USecurD

Anforderungsanalyse (Interviewergebnisse)

Projekt	USecureD – Usable Security by Design
Förderinitiative	Einfach intuitiv – Usability für den Mittelstand
Förderkennzeichen	01MU14002
Arbeitspaket	AP 1.2
Datum	31.01.2016
Autor	Hartmut Schmitt (HK Business Solutions)
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. In diesem Dokument sind die Ergebnisse der Stakeholder- und Endanwenderinterviews zusammengefasst.

Schlagworte

Anforderungen an Usable Security, Untersuchungsergebnisse, Interviews, Requirements Engineering, IT-Security, Usability, User Experience

Inhaltsverzeichnis

1 Vorgehensweise

Zur Durchführung der Interviews wurden mehrere Termine mit IKT-Anwenderunternehmen aus dem Kundenkreis von 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 sind. 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 HK Business Solutions und Technische Hochschule Köln vorab einen Interviewleitfaden und eine Datenschutzvereinbarung.

2 Ergebnisse

2.1 Teilnehmerfeld

An den Interviews nahmen insgesamt 10 Teilnehmer (7 w, 3 m) teil. Sie üben in den kleinen und mittleren Unternehmen (6 bis 75 Mitarbeiter) unterschiedliche Funktionen aus: Geschäftsführung, Assistenz der Geschäftsführung, Buchhaltung und Auftragsbearbeitung (je zwei Teilnehmer), Versand und Bürokauffrau (je ein Teilnehmer). Die durchschnittliche Berufserfahrung der Teilnehmer in der aktuellen Funktion beträgt 15 Jahre (min = 0,5, max = 40). Alle Teilnehmer arbeiten in Einzel- bzw. Doppelbüros.

Sämtliche Befragten nutzen beruflich einen PC. Im privaten Umfeld werden neben Smartphones (alle Teilnehmer) vor allem PCs (sechs Teilnehmer), Laptops (fünf Teilnehmer) und Tablets (vier Teilnehmer) genutzt. Im beruflichen Umfeld nutzen sämtliche Befragten ihre PCs und anderen Geräte täglich; vier Teilnehmer geben an, dass diese berufliche Nutzung sehr intensiv ist.

Ihre Kenntnisse bei der Nutzung von PCs (Internet, E-Mail, Office) und Smartphones bzw. Mobilgeräten beurteilen die Befragten von nicht gut bis sehr gut („Tekkie“). Die Mehrheit der Teilnehmer (70 %) schätzt ihre Kenntnisse als „eher gut“ bzw. „ausreichend für die Arbeit“ ein.

2.2 Usability und Sicherheit

Frage: 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?

> Zwei von zehn Teilnehmern kennen den Begriff Usability und übersetzen diesen mit Anwender- bzw. Benutzerfreundlichkeit. Weitere drei Teilnehmer erraten die richtige Bedeutung. Der Hälfte der Teilnehmer ist der Begriff unbekannt.

Frage: Wie schätzen Sie die Relevanz von Usability in Software-Produkten ein?

> Die Relevanz des Themas Usability wird von allen Teilnehmern als „hoch“ (sieben Teilnehmer) bzw. „sehr hoch“ (drei Teilnehmer) eingeschätzt. Begründet wird dies u. a. mit einer besseren Akzeptanz der Produkte und mit einer höheren Arbeitseffizienz.

Frage: Gibt es Usability-Leitfäden oder Usability-Checklisten für Software, die in Ihrem Unternehmen Anwendung finden?

> In keinem der Unternehmen gibt es aktuell Usability-Leitfäden oder Usability-Checklisten für Software.

Frage: Wissen Sie, was in diesem Zusammenhang IT-Sicherheit bedeutet? Wie würden Sie diese beschreiben?

> Vom Begriff IT-Sicherheit haben sieben der zehn der Befragten zumindest ein ungefähres Verständnis („Virenschutz“, „Datenschutz“, „Schutz vor Angriffen“). Drei Teilnehmer machen keine Angabe.

Frage: 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)?

> Den aktuellen Schutz der Daten im eigenen Unternehmen schätzt ein Teilnehmer als „sehr gut“, zwei Teilnehmer als „gut“, sechs Teilnehmer als „durchschnittlich“ und ein Teilnehmer als „nicht gut“ ein.

Frage: Gibt es Sicherheitsguidelines oder Sicherheitschecklisten für Software, die in Ihrem Unternehmen Anwendung finden?

> In keinem der Unternehmen werden aktuell Sicherheitsguidelines oder Sicherheitschecklisten für Software angewendet.

