ und „PQ4Agile – Produktqualität für Agile Softwareentwicklung“. In diesen Verbundprojekten war er an der Entwicklung von Software-Engineering-Konzepten beteiligt, die zu einer motivierten und intuitiven Nutzung geschäftlicher Anwendungssoftware beitragen. Auf den Ergebnissen dieser Projekte konnte im USecureD-Vorhaben direkt aufgebaut werden:

Ziel des Projektes „FUN – Fun of Use für Geschäftsanwendungen“ war es, systematisch die Entwicklung von Business-Software zu unterstützen, die beim Benutzer positive Emotionen wie Freude auslöst. Es konnte nachgewiesen werden, dass es Interaktionspatterns gibt, die die Arbeitseffizienz, die Akzeptanz und den Nutzungswillen steigern ohne dass sie unmittelbar die Funktionalität der Software unterstützen (sog. UX-Patterns). Ergebnisse des FUN-Projektes waren ein Qualitätsmodell, validierte UX-Patterns und die Kreativitätstechnik KREA-FUN.

Der Arbeitsansatz des Projektes „FUN-NI – Fun of Use with Natural Interactions“ basierte auf der Identifikation, Evaluierung und Generalisierung von Patterns für eine möglichst natürliche und intuitive Mensch-Computer-Interaktion. Ergebnisse waren eine umfangreiche Patternsammlung und eine Toolbox mit leicht anwendbaren Evaluationswerkzeugen; diese ermöglichen eine Messung von „gefühlten“ Faktoren, z. B. intuitiver Benutzung, positiver Emotion und des psychologischen Grundbedürfnisses nach Sicherheit.

Im Projekt „IBIS – Gestaltung intuitiver Benutzung mit Image Schemata“ wurden die in den Kognitionswissenschaften entwickelten sog. Image Schemata erstmals systematisch und ingenieursmäßig in einen nutzerzentrierten Anforderungs- bzw. Designprozess integriert und dadurch für die Softwareentwicklung anwendbar gemacht. Die entstandene Methode unterstützt software-produzierende KMU dabei, intuitiv benutzbare und zugleich kreative Benutzungsschnittstellen zu entwickeln. Ergebnisse waren u. a. ein umfassendes Methodenhandbuch und Evaluierungswerkzeuge.

Im Forschungsprojekt „PQ4Agile – Produktqualität für Agile Softwareentwicklung“ wurde eine systematische Unterstützung für Anwender agiler Methoden entwickelt, die einen breiteren und erfolgreichen Einsatz dieser Methoden ermöglicht und die zu einer vorhersagbar hohen Qualität der entwickelten Produkte beiträgt. Die Hauptzielgruppe des Verbundvorhabens PQ4Agile sind kleine und mittlere Unternehmen der Softwareindustrie.

2.1.2 Technische Hochschule Köln

Prof. Dr.-Ing. Luigi Lo Iacono (https://www.th-koeln.de/personen/luigi.lo_iacono/) forscht an webbasierten Medienanwendungen und -technologien sowie an Web, Cloud und Usable Security. In all diesen Themengebieten bestehen umfangreiche Kenntnisse, die zum Großteil im Rahmen von geförderten Projekten erarbeitet wurden und in zahlreiche Publikationen gemündet sind. Die für das beantragte Projektvorhaben USecureD relevanten Vorarbeiten sind in Form von Veröffentlichungen in einschlägigen Fachzeitschriften und wissenschaftlichen Konferenzen erschienen und umfassen Übersichtsarbeiten, eigenentwickelte innovative Methoden und Verfahren im Web-Umfeld sowie Entwicklungsarbeiten auf dem Gebiet der Systementwicklung.

Die TH Köln und insbesondere der an USecureD beteiligte Prof. Dr.-Ing. Luigi Lo Iacono verfügen über eine außerordentlich gute Vernetzung mit fachlichen und akademischen Peers in Deutschland und Europa. Dies lässt sich an den zahlreichen wissenschaftlichen Veröffentlichungen und Gutachtertätigkeiten ablesen. Prof. Dr.-Ing. Luigi Lo Iacono ist als Gutachter für die Europäische Kommission im Rahmen der Evaluation der FP7-Forschungsprojekte TERESA und CloudSpaces tätig. Seine Aufgaben hier umfassen die Begutachtung der sicherheitsrelevanten Aktivitäten in den Projekten, wobei sich TERESA mit der Entwicklung patternbasierter und modellgetriebener Methoden und Verfahren befasst, die zur vertrauenswürdigen Implementierung von Sicherheitsmechanismen dienen sollen, und CloudSpaces die Entwicklung einer privaten Cloud-Infrastruktur zum Ziel hat.

Prof. Dr.-Ing. Luigi Lo Iacono ist Mitglied der Gesellschaft für Informatik und ist stellvertretender Sprecher der Fachgruppe E-Commerce und E-Government (ECOM) im Fachbereich Sicherheit der GI. Die Fachgruppe ECOM hat sich unter anderem das Ziel gesetzt, die Weiterentwicklung von Usable Security in E-Commerce-Anwendungen voranzutreiben und maßgeblich mitzugestalten. In diesem Zusammenhang beteiligt sich die Fachgruppe an den STE2PS-Aktivitäten zu den Themen Science, Teaching, and Engineering for Socio-Technical Experiences of Privacy and Security. Zudem hat die ECOM in Kooperation mit der TU Darmstadt den EIT/ICT-Workshop zum Thema Usable Security und Privacy organisiert, der am 10. März 2011 in Darmstadt stattgefunden hat.

Von der TH Köln sind in zahlreichen Kooperationen mit international ausgewiesenen Experten auf dem Gebiet Usable Security umfangreiche wissenschaftliche Arbeiten verfasst und publiziert worden. Auf dieser wissenschaftlich fundierten Basis wurden praktische Lösungsansätze entwickelt, die wesentliche Beiträge zum Fachgebiet und insbesondere neue Technologien für den praktischen Einsatz in webbasierten Anwendungslandschaften hervorgebracht haben. Einer der entwickelten Ansätze ist auf der 6. International Network Conference (INC 2010) mit dem Excellent Paper Award ausgezeichnet worden. Die dort vorgestellte Lösung zur transparenzerhöhten Maskierung von Passworteingaben wird nunmehr von einigen mittelständischen Unternehmen auf die Integration in die eigenen Produkte geprüft.

Die Resonanz aus der Forschungscommunity führte zu einer Reihe von eingeladenen Vorträgen, die wiederum in weiteren gemeinsamen Arbeiten und Publikationen mündeten. Die vorliegenden Erfahrungen und Kompetenzen auf dem Gebiet Usable Security sind zudem Bestandteil der Ausbildung von jungen Nachwuchsingenieuren im Rahmen spezialisierter Lehrveranstaltungen zur Mensch-Computer-Interaktion im Masterstudiengang Medientechnologie.

2.2 Notwendigkeit der Zuwendung

Die methodischen Entwicklungsarbeiten in USecureD fanden in einem innovativen und wissenschaftlich anspruchsvollen Forschungsgebiet statt. Zwar konnten die Partner bei sämtlichen Arbeiten auf das notwendige Experten-Knowhow und in Teilbereichen (z. B. bei der Evaluation) auf bereits validierte Werkzeuge zurückgreifen, die im Rahmen eigener Vorarbeiten entwickelt wurden. Trotzdem waren die Partner nicht in der Lage, den implizierten Aufwand aus Eigenmitteln zu bestreiten.

Kleine und mittelständische Hersteller wie die **HKBS** haben es aus mehreren Gründen schwer, sich erfolgreich als Lieferant innovativer Vorgehensmodelle und Produkte im IKT-Bereich zu positionieren. Die personelle und finanzielle Ausstattung erlaubt es oft nicht, neue und innovative Methoden zu testen, selbst dann nicht, wenn diese in künftigen Projekten viel Zeit und Geld sparen könnten und dadurch einen Wettbewerbsvorteil sichern würden. Zudem hängt das wirtschaftliche Potential innovativer Softwareprodukte stark von der Akzeptanz der Technologie durch die Benutzer ab. Es sind daher oft weitreichende Vorleistungen, z. B. die Entwicklung voll funktionstüchtiger Vorversionen, notwendig, bevor Innovationen auf ihre Akzeptanz bei den Benutzern evaluiert werden können. Da sich noch keine klar definierte Nachfrage für Softwareprodukte mit dem Qualitätsmerkmal Usable Security herausgebildet hatte, war für die HKBS eine ausschließlich aus Eigenmitteln finanzierte Forschung nicht möglich. Der Markt für neue und risikobehaftete Technologien ist in der Regel noch nicht entwickelt, so dass den anfänglich geringen Umsätzen hohe Kosten für Forschung und Entwicklung gegenüberstehen. Ein KMU wie die HKBS ist nicht in der Lage, diese Aufwände alleine zu tragen; vielmehr ist es auf eine geförderte Zusammenarbeit mit Forschungspartnern angewiesen, um innovative Methoden und Werkzeuge zu entwickeln.

Da die **TH Köln** nicht selbst wirtschaftlich tätig werden kann, ist auch sie bei der Erforschung des Themas Usable Security auf Zuwendungen angewiesen. Die prototypische Implementierung sowie die Evaluation in dieser Domäne sind zudem an konkrete Anwendungskontexte gebunden und dadurch sehr aufwendig. Daher benötigt die TH Köln zur Erforschung dieses innovativen Themenkomplexes sowohl eine Zusammenarbeit mit Herstellerunternehmen der IKT-Branche als auch den dadurch gegebenen Zugang zu Anwenderunternehmen.

Aus den dargelegten Gründen waren die Partner daher auf Förderungen angewiesen, um die angestrebten Methoden-, Prozess- und Produktinnovationen erfolgreich durchzuführen und um durch eine gute Vernetzung mit Partnerunternehmen sowie durch Wissenstransfer zu Industrie und Forschung zur Stärkung des Produktionsstandorts Deutschland beizutragen.

Alternative Finanzierungsmöglichkeiten für das Vorhaben waren seitens des Projektkonsortiums insbesondere im Hinblick auf eine Förderung durch EU-Programme geprüft worden. Das Vorhaben war für diese jedoch entweder thematisch unpassend oder aber aufgrund der Zusammensetzung des Konsortiums mit nationaler Konstellation und in Teilen mit nationalen Fokuspunkten ohne realistische Erfolgsaussichten. USecureD wies dagegen eine vollständige Übereinstimmung mit den Zielen der BMBF-Ausschreibung „Einfach intuitiv – Usability für den Mittelstand“ auf: Die Kernidee des Vorhabens bestand darin, Methoden und Werkzeuge zu entwickeln, mit denen kleine und mittelständische Unternehmen ihre Geschäftsprozesse effizienter und zugleich sicherer gestalten können. Neben der Steigerung der Wettbewerbsfähigkeit deutscher Mittelständler im nationalen und internationalen Wettbewerb lieferte das Projekt mit der Stärkung der Informationssicherheit deutscher Unternehmen also einen zusätzlichen Beitrag, der von Bundesinteresse ist.

3 Planung und Ablauf des Vorhabens

3.1 Lösungsidee

Aus Sicht des Konsortiums erschien es für die Entwicklung betrieblicher Software mit dem Qualitätsmerkmal Usable Security als besonders vielversprechend, einen konstruktiven Software-Engineering-Ansatz zu wählen (by Design). Die Hersteller müssen dann ihre Produkte nicht erst vollständig entwickeln, anschließend evaluieren und zuletzt nachbessern. Vielmehr können sie – nach dem Motto „Vorbeugen ist besser als heilen“ – in ihrem Software-Engineering-Prozess direkt auf validierte, praxistaugliche Lösungen zurückgreifen.

Um dies zu erreichen, sollten in USecureD erfolgreiche Ansätze des Usability-Engineerings, des User-Experience-Engineerings und des Security-Engineerings miteinander verknüpft werden: In einer Anforderungsanalyse sollten die aktuellen Herausforderungen und Potenziale im Umgang mit Sicherheitsmechanismen aus Benutzersicht identifiziert werden. Darauf aufbauend sollten Werkzeuge entwickelt werden, die die Entwicklung von benutzerfreundlicher und sicherer betriebswirtschaftlicher Anwendungssoftware unterstützen und die sich leicht in beliebige Software-Engineering-Prozesse kleiner und mittlerer Herstellerfirmen integrieren lassen. Mithilfe dieser Werkzeuge sollten schließlich prototypische Lösungen für einen konkreten Anwendungskontext entwickelt und zuletzt evaluiert werden.

Über die bisher durchgeführten Arbeiten und Projekte ging der Lösungsansatz des USecureD-Vorhabens hinaus, denn er erweiterte das Thema Usable Security erstmals um folgende Aspekte bzw. Eigenschaften:

- Der Lösungsansatz ist *motivationsfördernd*: Durch eine Verbesserung der User Experience sollen die Nutzer dazu animiert werden, sicherheitsrelevante Bedienelemente- und -dialoge in der dafür vorgesehenen Weise zu nutzen; es sollen hierfür Interaktionskonzepte verwendet werden, die nachweislich hedonische Qualität besitzen und auf diese Weise die Attraktivität der Software steigern.
- Der Lösungsansatz ist *patternbasiert*: Benutzerfreundliche, leicht verständliche und intuitiv bedienbare Sicherheitsmechanismen und -funktionen werden in Form von Design- und Interaktionspatterns dokumentiert. Die hieraus resultierende USecureD-Patternsammlung wird als Projektergebnis veröffentlicht und steht anderen Softwareherstellern kostenlos zur Verfügung.
- Der Lösungsansatz ist *konstruktiv* („by Design“): Die Verwendung von Guidelines und die einfache Integration validierter Usable-Security-Patterns in den Software-Engineering-Prozess ermöglicht Herstellern von E-Business-Anwendungen kürzere Produkteinführungszeiten und senkt zugleich das Entwicklungsrisiko für innovative Softwareprodukte.
- Der Lösungsansatz ist *KMU-tauglich*: Sämtliche Entwurfswerkzeuge werden so konzipiert, dass kleine und mittlere Hersteller diese leicht in ihren eigenen Softwareentwicklungsprozess integrieren und im eigenen Kontext anwenden können, ohne dass hierfür größere Prozessinnovationen, der Aufbau eines Expertenstabs oder die Einrichtung einer Laborumgebung notwendig wären. Auch das Auswahlwerkzeug und die Entscheidungshilfen für die Anwenderunternehmen der IKT-Branche werden so konzipiert, dass sie ohne Spezialkenntnisse für eine einfache, zielgerichtete Evaluation verwendet werden können.

3.2 Projektplan

3.2.1 Laufzeit, Arbeitspakete und Meilensteinplanung

Das Projekt war auf eine Laufzeit von 24 Monaten ausgelegt. In der ersten Projektphase sollten die inhaltlichen und methodischen Grundlagen für die weitere Projektarbeit gelegt werden; dies umfasste Analysen zu den Anwendungsbereichen und den Anforderungen an Usable Security sowie die Entwicklung eines Qualitätsmodells. In der zweiten Projektphase sollten die Gestaltungswerkzeuge sowie eine Evaluationsmethodik für IKT-Hersteller entwickelt werden und bei der Gestaltung bzw. Evaluierung prototypischer Implementierungen angewendet werden. Die dritte Projektphase sollte sich der Konzeptionierung, Entwicklung, Integration und Evaluierung einer USecureD-Plattform widmen, auf der IKT-Hersteller ihre Softwareprodukte evaluieren können. Im Zentrum der vierten geplanten Projektphase stand die Zielgruppe der IKT-Anwender, für die diverse Entscheidungshilfen (Checklisten, Auswahlwerkzeug und Demonstrator) entwickelt werden sollten. Der Wissenstransfer an sämtliche anvisierten Zielgruppen und das Management des USecureD-Projekts sollten begleitend während der gesamten Projektlaufzeit stattfinden.

Das Projekt USecureD war in fünf inhaltliche Arbeitspakete sowie ein Projektmanagement-Arbeitspaket unterteilt. Der in Abbildung 2 dargestellte Projektstrukturplan zeigt die Gliederung des Projekts in Arbeitspakete und Teilaufgaben. Diese Struktur blieb während der Projektdurchführung unverändert:

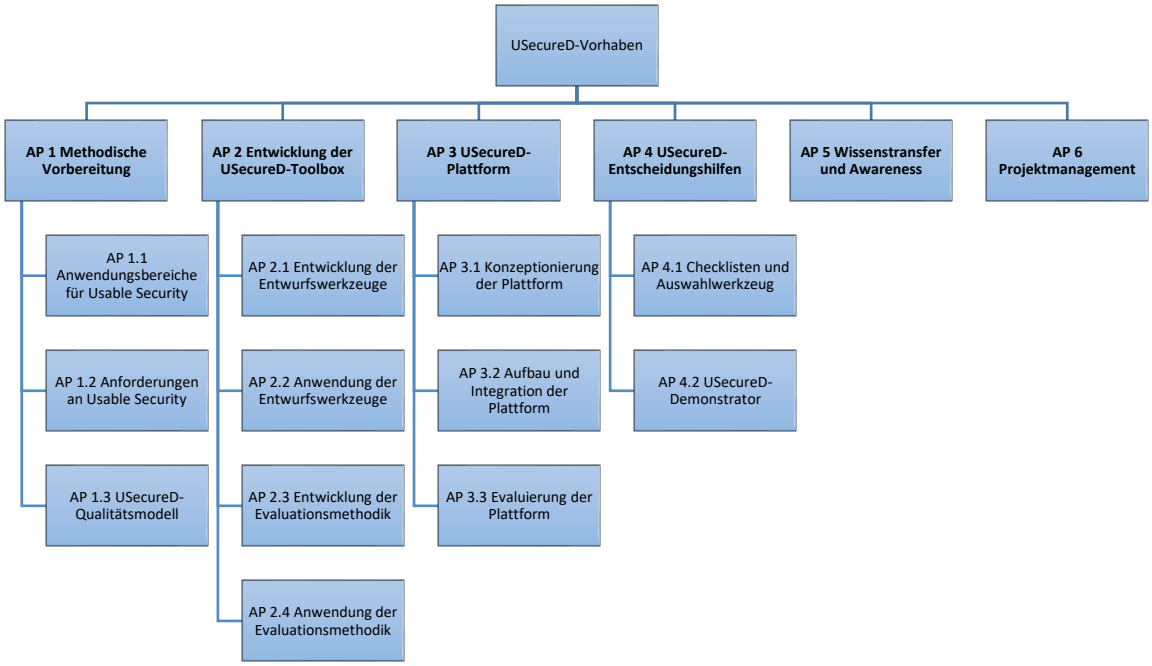


Abbildung 2: Projektstrukturplan des USecureD-Vorhabens

Durch den Abschluss wichtiger (Teil-)Arbeitspakete ergaben sich folgende Meilensteine des USecureD-Projekts:

- **Meilenstein 1** (nach 6 Monaten): Die methodische Vorbereitung des USecureD-Projekts (AP 1) ist abgeschlossen: Die Anwendungsbereiche und Anwendungsfälle (Use Cases) für Usable Security sind dokumentiert. Die Anforderungen an Usable Security aus Anwendersicht sind erhoben und analysiert. Das USecureD-Qualitätsmodell ist fertiggestellt.
- **Meilenstein 2** (nach 9 Monaten): Die Entwicklung der USecureD-Entwurfswerkzeuge (AP 2.1) ist abgeschlossen: Die Gestaltungslösungen für den Bereich Usable Security sind in Form einer Patternsammlung mitsamt einer Beschreibungsvorlage (Patterntemplate) dokumentiert. Die USecureD-Entwicklungsrichtlinien für Anwendungsentwickler und das entsprechende Guideline-Tool sind fertiggestellt.
- **Meilenstein 3** (nach 15 Monaten): Die Entwicklung der USecureD-Evaluierungswerkzeuge (AP 2.3) ist abgeschlossen: Die Usable-Security-Metriken sind definiert und es stehen entsprechende praxistaugliche Messwerkzeuge zur Verfügung. Die Arbeitshilfen für die Durchführung von Usable-Security-Evaluationen und das Anwenderhandbuch für die USecureD-Toolbox sind fertiggestellt.
- **Meilenstein 4** (nach 18 Monaten): Die Entwicklung und Integration der USecureD-Plattform (AP 3.2) sowie die Entwicklung der Checklisten und des Auswahlwerkzeugs (AP 4.1) sind abgeschlossen: Die USecureD-Plattform ist vollständig aufgebaut und steht für eine Qualitätsüberprüfung bereit. Die Plattform-Werkzeuge für die Erstellung, Durchführung und Auswertung von Usable-Security-Tests (USecureD-Fragebogeneditor, USecureD-Umfragetool und USecureD-Auswertungstool) sind entwickelt. Die Integration sämtlicher USecureD-Werkzeuge für die Zielgruppe IKT-Hersteller in die Plattform ist abgeschlossen. Die USecureD-Checklisten und das Auswahlwerkzeug für IKT-Anwender sind fertiggestellt.
- **Meilenstein 5** (nach 24 Monaten, Projektabschluss): Die Entwicklung des USecureD-Demonstrators (AP 4.2) ist abgeschlossen. Sämtliche Projektergebnisse liegen vollständig aufbereitet vor: Der USecureD-Demonstrator ist fertig implementiert und steht mitsamt Begleitleitfaden für

die weitere Projektverbreitung zur Verfügung. Basierend auf den Erfahrungen aus der Anwendung und Evaluation im Projekt wurden alle Ergebnisse des USecureD-Vorhabens nach Bedarf angepasst und finalisiert.

3.2.2 Risikomanagement und Abbruchkriterien

Mögliche Projektrisiken – inhaltlich-technische, personelle sowie wirtschaftliche Risiken – wurden von den Partnern im Vorfeld des Projekts untersucht und bewertet. Durch die Zusammensetzung des Konsortiums und die Ausgestaltung des Projektplans wurde versucht, alle identifizierten Risiken gezielt zu minimieren. Da innerhalb eines Forschungsvorhabens nicht sämtliche Risiken von vornherein ausgeschlossen werden können, wurden für USecureD folgende Abbruchkriterien definiert, die zu relativ frühen Zeitpunkten (nach dem 6., 9. bzw. 15. Monat) überprüft werden konnten:

- **Abbruchkriterium 1**: Es kann kein tragfähiges USecureD-Qualitätsmodell entwickelt werden: Das Konsortium ist nicht in der Lage, ein ganzheitlichen Qualitätsverständnis für den Bereich Usable Security zu erarbeiten bzw. dieses adäquat zu dokumentieren.
- **Abbruchkriterium 2**: Die Entwicklung der USecureD-Entwurfswerkzeuge schlägt fehl: Es gelingt dem Konsortium nicht, eine USecureD-Patternsammlung, USecureD-Entwicklungsrichtlinien für Anwendungsentwickler sowie eine entsprechende Werkzeugunterstützung (Guideline-Tool) zu erarbeiten.
- **Abbruchkriterium 3**: Die Entwicklung der USecureD-Evaluierungswerkzeuge schlägt fehl: Das Konsortium ist nicht in der Lage, geeignete Metriken für den Bereich Usable Security zu definieren und entsprechende Werkzeuge für deren Evaluation zur Verfügung zu stellen.

Mögliche Fortschritte durch wissenschaftliche oder technische Entwicklungen außerhalb des Konsortiums, die einzelne USecureD-Ergebnisse vorwegnehmen, wurden explizit nicht als Risiko betrachtet. Vielmehr sollten derartige Entwicklungen möglichst frühzeitig erkannt, aufgegriffen und in das Projekt integriert werden, mit dem Ziel, höherwertige und weitreichendere Ergebnisse zu erreichen.

3.2.3 Wechselwirkung/Interaktion zwischen den Partnern

Alle Arbeitspakete des USecureD-Vorhabens sollten von den beiden Partnern in enger inhaltlicher und organisatorischer Abstimmung gemeinschaftlich bearbeitet werden. Hierbei wurden folgende Schwerpunkte der Projektarbeit vereinbart:

Die HKBS sollte als Technologiepartner für die technische Implementierung der Usable-Security-Konzepte verantwortlich sein; dies umfasste jeweils mehrere USecureD-Werkzeuge für IKT-Anwender und IKT-Hersteller, die Entwicklung von Prototypen, also Instanziierungen von USecureD-Konzepten in konkreten Anwendungskontexten, sowie die Entwicklung eines Demonstrators, der diese Konzepte generalisiert und für IKT-Anwender aller Branchen erlebbar und „begreifbar“ macht. Bei sämtlichen anderen Arbeitspaketen, also den methodischen Vorarbeiten, der Evaluation der prototypischen Implementierungen, Verbreitung des Projekts usw., war eine enge Zusammenarbeit der HKBS mit der TH Köln geplant. Als Konsortialführer des Projekts sollte die HKBS zudem sämtliche zu erbringende Arbeiten koordinieren.

Die TH Köln sollte im USecureD-Projekt maßgeblich Aufgaben im Bereich der Analyse, Konzeption und Evaluation gebrauchstauglicher IKT-Sicherheitsmechanismen in betrieblichen Anwendungssystemen durchführen. Dies sollte in enger Kooperation mit der HKBS erfolgen, aber auch mit den assoziierten Partnern. Hieraus sollte die TH Köln die HKBS bei der Entwicklung der prototypischen Implementierungen unterstützen, auf deren Grundlage die Evaluation erfolgen sollte. Aufgabe der TH Köln war es ferner, die sich aus diesen Aktivitäten ergebenden Guidelines und Patterns zur Anwendung der evaluierten Maßnahmen und Verfahren in eine Webplattform zu integrieren, die es KMU ermöglicht, eigene webbasierte Softwareprodukte gegen die Guidelines und Patterns zu testen.

Die HKBS und die TH Köln sollten gemeinschaftlich für eine starke Außendarstellung des Projekts sorgen: Die HKBS sollte als Hauptansprechpartner für sämtliche Belange des Projekts fungieren und insbesondere die Verbreitung im IKT-Bereich (Hersteller- und Anwenderunternehmen) vorantreiben, während die TH Köln als zentraler Ansprechpartner für Forschung und Wissenschaft zur Verfügung stehen sollte.

3.2.4 Zusammenarbeit mit Dritten

Das Konsortium wurde ergänzt durch sechs assoziierte Partner (Technische Universität Berlin, Bundesamt für Sicherheit in der Informationstechnik, Fraunhofer-Institut für Experimentelles Software Engineering, saar.is - saarland.innovation&standort e.V., Ha-Ra Umwelt- und Reinigungstechnik GmbH und Bruno Zimmer e.K.). Die assoziierten Partner sollten im Projektverlauf nach Bedarf in die inhaltliche Arbeit mit einbezogen werden. Hierdurch sollten die Entwicklungen an den entsprechenden Stellen durch eine unabhängige Sicht bereichert werden.

Mit dem Fraunhofer IESE, dem BSI und der TU Berlin sollten Workshops ausgerichtet werden, in denen die jeweiligen Interessen und mögliche gemeinsame Aktivitäten bzw. Kooperationen diskutiert werden. Zudem sollten an diese Partner (vorläufige) Projektergebnisse übergeben werden, um Feedback einzuholen bzw. um die Arbeiten zu validieren. Die Rolle der saar.is war vorwiegend die eines Multiplikators. Ha-Ra bzw. Bruno Zimmer sind Kundenunternehmen der HKBS, die vor allem im Rahmen der Anforderungserhebung an Usable Security und im Rahmen der Evaluation der erarbeiteten (prototypischen) Lösungen eingebunden werden sollten.

3.3 Ablauf

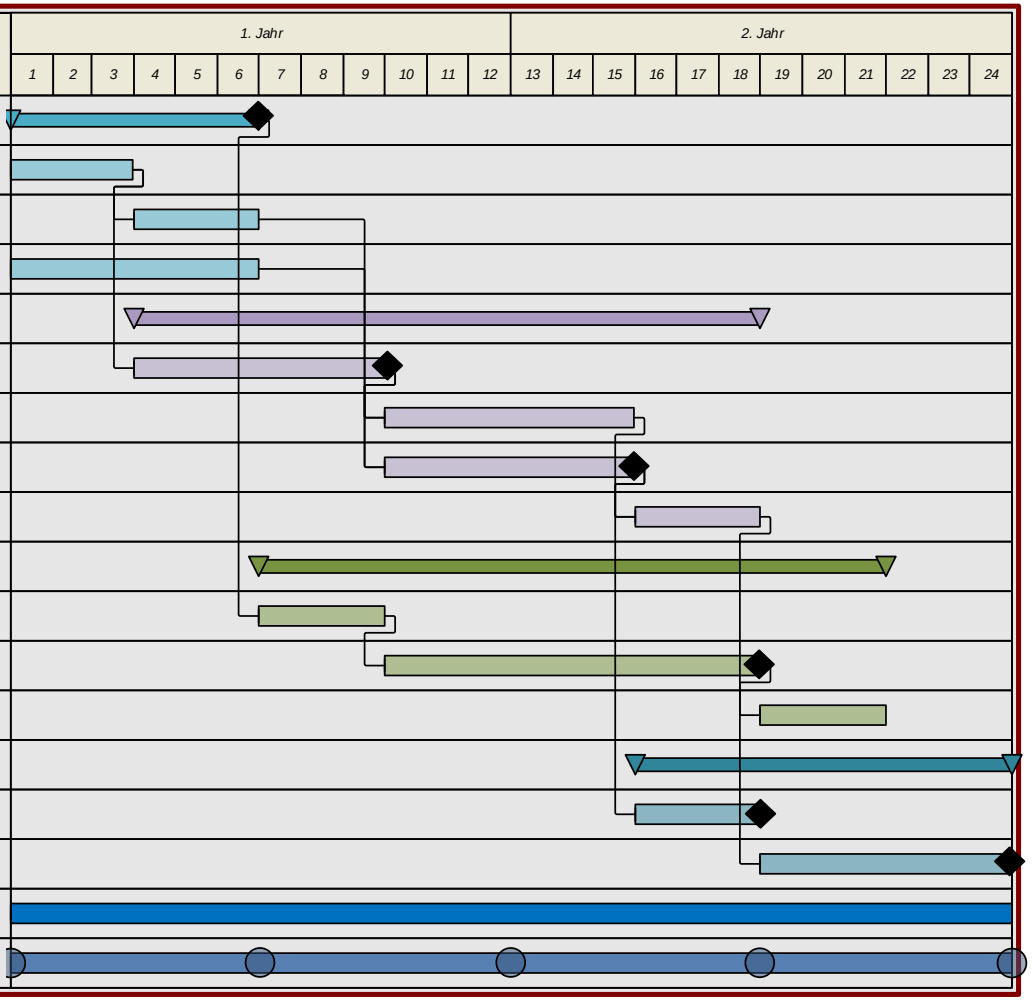
Für das Projekt wurde ein paralleles Phasenmodell gewählt; diese Vorgehensweise erlaubte es in vielen Fällen, neue Projektphasen bzw. Arbeitspakete zu starten, ohne dass der Vorgänger (Projektphase bzw. Arbeitspaket) hierfür abgeschlossen sein musste. Abbildung 3Abbildung 3 stellt die zeitliche Verteilung sämtlicher Projektaktivitäten – insbesondere die zeitliche Überlappung der Projektphasen und einzelner Arbeitspakete – in Form eines Balkendiagramms dar.

Aufgrund von Verzögerungen während der Antragstellung wurden die inhaltlichen Arbeiten nach Rücksprache mit dem Projektträger erst nach Erhalt des Zuwendungsbescheids aufgenommen. Hierdurch kam es zu einem planabweichenden Projektbeginn, der insbesondere die Teilarbeitspakete AP 1.1 und AP 1.3 betraf. Entsprechende Verzögerungen konnten im weiteren Projektverlauf ausgeglichen werden.

Im Zuge der Projektdurchführung wurde die Laufzeit einzelner Arbeitspakete in Rücksprache mit dem Projektträger verlängert, um die Arbeiten in diesen Arbeitspaketen intensivieren bzw. ergänzen zu können. Zu nennen sind hier insbesondere die längere Laufzeit der USecureD-Onlinestudie, durch die es möglich war, eine bessere Basis für die statistische Auswertung zu erhalten, sowie die Verlängerung der Anwendungsphase der Entwurfswerkzeuge bzw. der Evaluationsmethodik, durch die es möglich war, bei einer größeren Anzahl von Anwenderunternehmen Evaluationen durchzuführen. Auch hier konnten entsprechende Verzögerungen im weiteren Projektverlauf ausgeglichen werden.

