

Usable Security: Usability als Beitrag zu mehr IT-Sicherheit



World Usability Day
Würzburg, 10.11.2016

Hartmut Schmitt, HK Business Solutions GmbH

Sicherheitsmechanismen mit schlechter Usability ...

- erfordern zusätzliche Prozessschritte.
- sind leistungsverringend.
- werden von Nutzern als Hürde wahrgenommen.

Folge:

Das Nutzerverhalten passt sich entsprechend an.

Beispiel: Sicherheitswarnungen

Problem:

Nutzer können oft keine informierte Entscheidung treffen.

- keine Kontextinformationen
- Risiken nur unvollständig beschrieben
- Handlungsoptionen und Folgen unklar

Folge:

Warnungen werden ignoriert.

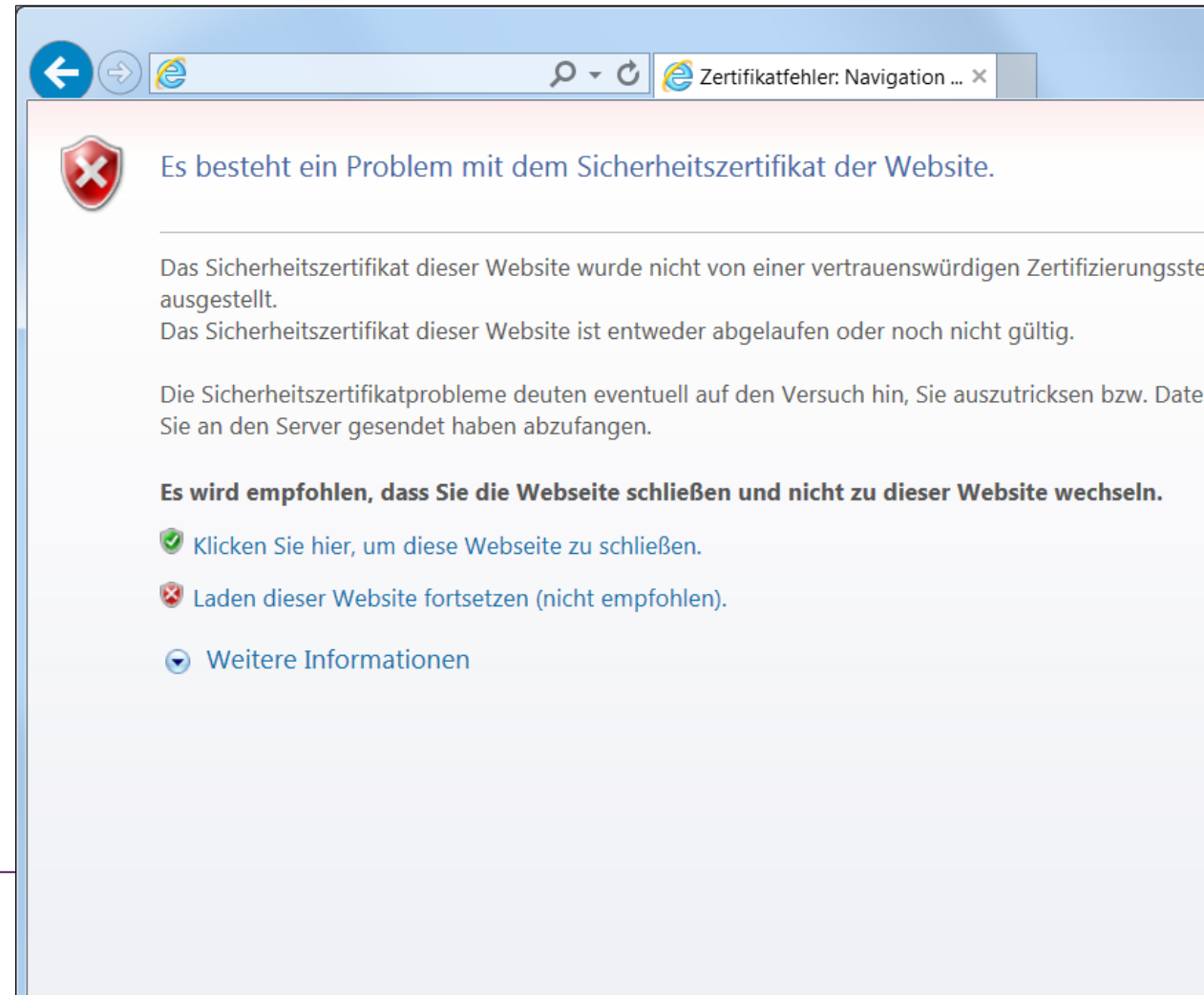
Beispiel: Zertifikatfehler

Probleme:

- fast 100 % Falschmeldungen (false positives)
- Gewöhnungseffekte

Folge:

Warnungen werden ignoriert.