2.3 Sicherheitsmechanismen

Frage: Wie schätzen Sie die Relevanz von IT-Sicherheit und Sicherheitsmechanismen in Software-Produkten ein?

Die Relevanz von IT-Sicherheit und Sicherheitsmechanismen in Software-Produkten wird von acht Teilnehmern als hoch eingeschätzt. Zwei Teilnehmer machen keine Angabe.

Frage: Gibt es Sicherheitsmechanismen, die Sie bei Ihrer Arbeit verwenden?

Als Sicherheitsmechanismen, die bei der Arbeit verwendet werden, nennen die Teilnehmer spontan Antivirensoftware (drei Nennungen), Datensicherung (zwei Nennungen), PINs, User Logins und das Sperren von PCs (je eine Nennung).

Frage: Was denken Sie über die Verwendung von Sicherheitsmechanismen während Ihrer Arbeit?

Mehrere Teilnehmer bezeichnen die Verwendung von Sicherheitsmechanismen als wichtig (drei Teilnehmer) bzw. als angebracht (ein Teilnehmer). Drei Teilnehmer sprechen konkrete Gefahren an („Internet", „Ergebnisseiten im Internet", „suspekte E-Mails"), die solche Mechanismen notwendig machen. Ein Teilnehmer bezeichnet diese Mechanismen als hinderlich.

Frage: Wie belastend wirken sich Sicherheitsmechanismen auf Ihre tägliche Arbeit bzw. Ihr Nutzungsverhalten aus?

Acht von zehn Teilnehmern finden Sicherheitsmechanismen nicht belastend. Ein Teilnehmer thematisiert „geringe Zeitverzögerungen", bei einem Teilnehmer stellt sich „oft ein ungutes Gefühl" ein.

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

Sieben von zehn Teilnehmern verwenden keine Organisations- bzw. Hilfsmittel. Zwei Teilnehmer nennen „abschließbare Türen", ein Teilnehmer führt „Erinnerungen und Aufgaben" an, die in Outlook bzw. handschriftlich hinterlegt werden.

Frage: Helfen sich die Kollegen/-innen dabei untereinander? Wenn ja, wie?

Die Hälfte der Teilnehmer gibt an, dass sich die Kollegen gegenseitig unterstützen, z. B. bei Unklarheiten. Vier Teilnehmer geben an, dass sich die Kollegen nicht untereinander helfen, ein Teilnehmer macht keine Angabe.

Frage: Wie viel Zeit wenden Sie für die Verwendung von Sicherheitsmechanismen pro Tag auf?

Die Teilnehmer wenden durchschnittlich 3,6 Minuten pro Tag für Sicherheitsmechanismen auf (min = 0, max = 15).

Frage: Konnten Sie schon mal Ihre Aufgabe aufgrund von Sicherheitsmechanismen nicht erledigen?

Jeweils ein Befragter schildert Schwierigkeiten beim Onlinebanking (Umgang mit PIN) bzw. beim Wiederherstellen von Daten, während eine Datensicherung läuft. Acht Befragte geben an, dass sie aufgrund von Sicherheitsmechanismen noch nicht daran gehindert wurden, eine Aufgabe zu erledigen. Als Gründe, weshalb Aufgaben nicht erledigt werden können, werden stattdessen Probleme wie Virenbefall oder das Alter des Computers angeführt.

Frage: Mussten Sie schon mal Sicherheitsmechanismen umgehen, um Ihre Arbeit machen zu können?

Neun Teilnehmer mussten bei ihrer Arbeit noch keine Sicherheitsmechanismen umgehen. Ein Teilnehmer gibt an, dass er die Antivirensoftware auf seinem Rechner abschalten musste, um die installierte DATEV-Software updaten zu können.

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

Sieben Teilnehmer geben an, dass sie noch nicht gegen Sicherheitsregeln verstoßen haben, zwei Teilnehmer können hierzu keine Angabe machen. Einer der Befragten schätzt, dass er unbewusst gegen Sicherheitsregeln verstößt.

Frage: Wie würde die für Sie perfekte sichere Arbeitsumgebung bzw. das perfekte sichere System mit dem Sie arbeiten aussehen?

Sechs der Teilnehmer beschreiben eine perfekte sichere Arbeitsumgebung jeweils als

- „ein System, das im Hintergrund läuft und keine tägliche bzw. wöchentliche Wartung benötigt“,
- „ein System, das darauf hinweist, wenn etwas nicht in Ordnung ist“,
- ein System mit Single-Sign-on,
- ein System mit Updates,
- ein System, bei dem „alles über Fingerabdruck“ funktioniert bzw.
- eine Umgebung, bei der jedes genutzte Programm mit einem Passwort geschützt ist und bei der jeder PC generell nach Arbeitsschluss ausgeschaltet wird.