Während der Projektlaufzeit (01.05.2015 – 30.04.2017) haben sich beim Ziel bzw. Ergebnis des Projekts und beim Lösungsweg bzw. der Vorgehensweise keine wesentlichen Änderungen gegenüber dem Projektplan ergeben; auch waren keine Änderungen in der Zielsetzung notwendig. Aufgrund externer Impulse durch Anwender der USecureD-Tools weitete die TH Köln die Entwicklung dieser Tools in enger Abstimmung mit dem Projektträger aus. Die TH Köln fügte eine programmatische Schnittstelle zu den Werkzeugen hinzu, die es Anwendern erlaubt, die USecureD-Tools tief in eigene softwaregestützte Produkte und Umgebungen zu integrieren. Diese zusätzlichen Aufwände konnten von der TH Köln ohne nennenswerte Verzögerungen im Arbeits- und Meilensteinplan realisiert werden.

ID	AP-Nr.	Bezeichnung	Dauer	Laufzeit
1	**AP 1**	**Methodische Vorbereitung**	**6 Monate**	**1.–6. Monat**
2	AP 1.1	Anwendungsbereiche für Usable Security	3 Monate	1.–3. Monat
3	AP 1.2	Anforderungen an Usable Security	3 Monate	4.–6. Monat
4	AP 1.3	USecureD-Qualitätsmodell	6 Monate	1.–6. Monat
5	**AP 2**	**USecureD-Toolbox**	**18 Monate**	**4.–18. Monat**
6	AP 2.1	Entwicklung der Entwurfswerkzeuge	6 Monate	4.–9. Monat
7	AP 2.2	Anwendung der Entwurfswerkzeuge	6 Monate	10.–15. Monat
8	AP 2.3	Entwicklung der Evaluierungsmethodik	6 Monate	10.–15. Monat
9	AP 2.4	Anwendung der Evaluationsmethodik	3 Monate	16.–18. Monat
10	**AP 3**	**USecureD-Plattform**	**15 Monate**	**7.–21. Monat**
11	AP 3.1	Konzeptionierung der Plattform	3 Monate	7.–9. Monat
12	AP 3.2	Entwicklung und Integration der Plattform	9 Monate	10.–18. Monat
13	AP 3.3	Evaluierung der Plattform	3 Monate	19.–21. Monat
14	**AP 4**	**USecureD-Entscheidungshilfen**	**9 Monate**	**16.–24. Monat**
15	AP 4.1	Checklisten und Auswahlwerkzeug	3 Monate	16.–18. Monat
16	AP 4.2	USecureD-Demonstrator	6 Monate	19.–24. Monat
17	**AP 5**	**Wissenstransfer und Awareness**	**24 Monate**	**1.–24. Monat**
18	**AP 6**	**Projektmanagement**	**24 Monate**	**1.–24. Monat**



Legende: Meilenstein Präsentationstermin vor dem Projektträger

Abbildung 3: Projektplan des USecureD-Vorhabens (Stand: 10/2014)

4 Wissenschaftlicher und technischer Stand

4.1 State-of-the-art in den betrachteten Domänen

4.1.1 Usable Security

Nach ISO 9241-11 bezeichnet Usability das Ausmaß, in dem ein Produkt von einem bestimmten Benutzer verwendet werden kann, um bestimmte Ziele in einem bestimmten Kontext effektiv, effizient und zufriedenstellend zu erreichen. Die Sicherheit zählt jedoch meist nicht zu den primären Zielen des Nutzers bei der Verwendung von IKT. Daher hatten Usability-Fragen, insbesondere aus Sicht des Durchschnittnutzers, in der traditionellen Forschung und Entwicklung sicherer Systeme nur eine untergeordnete Rolle gespielt und die Entwicklungsprozesse und Vorgehensmodelle des Security-Engineerings waren noch weitgehend von denen des Usability-Engineerings entkoppelt.

Heute bestehen kaum mehr Zweifel daran, dass sichere und benutzbare Systeme notwendig sind. Eine nahtlose Verbindung von Methoden und Werkzeugen zu einem integrierten Entwicklungsprozess muss allerdings erst noch hergestellt werden. Usable Security bezeichnet daher den interdisziplinären Ansatz, sicherheitsfördernde Verfahren für IKT-Systeme so auszugestalten, dass Benutzer bei ihren Zielen und Vorhaben unterstützt werden und dass diese nicht erschwert oder gar vollends verhindert werden.

4.1.2 Analytische und konstruktive Usabilitymethoden

Im Usability-Engineering kann man unterscheiden zwischen analytischen und konstruktiven Methoden. Analytische Methoden (z.B. Usability-Tests oder -Inspektionen) sind diagnostische Maßnahmen, die am Ende von Entwicklungsprozessen oder -phasen summativ eingesetzt werden und deren Ziel es ist, das erreichte Qualitätsniveau des Endsystems zu messen. Hierdurch können gefundene Qualitätsmängel allerdings nur noch dokumentiert werden und in anschließenden Entwicklungsfortführungen Berücksichtigung finden, siehe Abbildung 4.

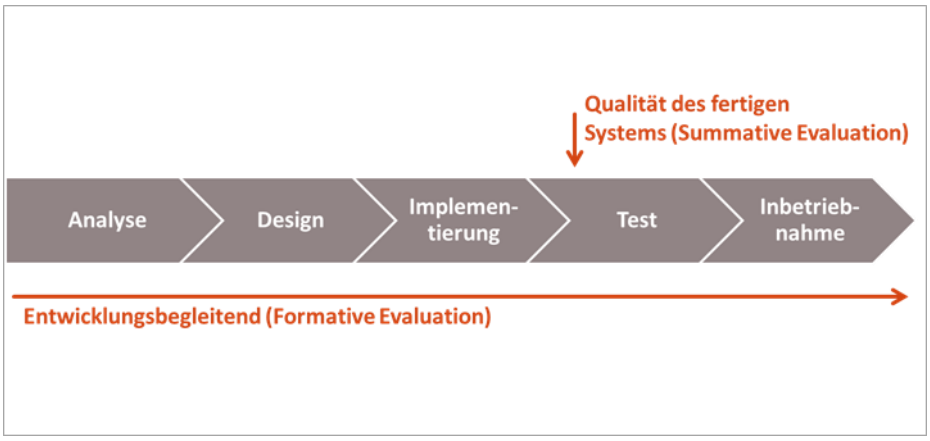


Abbildung 4: Einordnung formativer und summativer Evaluationen in den Softwareentwicklungsprozess

Um frühzeitiger – also noch im Softwareentwicklungszyklus – auf potenzielle Usabilityprobleme aufmerksam zu werden und auf diese eingehen zu können, empfiehlt sich der Einsatz konstruktiver Methoden, die formativ in den gesamten Prozess eingebettet sind. Konstruktive Methoden verwenden Techniken und Tools, die auf empirisch validierten Ergebnissen basieren, und sorgen somit dafür, dass sowohl das entwickelte Softwareprodukt als auch der zugrundeliegende Softwareentwicklungsprozess von vornherein bestimmte Eigenschaften und Qualitätsattribute besitzen. Zu den konstruktiven Methoden, die im beantragten Projekt zum Einsatz kommen sollten, zählen patternbasierte Ansätze (siehe Kapitel 4.1.3), Richtlinien, Prototyping und die Einbindung von Endbenutzern in frühen Entwicklungsphasen.

4.1.3 Patternbasierte Ansätze

Das Konzept sogenannter Patterns (Entwurfsmuster), also die Dokumentation bewährter Lösungsschablonen für wiederkehrende Entwurfsprobleme, kommt ursprünglich aus der Architektur und wurde von Gamma und Beck erfolgreich auf den Bereich Softwarearchitektur übertragen. Norman und Draper

machten erstmals den Vorschlag, Patterns auch im Bereich der Mensch-Computer-Interaktion einzusetzen; seitdem haben Patterns auch dort zunehmendes Interesse gefunden. Bei der Gestaltung von Benutzerschnittstellen können Interaktionspatterns und Usability Patterns genutzt werden, um bewährte Lösungen zu definierten Problemen der Interaktionsgestaltung zu dokumentieren. Sie tragen damit zur Erhöhung der Konsistenz von Benutzeroberflächen, zur Steigerung der Entwicklungseffizienz und zur Einhaltung von Entwicklungsrichtlinien bei. Es gibt zahlreiche bekannte Sammlungen von Usability- und Interaktionspatterns. Bei der Dokumentation dieser Patterns fehlt allerdings in der Regel ein klarer Bezug zum Thema Security.

Auch im Bereich Security-Patterns gibt es zahlreiche Vorarbeiten; diese wiederum sind meist ohne klaren Usability-Bezug. Bedeutsam für das beantragte Projekt waren insbesondere die Arbeiten von Hafiz, der Patterns aus verschiedenen Quellen zusammenführte und Vorschläge zur Kategorisierung von Security Patterns bzw. zu einer geeigneten Pattern Language machte. Der von Hafiz erstellte Katalog mit Pattern-Kurzbeschreibungen sollte für die Übertragung in die Domäne Usable Security auf Vollständigkeit geprüft, stärker detailliert und um die fehlende Usability-Komponente ergänzt werden.

Eine umfassende Sammlung mit Usable-Security-Patterns, die Softwareingenieure systematisch mit konkreten Gestaltungshilfen unterstützt, existierte vor dem USecureD-Vorhaben nicht. In der Literatur gab es verschiedene erfolgversprechende Ansätze, z.B. methodische Vorarbeiten oder bestehende Dokumentationen mit Pattern-Kurzbeschreibungen. Hier bestand der Bedarf, die bestehenden Ansätze zusammenzuführen, zu konsolidieren und weiter zu detaillieren. Zudem sollten – basierend auf der Analyse geschäftlicher Anwendungssysteme – noch weitere konkrete Gestaltungslösungen identifiziert und dokumentiert werden.

Von Röder wurde eine Methode vorgestellt, Patterns und Use Cases miteinander zu verknüpfen. Ziel seines Ansatzes war es, Use-Case-Spezifikationen dahingehend zu erweitern, dass Usability-Merkmale planmäßig realisiert und getestet werden können. Hierfür wurde ein geeigneter Pattern-Katalog entwickelt. Die Spezifikationsmethode wurde in mehreren Softwareprojekten validiert, jeweils in Verbindung mit dem Use-Case-Editor TULIP. Diese Methode sollte daher weiter generalisiert werden, z. B. im Hinblick auf Werkzeugunabhängigkeit und weitere Pattern-Domänen.

4.2 Anderweitige Forschungs- und Entwicklungsarbeiten

4.2.1 Initiative „Einfach intuitiv – Usability für den Mittelstand“

Die Erforschung des Themas Usable Security durch das Vorhaben USecureD stellte im Rahmen der Initiative „Einfach intuitiv – Usability für den Mittelstand“ ein Alleinstellungsmerkmal dar. Da sich sämtliche Projekte dieser Initiative in irgendeiner Weise mit dem Thema Usability befassten, gab es insofern Überschneidungen mit anderen Vorhaben innerhalb der Initiative. Diese Projekte sah das Konsortium allerdings nicht im Sinne einer Konkurrenz an, sondern es versuchte eine möglichst enge Abstimmung mit diesen Projekten herbeizuführen. Hierdurch sollte zum einen vermieden werden, dass dieselben Forschungsfragen in unterschiedlichen Projekten doppelt bearbeitet werden, zum anderen sollten durch einen Gedanken- und Informationsaustausch mit diesen Projekten möglichst sinnvolle Synergien für beide Seiten geschaffen werden.

4.2.2 Weitere Arbeiten außerhalb des Konsortiums

Mit dem jungen Thema der Verzahnung von Usability und Security beschäftigen sich auch andere Forschungseinrichtungen, Firmen oder Communities. Der Großteil der Arbeiten in dem Bereich widmet sich der Erarbeitung theoretischer Prozesse, deren Wirksamkeit bislang nicht überprüft wurde, oder analytischer Evaluationsmethoden.

Sasse & Flechais schlugen ein verzahntes Modell des „Faktors Mensch” (human factor) mit benutzerzentrierten Designprozessen vor, das sowohl das Produkt als auch den Entwicklungsprozess verbessern sollte. Allerdings fehlt es an einer nachweislichen Erprobung und Wirksamkeit dieses Modells sowie einer Bezugnahme zum Themenkomplex Funktionen von Security-Software.

Kroll-Peters beschäftigte sich mit der Entwicklung eines Fragebogens für benutzerzentrierte IT-Sicherheit, der die bislang vernachlässigte Interaktion des Benutzers mit dem System beachtet. Diese Arbeit konzentrierte sich auf die Studie des Verhaltens von Benutzern als Reaktion auf verschiedene virtuelle Bedrohungen im Kontext einer E-Learning-Plattform. Hinck untersuchte die Auswirkungen der Sicherheitsmechanismen auf die Usability in Bezug auf Führungskräfte; seine Arbeiten sind ebenfalls rein analytischer Art.

Im Projekt ATUS wurde das Systemtestverfahren USE (Usability Security Evaluation) entwickelt, um Systeme auf Usable Security hin zu evaluieren und zu inspizieren. Es wurde zudem ein Demonstrator aus dem Bereich des Identity-Managements als Proof-of-Concept entwickelt. Der maßgebliche Beitrag von ATUS blieb aber der mit USE vorgeschlagene benutzerzentrierte Security-Engineering-Prozess.

Auf europäischer Ebene befassten sich Teile der geförderten Forschungsrahmenprogramme FP6 und FP7 mit der Gebrauchstauglichkeit technischer Mechanismen zur Förderung von Security und Privacy. In diesem Zusammenhang sind insbesondere die Projekte PRIME, FIDIS und PrimeLife zu nennen. Die in diesen Projekten erarbeiteten Methoden, Verfahren und Technologien fokussieren wie das ATUS-Projekt auf Systeme zum Identitätsmanagement.

Dieser Schwerpunkt findet sich auch vorwiegend in internationalen Forschungs- und Entwicklungsarbeiten. Insgesamt kann festgehalten werden, dass das Feld Usable Security durch ein verstärktes Interesse aus der Industrie zunehmend an Relevanz gewinnt, dass aber bis dahin noch kein durchgängiger Ansatz zur gebrauchstauglichen Ausgestaltung von Sicherheitsmechanismen in betrieblichen Anwendungssystemen erarbeitet wurde, wie es im USecureD-Projektvorhaben anvisiert wurde.

4.3 Schutzrechte

Da sich USecureD im Grundsatz mit Methoden, Verfahren, Guidelines und Patterns befasste, standen keine Schutzrechte im Raum, die es als Stand der Technik zu berücksichtigen galt. Auch wurde nicht angestrebt, mit den im Projekt entwickelten Ansätzen ausschließlich oder vorrangig bestimmte proprietäre Lösungen zu unterstützen. Vielmehr standen in diesem Kontext Publikationen in Fachorganen im Zentrum. Das Anmelden eigener Schutzrechte war prinzipiell vorgesehen, sofern diese nicht mit den Projektzielen in Konflikt stehen, insbesondere in Hinblick auf die frei zugänglichen Projektergebnisse. Der Konsortialvertrag enthielt Regelungen in Bezug auf das Anmelden von Schutzrechten.

4.4 Verwendete Fachliteratur

Abran, Alain; Khelifi, Adel; Suryn, Witold; Seffah; Ahmed: Usability Meanings and Interpretations in ISO Standards. In: Software Quality Journal 11(4), S. 323-336. Kluwer Academic Publishers, Hingham, MA 2003

Adam, Sebastian; Dörr, Jörg; Eisenbarth, Michael; Groß, Anne: Using Task-oriented Requirements Engineering in Different Domains – Experiences with Application in Research and Industry. In: RE '09 – Proceedings of the 2009 17th IEEE International Requirements Engineering Conference, S. 267–272. IEEE Computer Society, Washington 2009

Adams, Anne & Sasse, Martina Angela: Users are not the enemy. In: Communications of the ACM 42(12), S. 40–46. ACM, New York, NY 1999

Akhawe, Devdatta & Porter Felt, Adrienne: Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In: Proceedings of the 22nd USENIX Security Symposium, S. 257-272. USENIX Association 2013

Alexander, Christopher; Ishikawa, Sara; Silverstein, Murray; Jacobson, Max; Fiksdahl-King, Ingrid; Angel, Shlomo: A Pattern Language: Towns, Buildings, Construction. Oxford University Press, New York 1977

Alexander, Ian F.: A Better Fit - Characterising the Stakeholders. In: CAiSE 2004 Workshops (2), S. 215-223. Riga Technical University, Riga 2004

American Association of Retired Persons: AARP Audience-Centered Heuristics. 2004. Verfügbar unter: http://redish.net/images/stories/PDF/AARP%20Audience-Centered%20Heuristics.pdf [26.06.2017]

Amt für Veröffentlichungen der Europäischen Union: Amtsblatt der Europäischen Union L 119 - Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Verfügbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [26.06.2017]

Anderson, Ross J.: Security Engineering, A Guide to Building Dependable Distributed Systems. John Wiley & Sons, New York 2008

Asaduzzaman, Muhammad; Roy, Chanchal K.; Monir, Samiul; Schneider, Kevin A.: Exploring API Method Parameter Recommendations. In: ICSME '15 Proceedings of the 2015 IEEE International Conference on Software Maintenance and Evolution, S. 271-280. IEEE Computer Society, Washington, DC 2015

Baardseth, Birgitte; Bleier, Thomas; Michaelis, Patrick; Petersohn, Marieke; Robin, Markus; Weinmann, Christoph: System Security Engineering für Manager: Entwicklung sicherer Systeme und sicherer Software. TeleTrusT – Bundesverband IT-Sicherheit e.V., 2015

Bahr, Gisela Susanne & Allen, William H.: Rational Interfaces for Effective Security Software: Polite Interaction Guidelines for Secondary Tasks. In: Universal Access in Human-Computer Interaction: Design Methods, Tools, and Interaction Techniques for eInclusion (UAHCI 2013 Proceedings Part I), S. 165–174. Springer, Berlin 2013

Balfanz, Dirk; Durfee, Glenn; Grinter, Rebecca E.; Smetters, Diana K.: In Search of Usable Security: Five Lessons from the Field. In: IEEE Security & Privacy 2(5). IEEE, 2004

Balzert, Helmut: Lehrbuch der Software-Technik - Software-Management, Software-Qualitätssicherung, Unternehmensmodellierung. Spektrum Akademischer Verlag, Heidelberg 1998

Bauer, Lujo; Bravo-Lillo, Cristian; Cranor, Lorrie; Fragkaki, Elli: Warning Design Guidelines. Technical Report CMU-CyLab-13-002. Carnegie Mellon University, Pittsburgh, PA 2013

Beck, Kent: Smalltalk Best Practice Patterns. Prentice Hall, Upper Saddle River 1996

Belk, Marios; Fidas, Christos; Germanakos, Panagiotis; Samaras, George: On Supporting Security and Privacy-Preserving Interaction through Adaptive Usable Security. In: Proceedings of the Second International Conference on Human Aspects of Information Security, Privacy, and Trust, S. 3-10. Springer New York, NY 2014

Ben-Asher, Noam; Meyer, Joachim; Möller, Sebastian; Englert, Roman: An Experimental System for Studying the Tradeoff between Usability and Security. In: ARES '09 International Conference on Availability, Reliability and Security. IEEE, 2009

Berander, Patrik; Damm, Lars-Ola; Eriksson, Jeanette; Gorschek, Tony; Henningsson, Kennet; Jönsson, Per; Kågström, Simon; Milicic, Drazen; Mårtensson, Frans; Rönkkö, Kari; Tomaszewski, Piotr: Software quality attributes and trade-offs. Blekinge Institute of Technology, 2005

Bernauer, Matthias: Benutzbare Benutzerauthentifizierung - Security and Usability of Passwords. 2006. Verfügbar unter: http://uni.matthias-bernauer.com/~bernauer/usability_of_passwords/usability_of_passwords.html [26.06.2017]

Beschnitt, Martin: Usability-Guidelines: Teil 1 – Definition & Abgrenzung. 2009. Verfügbar unter: http://www.usabilityblog.de/2009/08/usability-guidelines-teil-1-definition-abgrenzung/ [26.06.2017]

Beschnitt, Martin: Usability-Guidelines: Teil 2 – Vor- & Nachteile. 2009. Verfügbar unter: http://www.usabilityblog.de/2009/08/usability-guidelines-teil-2-vor-nachteile/ [26.06.2017]

Beschnitt, Martin: Usability-Guidelines: Teil 3 – Bestehende Guideline-Sets. 2009. Verfügbar unter: http://www.usabilityblog.de/2009/09/usability-guidelines-teil-3-bestehende-guideline-sets/ [26.06.2017]

Bevan, Nigel: Guidelines and Standards for Web Usability. In: Proceedings of HCI International 2005, Lawrence Erlbaum, Hillsdale, NJ 2005

Bilmajer, Laura; Scheid, Christine; Grosser, Julia: Betriebswirtschaftliche Software Enterprise Resource Planning: Effizienzsteigerung durch den Einsatz moderner ERP-Lösungen. eBusiness-Lotse Mainfranken, Würzburg 2015

Birolini, Alessandro: Zuverlässigkeit von Geräten und Systemen. Springer, Berlin 1997

Bitkom e.V.: Bitkom-Mittelstandsbericht 2017. Verfügbar unter: https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Mittelstandsbericht-2017.html [26.06.2017]

Bloch, Joshua: How to Design a Good API and Why It Matters. In: Companion to the 21st ACM SIGPLAN Symposium on Object-Oriented Programming Systems, Languages, and Applications (OOPSLA '06), S. 506-507. ACM, New York, NY 2006

Blythe, Jim; Koppel, Ross; Smith, Sean W.: Circumvention of Security: Good Users Do Bad Things. In: IEEE Security & Privacy 11(5), S. 80–83. IEEE, 2013

Bond, Michael K.: Understanding Security APIs. Dissertation. University of Cambridge, 2004

Bonneau, Joseph; Herley, Cormac; van Oorschot, Paul C.; Stajano, Frank: The quest to replace passwords: a framework for comparative evaluation of Web authentication schemes. Technical report 817, University of Cambridge Computer Laboratory. Cambridge 2012

Booch, Grady; Rumbaugh, James; Jacobson, Ivar: The Unified Modeling Language User Guide. Addison-Wesley, Boston 1999

Borchers, Jan O.: A Pattern Approach to Interaction Design. John Wiley & Sons, Chichester 2001

Boswell, Wendy: App Usability Guidelines from a User Perspective. 2012. Verfügbar unter: https://software.intel.com/en-us/blogs/2012/11/13/app-usability-guidelines-from-a-user-perspective [26.06.2017]

Brandt, Joel; Guo, Philip J.; Lewenstein, Joel; Dontcheva, Mira; Klemmer, Scott R.: Two Studies of Opportunistic Programming: Interleaving Web Foraging, Learning, and Writing Code. In: CHI '09 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, S. 1589-1598. ACM, New York 2009

Bravo-Lillo, Cristian Antonio: Improving Computer Security Dialogs: An Exploration of Attention and Habituation. Dissertation, Carnegie Mellon University, Pittsburgh, PA 2011

Braz, Christina; Seffah, Ahmed; M'Raihi, David: Designing a Trade-Off Between Usability and Security: A Metrics Based-Model. In: INTERACT'07 Proceedings of the 11th IFIP TC 13 international conference on Human-computer interaction (2), S. 114-126. Springer, Berlin 2007

Brubaker, Chad; Jana, Suman; Ray, Baishakhi; Khurshid, Sarfraz; Shmatikov, Vitaly: Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations. In: SP '14 Proceedings of the 2014 IEEE Symposium on Security and Privacy, S. 114-129. IEEE Computer Society, Washington, DC 2014

Bruch, Marcel; Monperrus, Martin; Mezini, Mira: Learning from Examples to Improve Code Completion Systems. In: ESEC/FSE '09 Proceedings of the the 7th joint meeting of the European software engineering conference and the ACM SIGSOFT symposium on The foundations of software engineering, S. 213-222. ACM, New York, NY 2009

Brull, Ruslana: Annotierung von Use Cases mit Usability Patterns. Diplomarbeit, Universität Stuttgart, Stuttgart 2011

Büllingen, Franz & Hillebrand, Annette: IT-Sicherheitsniveau in kleinen und mittleren Unternehmen: Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie. Bundesministerium für Wirtschaft und Technologie (BMWi), Berlin 2012

Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5. Bundesamt für Sicherheit in der Informationstechnik, Bonn 2008

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz – die Basis für Informationssicherheit. 2017. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html [26.06.2017]

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge – G 3 Menschliche Fehlhandlungen. 2016. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g03/g03.html [26.06.2017]

Bundesamt für Sicherheit in der Informationstechnik: IT Security Guidelines: IT-Grundschutz in brief. Bundesamt für Sicherheit in der Informationstechnik, Bonn 2007

Bundesamt für Sicherheit in der Informationstechnik: Leitfaden Informationssicherheit: IT-Grundschutz kompakt. Artikelnummer BSI-Bro12/311. Bundesamt für Sicherheit in der Informationstechnik – BSI, Bonn 2012

Bundesministerium der Justiz und für Verbraucherschutz: Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0). 2011. Verfügbar unter: http://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html [26.06.2017]

Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland 2016. BMI16013, 2016

Bundesministerium des Innern, Abteilung IT: Das V-Modell XT. Verfügbar unter: http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/V-Modell-XT/vmodell_xt_node.html [26.06.2017]

Burmester, Michael; Hassenzahl, Marc; Koller, Franz: Usability ist nicht alles – Wege zu attraktiven Produkten. In: i-com – Zeitschrift für interaktive und kooperative Medien, Ausgabe 1/2002, S. 32–40. Oldenbourg, Berlin 2002

Capgemini; Sogeti; HP: World Quality Report 2015-16, 7. Auflage.

Checkmarx Inc.: Secure Development Kit. 2015. Verfügbar unter: https://www.checkmarx.com/wp-content/uploads/2015/10/Poster.pdf [26.06.2017]

Chen, Eric; Pei, Yutong; Chen, Shuo; Tian, Yuan; Kotcher, Robert; Tague, Patrick: OAuth Demystified for Mobile Application Developers. In: CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, S. 892-903. ACM, New York, NY 2014

Chiasson, Sonia; Biddle, Robert; Somayaji, Anil: Even Experts Deserve Usable Security: Design guidelines for security management systems. In: Symposium on Usable Security and Privacy (SOUPS) Workshop at Usable IT Security Management (USM), S. 1-4. 2007

Ciampa, Mark: Are Password Management Applications Viable? An Analysis of User Training and Reactions. In: Information Systems Education Journal 9(2), S. 4-14. 2011

Cisco Systems Inc.: Cisco 2015 Annual Security Report. Cisco Systems Inc. 2015

Clarke, Steven: How Usable Are Your APIs?. In: Oram, Andy; Wilson, Greg (Hrsg.): Making Software: What Really Works, and Why We Believe It, S. 545–565. O'Reilly, 2010

Cockburn, Alistair: Writing Effective Use Cases. Addison-Wesley, Boston 2000

Common Weakness Enumeration: 2011 CWE/SANS Top 25 Most Dangerous Software Errors. 2011. Verfügbar unter: http://cwe.mitre.org/top25/ [26.06.2017]

Cooper, Alan: The Inmates Are Running The Asylum: Why High-Tech Products Drive Us Crazy and How to Restore the Sanity. Que, 2004

Cranor, Lorrie Faith: A Framework for Reasoning About the Human in the Loop. In: Proceedings of the 1st Conference on Usability, Psychology, and Security 2008, 1. Artikel. USENIX Association Berkeley, CA 2008

Cranor, Lorrie Faith & Garfinkel, Simson: Secure or Usable? In: IEEE Security & Privacy September/October 2004. IEEE, 2004

Cranor, Lorrie Faith & Garfinkel, Simson: Security and Usability: Designing Secure Systems that People Can Use. O'Reilly, Sebastopol 2005

DATEV eG: Unternehmenssoftware. 2017. Verfügbar unter: http://www.datev.de/portal/ShowPage.do?pid=dpi&nid=107145 [26.06.2017]

de Paula, Rogério; Ding, Xianghua; Dourish, Paul; Nies, Kari; Pillet, Ben; Redmiles, David; Ren, Jie; Rode, Jennifer; Silva Filho, Roberto: Two Experiences Designing for Effective Security. In: SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security, S. 25-34. ACM, New York, NY 2005

Deutschland sicher im Netz e.V.: DsiN-Sicherheitsindex 2017. 2017. Verfügbar unter: https://www.sicher-im-netz.de/downloads/dsin-sicherheitsindex-2017-0 [26.06.2017]

DeWitt, Alexander J. & Kuljis, Jasna: Aligning Usability and Security: A Usability Study of Polaris. In: SOUPS '06 Proceedings of the second symposium on Usable privacy and security, S. 1-7. ACM, New York, NY 2006

Dhamija, Rachna; Tygar, J. D.; Hearst, Marti: Why phishing works. In: CHI '06 CHI 2006 Conference on Human Factors in Computing Systems. ACM, New York 2006

Diefenbach, Sarah & Hassenzahl, Marc: Handbuch zur Fun-ni Toolbox: User Experience Evaluation auf drei Ebenen. 2010. Verfügbar unter: http://fun-ni.org/wp-content/uploads/Diefenbach+Hassenzahl_2010_HandbuchFun-niToolbox.pdf [26.06.2017]

Diefenbach, Sarah; Klein, Bernd; Klöckner, Kerstin; Schmitt, Hartmut: Schlussbericht des Vorhabens Fun of Use with Natural Interactions. 2011. Verfügbar unter: http://edok01.tib.uni-hannover.de/edoks/e01fb11/663607957.pdf [26.06.2017]

Dienst, Jonathan & Nious, Kevin: I-Team: Local Airports Vulnerable to Cyberattacks, Experts Warn / NBC New York. Verfügbar unter: http://www.nbcnewyork.com/news/local/hackers-airport-JFK-Newark-LaGuardia-Cyber-security-320674852.html [26.06.2017]

Diercks, Jürgen: Mengenlehre - Crowd Testing: Viele Tester schaffen bessere Software. In: iX 2014(1), S. 112-114. 2014

Dierks, Tim & Rescorla, Eric: The Transport Layer Security (TLS) Protocol Version 1.2. Network Working Group Request for Comments: 5246. Verfügbar unter: https://www.ietf.org/rfc/rfc5246.txt [27.06.2017]

Dillard, Kurt; Maldonado, José; Warrender, Brad: Microsoft Solutions for Security: Windows Server 2003 Security Guide. Microsoft Corporation, 2003

DIN Deutsches Institut für Normung e. V.: Ergonomie der Mensch-System-Interaktion - Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte (ISO/DIS 9241-11.2:2016); Deutsche und Englische Fassung EN ISO 9241-11:2016

DIN Deutsches Institut für Normung e. V.: Ergonomie der Mensch-System-Interaktion - Teil 110: Grundsätze der Dialoggestaltung (ISO 9241-110:2006); Deutsche Fassung EN ISO 9241-110:2006

DIN Deutsches Institut für Normung e. V.: Ergonomie der Mensch-System-Interaktion - Teil 210: Prozess der Gestaltung gebrauchstauglicher interaktiver Systeme (ISO 9241-210:2010); Deutsche Fassung EN ISO 9241-210:2010

DIN Deutsches Institut für Normung e. V.: Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten - Teil 11: Anforderungen an die Gebrauchstauglichkeit; Leitsätze (ISO 9241-11:1998); Deutsche Fassung EN ISO 9241-11:1998

DIN Deutsches Institut für Normung e. V.: Graphische Symbole - Sicherheitsfarben und Sicherheitszeichen - Registrierte Sicherheitszeichen (ISO 7010:2011); Deutsche Fassung EN ISO 7010:2012

DIN Deutsches Institut für Normung e. V.: Graphische Symbole - Sicherheitsfarben und Sicherheitszeichen - Teil 2: Registrierte Sicherheitszeichen (DIN 4844-2:2012-12)

DIN Deutsches Institut für Normung e. V.: Medizinprodukte - Qualitätsmanagementsysteme - Anforderungen für regulatorische Zwecke (ISO 13485:2016); Deutsche Fassung EN ISO 13485:2016

