

Interviewleitfaden

(AP 1.2 Anforderungen an Usable Security)

Projekt	USecureD – Usable Security by Design
Förderinitiative	Einfach intuitiv – Usability für den Mittelstand
Förderkennzeichen	01MU14002
Arbeitspaket	AP 1.2
Datum	31.10.2015
Autor	Hartmut Schmitt (HK Business Solutions), Peter Gorski (TH Köln)
Status	Final
Klassifikation	Öffentlich



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)

Abstract

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

Im Rahmen des Arbeitspakets 1.2 (Anforderungen an Usable Security) wurde eine breit angelegte Onlinestudie durchgeführt, mit der das Verständnis und der Stellenwert des Themas Usable Security & Privacy ermittelt wurde. Ziel der Studie war es, insbesondere die Schwierigkeiten von kleinen und mittleren Unternehmen (KMU) im Umgang mit Mechanismen der Informationssicherheit genauer zu identifizieren.

Unterstützend bzw. vertiefend zu der Studie wurden Interviews mit Stakeholdern und Endanwendern in mehreren Anwenderunternehmen der IKT-Branche durchgeführt und es wurden zwei Experten-Workshops mit assoziierten Projektpartnern durchgeführt. Dieses Dokument enthält den Leitfaden, der zur Durchführung der Stakeholder- bzw. Endanwenderinterviews erstellt wurde.

Schlagworte

Anforderungen an Usable Security, Interview, Befragung, Requirements Engineering, IT-Security, Usability, User Experience

Vorbemerkungen

Begrüßung

- Befragtem für Teilnahme danken
- Erläutern: Befragung wird durchgeführt im Rahmen eines Forschungsprojekts
- Thema der Befragung: Nutzung betrieblicher Software bei kleinen und mittelständischen Unternehmen
- Grund für Auswahl des Interviewpartners: typischer Anwender, daher persönliche Einschätzung und Anforderungen wichtig für Projekt

Ablauf des Interviews

- Abschließen der Datenschutzvereinbarung (s. hinten)
- erster Teil mit Fragen zur Person
- anschließend konkrete persönliche Einschätzungen und Anforderungen zu verschiedenen Themen bei der Nutzung betrieblicher Software

Hinweise zur Vorgehensweise

- kein richtig/falsch
- Einschätzungen werden nicht an Kollegen/Vorgesetzte weitergegeben
- ermuntern zu Lob/Kritik
- auch scheinbar Unwichtiges mitteilen
- Die Auswertung erfolgt anonym. Es besteht zu keiner Zeit die Möglichkeit die Antworten einer Personen oder einem Unternehmen zuzuordnen

eventuelle Fragen des Teilnehmers beantworten

achten auf:

- *Offene Fragen*
- *Befragte mit konkreten Begriffen erläutern lassen*
- *keine geschlossenen Fragen (ja/nein)*
- *keine Suggestivfragen*
- *keine Warum-Fragen (Befragte soll sich nicht rechtfertigen)*
- *keine Widersprüche in den Antworten aufzeigen*
- *keine Bewertung vornehmen*

Beobachtungen im Unternehmen

1. Anzahl der Räume

2. Anzahl der Mitarbeiter

3. Anzahl der Mitarbeiter pro Raum

4. Sonstige Besonderheiten

Geschlecht des Teilnehmers

m w

----- Start Interview -----

Fragen zur Person

1. Was ist Ihr **Beruf** bzw. Ihre **Funktion** im Unternehmen?

2. Wie viele Jahre **Erfahrung** haben Sie in diesem Bereich?

____ Jahre

3. Wie sind Ihre Vorkenntnisse in Bezug auf die **Nutzung von PCs** (Internet, E-Mail, Office) und **Handys** bzw. Mobilgeräten – sowohl geschäftlich als auch privat?

4. **Wo** und mit **welchen Geräten** (PC, Mobilgeräte) arbeiten Sie geschäftlich bzw. privat? Haben Sie ein eigenes Büro? Sind Sie oft unterwegs?