Vier Teilnehmer haben keine Vorstellung davon, wie ein perfektes sicheres System aussehen könnte.

Frage: Was zeichnet Ihrer Meinung nach gute Sicherheitsmechanismen aus?

- Dass diese im Verborgenen stattfinden? (ja: 5 Teilnehmer, nein: 2 Teilnehmer, keine Angabe: 3 Teilnehmer)
- Dass diese transparent sind? (ja: 4 Teilnehmer, nein: 4 Teilnehmer, keine Angabe: 2 Teilnehmer)
- Dass diese nachvollziehbar sind? (ja: 8 Teilnehmer, nein: 0 Teilnehmer, keine Angabe: 2 Teilnehmer)
- Dass diese möglichst einfach anwendbar sind? (ja: 10 Teilnehmer nein: 0 Teilnehmer, keine Angabe: 0 Teilnehmer)

Frage: Fallen Ihnen konkrete Sicherheitsmechanismen ein, die in Ihrem Unternehmen genutzt werden oder genutzt werden sollten? (Mehrfachnennungen möglich)

Von den Teilnehmern werden folgende Sicherheitsmechanismen genannt: Antivirensoftware (fünf Teilnehmer), Passwörter (drei Teilnehmer), elektronischer Schlüssel für den Serverraum (zwei Teilnehmer), Datenbankverschlüsselung, Kopien der Daten im Tresor und Fehlermeldungen, die am Bildschirm erscheinen (jeweils ein Teilnehmer). Drei Teilnehmer machen keine Angabe.

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

- Firewall (ja: 7 Teilnehmer, nein: 2 Teilnehmer, keine Angabe: 1 Teilnehmer)
- Virenschutz (ja: 10 Teilnehmer, nein: 0 Teilnehmer, keine Angabe: 0 Teilnehmer)
- Passwortmanager (ja: 4 Teilnehmer, nein: 1 Teilnehmer, keine Angabe: 5 Teilnehmer)
- Single Sign On (ja: 2 Teilnehmer, nein: 4 Teilnehmer, keine Angabe: 4 Teilnehmer)
- Kommunikations- und Datenverschlüsselung (ja: 1 Teilnehmer, nein: 1 Teilnehmer, keine Angabe: 8 Teilnehmer)
- Digitale Signaturen (ja: 2 Teilnehmer, nein: 3 Teilnehmer, keine Angabe: 5 Teilnehmer)
- Malwareschutz (ja: 8 Teilnehmer, nein: 0 Teilnehmer, keine Angabe: 2 Teilnehmer)
- Security-Tokens (ja: 0 Teilnehmer, nein: 2 Teilnehmer, keine Angabe: 8 Teilnehmer)
- Anti-Phishing-Tools (ja: 1 Teilnehmer, nein: 3 Teilnehmer, keine Angabe: 6 Teilnehmer)
- Spamfilter (ja: 8 Teilnehmer, nein: 0 Teilnehmer, keine Angabe: 2 Teilnehmer)
- Datensicherung (ja: 10 Teilnehmer, nein: 0 Teilnehmer, keine Angabe: 0 Teilnehmer)

2.4 Handlungsbedarf

25. Fallen Ihnen weitere Sicherheitsmechanismen ein, die in Ihrem Unternehmen genutzt werden könnten oder genutzt werden sollten? (Mehrfachnennungen möglich)

Von jeweils einem Teilnehmer werden folgende Sicherheitsmechanismen genannt, die genutzt werden könnten bzw. sollten: Firewall, persönliche Passwörter (statt Gruppenkennungen) und mechanische Absicherung des Serverraums. Sieben Teilnehmer machen keine Angabe.

26. Gibt es Bereiche, in denen Sie akuten Handlungsbedarf für Usable Security sehen? (Mehrfachnennungen möglich)

Von jeweils einem Teilnehmer wird Handlungsbedarf in diesen Bereichen angesprochen: Einrichtung von Antivirensoftware, Einrichtung von Back-ups für alle PCs, generelle Vereinfachung entsprechender Mechanismen. Sieben Teilnehmer machen keine Angabe.