DIN Deutsches Institut für Normung e. V.: Qualitätsmanagementsysteme - Grundlagen und Begriffe (ISO 9000:2005); Dreisprachige Fassung EN ISO 9000:2005

Dörr, Jörg: Guidelines zur Erstellung von Use Cases. 2007. Verfügbar unter: http://www.re-wissen.de/opencms/Wissen/Techniken/Guidelines_zur_Erstellung_von_Use_Cases.html [26.06.2017]

Duala-Ekoko, Ekwa & Robillard, Martin P.: Asking and Answering Questions about Unfamiliar APIs: An Exploratory Study. In: ICSE '12 Proceedings of the 34th International Conference on Software Engineering, S. 266-276. IEEE Press, Piscataway, NJ 2012

Duala-Ekoko, Ekwa & Robillard, Martin P.: Using Structure-Based Recommendations to Facilitate Discoverability in APIs. In: ECOOP'11 Proceedings of the 25th European Conference on Object-Oriented Programming, S. 79-104. Springer, Berlin 2011

e-teaching.org Redaktion: Bestandteile eines Entwurfsmusters. 2015. Verfügbar unter: https://www.e-teaching.org/didaktik/konzeption/entwurfsmuster/beschreibungsformat/index_html [26.06.2017]

Eckert, Claudia: IT-Sicherheit, Konzepte – Verfahren – Protokolle. Oldenbourg Verlag, München 2008

Egele, Manuel; Brumley, David; Fratantonio, Yanick; Kruegel, Christopher: An Empirical Study of Cryptographic Misuse in Android Applications. In: CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, S. 73-84. ACM New York, NY 2013

Egelman, Serge: Trust Me: Design Patterns for Constructing Trustworthy Trust Indicators. Dissertation. Carnegie Mellon University, Pittsburgh, PA 2009

Egelman, Serge; Cranor, Lorrie Faith; Hong, Jason: You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In: CHI '08: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, S. 1065-1074. ACM, New York, NY 2008

Ellis, Brian; Stylos, Jeffrey; Myers, Brad: The Factory Pattern in API Design: A Usability Evaluation. In: ICSE '07 Proceedings of the 29th international conference on Software Engineering, S. 302-312. IEEE Computer Society, Washington, DC 2007

embedded projects GmbH: Warenwirtschaft von Open-Source bis Premium - ERP, CRM und vieles mehr. Verfügbar unter: https://www.wawision.de/ [26.06.2017]

Espinha, Tiago; Zaidman, Andy; Gross, Hans-Gerhard: Web API growing pains: Stories from client developers and their code. In: IEEE Conference on Software Maintenance, Reengineering and Reverse Engineering, Software Evolution Week (CSMR-WCRE ’14). IEEE, 2014

Fahl, Sascha; Harbach, Marian; Muders, Thomas; Baumgärtner, Lars; Freisleben, Bernd; Smith, Matthew: Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security, S. 50–61. ACM New York, NY 2012

Fahl, Sascha; Harbach, Marian; Perl, Henning; Koetter, Markus; Smith, Matthew: Rethinking SSL Development in an Appified World. In: CCS '13 Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM New York, NY 2013

Fernandez, Eduardo B. & Muñoz-Arteaga, Jaime: Extending a Secure Software Methodology with Usability Aspects. In: Proceedings of the Third International Workshop on Software Patterns and Quality (SPAQu’09), S. 48-49. GRACE Center, Tokio 2009

Ferreira, Andrei; Rusu, Cristian; Roncagliolo Silvana: Usability and Security Patterns. In: ACHI '09 Proceedings of the 2009 Second International Conferences on Advances in Computer-Human Interactions, S. 301-305. IEEE Computer Society, Washington, DC 2009

Fetzer, Karin; Heß, Anne; Lange, Kristin; Löffler, Diana; Maier, Andreas; Schmitt, Hartmut; Weber, Sebastian: Schlussbericht des Vorhabens Gestaltung intuitiver Benutzung mit Image Schemata. 2013. Verfügbar unter: http://edok01.tib.uni-hannover.de/edoks/e01fb13/767197879.pdf [26.06.2017]

FIDO Alliance: FIDO Alliance Download Specifications. 2017. Verfügbar unter: https://fidoalliance.org/download/ [26.06.2017]

Fischer-Hübner, Simone; Grimm, Rüdiger; Lo Iacono, Luigi; Möller, Sebastian; Müller, Günter; Volkamer, Melanie: Gebrauchstaugliche Informationssicherheit. In: <kes> Die Zeitschrift für Informations-Sicherheit, Ausgabe 4/2011, S. 6–10. SecuMedia, Ingelheim 2011

Fischer-Hübner, Simone; Lo Iacono, Luigi; Möller, Sebastian: Usable Security and Privacy. In: Datenschutz und Datensicherheit – DuD, Ausgabe 11/2010, S. 773–782. Springer Gabler, Wiesbaden 2010

Flechais, Ivan; Mascolo, Cecilia; Sasse, M. Angela: Integrating Security and Usability into the Requirements and Design Process. In: International Journal of Electronic Security and Digital Forensics 1(1), S. 12-26. Inderscience Publishers, Genf 2007

Fogg, B.J.: Persuasive Technology: Using Computers to Change What We Think and Do. Morgan Kaufman, San Francisco, CA 2003

Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO: FutureID. 2017. Verfügbar unter: http://www.futureid.eu/index.php [27.06.2017]

Fraunhofer-Institut für Experimentelles Software Engineering IESE: Experimentelles und exploratives Prototyping durchführen. 2015. Verfügbar unter: http://www.pq4agile.de/PQ4WP/wp-content/uploads/2015/02/PQ4Agile-AP-2.2-Experimentelles-und-exploratives-Prototyping-durchf%C3%BChren-V.11.pdf [26.06.2017]

Fraunhofer-Institut für Experimentelles Software Engineering IESE: Severity Rating durchführen. 2015. Verfügbar unter: http://www.pq4agile.de/PQ4WP/wp-content/uploads/2015/02/PQ4Agile-AP-2.2-Severity-Rating-durchf%C3%BChren-V.11.pdf [26.06.2017]

Freier, Alan O.; Karlton, Philip; Kocher, Paul C.: The Secure Sockets Layer (SSL) Protocol Version 3.0. Request for Comments: 6101. 2011. Verfügbar unter: https://tools.ietf.org/html/rfc6101 [27.06.2017]

Furnell, Steven M.; Jusoh, Adila; Katsabas, Dimitris: The challenges of understanding and using security: A survey of end-users. Computers & Security 25(1), S. 27-35. Elsevier, Oxford 2006

Furnell, Steven; Katsabas, Dimitris; Dowland, Paul; Reid, Fraser: A Practical Usability Evaluation of Security Features in End-User Applications. In: New Approaches for Security, Privacy and Trust in Complex Environments: Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007), S. 205–216. Springer US, New York 2007

Gamma, Erich; Helm, Richard; Johnson, Ralph; Vlissides, John: Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley, Boston 1995

Garfinkel, Simson L.: Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable. Dissertation, Massachusetts Institute of Technology, Cambridge 2005

Garfinkel, Simson & Richter Lipford, Heather: Usable Security: History, Themes, and Challenges. Morgan & Claypool, 2014

Garfinkel, Simson L., Margrave, David; Schiller, Jeffrey I.; Nordlander, Erik; Miller, Robert C.: How to Make Secure Email Easier To Use. In: CHI 2005: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, S. 701-710. ACM, New York 2005

Garst, Martin; Klein, Rudolf; Klöckner, Kerstin; Schmitt; Hartmut: Schlussbericht FUN – (F)UN of (U)se für Geschäftsa(N)wendungen. 2009. Verfügbar unter: http://edok01.tib.uni-hannover.de/edoks/e01fb09/611335816.pdf [26.06.2017]

Gentner, Dedre & Stevens, Albert L.: Mental Models. Lawrence Erlenbaum Associates, Hillsdale, NJ 1983

Georgiev, Martin; Iyengar, Subodh; Jana, Suman; Anubhai, Rishita; Boneh, Dan; Shmatikov, Vitaly: The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software. In: CCS '12 Proceedings of the 2012 ACM Conference on Computer and Communications Security. ACM, New York, NY 2012

Gerd tom Markotten, Daniela: Benutzbare Sicherheit in informationstechnischen Systemen. Rhombos, Berlin 2004

Gerd Tom Markotten, Daniela: User-Centered Security Engineering. In: Proceedings of the 4th Nord EurOpen/Usenix Conference (NordU 2002). 2002

German UPA e.V., Arbeitskreis Qualitätsstandards: German UPA Qualitätsstandard für Usability Engineering. 2012. Verfügbar unter: http://germanupa.de/data/mediapool/n070_qualitaetsstandard_der_german_upa.pdf [26.06.2017]

Gesellschaft für Informatik e.V., Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“: Social Media Leitlinie. 2016

Google Inc.: Best Practices for Security & Privacy: Android Developers. 2017. Verfügbar unter: https://developer.android.com/training/best-security.html [27.06.2017]

Government Communications Headquarters; Centre for the Protection of National Infrastructure: Password Guidance: Simplifying Your Approach. 2015. Verfügbar unter: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf [26.06.2017]

Grabski, Bastian & Krüger, Lars: Analysen zu Qualität und Qualitätsmanagement von Software und Dienstleistungen. Technical report (Internet). 2009. Verfügbar unter: http://www.inf.ovgu.de/inf_media/downloads/forschung/technical_reports_und_preprints/2009/2009_internet/TechReport15.pdf [26.06.2017]

Grady, Robert B. & Caswell, Deborah L.: Software Metrics: Establishing a Company-Wide Program. Prentice Hall, Englewood Cliffs 1987

Green, Matthew & Smith, Matthew: Developers are Not the Enemy!: The Need for Usable Security APIs. IEEE Security & Privacy 14(5), S. 40–46. IEEE Educational Activities Department, Piscataway, NJ 2016

Green, Matthew & Smith, Matthew: Developers Are Users Too: Designing Crypto and Security APIs That Busy Engineers and Sysadmins Can Use Securely. Verfügbar unter https://www.usenix.org/conference/hotsec15/summit-program/presentation/green [27.06.2017]

Gronau, Norbert: Enterprise Resource Planning: Architektur, Funktionen und Management von ERP-Systemen, 2. Auflage. Oldenbourg Verlag, München 2010

Gruschka, Nils & Lo Iacono, Luigi: Password Visualization Beyond Password Masking. In: Proceedings of the Eighth International Network Conference (INC 2010), S. 179–188. University of Plymouth, Plymouth 2010

Gruschka, Nils; Jensen, Meiko; Lo Iacono, Luigi: A Design Pattern for Event-Based Processing of Security-enriched SOAP Messages. In: ARES 2010 – Fifth International Conference on Availability, Reliability, and Security, S. 410–415. IEEE Computer Society, Washington 2010

Hafiz, Munawar & Adamczyk, Paul: The Nature of Order: From Security Patterns to a Pattern Language. In: SPLASH'12 Proceedings of the 3rd annual conference on Systems, programming, and applications: software for humanity, S. 75–76. ACM, New York 2012

Hafiz, Munawar, Adamczyk, Paul; Johnson, Ralph E.: Towards an Organization of Security Patterns. In: IEEE Software 24 (4), S. 52–60. IEEE Computer Society Press, Los Alamitos 2007

Hafiz, Munawar, Adamczyk, Paul; Johnson, Ralph: Growing a Pattern Language (for Security). In: Onward! 2012 Proceedings of the ACM international symposium on New ideas, new paradigms, and reflections on programming and software, S. 139–158. ACM, New York 2011

Hammer, Volker & Schuler, Karin: Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Version 1.0.2. Secorvo Security Consulting GmbH, Karlsruhe 2013

Hardee, Jefferson B.; West, Ryan; Mayhorn, Christopher B.: To Download or Not to Download: An Examination of Computer Security Decision Making. interactions - A contradiction in terms? 13(3), S. 32–37. ACM, New York, NY 2006

Hardt, Dick: The OAuth 2.0 Authorization Framework. Request for Comments: 6749. 2012. Verfügbar unter: https://tools.ietf.org/html/rfc6749 [27.06.2017]

Hassenzahl, Marc: The Thing and I: Understanding the Relationship Between User and Product. In: Funology: From Usability to Enjoyment, S. 31-42. Kluwer Academic Publishers, Dordrecht 2004

Hassenzahl, Marc; Burmester, Michael; Koller, Franz: AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität. In: Mensch & Computer 2003: Interaktion in Bewegung, S. 187–196. B.G. Teubner, Stuttgart 2003

Hassenzahl, Marc; Diefenbach, Sarah; Göritz, Anja: Needs, affect, and interactive products – Facets of user experience. In: Interacting with Computers 22(5), S. 353–362. Elsevier 2010

Herzog, Almut: Usable Security Policies for Runtime Environments. Dissertation, Linköpings universitet. Linköping 2007

Herzog, Almut & Shahmehri, Nahid: Usable Set-up of Runtime Security Policies. Information Management & Computer Security 15(5), S. 394-407. Emerald Group 2007

Herzwurm, Georg & Mikusz, Martin: Qualitätsmerkmale von Software. 2016. Verfügbar unter: http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/is-management/Systementwicklung/Management-der-Systementwicklung/Software-Qualitatsmanagement/Qualitatsmerkmale-von-Software/index.html [26.06.2017]

Hesseler, Martin & Görtz, Marcus: ERP-Systeme im Einsatz: Bearbeitung typischer Geschäftsvorfälle mit Microsoft Dynamics NAV 5.0. W3L, Dortmund 2009

Hinck, Thorsten: Business-Intelligence-Systeme im Spannungsfeld zwischen Usability und Sicherheit. Dissertation, Eberhard Karls Universität Tübingen, Tübingen 2010

Hirsch, Tobias; Lo Iacono, Luigi; Wechsung, Ina: How much Network Security must be Visible in Web Browsers? In: Trust, Privacy and Security in Digital Business – Proceedings of 9th International Conference TrustBus 2012, S. 1–16. Springer, Heidelberg 2012

Hochschule für Technik und Wirtschaft Chur: Usabilitymethoden. 2013. Verfügbar unter: http://www.cheval-lab.ch/was-ist-usability/usabilitymethoden/#c299 [26.06.2017]

Hochschule Ostwestfalen-Lippe: Informations- und Managementsysteme. Verfügbar unter: http://www.hs-owl.de/fb8/fachgebiete/umweltinformationssysteme/informations-und-managementsysteme.html [26.06.2017]

Hodges, Jeff & Jackson, Collin: HTTP Strict Transport Security (HSTS). Request for Comments: 6797. 2012. Verfügbar unter: https://tools.ietf.org/html/rfc6797 [27.06.2017]

Hof, Hans-Joachim: User-Centric IT Security: How to Design Usable Security Mechanisms. In: CENTRIC 2012 - The Fifth International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, S. 7-12. IARIA 2012

Howard, Michael: Attack Surface: Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users. In: MSDN Magazine November 2004. Verfügbar unter: https://msdn.microsoft.com/magazine/ee310108 [28.06.2017]

Howe, Adele E.; Ray, Indrajit; Roberts, Mark; Urbanska, Malgorzata; Byrne, Zinta: The Psychology of Security for the Home Computer User. In: SP '12 Proceedings of the 2012 IEEE Symposium on Security and Privacy, S. 209–223. IEEE Computer Society, Washington, DC 2012

Hurtienne, Jörn: Image schemas and design for intuitive use. Exploring new guidance for user interface design. Dissertation, Technische Universität Berlin, Berlin 2011

Industrial Control Systems Cyber Emergency Response Team: Morpho Itemiser 3 Hard-Coded Credential ICS-CERT. 2014. Verfügbar unter: https://ics-cert.us-cert.gov/advisories/ICSA-14-205-01 [26.06.2017]

Institut für Mittelstandsforschung Bonn: IfM Bonn: Mittelstand im Überblick. 2017. Verfügbar unter: http://www.ifm-bonn.org/statistiken/mittelstand-im-ueberblick/ [26.06.2017]

International Organization for Standardization: Information processing systems; Open Systems Interconnection; basis reference model; Part 2: Security architecture (ISO 7498-2:1989-02)

International Organization for Standardization: Information technology - Software product evaluation - Quality characteristics and guidelines for their use (ISO/IEC 9126:1991-12)

International Organization for Standardization: Software engineering – Product quality – Part 1: Quality model (ISO/IEC 9126-1:2001-06)

International Organization for Standardization: Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models (ISO/IEC 25010:2011-03)

International Organization for Standardization; IEC – International Electrotechnical Commission: Software-Engineering - Qualitätskriterien und Bewertung von Softwareprodukten (SQuaRE) - Qualitätsmodell und Leitlinien. 2011

Jacobson, Ivar; Christerson, Magnus; Jonsson, Patrik; Övergaard, Gunnar: Object Oriented Software Engineering: A Use Case Driven Approach. Addison-Wesley, Boston 1992

Jaferian, Pooya: Heuristics for Evaluating IT Security Management Tools. In: Symposium on Usable Privacy and Security (SOUPS) 2011, July 20-22. Pittsburgh 2011

Johnson, Maritza L.: Toward Usable Access Control for End-users: A Case Study of Facebook Privacy Settings. Columbia University, 2012

Johnston, J.; Eloff, Jan; Labuschagne, Les: Security and Human Computer Interfaces. In: Computers and Security 22 (8), S. 675–684. Elsevier Advanced Technology Publications, Oxford 2003

Jøsang, Audun; AlFayyadh, Bander; Grandison, Tyrone; AlZomai, Mohammed; McNamara, Judith: Security Usability Principles for Vulnerability Analysis and Risk Assessment. In: ACSAC '07 Proceedings of the 23rd Annual Computer Security Applications Conference. IEEE, 2008

Just, Mike: Designing Authentication Systems With Challenge Questions. In: Cranor, Lorrie Faith & Garfinkel, Simson (Hrsg.): Security and Usability: Designing Secure Systems that People Can Use, S. 143-155. O'Reilly, Sebastopol 2005

Kainda, Ronald; Flechais, Ivan; Roscoe, A.W.: Security and Usability: Analysis and Evaluation. Oxford University Computing Laboratory, Oxford 2010

Kalmar, Ralf: Virtuelles Software Engineering Kompetenzzentrum: Interne und externe Qualität. 2017. Verfügbar unter: http://www.software-kompetenz.de/?15572 [26.06.2017]

Kapadia, Apu: A Case (Study) For Usability in Secure Email Communication. In: IEEE Security & Privacy 5(2). IEEE Educational Activities Department, Piscataway, NJ 2007

Katsabas, Dimitris; Furnell, Steven M.; Dowland, Paul S.: Using Human Computer Interaction principles to promote usable security. In: Proceedings of The Fifth International Network Conference 2005, S. 235-242. University of the Aegean / University of Plymouth 2005

Kern, Christoph: Preventing Security Bugs through Software Design. Verfügbar unter https://www.usenix.org/node/190806 [27.06.2017]

Kindermann TCV: 101 Geschäftsvorfälle abgebildet in Microsoft Dynamics: Dynamics NAV 5.0 und 2009 Classic Client. TEIA Internet Akademie und Lehrbuch Verlag, Berlin 2010

Kirovski, Darko; Drinic, Milenko; Potkonjak, Miodrag: Enabling Trusted Software Integrity. In: ASPLOS X Proceedings of the 10th International Conference on Architectural Support for Programming Languages and Operating Systems, S. 108-120. ACM, New York, NY 2002

Klees, Maria: Praxishandbuch IT- und Informationssicherheit. E-Commere-Center Handel, Köln 2011

Klöckner; Kerstin & Kohler; Kirstin: Softwareentwickler als Interaktionsgestalter: Erfahrungen zu Einsatz und Verwendung von Interaktionspattern. In: Usability Professionals 08: Wissen. Können. Tun., S. 83–87. Oldenbourg, München 2008

Komanduri, Saranga; Shay, Richard; Gage Kelley, Patrick; Mazurek, Michelle L.; Bauer, Lujo; Christin, Nicolas; Cranor, Lorrie Faith; Egelman, Serge: Of Passwords and People: Measuring the Effect of Password-Composition Policies. In: CHI 2011 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, S. 2595–2604. ACM, New York, NY 2011

Kommission der Europäischen Gemeinschaften: Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, Aktenzeichen K(2003) 1422, Amtsblatt der Europäischen Union. 2003. Verfügbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=EN [26.06.2017]

Koukouletsos, Kostas; Khazaei, Babak; Dearden, Andy; Ozcan, Mehmet: Teaching Usability Principles with Patterns and Guidelines. In: Kotzé, Paula; Wong, William; Jorge, Joaquim; Dix, Alan; Silva, Paula Alexandra (Hrsg.): Creativity and HCI: From Experience to Design in Education, S. 159-174, Springer US 2009

Kranch, Michael & Bonneau, Joseph: Upgrading HTTPS in Mid-Air: An Empirical Study of Strict Transport Security and Key Pinning. 2015 Network and Distributed System Security (NDSS). Internet Society, 2015

Krohne, Heinz Walter; Egloff, Boris; Kohlmann, Carl-Walter; Tausch, Anja: Untersuchungen mit einer deutschen Version der "Positive and Negative Affect Schedule" (PANAS). Diagnostica 42 (2), S. 139-156. Hogrefe, Göttingen 1996

Kroll-Peters, Olaf: Evaluationsmethoden für benutzerzentrierte IT-Sicherheit. Dissertation, Technische Universität Berlin, Berlin 2010

Laubheimer, Page: Preventing User Errors: Avoiding Unconscious Slips. 2015. Verfügbar unter: https://www.nngroup.com/articles/slips/ [26.06.2017]

Levin, Timothy E.; Irvine, Cynthia E.; Benzel, Terry V.; Bhaskara, Ganesha; Clark, Paul C.; Nguyen, Thuy D.: Design Principles and Guidelines for Security. SecureCore Technical Report. 2007. Verfügbar unter: ftp://ftp.isi.edu/isi-pubs/tr-648.pdf [26.06.2017]

Li, Qing & Clark, Greg: Mobile Security: A Look Ahead. In: IEEE Security & Privacy 11(1), S. 78-81. IEEE 2013

Li, Wanpeng & Mitchell, Chris J.: Security Issues in OAuth 2.0 SSO Implementations. In: Information Security: 17th International Conference, ISC 2014, Proceedings, S. 529-541. Springer, 2014

Lo Iacono, Luigi; Kauer, Michaela; Volkamer, Melanie: Gebrauchstaugliche Nutzerauthentifizierung. In: digma, Zeitschrift für Datenrecht und Informationssicherheit, Ausgabe 4/2011,

S. 172–175. Schulthess Juristische Medien, Zürich 2011

Lo Iacono, Luigi; Viet Nguyen, Hoai; Hirsch, Tobias; Baiers, Maurice; Möller, Sebastian: UI-Dressing to detect Phishing. Accepted Paper: 6th International Symposium on Cyberspace Safety and Security 2014

Lynch, Patrick J. & Horton, Sarah: Contents Web Style Guide 3. 2009. Verfügbar unter: http://webstyle-guide.com/wsg3/ [26.06.2017]

Maier, Andreas; Schmitt, Hartmut; Rost, Dominik: PQ4Agile-Qualitätsmodell. 2014. Verfügbar unter: http://www.pq4agile.de/PQ4WP/wp-content/uploads/2014/06/PQ4Agile-AP-1.2-Qualit%C3%A4tsmodell-V.2.pdf [26.06.2017]

Mangold, Thomas: Warum du unbedingt mit Checklisten arbeiten solltest. 2013. Verfügbar unter: http://selbst-management.biz/warum-du-unbedingt-mit-checklisten-arbeiten-solltest/ [26.06.2017]

Mayhew, Deborah J.: Principles and Guidelines in Software User Interface Design. Prentice Hall, Englewood Cliffs, NJ 1992

McCall, Jim A.; Richards, Paul K.; Walters, Gene F.: Factors in Software Quality. US Rome Air Development Center Reports I-III. U.S. Department of Commerce, Washington 1977

McLellan, Samuel G., Roesler, Alvin W.; Tempest, Joseph T.; Spinuzzi, Clay I.: Building More Usable APIs. In: IEEE Software 15(3), S. 78–86. IEEE Computer Society Press, Los Alamitos, CA 1998

Mendoza González, Ricardo; Muñoz-Arteaga, Jaime; Vargas Martin, Miguel; Álvarez-Rodriguez, Francisco; González Calleros, Juan: A Pattern Methodology to Specify Usable Security in Websites. In: Twentieth International Workshop on Database and Expert Systems Applications, S. 155–159. IEEE Computer Society, Washington 2009

MFG Medien- und Filmgesellschaft Baden-Württemberg mbH: Online-Befragung zum Thema User Experience. 2014. Verfügbar unter: https://innovation.mfg.de/de/standort/kreativwirtschaft/kommunikation-marketing/online-befragung-zum-thema-user-experience-1.25155 [26.06.2017]

Microsoft Corporation: Error and Informational Message Guidelines. 2010. Verfügbar unter: https://msdn.microsoft.com/en-us/library/bb158646.aspx [26.06.2017]

Microsoft Corporation: Pakete und Funktionalitäten in Microsoft Dynamics NAV 2013. Microsoft Deutschland, Unterschleißheim 2013

Microsoft Corporation: Privacy Guidelines for Developing Software Products and Services, Version 3.1. 2008

Microsoft Corporation: Produkt-und Funktionsüberblick für Microsoft Dynamics NAV 2015. Verfügbar unter: http://download.microsoft.com/download/E/6/2/E626FB36-36B9-4A73-9268-C133F0B4C672/Microsoft_Dynamics_NAV_2015_Produkt-und_Funktions%C3%BCberblick_DE_Feb2015.pdf [26.06.2017]

Microsoft Corporation: User Interface Text Guidelines. Verfügbar unter: https://msdn.microsoft.com/en-us/library/bb158574.aspx [26.06.2017]

Mooty, Mathew; Faulring, Andrew; Stylos, Jeffrey; Myers, Brad A.: Calcite: Completing Code Completion for Constructors Using Crowds. In: VLHCC '10 Proceedings of the 2010 IEEE Symposium on Visual Languages and Human-Centric Computing, S. 15-22. IEEE Computer Society, Washington, DC 2010

Müller, Günter & Wohlgemuth, Sven: Sichere IT-Systeme. In: INFORMATIK 2003 Innovative Informatikanwendungen, Band 1, S. 87–90. Köllen, Frankfurt am Main 2003

Muñoz-Arteaga, Jaime; Mendoza González, Ricardo; Vargas Martin, Miguel; Vanderdonckt, Jean; Álvarez-Rodriguez, Francisco; González Calleros, Juan: A Method to Design Information Security Feedback Using Patterns and HCI-Security Criteria. In: Lopez Jaquero, Victor; Montero Simarro, Francisco Molina; Masso, Jose Pascual; Vanderdonckt, Jean (Hrsg.): Computer-Aided Design of User Interfaces VI, S. 283–94. Springer, London 2009

myfactory International: manual.ERP: ERP-Basishandbuch. 2009. Verfügbar unter: http://www.myfactory.com/inside/CustomUpload/374O357O340O370O356O369O350O364O376O357O352O354O371O366O369O376O326O364O353O327O/Handbuch_ERP_1.pdf [26.06.2017]

National Research Council of the National Academies: Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop. National Academies Press, Washington, D.C. 2010

Nazario, Jose: Defense and Detection Strategies against Internet Worms. Artech House, Boston, MA 2004

Nielsen, Jakob: 10 Usability Heuristics for User Interface Design. 1995. Verfügbar unter: https://www.nngroup.com/articles/ten-usability-heuristics/ [26.06.2017]

Nielsen, Jakob: Error Message Guidelines. 2001. Verfügbar unter: https://www.nngroup.com/articles/error-message-guidelines/ [26.06.2017]

Nielsen, Jakob: How to Conduct a Heuristic Evaluation. 1995. Verfügbar unter: https://www.nngroup.com/articles/how-to-conduct-a-heuristic-evaluation/ [26.06.2017]

Nielsen, Jakob: Severity Ratings for Usability Problems. 1995. Verfügbar unter: https://www.nngroup.com/articles/how-to-rate-the-severity-of-usability-problems/ [26.06.2017]

Nielsen, Jakob: Sixty Guidelines From 1986 Revisited. Verfügbar unter: https://www.nngroup.com/articles/sixty-guidelines-from-1986-revisited/ [26.06.2017]

Nielsen, Jakob: Usability Engineering. Morgan Kaufmann, Burlington 1994

Nielsen, Jakob: Usability Inspection Methods. John Wiley & Sons, New York, NY 1994

Nielsen, Jakob & Tahir, Marie: Homepage Usability: 50 Websites Deconstructed. New Riders Publishing, Thousand Oaks, CA 2001

Nodder, Chris: Users and Trust: A Microsoft Case Study. In: Cranor, Lorrie Faith & Garfinkel, Simson (Hrsg.): Security and Usability: Designing Secure Systems that People Can Use, S. 589–606. O'Reilly, Sebastopol 2005

Norman, Donald A.: Design Rules Based on Analyses of Human Error. Communications of the ACM 26(4), S. 254–258. ACM, New York, NY 1983

Norman, Don: Privacy and car navigational systems. 1997. Verfügbar unter: https://catless.ncl.ac.uk/Risks/19/20#subj3 [28.06.2017]

Norman, Donald A.: The Way I See It: When security gets in the way. interactions 16(6), S. 60-63. ACM, New York, NY 2009

Norman, Donald A. & Draper, Steven W.: User Centered System Design: New Perspectives on Human-computer Interaction. CRC Press, Boca Raton 1986

Nurse, Jason R. C.; Creese, Sadie; Goldsmith, Michael; Lamberts, Koen: Guidelines for Usable Cybersecurity: Past and Present. In: 2011 Third International Workshop on Cyberspace Safety and Security (CSS), S. 21-26. IEEE 2011

Nymi Inc.: Nymi: Always On Authentication. 2017. Verfügbar unter: https://www.nymi.com/ [26.06.2017]

Ochs, Carsten: Emerging Trends in Software Development & Implications for IT Security: An Explorative Study. 2014. Verfügbar unter: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/SoftwareDevelopment-Fraunhofer_SIT.pdf [26.06.2017]

Omar, Cyrus; Yoon, YoungSeok; LaToza, Thomas D.; Myers, Brad A.: Active code completion. In: ICSE '12 Proceedings of the 34th International Conference on Software Engineering, S. 859-869. IEEE Press, Piscataway, NJ 2012

Oracle Corporation: Oracle E-Business Suite. 2017. Verfügbar unter: http://www.oracle.com/us/products/applications/ebusiness/overview/index.html [26.06.2017]

Organisation for Economic Co-operation and Development: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 2013. Verfügbar unter: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [28.06.2017]

OWASP Foundation: OWASP. Verfügbar unter: http://www.owasp.org [26.06.2017]

OWASP Foundation: OWASP Secure Coding Practices: Quick Reference Guide. Verfügbar unter: https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf [26.06.2017]

OWASP Foundation: OWASP Top 10 - 2013 - The Top Ten Most Critical Web Application Security Risks. Verfügbar unter: https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf [27.06.2017]

Pandhi, Dax: How to Create the Best User Experience for Your Application. 2006. Verfügbar unter: https://msdn.microsoft.com/en-us/library/aa468595.aspx [26.06.2017]

Patrick, Andrew S.; Briggs, Pamela; Marsh, Stephen: Designing systems that people will trust. In: Cranor, Lorrie Faith & Garfinkel, Simson (Hrsg.): Security and Usability: Designing Secure Systems That People Can Use, S. 75–99, O'Reilly, Sebastopol, CA 2005

Patrick, Andrew S.; Long, A. Chris; Flinn, Scott: HCI and Security Systems. In: CHI '03 Extended Abstracts on Human Factors in Computing Systems, S. 1056-1057. ACM, New York, NY 2003

Payne, Bryan D. & Edwards, W. Keith: A Brief Introduction to Usable Security. In: IEEE Internet Computing 12(3), S. 13-21. IEEE Educational Activities Department, Piscataway, NJ 2008

Pernice, Kara & Nielsen, Jakob: Usability Guidelines for Accessible Web Design. 2015. Verfügbar unter: https://www.nngroup.com/reports/usability-guidelines-accessible-web-design/ [26.06.2017]