Beispiel: Passwörter

Situation:

- z. T. sehr komplexe Passwortregeln
- wachsende Anzahl von Nutzerkonten

Problem:

- Das menschliche ist Gehirn nicht darauf ausgelegt, sich zufällige Zeichenfolgen zu merken.

Hinweistext:

Ihr neues Passwort muss sich von den letzten zwölf verwenden unterscheiden.

Das Passwort **darf nicht** ihren Benutzernamen enthalten.

Es muss **acht oder mehr Zeichen** haben.

Zwischen Groß- und Kleinschreibung wird unterschieden.

Es **muss mindestens** eine Ziffer enthalten.

Es kann folgende Sonderzeichen enthalten: _~.,\$()# @ & ! ?

Ein Großbuchstabe (deaktiviert)

Das Passwort muss mindestens einen Großbuchstaben

Ein Kleinbuchstabe (deaktiviert)

Das Passwort muss mindestens einen Kleinbuchstaben

Eine Ziffer (aktiviert)

Das Passwort muss mindestens eine Ziffer beinhalten.

Keine Umlaute (deaktiviert)

Das Passwort darf keine Umlaute enthalten.

Kein Leerzeichen (deaktiviert)

Das Passwort darf kein Leerzeichen enthalten.

Beispiel: Passwörter

Folge:

Passwortregeln werden missachtet.

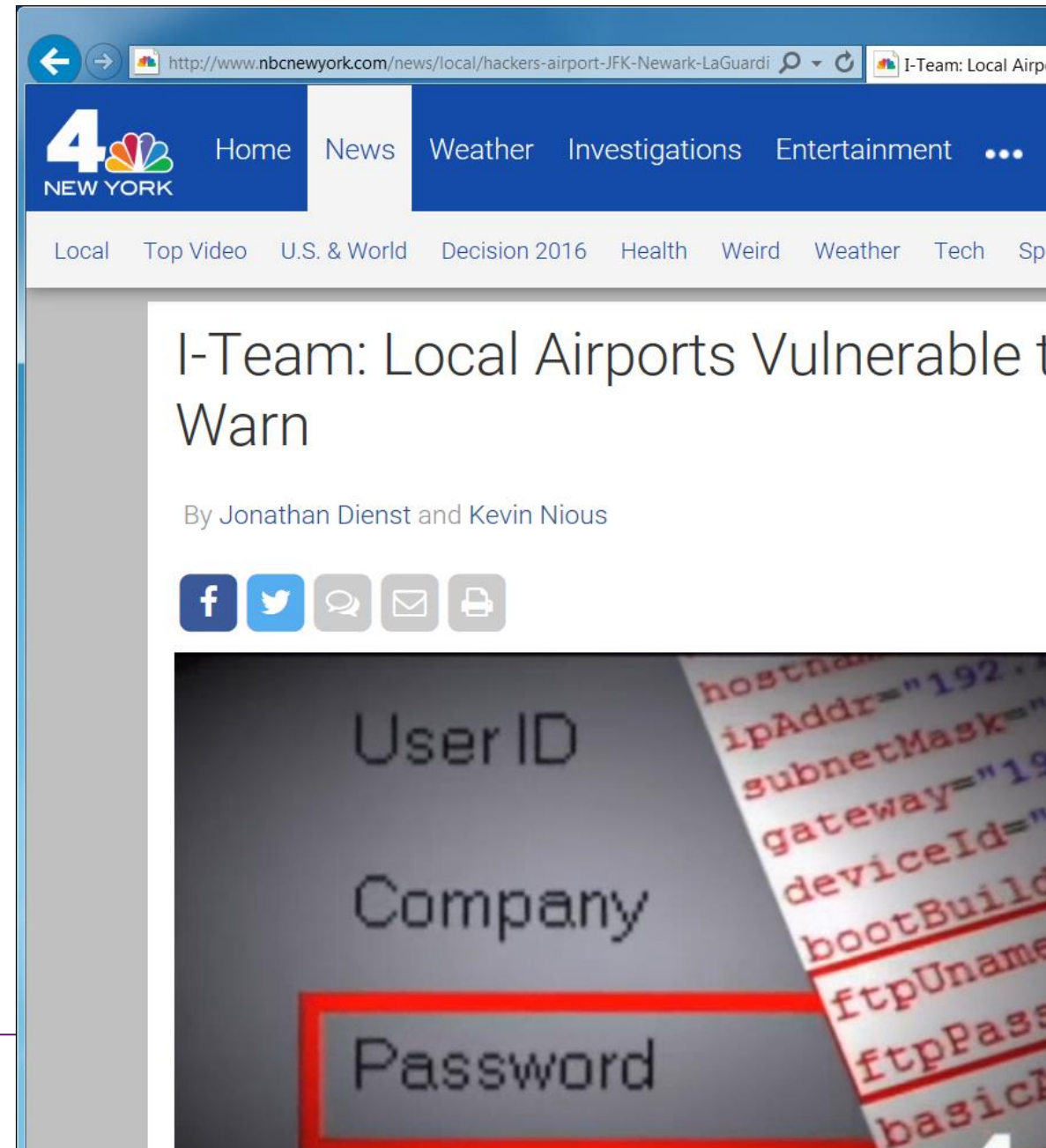
- Passwörter werden für mehrere Nutzerkonten verwendet.
- Gewählte Passwörter sind zu einfach (z. B. „Passw0rd“).
- Passwörter werden auf Post-its notiert.