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

- Zugriffskontrollsysteme (ja: 3 Teilnehmer, nein: 4 Teilnehmer, keine Angabe: 3 Teilnehmer)
- E-Mail-Sicherheit (ja: 4 Teilnehmer, nein: 3 Teilnehmer, keine Angabe: 3 Teilnehmer)
- Anti-Phishing (ja: 5 Teilnehmer, nein: 3 Teilnehmer, keine Angabe: 2 Teilnehmer)
- Datenspeicherung (z. B. in der Cloud) (ja: 1 Teilnehmer, nein: 5 Teilnehmer, keine Angabe: 4 Teilnehmer)
- Mobile Security (ja: 5 Teilnehmer, nein: 3 Teilnehmer, keine Angabe: 2 Teilnehmer)
- Social Media Privacy (z. B. Datenschutz bei der Nutzung von Facebook) (ja: 0 Teilnehmer, nein: 5 Teilnehmer, keine Angabe: 5 Teilnehmer)
- Softwareentwicklung (ja: 1 Teilnehmer, nein: 4 Teilnehmer, keine Angabe: 5 Teilnehmer)
- Administration von Sicherheitsfunktionen (ja: 3 Teilnehmer, nein: 4 Teilnehmer, keine Angabe: 4 Teilnehmer)

28. Fallen Ihnen weitere Bereiche ein?

Es fallen keinem Teilnehmer weitere Bereiche ein.

2.5 Auswahlkriterien

Frage: Was könnte Ihnen konkret bei der Auswahl gebrauchstauglicher betrieblicher Software helfen? (Mehrfachnennungen möglich)

Von den Teilnehmern je einmal genannt werden Produktvorstellungen, Demoversionen, Leitfäden, Guidelines und gute Beratung.

Frage: Nach welchen Kriterien wählt Ihr Unternehmen Software aktuell aus? (Mehrfachnennungen möglich)

Kriterien, die den Befragten spontan einfallen, sind die Funktionalität (zwei Nennungen), dass die Software den Anforderungen entspricht (zwei Nennungen), dass die Software nützlich ist (eine Nennung) und dass im Unternehmen Handlungsbedarf besteht (eine Nennung). Ferner wird von einem Teilnehmer angeführt, dass die Software leicht zu bedienen ist und dass bei Problemen ein Ansprechpartner erreichbar ist. Drei Teilnehmer machen keine Angabe zu den Auswahlkriterien.

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

Einige Teilnehmer vergeben in ihrer Rangfolge Plätze doppelt oder lassen manche Kriterien weg, daher ist eine transparente, zahlenmäßige Darstellung nur schwer möglich. Es ergeben sich jedoch sehr klare Tendenzen: Das Kriterium „Funktionalität“ wird von den Teilnehmern als am wichtigsten eingeschätzt (50 % nennen es auf Rang 1, 50 % auf Rang 2). Dahinter folgen die Kriterien „Usability“ (40 % Rang 1 und 40 % Rang 2), „Sicherheit“ (30 % Rang 1 und 20 % Rang 2) und „Performance“ (0 % Rang 1, 20 % Rang 2 und 60 % Rang 3). Das Kriterium „Hersteller“ landet bei allen Befragten auf dem letzten Rang.

Frage: Fallen Ihnen weitere Kriterien ein? (Mehrfachnennungen möglich)

Weitere Kriterien, die von den Teilnehmern je einmal genannt wurden, sind „persönlicher Ansprechpartner“ und „Preis“.

2.6 Aktuelle/geplante Maßnahmen

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

Vier Teilnehmer bestätigen die Bereitschaft, eigenes Personal für Spezialthemen zu schulen, vier Teilnehmer verneinen diese. Zwei Teilnehmer können keine Angabe machen, bestätigen aber, dass Schulungen sinnvoll wären.

Frage: Gibt es die Bereitschaft in Ihrem Unternehmen, spezialisierte Werkzeuge für den Bereich IT-Sicherheit einzusetzen?

Sechs Teilnehmer verneinen die Bereitschaft des Unternehmens, Spezialwerkzeuge einzusetzen. Zwei Teilnehmer bestätigen die grundsätzliche Bereitschaft, zwei Teilnehmer machen keine Angabe.

Frage: Gibt es die Bereitschaft in Ihrem Unternehmen, unabhängige Dienstleistungen für den Bereich IT-Sicherheit einzusetzen?

Fünf Teilnehmer bestätigen die Bereitschaft des Unternehmens, in unabhängige Dienstleistung zu investieren. Zwei Teilnehmer machen keine Angabe. Drei Teilnehmer sehen keine entsprechende Bereitschaft.

2.7 Weitere Anmerkungen

Von einem Teilnehmer wird angemerkt, dass sich viele Firmen eine eigene IT-Abteilung nicht leisten könnten; bei komplizierten Dingen sagte man sich dann „das lasse ich lieber, weil es im ersten Moment nicht wehtut“.