Perzel, Kimberly & Kane, David: Usability Patterns for Applications on the World Wide Web. Sixth Conference on Pattern Languages of Programs (PLoP 1999), 1999

Piccioni, Marco; Furia, Carlo A.; Meyer, Bertrand: An Empirical Study of API Usability. In: 2013 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement. IEEE 2013

Pohl, Hartmut: Taxonomie und Modellbildung in der Informationssicherheit. In: Datenschutz und Datensicherheit - DuD 28(11), S. 678-685. 2004

Porter Felt, Adrienne; Ainslie, Alex; Reeder, Robert W.; Consolvo, Sunny; Thyagaraja, Somas; Bettes, Alan; Harris, Helen; Grimes, Jeff: Improving SSL Warnings: Comprehension and Adherence. In: CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, S. 2893–2902. ACM New York, NY 2015

Portland Pattern Repository's Wiki: Principle of Least Astonishment. 2014. Verfügbar unter: http://wiki.c2.com/?PrincipleOfLeastAstonishment [28.06.2017]

PQ4Agile-Konsortium: PQ4Agile – Produktqualität für Agile Softwareentwicklung. Verfügbar unter: http://www.pq4agile.de [26.06.2017]

proALPHA Software: Infocenter proALPHA ERP. 2017. Verfügbar unter: https://www.proalpha.com/de/infocenter/ [26.06.2017]

Quinn, Stephen D.; Souppaya, Murugiah; Cook, Melanie; Scarfone, Karen: National Checklist Program for IT Products – Guidelines for Checklist Users and Developers. NIST Special Publication 800-70 Revision 3. National Institute of Standards and Technology, Gaithersburg, MD 2015

Reid, Brian: Reflections on Some Recent Widespread Computer Break-Ins. In: Denning, Peter J. (Hrsg.): Computers Under Attack: Intruders, Worms, and Viruses. ACM, New York, NY 1990

Richter, Michael & Flückiger, Markus D.: Usability Engineering kompakt – Benutzbare Software gezielt entwickeln. Erweiterte zweite Auflage, Spektrum Akademischer Verlag, Heidelberg 2010

Riethmüller, Christian E.: Was „moderne“ ERP-Systeme funktional bieten sollten. In: software markt, Ausgabe September 2012. Trovarit, Aachen 2012

Robillard, Martin P.: What Makes APIs Hard to Learn? Answers from Developers. In: IEEE Software 26 (6), S. 27–34. IEEE Computer Society Press, Los Alamitos, CA 2009

Röder, Holger: A pattern approach to specifying usability features in use cases. In: Proceedings of the 2nd International Workshop on Pattern-Driven Engineering of Interactive Computing Systems, S. 12–15. ACM, New York 2011

Röder, Holger: Usability Patterns. 2012. Verfügbar unter: http://www.usabilitypatterns.info/catalog/catalog.html [26.06.2017]

Röder, Holger: Usability Patterns – Eine Technik zur Spezifikation funktionaler Usability-Merkmale. Cuvillier, Göttingen 2012

Ross, Ron, Carrier Oren, Janet; McEvilley, Michael: Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems (NIST Special Publication 800-160 - Initial Public Draft). 2014. Verfügbar unter: http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf [26.06.2017]

Rost, Martin & Bock, Kirsten: Privacy By Design und die Neuen Schutzziele: Grundsätze, Ziele und Anforderungen. In: Datenschutz und Datensicherheit - DuD 35(1), S. 30-35. Vieweg 2011

Royer, Denis & Deuker, André: Future of IDentity in the Information Society. Verfügbar unter: http://www.fidis.net [26.06.2017]

Rudolph, Manuel & Schwarz, Reinhard: A Critical Survey of Security Indicator Approaches. In: ARES '12 Proceedings of the 2012 Seventh International Conference on Availability, Reliability and Security, S. 291-300. IEEE Computer Society, Washington, DC 2012

SAFECode - Software Assurance Forum for Excellence in Code: Fundamental Practices for Secure Software Development. 2. Auflage, 2011. Verfügbar unter: http://www.safecode.org/publication/SAFECode_Dev_Practices0211.pdf [26.06.2017]

Sage Software: Sage 100 - die ERP-Software für mittlere Unternehmen. 2017. Verfügbar unter: http://www.sage.de/software/sage-100-erp-software [26.06.2017]

Sage Software: Sage Software Onlinehilfen. Verfügbar unter: http://onlinehilfe.sage.de/onlinehilfe/ [26.06.2017]

Sage Software: Unternehmen Zukunft: Praxisleitfaden ERP. Sage Software, Frankfurt am Main 2011

Sahar, Farrukh: Tradeoffs between Usability and Security. In: ACSIT International Journal of Engineering and Technology 5(4), S. 434-437. 2013

Sakimura, Nat; Bradley, John; Jones, Michael B.; de Medeiros, Breno; Mortimore, Chuck: OpenID Connect Core 1.0 incorporating errata set 1. Verfügbar unter: http://openid.net/specs/openid-connect-core-1_0.html [27.06.2017]

Salm, Uwe & Norbert, Falk: ERP-Lösungen auf Basis Freier Software für kleine und mittlere Unternehmen und Handwerksbetriebe. Teil 1: Marktübersicht und Testberichte Lx-Office und openERP. Regionalcentrum für Electronic Commerce Anwendungen, Osnabrück 2010

Saltzer, Jerome H.: Topics in the Engineering of Computer Systems. 1997

Saltzer, Jerome H. & Schroeder, Michael D.: The Protection of Information in Computer Systems. In: Fourth ACM Symposium on Operating System Principles. 1974

SAP Deutschland SE & Co. KG: SAP Business One: Die Unternehmenssoftware für kleine und mittelständische Unternehmen - Lösungsüberblick. SAP Deutschland, Walldorf 2012

SAP SE: SAP Help Portal. 2017. Verfügbar unter: https://help.sap.com/viewer/product/SAP_BUSINESS_ONE_PRODUCT_LINE/Overview/en-US [26.06.2017]

Sarodnick, Florian & Brau, Henning: Methoden der Usability Evaluation: Wissenschaftliche Grundlagen und praktische Anwendung. 2. Auflage. Huber, Bern 2011

Sasse, M. Angela: “Technology Should Be Smarter Than This!”: A Vision for Overcoming the Great Authentication Fatigue. In: Secure Data Management, S. 33–36. Springer 2013

Sasse, Martina A. & Flechais, Ivan: Usable Security – Why do we need it? How do we get it? In: Cranor, Lorrie Faith & Garfinkel, Simson (Hrsg.): Security and Usability: Designing secure systems that people can use, S. 13–30. O'Reilly, Sebastopol 2005

Sasse, Martina Angela; Brostoff, Sacha; Weirich, Dirk: Transforming the “Weakest Link”: A Human-Computer Interaction Approach for Usable and Effective Security. In: BT Technology Journal 19(3), S. 122-131. Kluwer Academic Publishers, Hingham, MA 2001

Sasse, M. Angela; Smith, Matthew; Herley, Cormac; Lipford, Heather; Vaniea, Kami: Debunking Security-Usability Tradeoff Myths. In: IEEE Security & Privacy 14 (5), S. 33–39. IEEE Educational Activities Department, Piscataway, NJ 2016

Schaar, Peter: Privacy by Design. In: Identity in the Information Society 3(2), S. 267-274. 2010

Scheller, Thomas & Kühn, Eva: Influence of Code Completion Methods on the Usability of APIs. In: Proceedings of the IASTED International Conference Software Engineering (SE 2013), S. 760-767. 2013

Scheller, Thomas & Kühn, Eva: Influencing Factors on the Usability of API Classes and Methods. In: ECBS '12 Proceedings of the 2012 IEEE 19th International Conference and Workshops on Engineering of Computer-Based Systems, S. 232-241. IEEE Computer Society, Washington, DC 2012

Scheller, Thomas & Kühn, Eva: Usability Evaluation of Configuration-Based API Design Concepts. In: 1st International Conference on Human Factors in Computing & Informatics (SouthCHI 2013), S. 54-73. Springer, 2013

Schmitt, Hartmut: Checklisten verwenden. 2015 Verfügbar unter: http://www.pq4agile.de/PQ4WP/wp-content/uploads/2015/02/PQ4Agile-AP-2.2-Checklisten-verwenden-V.2.pdf [26.06.2017]

Schmitt, Hartmut & Heß, Anne: Ergebnisbericht: Use Cases in der Praxis. 2014. Verfügbar unter: http://www.hk-bs.de/Presse/wp-content/uploads/2014/03/Ergebnisbericht-Use-Cases-in-der-Praxis.pdf [26.06.2017]

Schmitt, Hartmut; Hess, Anne; Hess, Steffen; Maier, Andreas; Löffler, Diana; Hurtienne, Jörn: Intuitive Benutzbarkeit messen: Eine Evaluationstoolbox für Software, Apps und technische Produkte. 2014.

Verfügbar unter: http://germanupa.de/events/mensch-und-computer-2014/shortpaper/intuitive-benutzbarkeit-messen.html [26.06.2017]

Schmitz, Paul; Bons, Heinz; van Megen Rudolf: Software-Qualitätssicherung – Testen im Software-Lebenszyklus, 2. Auflage. Vieweg, Braunschweig 1983

Schneier, Bruce: Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons, New York, NY 2000

Schubert; Susanne & Müller; Daniel: Der IT-Sicherheitsmarkt in Deutschland Aktualisierung und Revision der Ergebnisse 2014: Studie. Bundesministerium für Wirtschaft und Energie (BMWi), Berlin 2014

Schuller; Andreas: Deliverable D22.4 Usability Requirements Analysis, SP 2, WP22. Verfügbar unter: http://www.futureid.eu/data/deliverables/year1/Public/FutureID_D22.04_WP22_v1.0_UsabilityRequirements.pdf [27.06.2017]

Schwaber; Ken & Sutherland; Jeff: The Scrum Guide. Verfügbar unter: https://www.scrum.org/resources/scrum-guide [26.06.2017]

Schweibenz, Werner & Thissen, Frank: Qualität im Web: Benutzerfreundliche Webseiten durch Usability Evaluation. Springer, Berlin 2002

Seffah, Ahmed; Donyaee, Mohammad; Kline, Rex B.; Padda, Harkirat K.: Usability measurement and metrics: A consolidated model. In: Software Quality Journal 14 (2), S. 159-178. Kluwer Academic Publishers, Hingham 2006

Sheldon, Kennon M.; Elliot, Andrew J.; Kim, Youngmee; Kasser, Tim: What is satisfying about satisfying events? Testing 10 candidate psychological needs. In: Journal of Personality and Social Psychology, Band 80, S. 325–339. American Psychological Association, Washington 2001

Shneiderman, Ben: The Future of Interactive Systems and the Emergence of Direct Manipulation. In: Proceedings of the NYU Symposium on User Interfaces, on Human Factors and Interactive Computer Systems, S. 1-28. Ablex Publishing, Norwood, NJ 1984

Shneiderman, Ben & Plaisant, Catherine: Designing the User Interface: Strategies for Effective Human-Computer Interaction, 4. Auflage, Addison-Wesley, Boston, MA 2004

Smetters, Diana K.: Usable Security: Oxymoron or Challenge? National Academy of Engineering Frontiers of Engineering Symposium. National Academy of Engineering Frontiers of Engineering Symposium, 2007

Smetters, Diana K. & Grinter, Rebecca E.: Moving from the Design of Usable Security Technologies to the Design of Useful Secure Applications. In: NSPW '02 Proceedings of the 2002 workshop on New security paradigms, S. 82-89. ACM, New York, NY 2002

Smith, Sidney L. & Mosier, Jane N.: Guidelines for designing user interface software. 1986. Verfügbar unter: http://hcibib.org/sam/ [26.06.2017]

Sommer, Dieter: PrimeLife - Privacy and Identity Management in Europe for Life. 2011. Verfügbar unter: http://primelife.ercim.eu [26.06.2017]

Sontow, Karsten; Treutlein, Peter; Sontow, Rainer; Trovarit AG: ERP-Praxis im Mittelstand. Marktübersicht – Kenngrößen – Anwenderzufriedenheit. 2011

SOPHISTen: Die kleine RE-Fibel. 2. Auflage. SOPHIST GmbH, Nürnberg 2015

Sorge, Christoph; Gruschka, Nils; Lo Iacono, Luigi: Sicherheit in Kommunikationsnetzen. Oldenbourg Verlag, München 2013

Steel, Christopher; Nagappan, Ramesh; Lai, Ray: Core Security Patterns. Prentice Hall, Upper Saddle River 2005

Steel, Graham: Formal Analysis of Security APIs. In: van Tilborg, Henk C.A.; Jajodia, Sushil (Hrsg.): Encyclopedia of Cryptography and Security, S. 492-494. Springer US, 2011

Stobert, Elizabeth; Chiasson, Sonia; Biddle, Robert: Persuasion, Social Graces, and Computer Security. Carleton University

Stylos, Jeffrey & Clarke, Steven: Usability Implications of Requiring Parameters in Objects' Constructors. In: ICSE '07 Proceedings of the 29th International Conference on Software Engineering, S. 529-539. IEEE Computer Society, Washington, DC 2007

Stylos, Jeffrey & Myers, Brad: Mapping the Space of API Design Decisions. In: 2007 IEEE Symposium on Visual Languages and Human-Centric Computing, S. 50-57. IEEE Computer Society, Washington, DC 2009

Stylos, Jeffrey & Myers, Brad A.: Mica: A Web-Search Tool for Finding API Components and Examples. In: VLHCC '06 Proceedings of the Visual Languages and Human-Centric Computing, S. 195 - 202. IEEE Computer Society, Washington, DC 2006

Stylos, Jeffrey & Myers, Brad A.: The Implications of Method Placement on API Learnability. In: SIGSOFT '08/FSE-16 Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of Software Engineering, S. 105-112. ACM, New York, NY 2008

Stylos, Jeffrey; Clarke, Steven; Myers, Brad: Comparing API Design Choices with Usability Studies: A Case Study and Future Directions. In: 18th Workshop of the Psychology of Programming Interest Group (PPIG '06), S. 131-139. 2006

Sun, San-Tsai & Beznosov, Konstantin: The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems. In: CCS '12 Proceedings of the 2012 ACM Conference on Computer and Communications Security, S. 378-390. ACM, New York, NY 2012

Sunshine, Joshua; Egelman, Serge; Almuhimedi, Hazim; Atri, Neha; Cranor, Lorrie Faith: Crying wolf, An empirical study of SSL warning effectiveness. In: SSYM'09 Proceedings of the 18th conference on USENIX Security Symposium, S. 399–416. USENIX Association, Berkeley 2009

SysSec-Konsortium: The Red Book: A Roadmap for Systems Security Research. 2013

Thome, Rainer: Betriebswirtschaftliche Software Enterprise Resource Planning: 11 Lösungen im Überblick. eBusi-ness-Lotse Mainfranken, Würzburg 2014

Tidwell, Jenifer: Designing Interfaces: Patterns for Effective Interaction Design. O'Reilly, Sebastopol 2005

Toxboe, Anders: UI Patterns - User Interface Design Pattern Library. 2017. Verfügbar unter: http://ui-patterns.com [26.06.2017]

Travis, David: 247 web usability guidelines. 2015. Verfügbar unter: http://www.userfocus.co.uk/resources/guidelines.html [26.06.2017]

Trovarit AG: ERP in der Praxis - Anwenderzufriedenheit, Nutzen & Perspektiven 2014/2015. Management Summary. Achen 2014

U. S. Department of Health and Human Services: Research-Based Web Design & Usability Guidelines. 2006. Verfügbar unter: http://www.usability.gov/sites/default/files/documents/guidelines_book.pdf [26.06.2017]

U.S. Department of Health, Education, And Welfare: Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. 1973

Ullrich, Daniel & Diefenbach, Sarah: INTUI. Exploring the Facets of Intuitive Interaction. In: Mensch & Computer 2010 (S. 251-260). München: Oldenbourg 2010

Usability Body of Knowledge: Cognitive Walkthrough. 2010. Verfügbar unter: http://www.usabilitybok.org/cognitive-walkthrough [26.06.2017]

Usability Body of Knowledge: Prototyping Methods. 2010. Verfügbar unter: http://usabilitybok.org/prototyping-methods [26.06.2017]

Usability First: Usability Glossary - low-fidelity prototype. 2015. Verfügbar unter: http://www.usabilityfirst.com/glossary/low-fidelity-prototype/ [26.06.2017]

Usability First (2015): Usability Glossary - high-fidelity prototype. 2015. Verfügbar unter: http://www.usabilityfirst.com/glossary/high-fidelity-prototype/ [26.06.2017]

Usability in Germany (UIG) e.V.: Personas. 2016. Verfügbar unter: http://www.usability-in-germany.de/definition/personas [26.06.2017]

van Welie, Martijn: A Pattern Library for Interaction Design. 2008. Verfügbar unter: http://www.welie.com [26.06.2017]

Wagner, Stefan: Software Product Quality Control. Springer, Heidelberg 2013

Wallmüller, Ernest: Qualitätsmodelle im Software Engineering: Boden unter den Füssen. In: MQ - Management und Qualität 2002(9). Galledia, Berneck 2002

Wang, Hui; Zhang, Yuanyuan; Li, Juanru; Liu, Hui; Yang, Wenbo; Li, Bodong; Gu, Dawu: Vulnerability Assessment of OAuth Implementations in Android Applications. In: ACSAC 2015 Proceedings of the 31st Annual Computer Security Applications Conference, S. 61-70. ACM, New York, NY 2015

Wang, Rui; Chen, Shuo; Wang, XiaoFeng: Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services. In:

SP '12 Proceedings of the 2012 IEEE Symposium on Security and Privacy, S. 365-379. IEEE Computer Society, Washington, DC 2012

Watson, David; Clark, Lee Anna; Tellegen, Auke: Development and validation of brief measures of positive and negative affect: The PANAS scales. In: Journal of Personality and Social Psychology, Band 54, S. 1063–1070. American Psychological Association, Washington 1988

Website Standards Association: Business Website Usability Guidelines. 2008

Wenk, Oliver: Mit Checklisten Zeit sparen und Nerven schonen – Wie funktioniert das? 2011. Verfügbar unter: http://www.gruenderhelden.de/mit-checklisten-zeit-sparen-und-nerven-schonen-wie-funktioniert-das/ [26.06.2017]

Whitten, Alma: Making Security Usable. PhD thesis, Carnegie Mellon University, Pittsburgh, PA 2004

Whitten, Alma & Tygar, J. D.: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: Proceedings of the 8th Conference on USENIX Security Symposium, Washington, D.C. 1999

Winkelmann, Axel: Enterprise Resource Planning - Enzyklopaedie der Wirtschaftsinformatik. 2013. Verfügbar unter: http://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/informationssysteme/Sektorspezifische-Anwendungssysteme/enterprise-resource-planning [26.06.2017]

Winter, Sebastian; Wagner, Stefan; Deissenboeck, Florian: A Comprehensive Model of Usability. In: Engineering Interactive Systems (EIS 2007 Joint Working Conferences EHCI 2007, DSV-IS 2007, HCSE 2007), S. 106 - 122. Springer, Berlin 2008

Wogalter, Michael S.: Communication-Human Information Processing (C-HIP) Model. In: Wogalter, Michael S. (Hrsg.): Handbook of Warnings, S. 51-61. Lawrence Erlbaum Associates, Mahwah, NJ 2006

Wogalter, Michael S.: Purposes and Scope of Warnings. In: Wogalter, Michael S. (Hrsg.): Handbook of Warnings, S. 3-9. Lawrence Erlbaum Associates, Mahwah, NJ 2006

Wogalter, Michael S.& Usher, Mary O.: Effects of Concurrent Cognitive Task Loading on Warning Compliance Behavior. In: Proceedings of the Human Factors and Ergonomics Society 43rd Annual Meeting, S. 525-529, 1999

Woywode, Michael; Mädche, Alexander; Wallach, Dieter; Plach, Marcus (2012): Gebrauchstauglichkeit von Anwendungssoftware als Wettbewerbsfaktor für kleine und mittlere Unternehmen (KMU): Abschlussbericht. Verfügbar unter: https://www.usability-in-germany.de/uig-studie [26.06.2017]

Yahoo Developer Network: Yahoo Design Pattern Library. Verfügbar unter: http://developer.yahoo.com/ypatterns [26.06.2017]

Yee, Ka-Ping: Aligning Security and Usability. IEEE Security & Privacy 2(5), S. 48-55. IEEE Educational Activities Department, Piscataway, NJ 2004

Yee, Ka-Ping: Guidelines and strategies for secure interaction design. In: Cranor, Lorrie Faith & Garfinkel, Simson (Hrsg.): Security and Usability: Designing Secure Systems That People Can Use, S. 247–273, O'Reilly, Sebastopol, CA 2005

Yee, Ka-Ping: Secure Interaction Design and the Principle of Least Authority. CHI 2003 Workshop on Human-Computer Interaction and Security Systems, 2003

Yee, Ka-Ping: User Interaction Design for Secure Systems. In: ICICS '02 Proceedings of the 4th International Conference on Information and Communications Security, S. 278–290, Springer, London 2002

Yeratziotis, Alexandros; van Greunen, Darelle; Pottas, Dalenca: A Framework for Evaluating Usable Security: The Case of Online Health Social Networks. In: Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2012), S. 97-107. Plymouth University, Plymouth 2012

Ylönen,Tatu: SSH: Secure Login Connections over the Internet. In: SSYM'96 Proceedings of the 6th conference on USENIX Security Symposium, Focusing on Applications of Cryptography (6), S. 4. USENIX Association, Berkeley, CA 1996

Zapata Aspiazu, Laura: Development of a Model for Security and Usability. Master Thesis, Universidad Politécnica de Madrid, Madrid 2013

Zhong, Hao; Xie, Tao; Zhang, Lu; Pei, Jian; Mei, Hong: MAPO: Mining and Recommending API Usage Patterns. In: Proceedings of the 23rd European Conference on Object-Oriented Programming, S. 318–343. Springer, Berlin 2009

Zibran, Minhaz F.; Eishita, Farjana Z.; Roy, Chanchal K.: Useful, But Usable? Factors Affecting the Usability of APIs. In: WCRE '11 Proceedings of the 2011 18th Working Conference on Reverse Engineering, S. 151–155. IEEE Computer Society, Washington, DC 2011

Ziske, Christine; Goetz, Christoph F.-J.; Mende-Stief, Kerstin; Barth, Michael; Arendt, Henning: Vertrauen und IT-Sicherheit: Vertrauensmodelle für die Informationsgesellschaft. TeleTrusT – Bundesverband IT-Sicherheit e.V., Berlin 2015

Zurko, Mary Ellen: IBM Lotus Notes/Domino: Embedding Security in Collaborative Applications. In: Cranor, Lorrie Faith & Garfinkel, Simson (Hrsg.): Security and Usability: Designing Secure Systems that People Can Use, S. 607–622. O'Reilly, Sebastopol 2005

Zurko, Mary Ellen & Simon, Richard T.: User-Centered Security. In: NSPW '96 Proceedings of the 1996 workshop on New security paradigms, S. 27-33. ACM, New York, NY 1996

4.5 Benutzte Informations- und Dokumentationsdienste

Von den Partnern wurden im Rahmen des Projekts diverse Informations- und Dokumentationsdienste genutzt, um Informationen zu gewinnen, aber auch um Neuigkeiten aus dem USecureD-Projekt zu verbreiten. Neben einschlägigen wissenschaftlichen Distributionsplattformen (https://www.ieee.org/index.html, https://dl.acm.org/, http://www.springer.com/de/, https://www.usenix.org/, https://www.elsevier.com/), der freien Enzyklopädie Wikipedia (http://www.wikipedia.de), dem Glossar des Mozilla Developer Network (https://developer.mozilla.org/en-US/docs/Glossary) und diversen Nachrichtenportalen für Softwareentwickler sind hier insbesondere die Newsletterdienste folgender Organisationen zu nennen:

- Allianz für Cyber-Sicherheit (https://www.allianz-fuer-cybersicherheit.de/)
- Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom, www.bitkom.org)
- Bundesverband IT-Mittelstand e. V. (BITMi, www.bitmi.de)
- Bundesverband IT-Sicherheit e.V. (TeleTrusT, http://www.teletrust.de/)
- German Usability Professionals Association e.V. (German UPA, http://www.germanupa.de)
- Security - Usability - Society research group (SECUSO, https://www.secuso.informatik.tu-darmstadt.de/en/secuso/)
- Software Cluster (http://www.software-cluster.org)

5 Zusammenarbeit mit anderen Stellen

Im Zentrum der Zusammenarbeit mit Dritten stand der Aufbau des USecureD-Kompetenzzentrums, in dem Experten aus Wissenschaft und Forschung sowie Anwender aus der softwareproduzierenden Industrie, aber auch Usability-Beratungshäuser und Endanwender einen Rahmen zum Austausch und zur gegenseitigen Befruchtung vorfanden. Neben den im Folgenden genannten Partnern, mit denen sehr detaillierte und konkrete Kooperationen im Rahmen von USecureD ausgearbeitet und vereinbart wurden, sollten im Rahmen des Projekts weitere Kooperationen etabliert werden. Beispielsweise waren im Rahmen des Projekts Expertenworkshops geplant, die mit Peers verschiedener Universitäten ausgerichtet werden sollten. Ferner planten die Konsortialpartner, beim Berufsverband der Deutschen Usability und User Experience Professionals einen Arbeitskreis zum Thema Usable Security zur Gründung vorzuschlagen.

Durch die Zusammenarbeit mit mehreren Anwendungspartnern sollte sichergestellt werden, dass die im USecureD-Projekt entwickelten Konzepte, Methoden und Werkzeuge, insbesondere die veröffentlichten Deliverables, auf beliebige Anwendungsdomänen übertragbar sind. Vorgesehen waren in diesem Zusammenhang insbesondere Pilotprojekte bei den mittelständischen IKT-Anwenderunternehmen Ha-Ra Umwelt- und Reinigungstechnik und Bruno Zimmer. Zudem wurde angestrebt, über die Aktivitäten des Kompetenzzentrums zur Projektlaufzeit weitere potentielle Anwendungspartner zu gewinnen, um deren Feedback zu den erarbeiteten Ergebnissen einholen zu können. Neben den Online-Kanälen sollte hierzu insbesondere die Ansprache möglicher Interessenten in Seminaren, Workshops und Vorträgen des Kompetenzzentrums genutzt werden.

5.1 Technische Universität Berlin

Das Quality and Usability Lab am Institut für Softwaretechnik und Theoretische Informatik der Technischen Universität Berlin (http://www.qu.tu-berlin.de) forscht und lehrt unter der Leitung von Prof. Dr.-Ing. Sebastian Möller auf verschiedenen Gebieten der Mensch-Maschine-Interaktion, insbesondere an der Messung und Vorhersage von wahrgenommener Qualität und Gebrauchstauglichkeit, der Erfassung und Modellierung von Nutzerverhalten sowie der wahrgenommenen Sicherheit und Privatsphäre. Dabei entwickelt das Quality and Usability Lab Evaluationsmethoden und Beschreibungsmodelle, die bereits vielfach in durch die öffentliche Hand (DFG, EU, EIT) und in industriell (insbesondere durch die Deutsche Telekom) geförderten Projekten eingesetzt wurden.

Das Quality and Usability Lab sollte das USecureD-Projekt beratend unterstützen und kostenneutral zu verschiedenen USecureD-Aktivitäten beitragen. Hierzu zählten u. a. die Beteiligung an den Expertenworkshops sowie Beiträge zum Anforderungskatalog und zum USecureD-Qualitätsmodell.

5.2 Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI, http://www.bsi.bund.de), 1991 gegründet, ist eine zivile obere Bundesbehörde im Geschäftsbereich des Bundesministeriums des Innern, die für Fragen der IT-Sicherheit zuständig ist. Im BSI sind zirka 600 Mitarbeiter beschäftigt (Stand 2014). Das BSI ist die zentrale Zertifizierungsstelle für die Sicherheit von IT-Systemen in Deutschland (Computer- und Datensicherheit, Datenschutz). Prüfung und Zertifizierung durch das BSI ist möglich in Bezug auf die Standards des IT-Grundschutzhandbuchs, des Grünbuchs, ITSEC und Common Criteria. Das BSI gibt die IT-Grundschutz-Kataloge heraus, die Empfehlungen für Standardschutzmaßnahmen für typische IT-Systeme enthalten. In diesen Katalogen werden nicht nur technische, sondern auch organisatorische, personelle und infrastrukturelle Maßnahmen erörtert. Das BSI veröffentlicht außerdem regelmäßig Studien, Richtlinien, Infoblätter und Broschüren zum Thema IT-Sicherheit.

Das Referat C 12: Cyber-Sicherheit in kritischen IT-Systemen, Anwendungen und Architekturen war an der Kooperation mit dem USecureD-Projekt interessiert, da sich viele der Themen des Referats C 12 im Kern mit verteilten Anwendungen auf Basis von Internet- und Webtechnologien befassen, die verstärkt Einzug in kritische Infrastrukturen erhalten. Die Gebrauchstauglichkeit von Sicherheitsmechanismen hat in diesen Anwendungsgebieten eine enorm wichtige Funktion. Das Referat C 12 sollte das USecureD-Projekt daher beratend unterstützen und kostenneutral an verschiedenen Aktivitäten mitwirken.

5.3 saarland.innovation&standort e. V.

saar.is – saarland.innovation&standort e. V. (http://www.saaris.de/) ist die Nachfolge-Dachmarke der früheren ZPT, der viele Jahre erfolgreich für die Unternehmen der Saarwirtschaft tätigen Zentrale für Produktivität und Technologie. Ihre Aufgabe ist es, saarländischen Unternehmen durch Information, Beratung, Weiterbildung und Kooperationsvermittlung zu helfen, ihre Wettbewerbsfähigkeit zu verbessern und neue Produkte und Verfahren zu entwickeln und erfolgreich zu vermarkten. Mit ihren IT- und E-Business-Aktivitäten (Vortragsveranstaltungen, Seminaren sowie technisch und betriebswirtschaftlich ausgerichteten Betriebsberatungen) erreicht saar.is jährlich mehr als 1.000 Unternehmen. saar.is wird getragen und finanziert von der saarländischen Landesregierung; die Geschäftsführung wird von der Industrie- und Handelskammer des Saarlandes wahrgenommen. saar.is leitete das Projekt eBusiness-Lotse Saar, eines von bundesweit etwa 40 Zentren, die vom BMWi im Rahmen der Initiative eKompetenz-Netzwerk für Unternehmen gefördert wurden. An saar.is angegliedert sind ein Büro des Enterprise Europe Network sowie ein Patentinformationszentrum. Die Einbindung in die Cluster Automotive, Healthcare und IT ermöglicht einen sehr guten Zugang zu diesen saarländischen Schlüsselbranchen sowie zu den entsprechenden wissenschaftlichen Einrichtungen. Mit den saarländischen Hochschulen (Universität des Saarlandes, Hochschule für Technik und Wirtschaft) werden regelmäßig Technologietransfer-Veranstaltungen durchgeführt. saar.is ist sowohl regional als auch auf Bundesebene und EU-Ebene seit vielen Jahren in Netzwerken aktiv. Neben den genannten Organisationen umfasst das saar.is-Netzwerk den Deutschen Verband für Technologietransfer und Innovation (DTI), die TechnologieAllianz, das Rationalisierungs- und Innovationszentrum der Deutschen Wirtschaft (RKW), it.saarland, die Kontaktstelle für Wissens- und Technologietransfer der Universität des Saarlandes (KWT), das Institut für Technologietransfer an der HTW des Saarlandes (FITT), die Saarland Offensive für Gründer (SOG) und das Business Angels Netzwerk Saarland (BANS).

Als assoziierter Partner sollte saar.is insbesondere zur Erhebung von Anforderungen an Usable Security bzw. an die entwickelten Methoden und Werkzeuge, zur Verbreitung und Vernetzung des USecureD-Projekts sowie zum Wissenstransfer beitragen.

