USecurD

Principle-Template

Deliverable E2.1

Projekt	USecureD – Usable Security by Design
Förderinitiative	Einfach intuitiv – Usability für den Mittelstand
Förderkennzeichen	01MU14002
Arbeitspaket	AP 2.1
Fälligkeit	31.01.2016
Autor	Peter Nehren (TH Köln)
Status	Final
Klassifikation	Öffentlich

HKBS

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

KMU
(Konsortialführer)

Technology
Arts Sciences
TH Köln

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

Hochschule
(Konsortialpartner)

Mittelstand-Digital

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

Abstract

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

Prinzipien, bzw. Principles, sind das abstrakteste dieser Entwurfswerkzeuge. Sie basieren auf früheren Erfahrungen, Designs oder wissenschaftlichen Erkenntnissen und sind für viele Anwendungsbereiche gültig. Dabei unterstützen sie Softwarearchitekten und -entwickler, sodass schon während der Planungsphase von Softwareprojekten auf Prinzipien der Usable-Security-Forschung geachtet werden kann. Auch Käufern solcher Produkte bieten sie die Möglichkeit, Anforderungen und Kriterien für ihre konkreten Anwendungsfälle besser definieren zu können.

Das Ziel dieses Deliverables war die Erstellung eines Beschreibungstemplate, welches zur einheitlichen Dokumentation der USecureD-Principles dient.

Schlagworte

Usable Security, IT-Security, Principles, Prinzipien, Grundsätze, Entwurfswerkzeug, Template

Inhaltsverzeichnis

1 Vorgehensweise

Prinzipien als abstrakteste Entwurfswerkzeuge basieren auf früheren Erfahrungen, Designs oder wissenschaftlichen Erkenntnissen und sind allgemein für viele Anwendungsbereiche gültig. Neben Softwarearchitekten und –entwicklern unterstützen sie auch Käufer von Softwareprodukten beim Definieren von Anforderungen und Kriterien für ihre konkreten Anwendungsfälle.

Ziel dieses Deliverables war die Erstellung eines Beschreibungstemplates zur einheitlichen Dokumentation von Usable-Security-Principles. Die 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 Teil der USecureD-Plattform ist. Im Folgenden wird die analytische Methodik zur Entwicklung des Principle-Templates beschrieben.

Zunächst wurde der derzeitige Stand der Forschung im Bereich Usable-Security-Principles, durch eine umfassende Literaturrecherche, erfasst. Existierende Prinzipien verschiedener Autoren wurden gesammelt und analysiert. Maßgeblich sind die Ergebnisse von Whitten und Tygar (Whitten and Tygar, 1999), Garfinkel (Garfinkel, 2005), Yee (Yee, 2002), Furnell et al. (Furnell et al., 2006), Chiasson et. al (Chiasson et al., 2007) und Hof (Hof, 2012) eingeflossen.
Anschließend wurde untersucht, welche wiederkehrenden Merkmale in den von den Autoren beschrieben 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 motivierenden 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 Principle-Datenbank, und Angaben zu den *Quellen*. Durch die Verknüpfung der Projektergebnisse ist zudem das Merkmal *Richtlinien* hinzugekommen. In dem Feld werden Verknüpfungen zu USecureD-Richtlinien dokumentiert, welche bei der Umsetzung des Prinzips helfen können.
Darüber hinaus wurde eine *Log History,* d. h. ein Feld zur Dokumentation von Protokollereignissen, hinzugefügt.

2 Principle-Template

Name	*eindeutiger Name des Prinzips*
Quellen	*Quellenangaben und Literaturhinweise zu dem beschriebenen Prinzip*
Synonyme	*bekannte Synonyme bzw. anderssprachige Namen für das beschriebene Prinzip*
Intention	*Beschreibung der Absichten, welche das Prinzip verfolgt*
Motivation	*Beschreibung des Kontextes bzw. der Umstände, welche dazu motivieren das Prinzip anzuwenden*
Beispiele	*bekannte Verwendungen und Illustrationen des beschriebenen Prinzips*
Richtlinien	*Richtlinien, durch welche das Prinzip umgesetzt werden kann*
Tags	*Zum Prinzip passende Schlagworte, um die Durchsuchbarkeit des Katalogs auf der USecureD-Plattform zu verbessern*
Log History	*Feld zur Protokollierung von Ereignissen, wie zum Beispiel das aktuelle Änderungsdatum des Prinzips*

3 Beispiel Prinzip

Name	*Geringste Überraschung*
Quellen	*S. L. Garfinkel. Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable. PhD thesis, Massachusetts Institute of Technology, 2005.*
Synonyme	*Least Surprise, Least Astonishment*
Intention	*Stelle sicher, dass das System sich so verhält, wie der Nutzer dies erwartet.*
Motivation	*Saltzer und Schroeder haben 1975 das Prinzip der "psychologischen Akzeptanz" (Saltzer and Schroeder 1975) eingeführt. Seitdem wurde es generell in das Prinzip (oder die Regel) der "geringsten Überraschung" oder der "minimalen Verwunderung" umgeformt. Das Prinzip der geringsten Überraschung besagt, dass das System mit den Erfahrungen, Erwartungen und dem mentalen Modell des Nutzers übereinstimmen sollte. Im Kontext der Computersicherheit bedeutet dies, dass der Computer eine Aktion nicht in unsicherer Weise durchführen sollte, wenn der Nutzer eine sichere Ausführung erwartet.*
Beispiele	*Füllt ein Nutzer auf einer SSL-verschlüsselten Webseite ein Formular aus, sollte der Browser ihn warnen, wenn die Übermittlungsfunktion des Formulars die Daten unverschlüsselt zum Webserver sendet. Genauso sollte, wenn der Nutzer das Löschen einer Datei veranlasst und diese Datei aus der Liste aller Dateien verschwindet, die Datei auch tatsächlich gelöscht werden.*
Richtlinien	[Technische Probleme kommunizieren] [Warnung vor Timeouts] [Benachrichtigung bei fehlgeschlagener Datenübertragung]
Tags	*Erwartungskonformität*
Log History	*[01.01.2016]: Translated to german*

4 Quellen

Chiasson, S., Biddle, R., and Somayaji, A. (2007). Even Experts Deserve Usable Security: Design guidelines for security management systems.

Furnell, S.M., Jusoh, A., and Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. Comput. Secur. *25*.

Garfinkel, S.L. (2005). Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable. Massachusetts Institute of Technology.

Hof, H.-J. (2012). User-Centric IT Security. In The Fifth International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services, (IARIA),

Whitten, A., and Tygar, J.D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8, (Berkeley, CA, USA: USENIX Association), pp. 14–14.

Yee, K.-P. (2002). User Interaction Design for Secure Systems. In Proceedings of the 4th International Conference on Information and Communications Security, (London, UK, UK),