5. Wie **intensiv nutzen** Sie diese Geräte? Welche geschäftlichen Arbeiten machen Sie am häufigsten mit diesen Geräten?

Usability und Sicherheit

6. In unserem Interview geht es um das Thema Nutzung (betrieblicher) Software. Wissen Sie, was in diesem Zusammenhang der Begriff **Usability bedeutet**? Wie würden Sie diesen beschreiben?

[Erläutern: Usability ist das Ausmaß, in dem ein Produkt durch bestimmte Nutzer in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen.]

7. Wie schätzen Sie die **Relevanz von Usability** in Software-Produkten ein?

8. Gibt es **Usability-Leitfäden** oder **Usability-Checklisten** für Software, die in Ihrem Unternehmen Anwendung finden?

8. Wissen Sie, was in diesem Zusammenhang **IT-Sicherheit bedeutet**? Wie würden Sie diese beschreiben?

[Erläutern: Unter IT-Sicherheit versteht man Maßnahmen, die beabsichtigte Angriffe auf IT-Systeme, gespeicherte und übertragende Daten sowie Kommunikationsbeziehungen vereiteln.]

9. Wie sind die **Daten** im Unternehmen, in dem Sie arbeiten, Ihrer Meinung nach **geschützt** (auf einer Skala von 1 bis 5, 1 = nicht sehr gut geschützt, 3 = durchschnittlich gut geschützt, 5 = sehr gut geschützt)?

1 2 3 4 5

10. Gibt es **Sicherheitsguidelines** oder **Sicherheitschecklisten** für Software, die in Ihrem Unternehmen Anwendung finden?

Sicherheitsmechanismen

11. Wie schätzen Sie die Relevanz von **IT-Sicherheit** und **Sicherheitsmechanismen** in Software-Produkten ein?

12. Gibt es **Sicherheitsmechanismen**, die Sie bei Ihrer Arbeit verwenden?

13. Was denken Sie über die **Verwendung von Sicherheitsmechanismen** während Ihrer Arbeit?

14. Wie **belastend** wirken sich **Sicherheitsmechanismen** auf Ihre tägliche Arbeit bzw. Ihr Nutzungsverhalten aus?

15. Wie organisieren Sie Ihre Aufgaben, die mit Informationssicherheit zu tun haben? Verwenden Sie dazu **Hilfsmittel** (Erinnerungen, Todos, Checklisten...)?

16. Helfen sich die **Kollegen/-innen** dabei **untereinander**? Wenn ja, wie?

17. Wie viel **Zeit** wenden Sie für die Verwendung von **Sicherheitsmechanismen** pro Tag auf?

____ Stunden ____ Minuten

18. Konnten Sie schon mal Ihre **Aufgabe** aufgrund von Sicherheitsmechanismen **nicht erledigen**?

19. Mussten Sie schon mal **Sicherheitsmechanismen umgehen**, um Ihre Arbeit machen zu können?

20. Kommt es vor, dass Sie Sicherheitsregeln nicht einhalten? Falls ja, wie oft, z. B. pro Woche?

____ mal

21. Wie würde die für Sie perfekte sichere Arbeitsumgebung bzw. das perfekte sichere System mit dem Sie arbeiten aussehen? Was könnte das?

22. Was zeichnet Ihrer Meinung nach **gute Sicherheitsmechanismen** aus?

- dass diese im Verborgenen stattfinden?
- dass diese transparent sind?
- dass diese nachvollziehbar sind?
- dass diese möglichst einfach anwendbar sind?

23. Fallen Ihnen **konkrete Sicherheitsmechanismen** ein, die in Ihrem Unternehmen genutzt werden oder genutzt werden sollten?