5.4 Ha-Ra Umwelt- und Reinigungstechnik GmbH

Die Ha-Ra Umwelt- und Reinigungstechnik GmbH (kurz Ha-Ra, http://www.ha-ra.de) ist seit mehr als 40 Jahren kompetenter Partner zur Lösung von Reinigungsproblemen im Haushalt und in professionellen Bereichen. Das Ha-Ra Reinigungssystem hilft den Kunden dabei, Verschmutzungen umweltfreundlich, schnell und sauber zu reinigen. Als innovatives, leistungsstarkes Unternehmen erschließt sich Ha-Ra zudem kontinuierlich neue Geschäftsfelder, z.B. mit Kosmetik-, Wellness-, Nahrungsergänzungs- und Tierpflegeprodukten. Ha-Ra ist heute weltweit in über 50 Ländern vertreten und beschäftigt an seinem saarländischen Standort weit über 100 Mitarbeiter.

Ha-Ra sollte im USecureD-Projekt als assoziierter Anwendungspartner mitwirken. Neben der Anforderungserhebung, die die Grundlage für prototypische Implementierungen durch HKBS in einem Pilotprojekt bildete, sollte Ha-Ra für die praxisnahe Evaluierung bzw. Validierung der im USecureD-Projekt erarbeiteten Lösungsansätze zur Verfügung stehen.

5.5 Bruno Zimmer e.K.

Die Ölmühle von Bruno Zimmer (kurz: brunozimmer, http://www.brunozimmer.de) mit Sitz in Oberthal/ Saar steht seit über 20 Jahren für eine Vielfalt an besten Pflanzenölen, Naturkost & Wellnessprodukten. Als traditioneller Familienbetrieb mit mehr als 70 Mitarbeitern vereint das Unternehmen alte Handwerkskunst mit moderner Technik. Ein eigenes Labor und eine konsequente Ausgangskontrolle bei brunozimmer stellen sicher, dass nur qualitativ erstklassige Produkte erzeugt werden. Seit 2003 vertreibt die Ölmühle ihre Waren auch über das Internet. Für brunozimmer als qualitätsorientiertes Herstellerunternehmen gibt es ein erhöhtes Sicherheitsbedürfnis in Hinsicht auf die Angreifbarkeit von außen und die Sicherheit in der Datenverwaltung, wobei die Rezepturen und Herstellungsverfahren des Unternehmens in besonderem Maße vertraulich sind.

Im USecureD-Projekt sollte brunozimmer als assoziierter Anwendungspartner in einem Pilotprojekt mitwirken. In Zusammenarbeit mit HK Business Solutions sollten insbesondere die funktionalen und nichtfunktionalen Anforderungen an einen konkreten Geschäftsprozess im Bereich Warenwirtschaft erhoben werden. Nachdem von HK Business Solutions prototypische Lösungsansätze für diese Anforderungen erarbeitet wurden, sollte brunozimmer zudem für die praxisnahe Evaluierung und Validierung dieser Lösungen zur Verfügung stehen.

5.6 Fraunhofer-Institut für Experimentelles Software Engineering

Das Fraunhofer-Institut für Experimentelles Software Engineering (https://www.iese.fraunhofer.de/) wurde 1996 als erste Einrichtung der Fraunhofer-Gesellschaft für Angewandte Forschung in Rheinland-Pfalz gegründet. Es hat sich in kurzer Zeit zu einem international führenden Kompetenzzentrum für Software Engineering entwickelt. Ob Software im Auto, Flugzeug oder Medizingerät, in größere Systeme eingebettet oder als eigenständige Anwendung: Immer bilden neueste wissenschaftliche Erkenntnisse und darauf aufbauend fortschrittliche Techniken und Werkzeuge die Basis der branchenübergreifenden Projektarbeit. Zu den unterschiedlichen Kompetenzen des IESE gehören im Bereich der Informationssysteme unter anderem User Experience Engineering und Security Engineering. Insbesondere weil KMU einen wesentlichen Anteil der Industriekunden des IESE bilden und zielgerichtetes Usability und Security Engineering eine immer zentralere Rolle spielt, werden auch Beratungsdienstleistungen zu diesem Thema stetig wichtiger.

Mit dem Fraunhofer IESE wurde das USecureD-Kompetenzzentrum kurz nach Projektstart um einen weiteren assoziierten Partner ergänzt. Das Fraunhofer IESE sollte das USecureD-Projekt beratend unterstützen und kostenneutral zu verschiedenen USecureD-Aktivitäten beitragen. Geplant waren u.a. die Beteiligung an den Expertenworkshops sowie Reviews verschiedener (Zwischen-)Ergebnisse.

6 Verwendung der Zuwendung und Projektergebnisse

Das USecureD-Vorhaben umfasste sechs Arbeitspakete. In den folgenden Kapiteln sind die Ziele dieser Arbeitspakete, die jeweilige Verwendung der Zuwendung sowie die erzielten Ergebnisse näher erläutert.

6.1 Arbeitspaket 1: Methodische Vorbereitung

Laufzeit: Mai – Oktober 2015

Lead: TH Köln

6.1.1 Ziele des Arbeitspakets

In diesem Arbeitspaket sollten die methodischen Grundlagen für das USecureD-Gesamtprojekt und für das Erreichen aller angestrebten Vorhabenziele geschaffen werden.

Ziel von **AP 1.1 Anwendungsbereiche für Usable Security** war es, eine umfassende Analyse durchzuführen, welche typischen Anwendungsbereiche und Anwendungsfälle es im Bereich Usable Security gibt, und die Ergebnisse dieser Analyse in Form von Use Cases zu dokumentieren. In **AP 1.2 Anforderungen an Usable Security** sollte eine umfassende Analyse durchgeführt werden, welche konkreten Anforderungen an Usable Security auf Anwenderseite bestehen und welches die aktuellen Sicherheitsschwachstellen der Benutzerinteraktion im Bereich (webbasierter) Geschäftsanwendungen sind. In **AP 1.3 USecureD-Qualitätsmodell** sollte ein ganzheitliches Qualitätsverständnis für den Bereich Usable Security entwickelt werden und in Form eines USecureD-Qualitätsmodells dokumentiert werden.

6.1.2 Verwendung der Zuwendung

Arbeitspaket 1 umfasste die folgenden Aktivitäten:

AP 1.1: Anwendungsbereiche für Usable Security

Analyse von Softwareprodukten und -services

Im ersten Schritt der Analyse wurden die Begriffswelten „Unternehmenssoftware“ und „betriebliche Software“ untersucht. Unternehmenssoftware (Business Software) bezieht sich auf alle Programme, die betriebliche Anwender bei Ihrer täglichen Arbeit unterstützen und diesen dabei helfen, Prozesse in ihrem Unternehmen zu optimieren. Hierbei kann unterschieden werden zwischen betriebswirtschaftlichen Anwendungen, technischen Anwendungen, Management- und Informationssystemen sowie Anwendungen zur Unterstützung der betrieblichen Abläufe. Betriebswirtschaftliche Anwendungen werden von vielen Herstellern zu Produktsuiten zusammengefasst und als Enterprise-Resource-Planning (ERP)-Systeme vermarktet; diese Anwendungen bilden nach dem Verständnis vieler Nutzer den Kern der Unternehmenssoftware und werden auch oft verallgemeinernd als Unternehmenssoftware bezeichnet.

Im nächsten Schritt wurde festgelegt, welche Arten betrieblich genutzter Software bei der späteren Analyse der Anwendungsfälle betrachtet werden sollten. Der Bereich betriebswirtschaftliche Anwendungen sollte den Schwerpunkt der Untersuchung bilden. ERP-Standardprodukte sind bei mittelständischen Anwenderunternehmen sehr beliebt; sie werden von Nutzergruppen verwendet, die hinsichtlich Vorerfahrung, Security-Expertise und Usability-Anforderungen sehr heterogen sind. Aufgrund der starken Verbreitung dieser Produkte sollte mit den anvisierten Projektergebnissen eine möglichst breite Zielgruppe angesprochen werden.

Technische Anwendungen wurden von der weiteren Betrachtung weitgehend ausgeschlossen. Eine Ausnahme bildeten die Tools für Softwareentwickler, da insbesondere mittelständische Softwarehersteller als Zielgruppe im Fokus des USecureD-Projekts standen und daher auch typische Werkzeuge, Programmierschnittstellen und Frameworks, mit denen Entwickler in diesen Unternehmen arbeiten, untersucht werden mussten. Bei den Management- und Informationssystemen bzw. bei den Anwendungen zur Unterstützung der betrieblichen Abläufe wurden jeweils bestimmte Teilbereiche betrachtet, nämlich Teilbereiche, die einen starken Security-Bezug haben bzw. die für eine Vielzahl von Unternehmen relevant sind (z. B. Projektverwaltung, Controlling).

Entwicklung des USecureD-Use-Case-Templates

In der Literatur gibt es eine Vielzahl von Schablonen, Vorlagen und Empfehlungen, die bei der Ausarbeitung von Use Cases (deutsch: Anwendungsfällen) genutzt werden können. Da dem Konsortium keine Vorlage zur Dokumentation von Anwendungsfällen im Bereich Usable Security bekannt war, sollte

im Rahmen des Projekts ein entsprechendes Template auf Basis grundlegender Arbeiten zum Thema Use Cases erstellt werden. Bei der Auswahl geeigneter Templatefelder flossen die Ergebnisse einer aktuellen Studie ein, die die HKBS und das Fraunhofer-Institut für Experimentelles Software Engineering IESE im Auftrag des Arbeitskreises „Use Cases in Forschung und industrieller Praxis“ der Gesellschaft für Informatik e.V. – Fachgruppe Requirements Engineering durchgeführt hatten und bei der der aktuelle Einsatz von Use Cases in der Praxis des Software & Systems Engineering untersucht wurde.

Zusätzlich zu bekannten Use-Case-Attributen (ID, Beschreibung, Akteur usw.), mit denen grundlegende Informationen zum Use Case erfasst werden, wurden fünf neue Attribute eingeführt. Zwei dieser Felder (Sicherheitsrisiken, Gefährdung) tragen dem Projektschwerpunkt IT-Security Rechnung, die drei übrigen Felder (Qualitätsmerkmale, Entwicklungsrichtlinien, Patterns) sollten eine Verknüpfung mit Projektergebnissen ermöglichen, die im weiteren Verlauf von USecureD erarbeitet werden.

Erstellung der USecureD-Use-Case-Sammlung

Zur Erstellung der Use-Case-Sammlung wurden zunächst typische Anwendungsfälle betrieblicher Software identifiziert. Hierfür wurde eine Reihe von Softwareanwendungen aus dem Bereich betriebswirtschaftliche Anwendungen untersucht, wobei verschiedene Techniken der Systemarchäologie zum Einsatz kamen: Bei mehreren ERP-Systemen (Produkte von Sage und myfactory) wurde eine Systemanalyse (Ist-Analyse) durchgeführt. Viele weitere Produkte wurden mittels dokumentbasierter Techniken (Analyse von Marketingbroschüren, Benutzerhandbüchern, Onlinehilfen u. ä.) analysiert. Betrachtet wurden Produkte der ERP-Hersteller mit den größten Marktanteilen (SAP Business One, Microsoft Dynamics NAV, Oracle), kleinere kommerzielle Produkte für die Zielgruppe KMU sowie Open-Source-Systeme. Unterstützend wurden verschiedene Fachbücher und Studien zum Funktionsumfang bzw. Einsatz von ERP-Systemen analysiert.

Anschließend wurden die gesammelten Anwendungsfälle in mehreren Expertenworkshops konsolidiert. Hierbei wurden die Anwendungsfälle inhaltlich geclustert und es wurden Doubletten sowie Anwendungsfälle mit untergeordneter Relevanz (z. B. zu geringe Häufigkeit des Auftretens) getilgt. Anschließend wurden die Workshopergebnisse strukturiert in Form von Use-Case-Diagrammen dokumentiert. Als Bezeichnung für das jeweilige System in den Use-Case-Diagrammen wurden typische Modulbezeichnungen verwendet, wie sie von Softwareherstellern für die Module ihrer ERP-Systeme verwendet werden, z. B. Warenwirtschaft, Produktion oder Finanzbuchhaltung. Hierbei ist zu berücksichtigen, dass die modulare Aufteilung der ERP-Systeme bei den einzelnen Herstellern sehr unterschiedlich ist und dass es zwischen den Modulen und Einsatzbereichen fließende Übergänge gibt. Als Bezeichnung für die Akteure in den Use-Case-Diagrammen wurden typische Rollenbezeichnungen verwendet, wie sie in kleinen und mittleren Unternehmen anzutreffen sind, z. B. Einkäufer, Lagerist, Produktionsleiter bzw. -mitarbeiter oder Auftragsbearbeiter.

Im nächsten Schritt wurden sämtliche Anwendungsfälle identifiziert, bei denen ein erhöhter Sicherheitsbedarf besteht und die insofern einen besonderen Bezug zum Thema Usable Security haben. Dies gilt insbesondere für Anwendungsfälle, bei denen Fakturaänderungen stattfinden, bei denen Lagerbewegungen stattfinden oder bei denen das betrachtete System mit einem Drittsystem kommuniziert. Die entsprechenden Use Cases wurden in den erstellten Use-Case-Diagrammen farblich hervorgehoben.

Im letzten Schritt wurden sechs Anwendungsfälle exemplarisch ausgearbeitet. Bei der Auswahl der Beispiel-Use-Cases wurde darauf geachtet, dass diese aus unterschiedlichen Handlungsfeldern stammen und verschiedene Sichten auf das System widerspiegeln (Sicht des Endanwenders, des Systemadministrators und des Entwicklers). Als Beschreibungsvorlage wurde das im Projekt entwickelte Use-Case-Template verwendet. Die USecureD-Entwicklungsrichtlinien und -Patterns, die erst im weiteren Projektverlauf erarbeitet wurden, wurden für die finale Version der Use-Case-Sammlung bei den exemplarischen Use Cases ergänzt.

AP 1.2: Anforderungen an Usable Security

Durchführung einer Onlinestudie

Mit der USecureD-Studie sollte der Kenntnisstand zum Thema Usable Security und das Bewusstsein in Unternehmen (vor allem KMU) erhoben werden. Die Online-Studie startete am 30.10.2015 und endete am 20.12.2015. Sie wurde mit der Software Limesurvey erstellt, einer frei verfügbaren und quelloffenen Webanwendung für Online-Umfragen. Die Umfragen wurden als strukturiertes Interview ausgelegt und bestanden aus insgesamt 42 Fragen. In Abhängigkeit der gegebenen Antworten mussten die Teilnehmer eine unterschiedliche Anzahl und ggf. auch unterschiedliche Fragen beantworten. Der Umfragekatalog der Online-Studie bestand aus sechs Fragegruppen. In der ersten Fragegruppe wurden demogra-

phische Fragen gestellt. Die zweite Fragegruppe bestand aus allgemeinen Fragen zum Thema Usability. In der dritten Fragegruppe mussten die Teilnehmer allgemeine Fragen zum Thema IT-Sicherheit beantworten. Die vierte Fragegruppe beinhaltete allgemeine Fragen über die Einordnung und Relevanz von Usable Security. Die letzten beiden Fragengruppen enthielten jeweils Fragen über den aktuellen Umsetzungsgrad und die Investitionsbereitschaft für Usability und IT-Sicherheit in Softwareentwickler- bzw. Softwareanwenderunternehmen.

Als Distributionskanäle für die Bekanntmachung der Online-Studie wurden verschiedene Plattformen gewählt. Ankündigungen wurden auf den Webseiten von USecureD, Mittelstand-Digital, dem German UPA Arbeitskreis „Usable Security und Privacy“, HKBS, saar.is und eBusiness-Lotse OWL platziert. Im Bereich der sozialen Medien wurde die Usable-Security-Gruppe bei Xing und sowohl die Facebook- als auch die Google-Plus-Seite des Fraunhofer SIT genutzt. Zudem wurde versucht potenzielle Teilnehmer über die Mailinglisten der GI-Fachgruppe SICHERHEIT und die Vorlesung Daten- und Anwendungssicherheit des Master-Studiengangs Medientechnologie an der TH Köln zu akquirieren. Insgesamt wurden 154 Fragebögen erfasst, von denen 118 vollständig beantwortet wurden. Berücksichtigung in der Auswertung fanden ausschließlich vollständig beantwortete Fragebögen.

Durchführung von Interviews und Workshops

Um die Anforderungen von (ausgewählten) IKT-Anwenderunternehmen eingehend zu erheben, wurden parallel zur Onlinestudie vertiefende Interviews und Workshops durchgeführt.

Zur Durchführung der Interviews wurden mehrere Termine mit den assoziierten Partnern Ha-Ra und brunozimmer sowie zwei anderen Kunden der HKBS vereinbart. Die Interviews wurden vor Ort in den Unternehmen am Arbeitsplatz der Befragten durchgeführt. Auf diese Weise war es möglich, Beobachtungen in den Unternehmen bzw. am Arbeitsplatz der Anwender zu machen, die relevant für die Untersuchung waren. An den Interviews nahmen Teilnehmer aus unterschiedlichen Abteilungen von vier kleinen und mittleren Unternehmen aus dem Saarland teil. Die Dauer der Interviews betrug zwischen ca. 30 und ca. 50 Minuten. Die Interviews wurden in Form halbstrukturierter Interviews geführt. Hierzu erstellten die Projektpartner vorab einen Interviewleitfaden und eine Datenschutzvereinbarung.

Mit den assoziierten Partnern saar.is und Fraunhofer IESE wurde jeweils ein Expertenworkshop durchgeführt. Ziel dieser Workshops war es, die Erfahrungen der Teilnehmer aus einer Vielzahl von IT-Projekten mit Anwenderunternehmen aus der IKT-Branche zu erheben. Hierdurch sollte das in der Onlinestudie bzw. den Einzelinterviews erhobene Meinungsbild bestätigt bzw. abgerundet werden. Als Grundlage der Workshops diente der Leitfaden, der für die Durchführung der halbstrukturierten Endanwender- bzw. Stakeholder-Interviews angefertigt wurde; dieser Leitfaden wurde für die Durchführung der Workshops entsprechend angepasst. Die Dauer der Workshops betrug jeweils ca. 2,5 Stunden. Teilnehmer des saar.is-Workshops waren drei Mitglieder des Technologietransfer-Teams, Teilnehmer des IESE-Workshops waren zwei Experten aus den Bereichen IT-Security und ein Experte aus dem Bereich Usability / User Experience.

AP 1.3: USecureD-Qualitätsmodell

Analyse bestehender Softwarequalitätsmodelle

Die zugrunde gelegte Methodik zum Erarbeiten des USecureD-Qualitätsmodells basierte auf einer strukturierten Analyse verfügbarer Arbeiten auf den verschiedenen involvierten Teilgebieten. Untersucht wurden insbesondere die Qualitätsmodelle von McCall et al., das FURPS-Modell sowie die Modelle der ISO-Normen 9126 und 25010. Da das Qualitätsmodell der ISO-Norm 25010 das aktuell umfangreichste Softwarequalitätsmodell darstellt, dienten seine Teilbereiche Gebrauchstauglichkeit, Sicherheit und Nutzungsqualität als Basis für das USecureD-Qualitätsmodell.

Entwicklung und Dokumentation des USecureD-Qualitätsmodells

Die genannten Teilbereiche der ISO-Norm 25010 wurden um einzelne Teilmerkmale erweitert, die aus anderen Normen bzw. aus der Literatur übernommen wurden. Ziel dieser Erweiterung war nicht, ein balanciertes Qualitätsmodell zu entwickeln, bei dem alle Merkmale eine gleiche Tiefe an Teilmerkmalen aufweisen, sondern ein Modell zu erreichen, das eine möglichst einfache, nachvollziehbare und vergleichbare Bewertung der Softwarequalität erlaubt. Abbildung 5 illustriert das erarbeitete integrierte Qualitätsmodell für Usable Security.

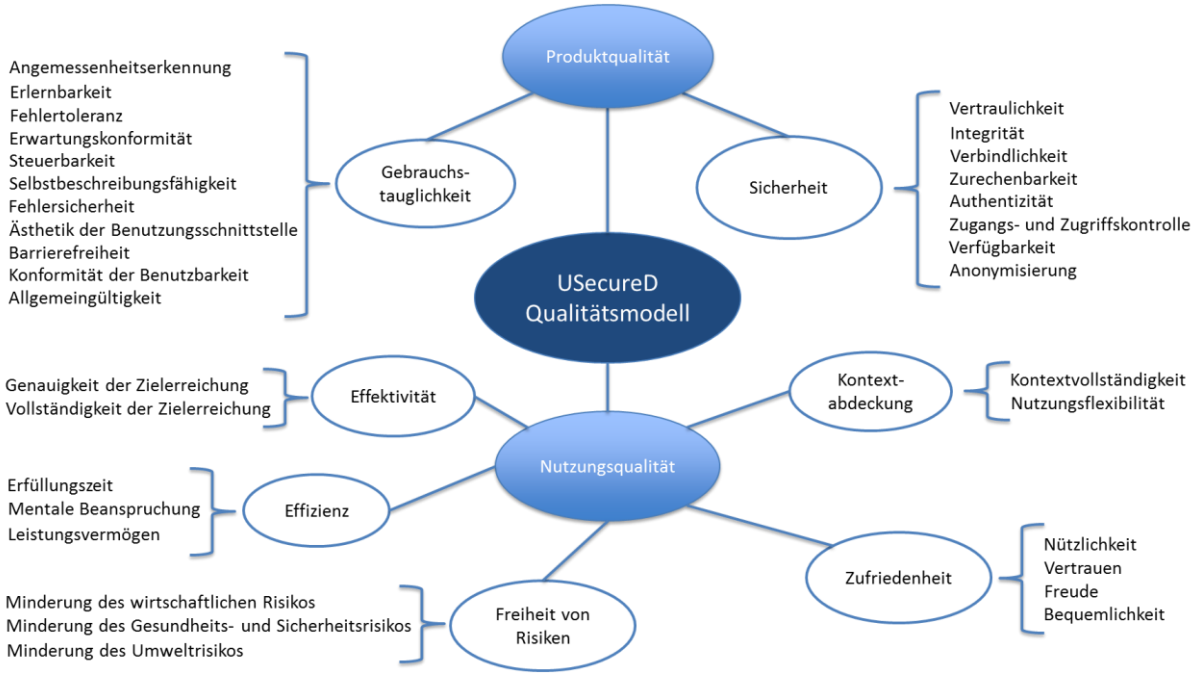


Abbildung 5: Integriertes Qualitätsmodell für Usable Security

Bei der Dokumentation des Qualitätsmodells wurden für alle Teilmerkmale die jeweiligen Quellen angegeben. Für die Beschreibung der (Teil-)Merkmale wurden die Definitionen und Anmerkungen der genannten Normen und relevanten Arbeiten übernommen. Im weiteren Projektverlauf wurden für bestimmte Teilmerkmale, die im Rahmen empirischer Evaluationen überprüft wurden, geeignete Metriken und Indikatoren ermittelt und es wurden die Beziehungen zwischen einzelnen Teilmerkmalen untersucht. Die Ergebnisse dieser Arbeiten wurden in der finalen Version dieses Dokuments bei den entsprechenden (Teil-)Merkmalen ergänzt.

6.1.3 Ergebnisse

Im Rahmen von Arbeitspaket 1 haben die Partner folgende Ergebnisse erarbeitet:

- **E 1.1 USecureD-Use-Case-Template**
  Beschreibungstemplate für Anwendungsfälle im Bereich Usable Security
  (https://www.usecured.de/UseWP/wp-content/uploads/2015/11/E-1.1-USecureD-Use-Case-Template-V.1.pdf)
- **E 1.2 USecureD-Use-Case-Sammlung**
  Sammlung von Anwendungsfällen im Bereich Usable Security
  (https://www.usecured.de/UseWP/wp-content/uploads/2015/04/E-1.2-USecureD-Use-Case-Sammlung-V.2.pdf)
- **E 1.3 USecureD-Studie**
  Entwicklung und Durchführung einer Onlinestudie zu den Anforderungen an Usable Security (N=118)
- **E 1.3b USecureD-Interviewleitfaden**
  Interviewleitfaden zur Erhebung von Anforderungen an Usable Security
  (https://www.usecured.de/UseWP/wp-content/uploads/2016/02/USecureD-Interviewleitfaden-V.1.pdf)
- **E 1.3c USecureD Anforderungsanalyse (Interviewergebnisse)**
  Durchführung und Auswertung einer Anforderungserhebung für den Bereich Usable Security mit Endanwendern/Stakeholdern (N=10) (https://www.usecured.de/UseWP/wp-content/uploads/2016/02/USecureD-Anforderungsanalyse-Interviewergebnisse-V.1.pdf)
- **E 1.3d USecureD-Fragenkatalog Workshop**
  Fragenkatalog zur Erhebung von Anforderungen an Usable Security
  (https://www.usecured.de/UseWP/wp-content/uploads/2016/02/USecureD-Fragenkatalog-Workshop-V.1.pdf)

- **E 1.3e Ergebnisse der USecureD-Studie**
  Auswertung der Onlinestudie zu den Anforderungen an Usable Security und die daraus gewonnen Ergebnisse/Erkenntnisse (https://www.usecured.de/UseWP/wp-content/uploads/2015/04/USecureD-Anforderungsanalyse-Online-Studienergebnisse-V.1.pdf)
- **E 1.4 USecureD-Qualitätsmodell**
  Dokumentation eines ganzheitlichen Qualitätsverständnisses für den Bereich Usable Security (https://www.usecured.de/UseWP/wp-content/uploads/2015/04/E-1.4-USecureD-Qualit%C3%A4tsmodell-V.2.pdf)
- **USecureD-Anforderungsdokumente**
  Ergebnisse von 10 Einzelinterviews mit Stakeholdern/Nutzern aus vier Kundenunternehmen der HKBS und Ergebnisse von zwei Expertenworkshops mit den assoziierten Partnern Fraunhofer IESE und saar.is

Mit Ausnahme der Anforderungsdokumente sind diese Ergebnisse auf der Projektwebsite frei zugänglich. Wissenschaftliche Erkenntnisse und Ergebnisse dieses Arbeitspakets mündeten außerdem in Publikationen und Präsentationen, die als Ergebnisse des AP 5 aufgeführt sind.

6.2 Arbeitspaket 2: Entwicklung der USecureD-Toolbox

Laufzeit: August 2015 – Oktober 2016

Lead: HKBS

6.2.1 Ziele des Arbeitspakets

In diesem Arbeitspaket sollten Entwurfs- und Evaluierungswerkzeuge erarbeitet werden, die Softwareingenieure bzw. -entwickler und Qualitätsmanager in IKT-Herstellerunternehmen bei der Realisierung und Evaluierung von Anwendungssoftware mit dem Qualitätsmerkmal Usable Security unterstützen. Sämtliche entwickelte Werkzeuge sollten in einer Toolbox zusammengestellt und veröffentlicht werden.

Ziel von **AP 2.1 Entwicklung der Entwurfswerkzeuge** war es, Entwurfswerkzeuge zu entwickeln, die Softwarearchitekten und Entwickler bei der Auswahl und Umsetzung benutzerfreundlicher Sicherheitsfunktionen und -mechanismen im Kontext betrieblicher Anwendungssoftware unterstützen. Darauf aufbauend sollten in **AP 2.2 Anwendung der Entwurfswerkzeuge** die in AP 1.2 ermittelten Usability- und Sicherheitsanforderungen mehrerer Anwenderunternehmen der IKT-Branche mit Hilfe der in AP 2.1 entwickelten USecureD-Entwurfswerkzeuge in technische Implementierungen überführt werden. In **AP 2.3 Entwicklung der Evaluationsmethodik** sollte eine leichtgewichtige Evaluationsmethodik entwickelt werden, die kleine und mittlere IKT-Anbieter in die Lage versetzt, mit effizienten, praxistauglichen Werkzeugen selbständig im eigenen Kontext Usable-Security-Evaluationen von Softwareanwendungen durchzuführen. Darauf aufbauend sollten in **AP 2.4 Anwendung der Evaluationsmethodik** die in AP 2.2 entwickelten prototypischen Implementierungen mit Hilfe der in AP 2.3 ausgewählten bzw. entwickelten Evaluationswerkzeuge bewertet werden. Hierzu sollte eine Usable-Security-Evaluation durchgeführt werden, insbesondere mit den Endanwendern der IKT-Anwenderunternehmen, deren Anforderungen in AP 1.2 erhoben wurden.

6.2.2 Verwendung der Zuwendung

Arbeitspaket 2 umfasste die folgenden Aktivitäten:

AP 2.1 Entwicklung der Entwurfswerkzeuge

Entwicklung des USecureD-Patterntemplates

Für die Dokumentation der Usable-Security-Patterns wurde ein Beschreibungstemplate (siehe Anhang, Abbildung 15) entwickelt, mit dem sichergestellt werden sollte, dass alle erarbeiteten Usable-Security-Patterns in geeigneter und einheitlicher Form beschrieben sind und dass diese möglichst einfach auf unterschiedliche Geschäftsdomänen übertragen und nahtlos in beliebige Softwareentwicklungsprozesse integriert werden können. Zusätzlich zu bekannten Pattern-Attributen (Name, Kontext, Problem, Lösung usw.), mit denen grundlegende Informationen zum Pattern erfasst werden, wurden neue Attribute eingeführt (Abhängigkeiten, Beziehungen, Prinzipien, Use Cases, Check Listen, Entwicklungsrichtlinien, Tags, Log History); diese Attribute ermöglichten unter anderem eine Verknüpfung mit den entsprechenden Projektergebnissen, die ebenfalls in USecureD erarbeitet wurden.

Aufbau der USecureD-Patternsammlung

Für die Domäne Usable Security gab es zum Zeitpunkt des USecureD-Projektstarts keine Sammlung entsprechender Patterns. Basierend auf einer umfassenden Literaturrecherche des Konsortiums konnten insgesamt 47 Usable-Security-Patterns zusammengetragen werden. Diese englischsprachigen Patterns wurden auf Grundlage des zuvor erarbeiteten Patterns in ein einheitliches Format gebracht und außerdem ins Deutsche übertragen.

Durch eine umfassende Analyse der Patterns wurden Verknüpfungen und Abhängigkeiten der Patterns untereinander hergestellt. Dadurch wurde der Katalog zu einer sogenannten Mustersprache bzw. Pattern Language weiterentwickelt (siehe Abbildung 6). Besonders hervorzuheben ist daher das Attribut „Beziehungen“, wodurch diese Verknüpfungen beschrieben werden. Auf der USecureD-Plattform wurden diese Beziehungen als Links implementiert und in Form einer interaktiven Grafik visualisiert, wodurch eine schnelle Navigation zwischen Patterns, die in einer Beziehung zueinanderstehen, gewährleistet werden kann.

Im Rahmen der Analyse wurden den Patterns des Weiteren Prinzipien zugeordnet, wodurch in dem Attribut „Prinzipien“ direkt ersichtlich wird, welchen abstrakteren Zielen bzw. Grundsätzen das Pattern dient. Im Hinblick auf eine effektive Durchsuchbarkeit der Pattern-Datenbank wurden unter dem Attribut „Tag“ Schlagworte gesammelt, die dem jeweiligen Pattern zuzuordnen sind. Diese Schlagworte entstammen größtenteils aus dem USecureD-Qualitätsmodell. Damit wird gewährleistet, dass bei der Suche nach Patterns zur Verbesserung einzelner Merkmale des Qualitätsmodells passende Patterns in der Datenbank gefunden werden können. Darüber hinaus wurde eine „Log History“, also ein Feld zur Dokumentation von Protokollereignissen, hinzugefügt. In diesem Feld können vorgenommene Änderungen und Bearbeitungszeiten dokumentiert werden.

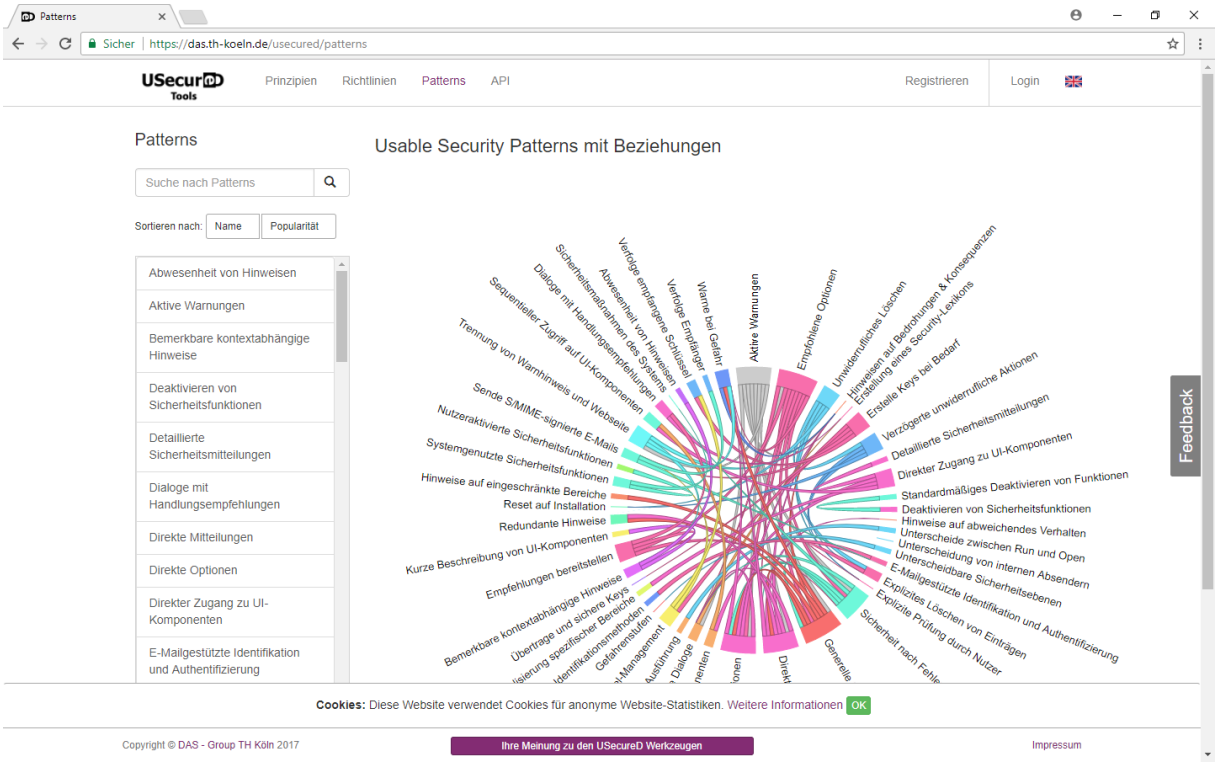


Abbildung 6: USecureD-Patternsammlung

Erarbeitung der USecureD-Entwicklungsrichtlinien

Um eine geeignete Beschreibungsvorlage zu entwickeln, wurden zunächst allgemeine Informationen zu Richtlinien recherchiert, insbesondere zu Usability Guidelines. Im nächsten Schritt wurden diverse Veröffentlichungen zu Guidelines bzw. frei zugängliche Guideline-Sammlungen untersucht, insbesondere hinsichtlich Aufbau und Strukturierung der Guidelines. Die Autoren bzw. Herausgeber dieser Guidelines waren Wissenschaftler, (Berufs-)Verbände, Organisationen (Regierungsbehörden, NGOs) und Software- bzw. Systemhersteller.

Thematisch können die untersuchten Guidelines unterschieden werden in einzelne Usable Security Guidelines bzw. Usable Security Guideline Sets, Arbeiten, die einzelne Guidelines vorstellen bzw. Hinweise zu Guidelines enthalten, allgemeine Richtlinien für die Gestaltung von Benutzeroberflächen, einzelne Usability Guidelines bzw. Usability-Guideline-Sammlungen, Usability-Heuristiken, Guidelines für Texte in Masken bzw. Meldungen, Arbeiten zur Fehlersicherheit bzw. Fehlertoleranz, Accessibility Guidelines, User Experience Guidelines, Trust Design Guidelines, Privacy Guidelines, Guidelines für die Erstellung von (Business) Websites bzw. Onlineshops, Guidelines für die Herstellung von Apps, einzelne Security Guidelines bzw. Security-Guideline-Sammlungen sowie Guidelines zum Umgang mit Passwörtern.

Im Rahmen der Sammlung und Konsolidierung dieser Guidelines (Strukturierung, Bilden von Clustern, Verschlagwortung) bildete sich eine Beschreibungsvorlage heraus, die als Deliverable dokumentiert wurde. Diese Vorlage wurde von den Projektpartnern unter Forschungs- und Praxisgesichtspunkten abgestimmt und anschließend für die Erstellung bzw. Dokumentation der USecureD-Richtlinien genutzt. Durch die Dokumentation der USecureD-Richtlinien wurde sichergestellt, dass das entwickelte Guideline-Template für die Zwecke im USecureD-Projekt geeignet ist. Bei der Erstellung der USecureD-Richtlinien wurden in vielen Fällen Guidelines verschiedener Autoren zusammengeführt, damit eine möglichst gut handhabbare Sammlung von Richtlinien entsteht, über die sich Softwareingenieur bzw. -entwickler schnell einen Überblick verschaffen können (siehe Abbildung 7). Insgesamt wurden 33 Richtlinien definiert, die auf Deutsch und auf Englisch vorliegen.

Abbildung 7: USecureD-Entwicklungsrichtlinien

Erarbeitung der USecureD-Prinzipien

Neben den beschriebenen Patterns und Richtlinien wurden im Rahmen des Projekts zusätzlich insgesamt 23 USecureD-Prinzipien definiert und dokumentiert (siehe Abbildung 8). Prinzipien als abstrakteste Entwurfswerkzeuge basieren auf früheren Erfahrungen, Designs oder wissenschaftlichen Erkenntnissen und sind allgemein für viele Anwendungsbereiche gültig. Neben Softwarearchitekten und -entwicklern unterstützen die USecureD-Prinzipien auch Käufer von Softwareprodukten beim Definieren von Anforderungen und Kriterien für ihre konkreten Anwendungsfälle.

Analog zur Vorgehensweise bei den Patterns und Richtlinien wurde ein Beschreibungstemplate zur einheitlichen Dokumentation der Usable-Security-Principles erstellt. Diese Vorlage ermöglicht das Beschreiben von Prinzipien verschiedener Autoren in einem gut leserlichen und einheitlichen Format. Dies ist Voraussetzung für eine übersichtliche Struktur des Principle-Katalogs, welcher ebenfalls Teil der USecureD-Plattform ist. Zur Entwicklung des Principle-Templates und des Principle-Katalogs wurde zunächst durch eine umfassende Literaturrecherche der derzeitige Stand der Forschung im Bereich

Usable-Security-Principles erfasst. Existierende Prinzipien verschiedener Autoren wurden gesammelt und analysiert.

Anschließend wurde untersucht, welche wiederkehrenden Merkmale in den von den Autoren beschriebenen Prinzipien vorkommen. Ausschlaggebend für die meisten sind dabei die Merkmale „Intention“ und „Motivation“. Diese Attribute beschreiben die Absicht bzw. den Zweck, den das Prinzip erfüllen soll, und dessen motivierende Umstände. Die extrahierten Merkmale wurden aufgrund der Anforderungen und Gegebenheiten des Projekts durch weitere Eigenschaften ergänzt. Die erweiterten Merkmale sind: „Synonyme“, unter denen das Prinzip noch bekannt ist, „Beispiele“ bei denen das Prinzip Anwendung findet, „Schlagworte“ zur Verbesserung der Durchsuchbarkeit der Prinzipien-Datenbank, und Angaben zu den Quellen. Durch die Verknüpfung der Projektergebnisse ist zudem das Merkmal „Richtlinien“ hinzugekommen. In diesem Feld werden Verknüpfungen zu USecureD-Richtlinien dokumentiert, welche bei der Umsetzung des Prinzips helfen können. Darüber hinaus wurde eine „Log History“, also ein Feld zur Dokumentation von Protokollereignissen hinzugefügt.

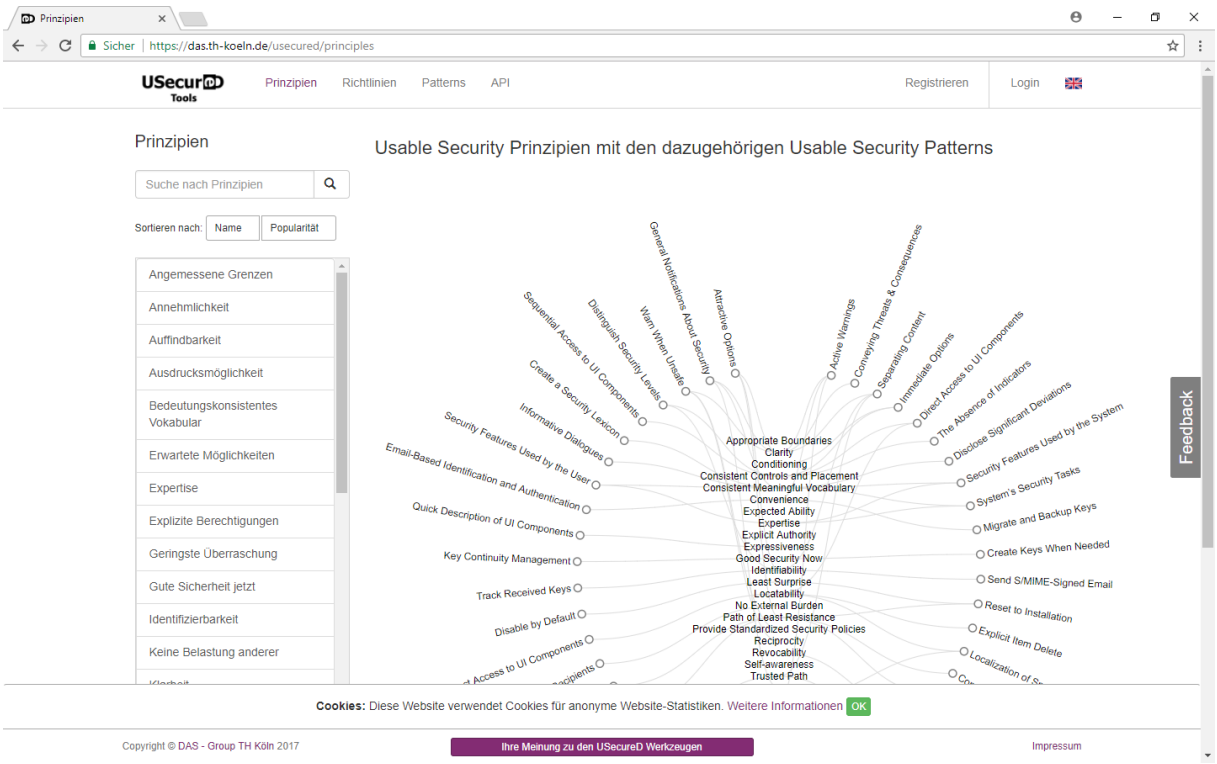


Abbildung 8: USecureD-Prinzipien

AP 2.2 Anwendung der Entwurfswerkzeuge

Die Entwurfs- und Gestaltungswerkzeuge wurden zur Projektlaufzeit in diversen Softwareentwicklungsprojekten angewendet, sowohl durch die Projektpartner als auch durch interessierte Firmen, die Kontakt mit dem Konsortium aufgenommen haben. Angewendet wurden je nach Projektkontext und Aufgabenstellung verschiedene Werkzeuge aller Werkzeugarten (Prinzipien, Richtlinien und Patterns). Die Erfahrungen, die die Entwickler der Projektpartner bei der Anwendung der Werkzeuge gemacht haben, wurden von in Form von Entwicklertagebüchern dokumentiert.

AP 2.3 Entwicklung der Evaluationsmethodik

Identifikation relevanter Qualitätskriterien

Ausgangspunkt für die Entwicklung des USecureD-Evaluationskonzepts war die Identifikation relevanter Qualitätskriterien. Die Bewertung von Prototypen bzw. Softwaresystemen parallel zum Entwicklungsprozess trägt maßgeblich zur Qualität eines Produktes bei und reduziert durch frühes Erkennen von Fehlern und Schwachstellen die gesamte Entwicklungszeit. Dadurch werden insbesondere verspätete Auslieferungen und Nachbesserungen vermieden, welche zusätzlich Geld und Ressourcen kosten. Um dies zu gewährleisten, wurden zunächst Qualitätskriterien identifiziert, die für den Themenbereich Usable Security relevant sind. Dies waren – neben einschlägigen IT-Security-Kriterien – insbesondere Effizienz und Effektivität bei der Bedienung des Softwareprodukts, die intuitive Nutzung des Produkts,

die wahrgenommene pragmatische bzw. hedonische Qualität des Softwareprodukts, die Attraktivität des Softwareprodukts sowie die Erfüllung psychologischer Grundbedürfnisse nach Autonomie, Kompetenz und Sicherheit.

Zielstellung innerhalb des USecureD-Projekts war es, eine leichtgewichtige Evaluationsmethodik zu entwickeln, die auf alle Entwicklungsstadien einer Anwendungssoftware angewandt werden kann und die aussagekräftige Resultate in Bezug auf das Qualitätsmerkmal Usable Security liefert. „Leichtgewichtig“ sollte in diesem Zusammenhang bedeuten, dass der Methodeneinsatz je nach Evaluationsfall an die Erfordernisse des konkreten Projekts angepasst werden kann, um so einen optimalen Einsatz der personellen und zeitlichen Ressourcen zu ermöglichen. Anhand der identifizierten Kriterien kann im Rahmen einer Produktbewertung bzw. Evaluation entschieden werden, welche dieser Kriterien im Einzelfall überprüft werden sollen bzw. bei der Evaluation im Vordergrund stehen sollen.

Auswahl bzw. Definition der USecureD-Metriken

Aufbauend auf den identifizierten Qualitätskriterien wurde im Rahmen einer Literaturrecherche ermittelt, welche konkreten Metriken bzw. Indikatoren genutzt werden können, um diese Kriterien zu überprüfen. Herangezogen wurden hierbei insbesondere die ISO 9241 (für den Bereich Usability), ein Modell von Kainda et al. (für den Bereich Sicherheit), verschiedene Arbeiten von Hassenzahl (für den Bereich User Experience) und eine Arbeit von Ullrich & Diefenbach (für den Bereich intuitive Nutzung). Die identifizierten Metriken und Indikatoren können Tabelle 1: Übersicht Empirische EvaluationTabelle 1 entnommen werden.

Tabelle 1: Übersicht Empirische Evaluation

Merkmal	**Kriterium**	**Metrik/Indikator**	**Messverfahren/ Instrument**
Usability	Effektivität – Vollständigkeit	erfolgreiche Bearbeitung	Beobachtung/Erfassung durch Versuchsleiter, dreistufige Effektivitätsskala
Usability	Effektivität – Genauigkeit	erfolgreiche Bearbeitung	Beobachtung/Erfassung durch Versuchsleiter, vierstufige Effektivitätsskala
Usability	Effizienz – Erfüllungszeit	benötigte Zeit pro Aufgabe	Zeitmessung durch Versuchsleiter
Usability	Effizienz – Mentale Beanspruchung	Mühelosigkeit	INTUI
Usability	Zufriedenheit	Emotionen des Probanden, Metriken für Merkmale User Experience (s. unten)	Beobachtung durch Versuchsleiter, Messverfahren/ Instrumente für Merkmale User Experience (s. unten)
Security	Aufmerksamkeit	Fehler durch fehlende Aufmerksamkeit	Beobachtung, Befragung durch Versuchsleiter
Security	Wachsamkeit	Fehler durch fehlende Wachsamkeit	Beobachtung, Befragung durch Versuchsleiter
Security	Konditionierung	Fehler durch Konditionierung	Beobachtung, Befragung durch Versuchsleiter

Security	Motivation	Vorteile durch Benutzung von Sicherheitsfunktionen, (Stör-)Anfälligkeit, Barrieren, Schwierigkeiten des Nutzers	Beobachtung, Befragung durch Versuchsleiter
Security	Einprägsamkeit	Erinnerung des Probanden	Beobachtung, Befragung durch Versuchsleiter
Security	Vorwissen/Erfahrung	erfolgreiche Bearbeitung, Übereinstimmung zwischen Produkt und mentalem Modell des Nutzers	Beobachtung, Befragung durch Versuchsleiter
User Experience	Pragmatische Qualität	4 Fragebogen-Items	AttrakDiff mini
User Experience	Hedonische Qualität – Identität	2 Fragebogen-Items	AttrakDiff mini
User Experience	Hedonische Qualität – Stimulation	2 Fragebogen-Items	AttrakDiff mini
User Experience	Attraktivität	2 Fragebogen-Items	AttrakDiff mini
User Experience	Positiver/negativer Affekt	10 Fragebogen-Items (5 positiver Affekt, 5 negativer Affekt)	PANAS (Kurzversion)
User Experience	Erfüllung der psychologischen Grundbedürfnisse nach „Autonomie“, „Kompetenz“ und „Sicherheit“	9 Fragebogen-Items (je 3 pro Bedürfnis)	Bedürfnisskalen
Intuitive Nutzung	Mühelosigkeit	5 Fragebogen-Items	INTUI
Intuitive Nutzung	Bauchgefühl	4 Fragebogen-Items	INTUI
Intuitive Nutzung	Magisches Erleben	4 Fragebogen-Items	INTUI
Intuitive Nutzung	Verbalisierungsfähigkeit	3 Fragebogen-Items	INTUI
Intuitive Nutzung	Globales Intuitivitätsurteil	1 Fragebogen-Item	INTUI

Auswahl der USecureD-Evaluationswerkzeuge und Entwicklung von Arbeitshilfen

Basierend auf den definierten USecureD-Metriken wurde im nächsten Schritt recherchiert, welche Methoden bzw. Werkzeuge zur Verfügung stehen, die für den jeweils aktuellen Entwicklungsstand eines Projekts erfahrungsgemäß gute Resultate erzielen. Der Fokus lag hierbei auf leicht anwendbaren und validierten Messwerkzeugen und Arbeitshilfen, aus denen insbesondere kleine und mittlere Softwarehersteller auswählen können. Denn gerade diesen Herstellern stehen bei der Evaluation oft nur eingeschränkte Personalressourcen, Zeitaufwände und Geldmittel zur Verfügung.

Die Auswahl geeigneter Messverfahren fiel zugunsten der fragebogenbasierten Werkzeuge AttrakDiff mini, PANAS, INTUI sowie dreier Bedürfnisskalen (Autonomie, Kompetenz und Sicherheit). Sämtliche Items dieser wissenschaftlich gut validierten Fragebögen wurden in Form eines neuen zweiseitigen Fragebogens zusammengefasst. Zu sämtlichen Abschnitten des Fragebogens gibt es Auswertungshilfen

und semiautomatische Berichtsinstrumente, die im Rahmen des USecureD-Projekts genutzt werden konnten. Alle Qualitätskriterien, die durch diese Werkzeuge nicht abgefragt werden, können im Rahmen eines Versuchs durch einfache Maßnahmen wie z. B. Zeitmessung durch den Versuchsleiter oder durch Befragung und Beobachtung des Probanden überprüft werden. Die empfohlenen Messverfahren und Instrumente können ebenfalls Tabelle 1 entnommen werden.

Erstellung des USecureD-Toolbox-Handbuchs

Bei der Evaluierung eines Prototyps bzw. einer Software kann unterschieden werden zwischen einer analytischen Evaluation, bei der die Bewertung durch einen oder mehrere interne Mitarbeiter des Herstellers erfolgt, und einer empirischen Evaluation, bei der die Bewertung in der Regel durch mehrere Endnutzer oder externe Probanden erfolgt. Im veröffentlichten USecureD-Toolbox-Handbuch wurden für beide Anwendungsbereiche die Rahmenbedingungen beschrieben und es wurden entsprechende Methoden bzw. Werkzeuge vorgestellt. Die Anwendbarkeit der vorgestellten Werkzeuge unterscheidet sich vorwiegend dadurch, in welcher Entwicklungsstufe eines Produktes diese eingesetzt werden können und welche Zeit die Evaluation in Anspruch nimmt.

AP 2.4 Anwendung der Evaluationsmethodik

Die entwickelte Evaluationsmethodik wurde von den Projektpartnern in diversen Softwareentwicklungsprojekten angewendet. Insgesamt wurden Evaluationen mit vier Anwendungsfirmen durchgeführt, für die im Rahmen von AP 2.2 kleinere Entwicklungsprojekte durchgeführt wurden. Probanden waren jeweils einzelne Anwender in diesen Unternehmen, mit denen separat Evaluationen am eigenen Arbeitsplatz durchgeführt wurden. Hierbei haben die Probanden jeweils mehrere vordefinierte Aufgaben gelöst, wobei sie vom Versuchsleiter beobachtet wurden und die Bearbeitungszeit gemessen wurde. Anschließend haben die Probanden die Interaktion mit dem System (bzw. mit den Sicherheitsmechanismen des Systems) anhand des oben beschriebenen Fragenbogens bewertet. Die Auswertung der Evaluationsergebnisse ergab ein Bild, das auf positive Effekte schließen lässt, die sich durch die Nutzung der Entwurfs- und Gestaltungswerkzeuge erzielen lassen, insbesondere hinsichtlich der intuitiven Nutzung der entwickelten Produkte bzw. ihrer Sicherheitsmechanismen, des negativen Affekts (keine feststellbare negative Stimmungslage) und der wahrgenommenen pragmatischen Qualität der Produkte.

6.2.3 Ergebnisse

Im Rahmen von Arbeitspaket 2 haben die Partner folgende Ergebnisse erarbeitet:

- **E 2.1a USecureD-Pattern-Template**
  Beschreibungstemplate zur einheitlichen Dokumentation von Gestaltungsmustern im Bereich Usable Security https://www.usecured.de/UseWP/wp-content/uploads/2016/06/E-2.1-USecureD-Pattern-Template-V.1.1.pdf)
- **E 2.1b USecureD-Principle-Template**
  Beschreibungstemplate zur einheitlichen Dokumentation von Prinzipien im Bereich Usable Security (https://www.usecured.de/UseWP/wp-content/uploads/2016/06/E-2.1-USecureD-Principle-Template-V.1.1.pdf)
- **E 2.1c USecureD-Guideline-Template**
  Beschreibungstemplate zur einheitlichen Dokumentation von Entwicklungsrichtlinien im Bereich Usable Security (https://www.usecured.de/UseWP/wp-content/uploads/2015/04/E-2.1c-USecureD-Guideline-Template-V.1.pdf)
- **E 2.2a USecureD-Patternsammlung**
  Sammlung von bewährten, wiederverwendbaren und übertragbaren Gestaltungsmustern mit dem Qualitätsmerkmal Usable Security (https://das.th-koeln.de/usecured/patterns)
- **E 2.2b USecureD-Prinzipien**
  Sammlung von Prinzipien verschiedener Autoren für den Bereich Usable Security (https://das.th-koeln.de/usecured/principles)
- **E 2.3 USecureD-Entwicklungsrichtlinien** und
  E 2.4 USecureD-Guideline-Tool
  Entwicklungsrichtlinien, die das Qualitätsmerkmal Usable Security fördern und auf verschiedene Einsatzgebiete, Nutzungskontexte und Sicherheitsbedürfnisse abgestimmt sind (https://das.th-koeln.de/usecured/guidelines)
- **E 2.7 Evaluationsmethodik und -Handbuch** inkl.
  E 2.5 USecureD-Metriken und
  E 2.6 Evaluationswerkzeuge/Arbeitshilfen
  Variables Evaluierungskonzept inkl. Werkzeugen zur Bewertung des Qualitätsmerkmals

Usable Security (https://www.usecured.de/UseWP/wp-content/uploads/2015/04/E-2.7-Evaluationsmethodik-und-handbuch.pdf)

- **Prototypische Implementierungen** von USecureD-Konzepten
- **Empirische Qualitätsüberprüfung** der prototypischen Implementierungen

Mit Ausnahme der prototypischen Implementierungen und der Qualitätsüberprüfungen dieser Implementierungen sind die Ergebnisse dieses Arbeitspakets auf der Projektwebsite frei zugänglich. Wissenschaftliche Erkenntnisse und Ergebnisse des Arbeitspakets mündeten außerdem in Publikationen und Präsentationen, die als Ergebnisse des AP 5 aufgeführt sind.

6.3 Arbeitspaket 3: USecureD-Plattform

Laufzeit: November 2015 – Januar 2017

Lead: TH Köln

6.3.1 Ziele des Arbeitspakets

In diesem Arbeitspaket sollten alle Ergebnisse, die für die Zielgruppe IKT-Hersteller bestimmt sind, in einer zentralen Plattform gebündelt werden. Hierdurch sollte insbesondere mittelständischen Softwareunternehmen eine günstige Möglichkeit geboten werden, fundierte und umfangreiche Evaluationen ihrer Softwareprodukte durchzuführen. Hersteller sollten auf dieser Plattform nach Möglichkeit ihre Produkte registrieren und in konkreten Usable-Security-Tests bewerten lassen können – entweder durch eigene Nutzer oder durch externe Probanden, zu denen über die Plattform Kontakt hergestellt werden kann.

Ziel von **AP 3.1 Konzeptionierung der Plattform** war es, das fachliche und technische Konzept für den Aufbau und die Integration der Plattform zu liefern. Hierbei sollte auf den Ergebnissen der Teilarbeitspakete 2.1 und 2.3 aufgebaut werden, die nach ihrer Fertigstellung in die Plattform integriert werden sollten. Zudem sollten Werkzeuge konzipiert werden, die Testleiter beim Design individueller Tests (z. B. Editoren zum Erstellen von Testaufgaben und Fragebögen), bei der Durchführung und der Auswertung von Tests sowie bei der Interpretation der Testergebnisse unterstützen. Darauf aufbauend sollte in **AP 3.2 Aufbau und Integration der Plattform** das in AP 3.1 entwickelte fachliche und technische Konzept der USecureD-Plattform in eine technische Implementierung überführt werden; dies sollte den Aufbau der Plattform selbst und die Entwicklung von Werkzeugen zur Fragebogenkonstruktion, Datenerhebung und Evaluationsauswertung umfassen, die als Komponenten in die USecureD-Plattform integriert sein sollten. Ferner wurde angestrebt, in diesem Teilarbeitspaket sämtliche USecureD-Werkzeuge, die in AP 2.1 bzw. AP 2.3 für die Zielgruppe IKT-Hersteller entwickelt wurden, in die USecureD-Plattform zu integrieren. Ziel von **AP 3.3 Evaluierung der Plattform** war es, eine Qualitätsüberprüfung der in AP 3.2 aufgebauten USecureD-Plattform durchzuführen. Durch diese Studie, die mit ausgewählten Stakeholdern von IKT-Herstellerunternehmen sowie mit Empirie- bzw. Usability-und Usable-Security-Test-Experten durchgeführt werden sollte, sollte insbesondere die Funktionsweise aller in AP 3.2 entwickelten und integrierten Werkzeuge sichergestellt werden.

6.3.2 Verwendung der Zuwendung

Arbeitspaket 3 umfasste die folgenden Aktivitäten:

AP 3.1 Konzeptionierung der Plattform

Die USecureD-Plattform sollte auf den oben genannten Projektergebnissen aufbauen und diese in einer zentralen Umgebung bündeln. Ergänzend zu architektonischen Vorüberlegungen wurden von der TH Köln als Grundlage für die Konzeption der Plattform zunächst vergleichbare webbasierte Serviceplattformen, insbesondere (Crowd-)Testing-Plattformen und Usability-Testplattformen, recherchiert. Die Ergebnisse wurden in einer Feature-Wishlist mit insgesamt 14 Features aufbereitet und mit der HKBS abgestimmt. Zur besseren Verbreitung der USecureD-Plattform wurden von der HKBS Subdomains für die Plattform eingerichtet (platform.usecured.de bzw. plattform.usecured.de).

AP 3.2 Aufbau und Integration der Plattform

Um die USecureD-Plattform aufzubauen, wurde zunächst eine Laufzeitumgebung (Server) eingerichtet und es wurde ein Repository für die USecureD-Principles, -Patterns und -Guidelines aufgebaut. Für die technische Umsetzung war es notwendig die Plattform auf den Servern der TH Köln aufzusetzen. Zur

Aufbereitung der Plattforminhalte wurde ein Markdown-basiertes Datenformat mit templatebasierter HTML-Generierung genutzt.

Die Nutzer der USecureD-Plattform finden eine vollständige Sammlung sämtlicher erarbeiteten Usable Security Principles, Patterns und Guidelines vor, die in einheitlicher Weise dokumentiert sind. Für das Benutzerfrontend wurden ein entsprechender Navigationsmechanismus, ein Suchinterface (Volltextsuche) und diverse Sortierfunktionen (alphabetisch, nach Popularität) integriert. Sämtliche erstellten Principles, Guidelines und Patterns wurden in die Plattform integriert, inklusive weiterführender Informationen und aller verwendeten Quellen (im BibTeX-Funktion). Auf diese Weise schlägt die USecureD-Plattform eine Brücke zwischen teils theoretischen Erkenntnissen aus der Wissenschaft und Forschung und der Anwendung dieses Wissens in der Praxis.

Wichtige Features der Benutzeroberfläche sind die interaktiven Grafiken (vgl. Abbildungen 6-8), die beispielsweise die USecureD-Patternlanguage visualisieren. Hierfür wurden sämtliche Wissensinhalte gesichtet und es wurde analysiert, welche Prinzipien, Richtlinien und Patterns thematisch miteinander in Verbindung stehen. Um solche Verknüpfungen zu dokumentieren, wurden entsprechende Attribute in den Beschreibungstemplates genutzt. Auf diese Weise können unmittelbar weitere Prinzipien, Richtlinien und Patterns aufgefunden werden, die für die aktuelle Problemstellung geeignet sind. Wählt der Besucher der USecureD-Plattform beispielsweise die Prinzipien als Einstiegspunkt, so steht ihm eine durchgängige Werkzeugkette zur Verfügung, die ihm bei jedem der beschriebenen Prinzipien passende Richtlinien empfiehlt. Softwareentwickler, die in der direkten Verantwortung stehen, Sicherheitsfeatures zu implementieren, können dadurch gleich mehrere verschiedenartige Entwicklungswerkzeuge identifizieren, die Lösungen für die praktische Umsetzung bieten und einfach angewendet werden können.

Von der TH Köln wurde eine Registrierfunktion eingerichtet, damit sich Nutzer, die nicht Teil des Konsortiums sind, an der Plattform anmelden können. Hierdurch wird der Entwickler-Community die Möglichkeit gegeben, bereits eingepflegte Wissensinhalte zu kommentieren (z. B. eigene Erfahrungen oder Optimierungsvorschläge mitzuteilen) und auch selbst neue Principles, Patterns und Guidelines hochzuladen und zur Diskussion zu stellen. Prinzipiell kann die Plattform jedoch auch anonym genutzt werden. Das über die Plattform gesammelte Feedback (z. B. Anmerkungen oder Fehlerberichte) wurde intern diskutiert und gegebenenfalls in Anpassungen an der Plattform umgesetzt. Insbesondere wurde das Feedback der HKBS-Entwickler als Anwender der USecureD-Plattform an die TH Köln zurückgespiegelt. Zur Sicherstellung der Wartbarkeit/Erweiterbarkeit wurde die (Weiter-)Entwicklung der Plattform entsprechend dokumentiert.

API zum Abruf der Werkzeuge

Aufgrund der Anregung von Plattformbenutzern wurde die Funktionalität der USecureD-Plattform nach Rücksprache mit dem Projektträger um eine API zum maschinellen Abruf der Werkzeuge erweitert. Ein programmatischer Zugriff auf die Werkzeuge über eine REST-basierende API ermöglicht es Unternehmen, die Werkzeuge in eigene Prozesse zu integrieren oder für Evaluationen im eigenen Unternehmenskontext heranzuziehen. Als erster Schritt wurde das Datenbeschreibungsformat JSON (JavaScript Object Notation) als zusätzliche Repräsentation der Werkzeuge – neben HTML – festgelegt. Mit JSON können Daten leichtgewichtig beschrieben werden, wodurch dieses textbasierte Datenformat insgesamt eine weite Verbreitung gefunden hat. Ein Teil des Quellcodes der USecureD-Plattform wurde umstrukturiert und erweitert, sodass bei der Generierung der Werkzeuge neben der HTML-Repräsentation zusätzlich eine dazugehörige JSON-Repräsentation erstellt wird. Die JSON-Repräsentation enthält alle Informationen und Verknüpfungen, welche auch in den Beschreibungsvorlagen der Werkzeuge und auf der Plattform in HTML zu sehen sind (vom Browser gerendert). Darüber hinaus werden Listen aller verfügbaren Prinzipien, Richtlinien und Patterns generiert (ebenfalls im JSON-Format), in welchen Namen und Verlinkungen zu den einzelnen Werkzeugen enthalten sind. Wie für REST-basierende Web APIs üblich wird über den Accept-Header bestimmt, welche Repräsentation eines Werkzeugs zurückgeliefert wird (z. B. Accept: application/json für JSON). Da alle Werkzeuge in Englisch und Deutsch verfügbar sind, kann über den Accept-Language-Header zudem die Sprache des angeforderten Werkzeugs eingestellt werden.