24. Wissen Sie, ob die **folgenden Mechanismen** in Ihrem Unternehmen genutzt werden? (Hier nur bisher nichtgenannte erfragen)

- Firewall
- Virenschutz
- Passwortmanager
- Single Sign On
- Kommunikations- und Datenverschlüsselung
- Digitale Signaturen
- Malwareschutz
- Security-Tokens
- Anti-Phishing-Tools
- Spamfilter
- Datensicherung

Handlungsbedarf

25. Fallen Ihnen **weitere Sicherheitsmechanismen** ein, die in Ihrem Unternehmen genutzt werden könnten oder genutzt werden sollten?

26. Gibt es Bereiche, in denen Sie **akuten Handlungsbedarf** für Usable Security sehen?

27. Würden Sie sagen, dass es in den **folgenden Bereichen** in Ihrem Unternehmen aktuell **Handlungsbedarf** gibt?

- Zugriffskontrollsysteme
- E-Mail-Sicherheit
- Anti-Phishing
- Datenspeicherung (z. B. in der Cloud)
- Mobile Security
- Social Media Privacy (z. B. Datenschutz bei der Nutzung von Facebook)
- Softwareentwicklung
- Administration von Sicherheitsfunktionen

28. Fallen Ihnen **weitere Bereiche** ein?

Auswahlkriterien

29. Was könnte Ihnen konkret bei der **Auswahl gebrauchstauglicher betrieblicher Software** helfen?

30. Nach welchen **Kriterien** wählt Ihr Unternehmen Software aktuell aus?

31. Würden Sie sagen, dass die **folgenden Kriterien** bei der Softwareauswahl in Ihrem Unternehmen wichtig sind? Wenn ja, in welcher Rangfolge?

- Funktionalität
- Hersteller
- Performance
- Sicherheit
- Usability

32. Fallen Ihnen **weitere Kriterien** ein?

Aktuelle/geplante Maßnahmen

33. Gibt es die Bereitschaft in Ihrem Unternehmen, **eigenes Personal** für Spezialthemen im Bereich **IT-Sicherheit** zu schulen?

34. Gibt es die Bereitschaft in Ihrem Unternehmen, **spezialisierte Werkzeuge** für den Bereich **IT-Sicherheit** einzusetzen?

35. Gibt es die Bereitschaft in Ihrem Unternehmen, **unabhängige Dienstleistungen** für den Bereich **IT-Sicherheit** einzusetzen?

----- Ende Interview -----

Nachbefragung/Verabschiedung

- allgemeines Feedback: Wurden Inhalte oder Interviewfragen vermisst? Wenn ja, welche?
- Befragtem für Teilnahme danken
- Ergebnisse anbieten

Datenschutzvereinbarung

1. Die Teilnahme am Interview ist freiwillig. Das Interview wird im Rahmen eines Forschungsprojekts durchgeführt und dient der Ermittlung von Anforderungen bei der Nutzung betrieblicher Software.
2. Für die Durchführung und wissenschaftliche Auswertung des Interviews sind die HK Business Solutions GmbH und die Technische Hochschule Köln verantwortlich.
3. Die Verantwortlichen tragen dafür Sorge, dass alle erhobenen Daten streng vertraulich behandelt werden und ausschließlich zum vereinbarten Zweck verwendet werden.
4. Die/der Befragte erklärt ihr/sein Einverständnis mit der wissenschaftlichen Auswertung des Interviews.
5. Zu Auswertungszwecken wird ein schriftliches Protokoll des Interviews angefertigt. Namen und Ortsangaben der/des Befragten werden soweit erforderlich im Protokoll unkenntlich gemacht. In Veröffentlichungen wird sichergestellt, dass eine Identifikation der/des Befragten nicht möglich ist.
6. Die Verwertungsrechte (Copyright) des Interviews liegen beim Interviewer/-in bzw. Projektleiter/-in.
7. Die/der Befragte kann ihre/seine Einverständniserklärung innerhalb von 14 Tagen ganz oder teilweise widerrufen.

_____, den _____
Ort Datum

Interviewer(in) Befragte(r)