Nutzer der Plattform können eine Service-Beschreibung einsehen, die mit Hilfe des API-Beschreibungs-Frameworks Swagger erstellt wurde, welches in Entwicklerkreisen viel Verwendung findet. Diese Beschreibung kann in Programme wie Postman oder den Swagger Editor importiert werden, wodurch Entwickler einen schnellen Überblick über die Funktionalität der API erhalten und bereits mit Hilfe der Programmoberfläche erste API-Aufrufe tätigen können. Außerdem ermöglichen diese Programme die automatisierte Erstellung von Programmcode zum Abruf der Werkzeuge in verschiedenen Programmiersprachen. Somit bekommen Unternehmen die Möglichkeit, die im USecureD-Projekt erarbeiteten Werkzeuge in eigene Entwicklungs- oder Evaluierungsprozesse zu integrieren und z. B. für Qualitätserhebungen oder Assessments zu verwenden.

Umfrage- und Auswertungstools

In einer zweiten Entwicklungsphase wurden Werkzeuge konzipiert, implementiert und integriert, die Herstellerfirmen beim Design individueller Tests unterstützen. Die entsprechenden Werkzeuge zur Fragebogenkonstruktion, Datenerhebung und Evaluationsauswertung umfassen a) einen Fragebogen-Editor zum Erstellen von Tests, Aufgaben und Fragebögen, b) ein Umfragetool zur Unterstützung bei der Testdurchführung und Datenerhebung sowie c) ein Auswertungstool, das die Evaluationsauswertung und die Ergebnisinterpretation unterstützt. Zudem wurden die in AP 4.1 entwickelten Checklisten in die USecureD-Plattform integriert. Durch die Bündelung all dieser Werkzeuge bietet die Plattform insbesondere mittelständischen Softwareunternehmen eine günstige Möglichkeit, um fundierte und umfangreiche Evaluationen von Softwareprodukten durchzuführen. Hersteller können ihre Produkte registrieren und in konkreten Usable-Security-Tests bewerten lassen – entweder durch eigene Nutzer oder durch externe Probanden, zu denen über die Plattform Kontakt hergestellt werden kann. Die entsprechenden Werkzeuge bzw. Services sind nur für registrierte Nutzer zugänglich.

AP 3.3 Evaluierung der Plattform

Um die Funktionalität und Gebrauchstauglichkeit der entwickelten Werkzeuge zu überprüfen, wurde die USecureD-Plattform sowohl intern (im Rahmen verschiedener Probedurchläufe) als auch extern evaluiert. Hierdurch war es möglich, auf Grundlage des Nutzerfeedbacks Verbesserungen umzusetzen und so die Funktionalität und Gebrauchstauglichkeit der Plattform bzw. der integrierten Werkzeuge noch während der Projektlaufzeit iterativ zu verbessern.

6.3.3 Ergebnisse

Im Rahmen von Arbeitspaket 3 haben die Partner folgende Ergebnisse erarbeitet:

- **E 3 API der USecureD-Tools**
  Beschreibung der entwickelten Datenformate, exemplarisches JSON-Dokument und API-Spezifikation (https://www.usecured.de/UseWP/wp-content/uploads/2015/04/E-3-API-der-USecureD-Tools-V.1.0.pdf, https://das.th-koeln.de/usecured/assets/api/swagger.json)
- **E 3.1 USecureD-Plattform** inklusive
- **E 3.2 USecureD-Fragebogeneditor**
- **E 3.3 USecureD-Umfragetool**
- **E 3.4 USecureD- Auswertungstool**
  Zentrale Plattform mit den Entwurfs- Gestaltungs- und Evaluationswerkzeugen des USecureD-Projekts (https://das.th-koeln.de/usecured)
- **Spezifikation und Testkonzept der USecureD-Plattform**
- **Empirische Qualitätsüberprüfung der USecureD-Plattform**

Wissenschaftliche Erkenntnisse und Ergebnisse dieses Arbeitspakets mündeten in Publikationen und Präsentationen, die als Ergebnisse des AP 5 aufgeführt sind.

6.4 Arbeitspaket 4: USecureD-Entscheidungshilfen

Laufzeit: August 2016 – April 2017

Lead: HKBS

6.4.1 Ziele des Arbeitspakets

In diesem Arbeitspaket sollten Entscheidungshilfen für Anwenderunternehmen der IKT-Branche entwickelt werden. Durch diese Entscheidungshilfen sollte zum einen die Nachfrage nach Produkten mit dem Qualitätsmerkmal Usable Security verstärkt werden und zum anderen sollte potentiellen Käufern eine Orientierung im Softwaremarkt geboten werden und eine einfache und zielgerichtete Auswahl und Evaluation von geeigneten E-Business-Anwendungen ermöglicht werden.

Ziel von **AP 4.1 Checklisten und Auswahlwerkzeug** war es, Checklisten und ein Auswahlwerkzeug zu entwickeln. Beides sollte Anwenderunternehmen der IKT-Branche bei einer objektiven Auswahl und Evaluierung bedarfsgerechter Softwareprodukte unterstützen. Zugleich sollten die Unternehmen mit dem Auswahlwerkzeug in die Lage versetzt werden, ihre Produktnachfrage konkreter gegenüber IKT-Herstellern zu artikulieren. Checklisten und Auswahlwerkzeug sollten so konzipiert werden, dass sie auch ohne Spezialkenntnisse für eine einfache, zielgerichtete Produktevaluation herangezogen werden können. Ziel von **AP 4.2 USecureD-Demonstrator** war es, auf Grundlage der Implementierungen aus

AP 2.4 und der Evaluationsergebnisse aus AP 2.4 einen Demonstrator zu entwickeln, der vom Geschäftswissen und den Prozessen der prototypischen Implementierungen abstrahiert ist. Dieser Demonstrator sollte der weiteren Verbreitung des USecureD-Projektes bei Messen, Konferenzen und ähnlichen Veranstaltungen dienen; insbesondere sollte er kleine und mittlere Anwenderunternehmen zum Einsatz von IKT-Produkten mit dem Merkmal Usable Security motivieren. Es wurde angestrebt, mit dem Demonstrator Usable-Security-Konzepte „zum Anfassen“ zu bieten, mit denen potentielle Anwender die Tragkraft ihrer Entscheidungen besser einschätzen können.

6.4.2 Verwendung der Zuwendung

Arbeitspaket 4 umfasste die folgenden Aktivitäten:

AP 4.1 Checklisten und Auswahlwerkzeug

Erarbeiten der USecureD-Checklisten

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 und Patterns. 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: Benutzeroberfläche und Layout, Terminologie, Aufgabenorientierung und mentale Belastung, Steuerbarkeit, Erlernbarkeit und Hilfe, Fehlerprävention und Fehlerbehandlung, Systemhinweise und -feedback, Sicherheitswarnungen, E-Mails und Datenübertragung, Verschlüsselung und Signatur, Zugangs- und Zugriffskontrolle, Datenschutz und Datenlöschung, Formulare sowie Systementwicklung.

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

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

Entwicklung des USecureD-Auswahlwerkzeugs

Als technische Implementierung wurden die USecureD-Checklisten ebenfalls in die USecureD-Plattform integriert. Im Sinne eines Auswahlwerkzeugs kann der Anwender hier individuelle Checklisten generieren, die auf unterschiedliche Einsatzgebiete, Nutzungskontexte, Sicherheitsbedürfnisse und rechtliche Anforderungen abgestimmt sind.

AP 4.2 USecureD-Demonstrator

Um Anwender stärker für das Thema Usable Security zu sensibilisieren, haben die Partner einen webbasierten Demonstrator entwickelt, der die USecureD-Methoden und -Konzepte visualisiert und begreifbar macht. Das Frontend des Demonstrators setzt auf dem responsiven CSS-Framework Bootstrap auf und arbeitet mit jQuery als Javascript-Bibliothek. Neben Plugins wie Bootstrap-Datepicker und ProgressStep wurden bei der Implementierung diverse Bibliotheken für Graphics und Cliparts genutzt, z. B. Glyphicons, Flaticon und PublicDomainVectors.

Nach dem Starten des Demonstrators wird der Benutzer Schritt für Schritt durch mehrere sicherheitsrelevante Anwendungsfälle geführt. Anhand von Infotexten wird ihm hierbei die Bedienung des Demonstrators erläutert, insbesondere werden ihm die zugrundeliegenden Usable-Security-Konzepte erklärt. Beim Durchspielen der Anwendungsfälle erhält der Benutzer jeweils Informationen über die möglichen Folgen und die Tragweite seiner Entscheidungen, z. B. wenn er die E-Mail-Verschlüsselung und -Signatur im Demonstrator aktiviert oder deaktiviert. Bei Bedarf kann er weiterführende Informationen zu

den einzelnen USecureD-Werkzeugen abrufen, die in einem Anwendungsfall bzw. Bedienschritt angewendet wurden; diese sind jeweils in den Infotexten verlinkt.

Nutzerfeedback, das über die integrierte Feedback-Funktion des Demonstrators erhoben wurde, wurde im weiteren Projektverlauf eingearbeitet.

6.4.3 Ergebnisse

Im Rahmen von Arbeitspaket 4 haben die Partner folgende Ergebnisse erarbeitet:

- **E 4.1 USecureD-Checklisten**
  Checklisten für Anwenderunternehmen zur Auswahl von Softwareprodukten mit dem Qualitätsmerkmal Usable Security (https://www.usecured.de/UseWP/wp-content/uploads/2017/03/E-4.1-USecureD-Checklisten.pdf)
- **E 4.2 USecureD-Auswahlwerkzeug**
- **E 4.3 USecureD-Demonstrator inkl.**
  E 4.4 Begleitfaden zum USecureD-Demonstrator
  Webbasierter Demonstrator, der ausgewählte USecureD-Konzepte und Patterns in einer prototypischen Anwendung visualisiert (inkl. Erläuterungen) (https://www.usecured.de/Demonstrator/)

Wissenschaftliche Erkenntnisse und Ergebnisse dieses Arbeitspakets mündeten in Publikationen und Präsentationen, die als Ergebnisse des AP 5 aufgeführt sind.

6.5 Arbeitspaket 5: Wissenstransfer und Awareness

Laufzeit: Mai 2015 – April 2017

Lead: TH Köln

6.5.1 Ziele des Arbeitspakets

Mit diesem Arbeitspaket sollten die (Public) Awareness und die Sensibilisierung in Bezug auf das Thema Usable Security erhöht werden; dies sollte insbesondere dazu dienen, kleine und mittlere Anwenderunternehmen zum Einsatz von IKT-Produkten mit dem Merkmal Usable Security zu motivieren. Außerdem umfasste dieses Arbeitspaket sämtliche Aktivitäten der Partner, die der Verbreitung und Vernetzung des USecureD-Projekts, der Etablierung des USecureD-Kompetenzzentrums und dem Aufbau von Methodenkompetenz bei IKT-Herstellern dienten.

6.5.2 Verwendung der Zuwendung

Arbeitspaket 5 umfasste Aktivitäten in den folgenden Bereichen:

Veröffentlichungen

Eine Übersicht aller erfolgten und geplanten Veröffentlichungen der USecureD-Konsortialpartner (Stand: September 2017) befindet sich in Kapitel 11 dieses Schlussberichts. Daneben haben die Partner an diversen weiteren Calls for papers teilgenommen.

Beiträge zu Konferenzen, Tagungen, Workshops und Messen

Die USecureD-Partner haben zu folgenden Veranstaltungen **Vorträge beigesteuert**:

- 12. November 2015 – World Usability Day Frankfurt, Frankfurt/Main:
  „Security vs. Usability: Und der Gewinner ist …?“
- 29. Februar 2016 – REConf 2016, München:
  „Nutzerzentrierter Schutz sensibler Daten: Ergebnisse einer aktuellen Anforderungsanalyse“
- 2. März 2016 – Mittelstand-Digital-Kongress, Berlin:
  „Muss ich für hohe IT-Sicherheit auf Usability verzichten?“
- 23. März 2016 – UIG Frühjahrstagung 2016, Mannheim:
  „Usable Security: Welche Anforderungen haben Nutzer an gebrauchstaugliche Informationssicherheit?“
- 2. Juni 2016 – Bitkom-Fachausschuss Usability & User Experience (UUX), Bonn:
  „Nutzerzentrierte Informationssicherheit – Werkzeuge und Musterlösungen zur Integration von UUX & IT-Security“

- 10. Juni 2016 – Mittelstand-Digital Praxistag, Frankfurt/Main:
  „Usable Security – Musterlösungen für nutzerzentrierte Informationssicherheit“
- 27. Juni 2016 – 3. Forschungstag IT-Sicherheit NRW, Gelsenkirchen:
  „Usability Evaluation von Security-APIs“
- 21. Juli 2016 – 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA), Frankfurt/Main:
  „Towards the Usability Evaluation of Security-APIs“
- 4. November 2016 – Botan Crypto Library Workshop / Rohde & Schwarz, Bochum:
  „Usability Evaluation von Security APIs“
- 10. November 2016 – World Usability Day Würzburg, Würzburg:
  „Usable Security: Usability als Beitrag zu mehr IT-Sicherheit“
- 12. Dezember 2016 – Forschungskolloquium der TU Berlin, Berlin:
  „Towards the Usability Evaluation of Security APIs“
- 9. Februar 2017 – CAST-Workshop „Usable Security“, Darmstadt:
  „Usable Security Principles, Guidelines und Patterns“ und
  „Zur Gebrauchstauglichkeit von Security APIs“
- 18. Mai 2017 – 15. Deutscher IT-Sicherheitskongress, Bonn:
  „Usable Security by Design: Unterstützung für kleine und mittlere Softwarehersteller in frühen Phasen der Produktentwicklung“
- 14. September 2017 – 6. IT Sicherheitstag Mittelstand, Berlin:
  „Usable Security: Mit Benutzerfreundlichkeit zu mehr IT-Sicherheit“

Die Partner haben im Rahmen von Konferenzen und Tagungen bzw. bei interessierten Organisationen folgende **Workshops ausgerichtet bzw. mitorganisiert**:

- 6. September 2015 – Mensch und Computer 2015, Stuttgart:
  „Usable Security and Privacy: Nutzerzentrierte Lösungsansätze zum Schutz sensibler Daten“
- 7. September 2015 – Mensch und Computer 2016, Stuttgart:
  „UUX Construction Site - Usability und User Experience für den Mittelstand“
- 22. August 2016 – bee security GmbH, Köln:
  „USecureD Plattform“
- 4. September 2016 – Mensch und Computer 2016, Aachen:
  „Usable Security and Privacy: Ansätze und Lösungen zur nutzerzentrierten Entwicklung und Ausgestaltung von digitalen Schutzmechanismen“
- 5. September 2016 – Mensch und Computer 2016, Aachen:
  „Usable Security & Privacy: Ziele, Themen, Ausblick“
- 6. September 2016 – Mensch und Computer 2016, Aachen:
  „Sponsoren-Workshop Mittelstand-Digital“
- 15. September 2016 – Universität Bonn, Bonn:
  „USecureD Plattform“
- 9. Februar 2017 – CAST / Fraunhofer SIT, Darmstadt:
  „Usable Security“
- 30. Mai 2017 – Mittelstand-Digital Kongress 2017, Berlin
  „Wie können Sicherheitsfunktionen von Software benutzerfreundlicher gestaltet werden?“ (zweimaliger Workshop)
- 10. September 2017 – Mensch und Computer 2017, Regensburg:
  „3. Workshop Usable Security: Ziele der Usability und Security ausbalancieren“
- 11. September 2017 – Mensch und Computer 2017, Regensburg:
  „Benutzerfreundliche IT-Sicherheit: Prozessintegration und Werkzeuge“
- 12. September 2017 – Mensch und Computer 2017, Regensburg:
  „User Experience und Digitalisierung erfolgreich umgesetzt“

Die Partner waren bei folgenden weiteren Veranstaltungen (Konferenzen, Workshops und Messen) **mit einem Infostand präsent**:

- CAST- Usable Security Day 2015 (Darmstadt, 16.Juli 2015)
- IT-Sicherheitstag Saarland 2016 (Saarbrücken, 2. Februar 2016)
- #itsNRW – Bürgerdialog IT-Sicherheit in NRW (Köln, 20. Juni 2016)
- 1st European Workshop on Usable Security (EuroUSEC) (Darmstadt, 18. Juli 2016)
- Saarländischer IT-Tag 2016 (Saarbrücken, 6. Oktober 2016)
- 3. Tag der IT-Sicherheit Saar (Saarbrücken, 16. Februar 2017)

Darüber hinaus haben die Partner **an weiteren Veranstaltungen teilgenommen**:

- nrw.uniTS/ CPS.HUB NRW Workshop „Human-Centered Systems Security“ (Bochum, 14. November 2016)
- 3. Kölner IT-Security-Konferenz (24. November 2016)
- DIN Workshops „Usability und Security“ (Berlin, 22. Februar 2017 und 13. Juni 2017)

Im Rahmen der genannten Veranstaltungen haben die Partner Kontakte zu mehreren KMU und Forschungsprojekten sowie zu einem Chemiekonzern aufgebaut, die im weiteren Projektverlauf intensiviert wurden.

Online-Marketing und (Online-)PR

Zur Bekanntheitssteigerung des Projekts haben die Partner folgende Aktivitäten in den Bereichen Online-PR, Online-Marketing und Social-Media-Marketing durchgeführt:

- Aufbau und Betrieb der USecureD-Projektwebsite (http://www.usecured.de) mit sämtlichen veröffentlichten Projektergebnissen
- Einrichtung, Moderation und Administration der Xing-Gruppe „Usable Security“ (https://www.xing.com/communities/groups/usable-security-0f37-1072338)
- Versand und Online-Publikation mehrerer Pressemitteilungen
- Postings bei ca. 20 Xing-Gruppen zu den Themen IT-Security und Usability zur Bewerbung der Online-Studie und der USecureD-Plattform
- Publikation von aktuellen Nachrichten über das Projekt USecureD auf der DAS-Webseite der TH Köln

Sonstige Aktivitäten

- Etablierung und Leitung des Arbeitskreises „Usable Security & Privacy“ bei der German UPA (http://www.germanupa.de/aktivitaeten/arbeitskreise/usable-security-privacy/)
- Transfer der Projektinhalte in den Lehrveranstaltungen „Daten- und Anwendungssicherheit“ und „Hauptseminar“ an Studierende der Master-Studiengänge Medientechnologie und Technische Informatik der TH Köln
- abgeschlossene Bachelorarbeit an der TH Köln zum Thema „Evaluation von passiven Sicherheitshinweisen zur Kommunikation des Grades der Überprivilegierung von Android Apps“
- Teilnahme an der Allianz für Cyber-Sicherheit
- Teilnahme an der IT-Sicherheitsinitiative Saar
- Teilnahme an den Aktivitäten der Förderinitiative „Einfach intuitiv“ bzw. des Mittelstand-Digital-Arbeitsforums „Usability“
- Erstellung eines Praxisbeispiels für die Mittelstand-Digital-Publikation „Praxisbeispiele aus den Projekten der Initiative «Einfach intuitiv – Usability für den Mittelstand»“
- Anfertigung eines Roll-ups, mehrerer Projektposter und eines Projektflyers
- Erfolgreiche Beantragung des Prädikats „Projekt im Software-Cluster“

6.5.3 Ergebnisse

Im Rahmen von Arbeitspaket 6 haben die Partner folgende Ergebnisse erarbeitet:

- **E 5.1 USecureD-Projektwebsite**
  Projektwebsite (http://www.usecured.de) mit sämtlichen veröffentlichten Projektergebnissen
- **E 5.2 Fach- und Forschungsartikel**
  vgl. Kapitel 11
- **USecureD-Seminarkonzept und Schulungsunterlagen**
  für die akademische Ausbildung an der TH Köln und anderen deutschen Hochschulen sowie für berufliche Fortbildungen

Ergebnisse der Transferaktivitäten wie Fach- und Forschungsartikel oder Vortragsfolien wurden teilweise auf den Webseiten der Herausgeber bzw. Veranstalter veröffentlicht.

6.6 Arbeitspaket 6: Projektmanagement

Laufzeit: Mai 2015 – April 2017

Lead: HKBS

6.6.1 Ziele des Arbeitspakets

Ziel dieses Arbeitspakets war es, alle Arbeiten der Projektpartner zu koordinieren, die Projektausrichtung sowie den Projektfortschritt zu überwachen, zu dokumentieren und bei Bedarf im Rahmen der Zielsetzung anzupassen.

6.6.2 Verwendung der Zuwendung

Zu Projektbeginn wurden von allen Projektpartnern interne organisatorische Maßnahmen getroffen, die die Projektinitialisierung und den Projektablauf betreffen (Ressourcenplanung, Reporting, Dokumentation usw.). Es wurden die benötigten Infrastrukturen für das Projekt geschaffen und die hierfür erforderlichen Anschaffungen gemacht. Als zentrales Repository, insbesondere für den Dokumentenaustausch der Partner, diente eine OwnCloud-Installation mit gesicherten persönlichen Zugängen, die von der HKBS eingerichtet, administriert und betrieben wurde.

Im weiteren Projektverlauf koordinierte die HKBS als Konsortialführer und Projektleiter alle im Projekt zu erbringenden Arbeiten. Hierzu plante und moderierte die HKBS insbesondere die zweiwöchentlichen Telefonkonferenzen des Konsortiums. Projektmanagementaufgaben innerhalb der einzelnen Arbeitspakete lagen zudem beim Projektpartner, der die Leitung des jeweiligen Arbeitspakets innehatte. Zu Beginn der einzelnen Arbeitspakete wurde der Projektplan jeweils detaillierter ausgearbeitet und es wurden die konkreten Arbeitsergebnisse festgelegt.

Durch regelmäßige Konsortialtreffen wurden der Projektfortschritt und die Projektausrichtung kontrolliert, dokumentiert und im Rahmen der Zielsetzungen bedarfsweise angepasst. Darüber hinaus fanden kontinuierlich Arbeitstreffen statt, um die laufenden und anstehenden Arbeiten abzustimmen und um den Informationsaustausch zwischen den Partnern zu gewährleisten. Am 28.4.2016 fand an der TH Köln ein Statusseminar statt, in dem der aktuelle Stand des USecureD-Vorhabens dem Projektträger, dem Ministerium und der Begleitforschung vorgestellt wurden.

6.6.3 Ergebnisse

Im Rahmen von Arbeitspaket 6 haben die Partner folgende Ergebnisse erarbeitet:

- **E 6.1 Schlussbericht**
- **Zwischenberichte der Konsortialpartner und des Konsortialführers**
- **Gesprächsprotokolle**
  Protokolle der Telefonkonferenzen, des Statusseminars mit Vertretern des Ministeriums, des Projektträger und der Begleitforschung sowie der Konsortial- und Arbeitstreffen

Mit Ausnahme des vorliegenden Schlussberichts sind diese Ergebnisse als interne Dokumente nicht frei zugänglich.

7 Wichtigste Positionen des zahlenmäßigen Nachweises

7.1 HK Business Solutions

Während der Projektdurchführung sind bei HK Business Solutions Kosten entstanden, über die im Verwendungsnachweis im Detail berichtet wurde. Die Gesamtkosten verteilen sich auf 96,86 % Personalkosten, 1,33 % Abschreibungen auf vorhabenspezifische Anlagen, 0,98 % Reisekosten, 0,81 % Transfermaßnahmen des Konsortialführers und 0,02 % Materialkosten.

Der in der Gesamtvorhabenbeschreibung skizzierte Kostenrahmen wurde im Wesentlichen eingehalten. Durch die intensive Nutzung der USecureD-Werkzeuge und die Aufbereitung sämtlicher Projektergebnisse in der letzten Projektphase kam es bei den Personalkosten zu einer leichten Überschreitung der veranschlagten Gesamtaufwände. Bei allen übrigen Positionen sind weniger Kosten angefallen als geplant.

7.2 Technische Hochschule Köln

Während der Projektdurchführung sind bei der TH Köln Kosten entstanden, über die im Verwendungsnachweis im Detail berichtet wurde. Der in der Gesamtvorhabenbeschreibung skizzierte Kostenrahmen wurde vollständig eingehalten. Bei allen Positionen sind sogar leicht weniger Kosten angefallen als geplant. Nur bei den Reisekosten sind die Einsparungen bemerkenswert höher ausgefallen. Der Grund hierfür liegt in der Tatsache, dass viele der besuchten internationalen Konferenzen zufälligerweise in Europa stattgefunden haben und somit nicht – wie in der Planung veranschlagt – nach Amerika oder Asien gereist werden musste.

8 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Mit dem USecureD-Projekt konnte das Konsortium substanzielle Beiträge zu den förderpolitischen Zielen der Ausschreibung „Einfach intuitiv – Usability für den Mittelstand“ leisten. Sämtliche Methoden und Werkzeuge, die das Konsortium im Rahmen von USecureD entwickelt hat, wurden zur Projektlaufzeit in Pilotprojekten erprobt; basierend auf den hierbei gemachten Erfahrungen wurden diese Ergebnisse für den Praxiseinsatz optimiert, dokumentiert und in geeigneter Form veröffentlicht, so dass sie auch von Anwender- und Hersteller-KMU außerhalb des Konsortiums genutzt werden können.

Die Projektergebnisse ermöglichen kleinen und mittleren Herstellerunternehmen einen zügigen Markteintritt mit IT-Produkten, die gleichermaßen sicher und benutzerfreundlich sind. Dadurch haben diese KMU ein Alleinstellungsmerkmal und einen Wettbewerbsvorteil gegenüber ihren Mitbewerbern, insbesondere gegenüber großen, internationalen IT-Herstellern, und sie können sich besser am Markt behaupten. Gleichzeitig hat das USecureD-Projekt Möglichkeiten für mittelständische Anwenderunternehmen geschaffen, Usable Security als wichtiges Qualitätskriterium in den Auswahl- bzw. Entwicklungsprozess der betrieblichen Anwendungssoftware einzubeziehen.

Um das junge Thema Usable Security gemeinsam mit zusätzlichen Multiplikatoren in Praxis und Forschung voranzutreiben, wurde u. a. ein Arbeitskreis bei einem relevanten Berufsverband aufgebaut, eine wissenschaftliche Workshop-Reihe etabliert und eine Online-Community entwickelt. Damit die Nachhaltigkeit der Projektergebnisse gewährleistet ist, werden die Konsortialpartner auch langfristig als zentraler Ansprechpartner und Serviceanbieter für gebrauchstaugliche Informationssicherheit zur Verfügung stehen – sowohl für Anwender-, Hersteller- und Dienstleistungsunternehmen der IKT-Branche wie auch für Forscher und Wissenschaftler.

Der Verlauf der Arbeiten im USecureD-Vorhaben folgte der im Projektantrag formulierten Planung. Hierbei wurden die im Arbeitsplan formulierten Aufgaben erfolgreich bearbeitet und es waren keine zusätzlichen Ressourcen für das Projekt erforderlich. Vielmehr bestätigte sich, dass die Bearbeitungsdauer von 24 Monaten und die Höhe der gewährten Zuwendungen mit Blick auf den Neuheitswert der erzielten Ergebnisse notwendig und angemessen waren.

9 Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse

9.1 HK Business Solutions

Die USecureD-Ergebnisse bieten ein großes Potential, um Geschäftsanwendungen benutzerfreundlicher, effizienter und sicherer zu gestalten. Da diese Mehrwerte für alle IKT-Anwenderbranchen und für alle Einsatzgebiete betrieblicher Software relevant sind, geht die HKBS von einem zunehmenden Bedarf sowohl bei eigenen Bestandskunden als auch bei potentiellen Neukunden aus. Der Ansatz des USecureD-Projekts, zu effizienteren und zugleich sicheren Unternehmensprozessen beizutragen, ist sowohl für die unmittelbaren Anwender erstrebenswert als auch für die Unternehmen, bei denen die Geschäftsanwendungen im Einsatz sind. Daher rechnet die HKBS mit einer besonders großen Akzeptanz und Nutzungsmotivation von Produkten, die über das Qualitätsmerkmal Usable Security verfügen.

Die in USecureD erarbeiteten Gestaltungswerkzeuge, die implementierten Musterlösungen und die Evaluationsmethodik werden bei HKBS seit Projektende in entsprechende Kundenprojekte (Standardlösungen und Individualentwicklungen) transferiert. Da bereits während des Projekts eine Validierung und Optimierung dieser Ergebnisse stattfand, waren hierfür keine weiteren Aufwände notwendig. Durch den Einsatz der zur Projektlaufzeit validierten Werkzeuge und Methoden wird zugleich das Entwicklungsrisiko innovativer Produkte gesenkt.

Das erworbene Wissen zum Thema Usable Security wird für die HKBS bei künftigen Produktentwicklungen sehr hilfreich sein, um Stärken und Schwächen von Interaktionskonzepten, insbesondere hinsichtlich Usability und IT-Sicherheit, besser beurteilen zu können. Dies gilt gleichermaßen für den analytischen und konzeptionellen Bereich – mögliche Schwachstellen der Produkte können von Anfang vermieden werden, z. B. durch Anwendung der USecureD-Entwurfs- und Gestaltungswerkzeuge – wie für den Bereich Evaluation und Qualitätssicherung – Schwachstellen können gezielt aufgedeckt werden, z. B. durch Anwendung der USecureD-Evaluationswerkzeuge.

Die HKBS bietet im Rahmen ihres Dienstleistungsangebots bereits Schulungen bzw. Seminare und Beratungsdienstleistungen zu diversen IT-Themen an. Dieses Angebot kann mit dem Thema Usable Security weiter ausgebaut werden, z. B. mit Schulungsbausteinen zum Thema Usable Security, zur Nutzung der USecureD-Plattform bzw. einzelner Werkzeuge.

9.2 Technische Hochschule Köln

Vom übergeordneten Thema des USecureD-Projekts „Usable Security and Privacy“ geht ein großes Potential aus, was auch durch Außenstehende über die gesamte Projektlaufzeit bestätigt wurde. Um digitalisierte Produkte und Systeme benutzerfreundlich, effizient und sicher ausgestalten zu können, sind das Verständnis um und die Werkzeuge für Usable Security and Privacy unabdingbar. Die Relevanz dieses Qualitätsmerkmals wird durch die zunehmende Vernetzung und Digitalisierung in allen Anwenderbranchen weiter zunehmen, woraus sich ein steigender Bedarf an Know-how sowie adäquaten Werkzeugen und Lösungen ergibt. Hierin liegt eine große Chance für den Standort Deutschland, der seine komplexen und hochwertigen Produkte sowie Lösungen zukünftig vermehrt mit den Qualitätsmerkmalen Security und Usability ausstatten kann. Einen ersten und wesentlichen Beitrag steuert das USecureD-Projekt dazu bei.

Das erworbene und ausgebaute Wissen zum Thema Usable Security garantiert der TH Köln die wissenschaftliche Anschlussfähigkeit in dieser Domäne, auch auf internationaler Ebene. Durch die damit einhergehende Sichtbarkeit werden unmittelbar nach Projektende von USecureD Anschlussprojekte sowohl wissenschaftlicher als auch kommerzieller Natur erwartet. Entsprechende Anträge zur Fortführung der Forschungs- und Entwicklungsarbeiten sind gestellt worden. Drei Promotionsstellen im Bereich sind durch das BMBF (Start: Mai 2017) und das Land NRW (Start: März 2018) bewilligt worden. Zwei von der TH Köln für USecureD eingestellte Mitarbeiter, Herr Hoai Viet Nguyen und Herr Peter Leo Gorski) werden über die neuangeworbenen Drittmittel weiter beschäftigt. Ein weiterer Mitarbeiter wird das Team ab März 2018 verstärken. Das vorliegende Usable-Security-Know-how ist in zahlreiche Lehrangebote der TH Köln integriert. Die Universitäten in Bonn und Regensburg haben für das Wintersemester 2017/2018 angekündigt, die USecureD-Tools in eigenen Lehrveranstaltungen einzubetten. Dies alles trägt zur Ausbildung spezialisierter Nachwuchskräfte bei.

Die in USecureD erarbeiteten Werkzeuge, die implementierten Musterlösungen und die Evaluationsmethodik fließen in der USecureD-Plattform der TH Köln zusammen. Diese SaaS-Lösung stellt bereits jetzt viele der Werkzeuge kostenlos und diskriminierungsfrei zur Verfügung. Dies soll auch nach Projektende so bleiben, um allen Interessierten einen Zugang zum Knowhow und den Werkzeugen zu garantieren. Die Relevanz und Tragfähigkeit der USecureD-Werkzeuge haben sich schon während der Projektlaufzeit bestätigt. Durch den regen Austausch mit Anwendern der Werkzeuge, die aufgrund der zahlreichen

Verbreitungsaktivitäten im Projekt aufgebaut werden konnten, sind die Werkzeuge weiter verbessert und an besondere Anforderungen angepasst worden. So ist auf Anregung eines externen Anwenders eine programmatische Schnittstelle zu den USecureD-Tools entwickelt worden. Teile der USecureD-Plattform können grundsätzlich als Premium-Dienste kommerzialisiert werden. Da weitere Aufwände notwendig sind, um die Teilvorhabenergebnisse zu konsolidieren und in eine marktfähige SaaS-Lösung zu überführen, wird die TH Köln in einem Zeithorizont von zwölf Monaten evaluieren, ob dies im Rahmen eines Startups erfolgen wird.

Die aufgebauten Informationskanäle (Xing, Website) und Arbeitskreise in einschlägigen Gremien (German UPA, GI) sollen weiter betrieben und ausgebaut werden. Diese haben bereits zur Projektlaufzeit für einen stetigen Dialog und Austausch mit Unternehmen und Organisationen verschiedenster Art geführt, so dass sich eine Verselbstständigung dieser Aktivitäten abzeichnet. Dies zeigt zum einen das zunehmende Interesse am Thema und trägt zum anderen zur nachhaltigen Verstetigung der durch USecureD initiierten Impulse bei. Hierdurch wird eine wesentliche Voraussetzung für den wirtschaftlichen Erfolg geschaffen, den zukünftig deutsche Unternehmen und Organisationen durch die Berücksichtigung und Umsetzung von Usable Security and Privacy erzielen können.

Jüngste Bestrebungen innerhalb des DIN haben das Thema „Usable Security and Privacy“ zudem als relevant für die Standardisierung erkannt. Die TH Köln hat an den beiden bisher durchgeführten Workshops des DIN teilgenommen und die USecureD-Ergebnisse dort eingebracht. Hierüber soll eine weitere Verbreitung und Verstetigung der Projektergebnisse erzielt werden. Die TH Köln plant auch über die zeitlichen Grenzen des USecureD-Projekts in Standardisierungsaktivitäten aktiv beizutragen.

10 Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Vom Konsortium wurden während der gesamten Projektlaufzeit regelmäßig Informationsrecherchen zu den untersuchten Themengebieten durchgeführt, insbesondere zu neuen Untersuchungen, Forschungsansätzen oder Methoden im Bereich Usable Security. Die Diskussion dieser Themen in der wissenschaftlichen Community wurde von den Konsortialpartnern mitverfolgt bzw. mitgeführt und war von großer Bedeutung für das USecureD-Vorhaben. Zu nennen sind hier neben den Konferenz- und Tagungsteilnahmen des Konsortiums (vgl. AP 5) insbesondere die Leitung des Arbeitskreises „Usable Security & Privacy“ bei der German UPA, die Moderation der XING-Gruppe „Usable Security“ sowie die Abstimmung mit dem Projekt SIDATE (Universität Siegen).

Das Mitverfolgen bzw. -führen der Diskussion wurde von den Konsortialpartnern nicht im Sinne einer Gefährdung für das Projekt angesehen. Insbesondere wurden dem Konsortium keine Ergebnisse von dritter Seite bekannt, die die Durchführung der Arbeiten im USecureD-Vorhaben hätten behindern oder in Frage stellen können. Vielmehr stellte die Diskussion eine gewinnbringende Bereicherung des Projekts dar, denn zum einen diente sie als wertvolle Quelle für neue Forschungsansätze und -ideen, zum anderen belegte sie die wissenschaftliche Relevanz der Arbeiten und den Bedarf nach erprobten, praxis- und KMU-tauglichen Ergebnissen.

11 Erfolgte und geplante Veröffentlichungen

Neben der Veröffentlichung der Projektergebnisse in diesem Schlussbericht erfolgte eine Veröffentlichung von Teilergebnissen bereits während der Projektlaufzeit in folgenden Publikationen. Weiterhin besteht die Möglichkeit die Ergebnisse des USecureD-Vorhabens auf der Projektwebsite (https://www.usecured.de/) und der USecureD-Plattform (https://das.th-koeln.de/usecured) einzusehen.

11.1 Tagungsbeiträge

Luigi Lo Iacono, Hartmut Schmitt (2015): Usable Security and Privacy: Nutzerzentrierte Lösungsansätze zum Schutz sensibler Daten. In: Anette Weisbecker, Michael Burmester, Albrecht Schmidt (Hrsg.): Mensch und Computer 2015 - Workshopband, S. 617–620. De Gruyter, Berlin

Wolfgang Börger, Luigi Lo Iacono (2015): User Perception and Response to Computer Security Warnings. In: Anette Weisbecker, Michael Burmester, Albrecht Schmidt (Hrsg.): Mensch und Computer 2015 - Workshopband, S. 621-645. De Gruyter, Berlin

Peter Leo Gorski & Luigi Lo Iacono (2016): Towards the Usability Evaluation ofSecurity APIs. In: Nathan L. Clarke,Steven M. Furnell (Hrsg.): Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance HAISA 2016, S. 252-265, Plymouth University, Plymouth

Hartmut Schmitt, Luigi Lo Iacono, Sascha Wagner (2016): Workshop des Arbeitskreises „Usable Security & Privacy“: Ziele, Themen, Ausblick. In Steffen Hess, Holger Fischer (Hrsg.): Mensch und Computer 2016 – Usability Professionals. Gesellschaft für Informatik e.V. / German UPA e.V., Aachen

Luigi Lo Iacono, Hartmut Schmitt (2016): Usable Security and Privacy: Ansätze und Lösungen zur nutzerzentrierten Entwicklung und Ausgestaltung von digitalen Schutzmechanismen. In: Benjamin Weyers, Anke Dittmar: Mensch und Computer 2016 – Workshopband. Gesellschaft für Informatik e.V., Aachen

Peter Leo Gorski, Luigi Lo Iacono, Hartmut Schmitt, Peter Nehren, Hoai Viet Nguyen (2017): Usable Security by Design: Unterstützung für kleine und mittlere Softwarehersteller in frühen Phasen der Produktentwicklung. In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis: Tagungsband zum 15. Deutschen IT-Sicherheitskongress, S. 433–450. SecuMedia, Ingelheim

Luigi Lo Iacono, Hartmut Schmitt, Andreas Heinemann (2017): 3. Workshop Usable Security: Ziele der Usability und Security ausbalancieren. In: Manuel Burghardt, Raphael Wimmer, Christian Wolff, Christa Womser-Hacker (Hrsg.): Mensch und Computer 2017 – Workshopband, S. 245–247. Gesellschaft für Informatik e.V., Regensburg

Hartmut Schmitt, Edna Kropp (2017): Benutzerfreundliche IT-Sicherheit: Prozessintegration und Werkzeuge (UPA-Arbeitskreis Usable Security & Privacy). In: Steffen Hess, Holger Fischer (Hrsg.): Mensch und Computer 2017 – Usability Professionals, S. 375-380. German UPA e.V., Regensburg

Hartmut Schmitt & Luigi Lo Iacono (2017): Usable Security – Mit Benutzerfreundlichkeit zu mehr IT-Sicherheit. In: Tagungsband zum 6. IT-Sicherheitstag Mittelstand 2017 (angenommener Beitrag, Veröffentlichung im Herbst 2017)

11.2 Zeitschriftenbeiträge

Peter Leo Gorski, Luigi Lo Iacono, Hartmut Schmitt (2015): Usable Security und Privacy by Design – Teil 1: Benutzerzentrierte Entwicklung von Sicherheitsfunktionen. In: Software und Support Media GmbH (Hrsg.): Entwickler Magazin Ausgabe 2015 (6), S. 62–68. Software & Support Media, Frankfurt am Main

Hartmut Schmitt, Peter Nehren (2016): Usable Security and Privacy by Design – Teil 2: Anwendungsfälle und Musterlösungen für Unternehmenssoftware. In: Software und Support Media GmbH (Hrsg.): Entwickler Magazin Ausgabe 2016 (4), S. 18–23. Software & Support Media, Frankfurt am Main

Luigi Lo Iacono, Peter Leo Gorski, Josephine Grosse, Nils Gruschka (2016): Signalling over-privileged mobile applications using passive security indicators. In: Stephen Flowerday & Karen Renaud (Hrsg.): Journal of Information Security and Applications 34 (1), S. 27-33. Elsevier, Amsterdam

Luigi Lo Iacono, Hoai Viet Nguyen, Hartmut Schmitt (2016): Usable Security – Results from a Field Study. In: Jürgen Ziegler (Hrsg.): i-com – Journal of Interactive Media 15(2), S. 203–209. De Gruyter, Berlin

Hartmut Schmitt, Peter Nehren (2016): Usable Security and Privacy by Design – Teil 3: Entwicklungsrichtlinien für Produkte mit dem Qualitätsmerkmal „Usable Security“. In: Software und Support Media GmbH (Hrsg.): Entwickler Magazin Ausgabe 2016 (6), S. 32–37. Software & Support Media, Frankfurt am Main

Hartmut Schmitt, Peter Leo Gorski, Luigi Lo Iacono (2017): Usable Security – Benutzerfreundliche Sicherheitsfunktionen für Software und interaktive Produkte. In: Begleitforschung Mittelstand-Digital (Hrsg.): Wissenschaft trifft Praxis (6): Usability und User Experience in der Arbeitswelt von morgen, S. 5–13. Begleitforschung Mittelstand-Digital c/o WIK-Consult GmbH, Bad Honnef

Peter Nehren, Hartmut Schmitt, Luigi Lo Iacono (2017): Usable Security – Werkzeuge für Entwickler. In: Begleitforschung Mittelstand-Digital (Hrsg.): Wissenschaft trifft Praxis (6): Usability und User Experience in der Arbeitswelt von morgen, S. 14–20. Begleitforschung Mittelstand-Digital c/o WIK-Consult GmbH, Bad Honnef

Peter Leo Gorski, Luigi Lo Iacono (2017): Computer-Sicherheitswarnungen – Benutzerzentrierte Entwurfsansätze der Usable Security-Forschung. In: Begleitforschung Mittelstand-Digital (Hrsg.): Wissenschaft trifft Praxis (6): Usability und User Experience in der Arbeitswelt von morgen, S. 21–29. Begleitforschung Mittelstand-Digital c/o WIK-Consult GmbH, Bad Honnef

Hartmut Schmitt (2017): Usable Security and Privacy by Design – Teil 4: Metriken, Evaluationswerkzeuge und Testplattform. In: Software und Support Media GmbH (Hrsg.): Entwickler Magazin Ausgabe 2017 (3), S. 24–29. Software & Support Media, Frankfurt am Main

Peter Nehren, Hartmut Schmitt, Peter Leo Gorski (2017): Usable Security and Privacy by Design – Teil 5: Entscheidungshilfen für Anwender. In: Software und Support Media GmbH (Hrsg.): Entwickler Magazin Ausgabe 2017 (4), S. 30–38. Software & Support Media, Frankfurt am Main

11.3 Sonstiges

Hartmut Schmitt, Peter Nehren, Luigi Lo Iacono, Peter Leo Gorski (2017): Usable Security und Privacy by Design. E-Book. Software & Support Media, Frankfurt am Main. ISBN: 9783868027594

Luigi Lo Iacono, Hartmut Schmitt, Denis Feth, Timo Jakobi, Peter Leo Gorski, Peter Nehren, Markus Dölle, Edna Kropp, Sarah Hausmann, Anne Hofmeister, Arkadiusz Frydyada de Piotrowski, Mandy Balthasar (2017): Usable Security & Privacy: Nutzerzentrierter Schutz sensibler Daten. Fachschrift. German UPA e.V., Stuttgart

12 Anhang

Abbildung 9: Projektposter des USecureD-Vorhabens

Abbildung 10: Roll-Up des USecureD-Vorhabens

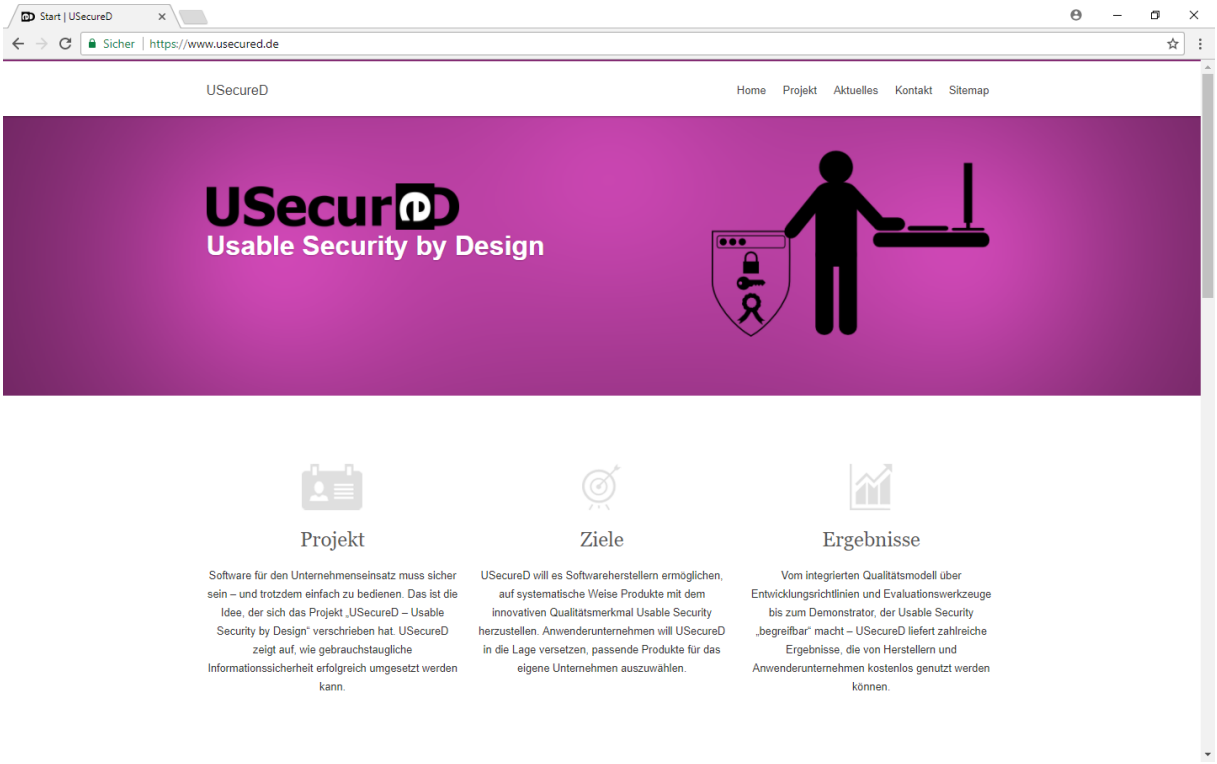


Abbildung 11: Startseite der USecureD-Website

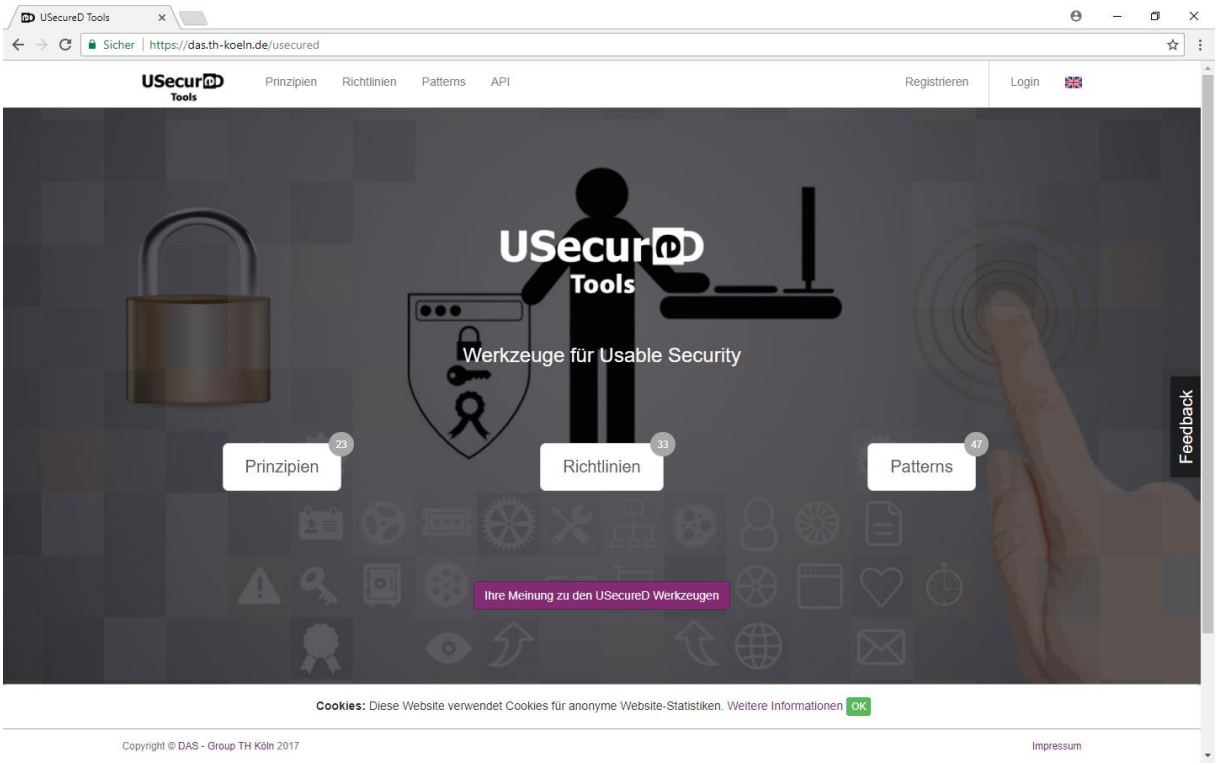


Abbildung 12: Startseite der USecureD-Plattform

Abbildung 13: Startseite des USecureD-Demonstrators

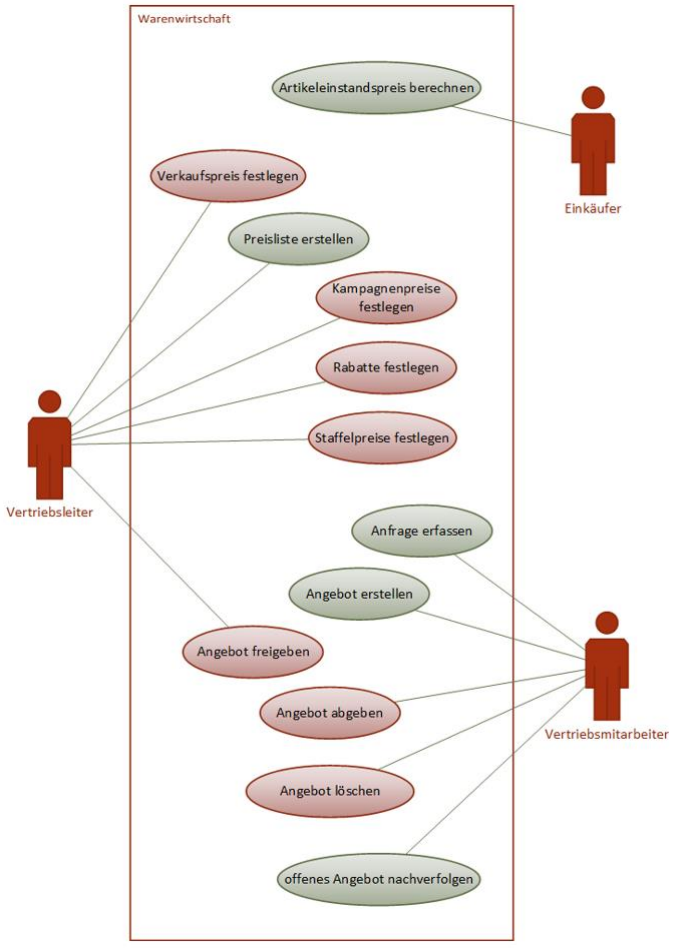


Abbildung 14: Use-Case-Diagramm (Beispiel „Vertrieb: Preiskalkulation, Angebote“)

2 Pattern-Template

Name	*eindeutiger Name des Patterns*
Quellen	*Quellenangaben und Literaturhinweise zu dem beschriebenen Pattern*
Synonyme	*bekannte Synonyme bzw. anderssprachige Namen für das beschriebene Pattern*
Kontext	*Beschreibung der wiederkehrenden Situation bzw. Ausgangslage, in der sich ein bestimmtes Problem ergibt und in der das Pattern anwendbar ist*
Problem	*Beschreibung des akuten Problems im gegebenen Kontext einschließlich der Einflussfaktoren und Anforderungen (z. B. Sicherheits- oder Usabilityziele, Bedingungen, Einschränkungen), die sich hierdurch ergeben*
Lösung	*Beschreibung einer bewährten Entwurfsform, die eine Auflösung der beschriebenen Anforderungen ermöglicht*
Beispiele	*bekannte Verwendungen und Illustrationen des beschriebenen Patterns*
Implementierung	*detailliertere Informationen zu dem beschriebenen Pattern, z. B. Spezifikation von funktionalen/nichtfunktionalen Anforderungen oder Hinweise zu Architekturkonzepten oder zur Implementierung*
Konsequenzen	*Vor- und Nachteile des Patterns, die z. B. durch Einflussfaktoren oder Anforderungen entstehen, die miteinander in Konflikt stehen, und die vor der Verwendung des Patterns abgewogen werden sollten*
Abhängigkeiten	*Abhängigkeiten von anderen Patterns*
Beziehungen	*Patterns, die ein ähnliches Problem adressieren wie das beschriebene Pattern oder die in Kombination mit dem beschriebenen Pattern verwendet werden können*
Prinzipien	*Prinzipien, die ein übergeordnetes Ziel darstellen, zu dessen Erreichen das Pattern beiträgt*
Richtlinien	*USecureD-Entwicklungsrichtlinien, bei deren Umsetzung das Pattern berücksichtigt werden kann*
Check Listen	*Checklisten, mit denen überprüft werden kann, ob das Pattern korrekt umgesetzt wurde*
Use Cases	*USecureD-Use-Cases, bei deren Umsetzung das Pattern verwendet werden kann*
Tags	*Zum Pattern passende Schlagworte, um die Durchsuchbarkeit des Katalogs zu verbessern*
Log History	*Feld zur Protokollierung von Ereignissen, wie zum Beispiel das aktuelle Updatedatum des Pattern*

Abbildung 15: USecureD-Patterntemplate

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-					

Abbildung 16: Checklisten (Beispiel „Aufgabenorientierung und mentale Belastung“ (Auszug)

HKBS

Benutzerfreundliche Sicherheitsfunktionen sind eminent wichtig, insbesondere bei Business-Software. Dank USecureD liegt jetzt erstmals eine umfassende Werkzeugsammlung vor, die wir in mehreren Pilotprojekten anwenden konnten.

Marco Hess
HK Business Solutions GmbH

HK Business Solutions

Die HK Business Solutions ist ein IT-Systemhaus, das sich auf betriebswirtschaftliche Software spezialisiert hat. Unsere Kunden sind vor allem kleine und mittlere Unternehmen unterschiedlicher Branchen mit bis zu 50 Bildschirm-Arbeitsplätzen.

Vorgehen

In unserer Rolle als Anwendungspartner konnten wir die USecureD-Projektergebnisse, beispielsweise Gestaltungswerkzeuge für benutzerfreundliche Sicherheitsfunktionen, gleich in mehreren Softwareprojekten für unsere Kunden anwenden.

Ziel der Zusammenarbeit

Unser Hauptantrieb ist es, bessere Lösungen für unsere Kunden zu schaffen. In Projekten wie USecureD können wir gemeinsam mit starken Partnern Produktinnovationen entwickeln, wozu wir als Kleinunternehmen sonst nicht in der Lage wären.

Warum USecureD? Was hat Sie an diesem Projekt interessiert?

Sicherheit und Gebrauchstauglichkeit sind wichtige Softwarequalitätsmerkmale. Bei Business-Software wird beides von vielen Anwenderunternehmen vorausgesetzt. Was bisher fehlte, waren Werkzeuge, die es unseren Entwicklern ermöglichen, systematisch auf das Qualitätsziel gebrauchstauglicher Informationssicherheit hinzuarbeiten.

USecureD stellt erstmals solche Werkzeuge zur Verfügung – auf Deutsch und passgenau für kleinere Herstellerfirmen. Das Projekt verschafft uns so einen Know-how-Vorsprung, auch gegenüber größeren Mitbewerbern.

Wie groß war der Zeitaufwand für Sie?

Eine aufwendige Einarbeitungsphase, wie sie bei neuen Vorgehensweisen sonst oft notwendig ist, gab es bei uns nicht. Die Projektergebnisse, insbesondere die Gestaltungswerkzeuge für Softwareentwickler, wurden in unserem wöchentlichen Developer Meeting kurz vorgestellt.

Anschließend verschaffte sich jeder Entwickler einen groben Überblick, schaute sich Werkzeuge, die für seine eigenen Projekte geeignet sind, näher an und probierte diese aus.

Wie ist Ihr Fazit?

Insgesamt wurden vom USecureD-Team über einhundert Werkzeuge entwickelt, angefangen bei eher abstrakten Gestaltungsprinzipien für benutzerfreundliche IT-Sicherheit über Richtlinien für Softwareentwickler bis hin zu konkreten Musterlösungen für Usable Security. All diese Werkzeuge stehen auf einer zentralen Plattform zur Verfügung, können leicht durchsucht werden und sind auf intelligente Weise miteinander verknüpft. Dadurch finden unsere Entwickler trotz der Fülle an Informationen bei fast allen Fragen sofort eine Antwort – oder bestenfalls gleich die passende Lösung für ihr Problem. Das macht die Arbeit effizient und sorgt dafür, dass bei den Sicherheitsfunktionen, die unser Team entwickelt, viele Usabilityprobleme gar nicht erst auftreten.

USecureD (Projektlaufzeit: 2015 - 2017)
Software für den Unternehmenseinsatz muss sicher sein – und trotzdem einfach zu bedienen. Das ist die Idee, der sich das Projekt „USecureD – Usable Security by Design" verschrieben hat. USecureD zeigt auf, wie gebrauchstaugliche Informationssicherheit erfolgreich umgesetzt werden kann. www.usecured.de

USecureD Mittelstand-Digital

Abbildung 17: Mittelstand-Digital Praxisbeispiel HKBS

bee/sec

Wir halten USecureD für einen sehr zukunftsfähigen Weg und sehen eine hohe Relevanz für unsere Beratungstätigkeit.

Dr. Lars Fink
bee security GmbH

bee security GmbH

bee security GmbH (bee/sec) ist ein Consultingunternehmen, das sich auf Cyber Security spezialisiert hat. Beratungsschwerpunkte sind ISMS, Penetration Testing und Security Architecture. Zu unseren Kunden gehören v.a. Großunternehmen aus dem DAX30 und Versicherungen.

Vorgehen

In einem Workshop wurden uns zunächst die Prämissen des USecureD-Projekts vorgestellt. Anschließend haben wir den Ansatz im Beraterkreis diskutiert und sind wieder auf das Team von Prof. Lo Iacono zugekommen, da wir den Ansatz sehr spannend und v.a. nachhaltig finden.

Ziel der Zusammenarbeit

Wir verstehen uns als Vordenker für unsere Kunden. In Projekten haben wir den Anspruch, Impulse zu setzen, die zu einer Verminderung der Angreifbarkeit oder zu einer Steigerung der Effizienz führen. Der Ansatz von USecured entspricht unserer Philosophie: Security by Design.

Warum USecureD? Was hat Sie an diesem Projekt interessiert?

Vulnerabilities lassen sich häufig mit den vorhandenen Mechanismen sehr gut mitigieren. Allerdings setzt dies ein Mitwirken der Nutzer und Administratoren voraus. In der Unternehmenswirklichkeit erweisen sich viele Maßnahmen als ineffektiv, weil sie aus Nutzersicht sehr anspruchsvoll (umständlich) sind.

Dies führt nicht nur zu verzögerten Arbeitsabläufen, sondern meist auch dazu, dass die Sicherheitsmechanismen umgangen oder ausgehebelt werden (Beispiel: komplexes, häufig zu änderndes Passwort wird per Post-it unter der Tastatur hinterlegt).

Der Ansatz von USecureD greift genau diese Problematik auf, indem es der Softwareentwicklung Designempfehlungen, Checklisten und Patterns an die Hand gibt, um einen gleichen oder höheren Sicherheitslevel bei besserer Usability zu erreichen. Wir halten dies für einen sehr zukunftsfähigen Weg.

Wie groß war der Zeitaufwand für Sie?

Der bisherige Zeitaufwand war überschaubar: in zwei Workshops mit der Projektgruppe aus der TH Köln haben wir den Ansatz gut kennengelernt.

Intern erfolgte eine Auseinandersetzung mit den Artefakten (Guidelines, Patterns etc.), eine Evaluation auf Relevanz in unseren Beratungsprojekten und die Integration in unseren „Cortex", das interne Wissensmanagementsystem von bee/sec. Insgesamt schätzen wir unseren Aufwand auf ungefähr vier Projekttage.

Wie ist Ihr Fazit?

Weiterhin sind wir von dem Ansatz von USecureD überzeugt. Unsere Berater können sich sehr gut einen Rückgriff auf die Guidelines, Patterns und Usable Security Prinzipien in entsprechenden Beratungsprojekten vorstellen. Unsere Mandanten haben in aller Regel eine Vielzahl eigenentwickelter Softwareplattformen, die häufig von sehr vielen Mitarbeitern des Unternehmens genutzt werden und in denen hochsensible Daten verarbeitet werden.
Von daher sehen wir eine hohe Relevanz für unsere Beratungstätigkeit. In einem sehr guten Austausch mit dem Team von Prof. Lo Iacono konnten wir anregen, dass die Artefakte in strukturierter Form per REST-API im JSON Datenformat bereitgestellt werden, so dass sie in internen Wikis für die Softwareentwicklung oder die Beratung (wie in unserem Fall) hinterlegt und effizient erschließbar gemacht werden.

USecureD (Projektlaufzeit: 2015 - 2017)
Software für den Unternehmenseinsatz muss sicher sein – und trotzdem einfach zu bedienen. Das ist die Idee, der sich das Projekt „USecureD – Usable Security by Design" verschrieben hat. USecureD zeigt auf, wie gebrauchstaugliche Informationssicherheit erfolgreich umgesetzt werden kann. www.usecured.de

USecureD

Mittelstand-Digital

Abbildung 18: Mittelstand-Digital Praxisbeispiel bee security

13 Abbildungsverzeichnis

14 Dokumentinformation

Titel: Schlussbericht des Vorhabens „Usable Security by Design“

Datum: 20.10.2017

Bericht: Schlussbericht des Projekts „USecureD – Usable Security by Design“, BMWi-Förderkennzeichen 01MU14002

Status: final

Klassifikation: öffentlich