Beispiel: Passwörter

Außerdem:

mangelhafte Unterstützung für
nicht-spezialisierte Entwickler

- Bsp.: Zugangsdaten werden im
Programmcod hinterlegt.



Situation heute

Bedarf nach besseren Lösungen ist bekannt.

Herausforderungen

- traditionelle Sichtweise im Security Engineering
- geringe Motivation des Nutzers
 - > Sicherheit i. d. R. nicht Primäraufgabe
- Sensibilisierung nicht ausreichend
 - > Nutzer sind sich der Risiken oft bewusst, machen aber trotzdem Fehler.
- verbreitete Wahrnehmung: Usability vs. Sicherheit
- Ausbalancieren von Usabilityzielen und Sicherheitszielen

Beispiel: Smartphone-Sperre

Usabilityziel

- umgehende Entsperrung des Smartphones
- Minimierung von Fehlerquellen
- keine Wiederholungen

Securityziel

- Schutz vor unberechtigttem Zugriff auf Daten im Smartphone

Beispiel: Smartphone-Sperre

Variante 1 – einfaches Berühren

Usability

- umgehende Entsperrung
- keine Fehlerquellen
- keine Wiederholungen

Security

- kein Schutz vor unbefugtem Zugriff

Beispiel: Smartphone-Sperre

Variante 2 – Entsperrmuster

Usability

- leicht verzögerter Zugang
- Fehlerquote und Wiederholungen abhängig vom Muster

Security

- Gefahren durch Shoulder Surfing Attacks und Smudge Attacks
- geringer Schutz vor unbefugtem Zugriff

Beispiel: Smartphone-Sperre

Variante 3 – PIN-Eingabe

Usability

- verzögerter Zugang
- Fehlerquote und Wiederholungshäufigkeit eher hoch

Security

- Gefahren durch Shoulder Surfing Attacks
- recht guter Schutz vor unbefugtem Zugriff

Beispiel: Smartphone-Sperre

Variante 4 – biometrisches Merkmal

Usability

- umgehende Entsperrung
- keine Fehlerquellen
- keine Wiederholungen

Security

- sehr guter Schutz vor unbefugtem Zugriff

Aber: biometrische Daten sind sehr sensible persönliche Daten!



Forschung zum Thema Usable Security

1975: Psychological acceptability als Designprinzip*

- “ease of use”
- “users ... automatically apply the protection mechanisms correctly”
- “user's mental image ... matches the mechanisms he must use”

1995–2000: grundlegende Studien und Veröffentlichungen

- Bedarf nach einer stärkeren Integration von Security Engineering und Usability Engineering
- “Usable Security”
- v. a. im anglo-amerikanischen Raum

*Saltzer & Schroeder (1975): The Protection of Information in Computer Systems

Projekt „Usable Security by Design“

- Förderinitiative „Einfach intuitiv – Usability für den Mittelstand“
- Laufzeit: 1.5.2015 – 30.4.2017
- Zielgruppe Anwenderfirmen: Nachfrage wecken, Produktauswahl unterstützen
- Zielgruppe Herstellerfirmen: Entwicklung systematisieren, Werkzeuge bereitstellen



Technology
Arts Sciences
TH Köln



Projekt „Usable Security by Design“

- Qualitätsmodell auf Basis des ISO-Standards 25010

E 1.4 USecureD-Qualitätsmodell (V.1).pdf - Adobe Acrobat Reader DC

Datei Bearbeiten Anzeige Fenster Hilfe

USecur

3.1 Aufbau des USecureD-Qualitätsmodells

Qualitätsbereich	Qualitätsmerkmal	Teilmerkmale
Produktqualität	Gebrauchstauglichkeit	Angemessenheitserkennung Erlernbarkeit Fehlertoleranz Erwartungskonformität Steuerbarkeit Selbstbeschreibungsfähigkeit Fehlersicherheit Ästhetik der Benutzungsschnittstelle Barrierefreiheit Konformität der Benutzbarkeit
	Sicherheit	Vertraulichkeit Integrität Nachweisbarkeit

E 1.4 USecureD-Qualitätsmodell (V.1).pdf - Adobe Acrobat Reader DC

Datei Bearbeiten Anzeige Fenster Hilfe

USecur

3.3 Nutzungsqualität

3.3.1 Effektivität

Genauigkeit und Vollständigkeit, mit der Nutzer bestimmte Ziele erreichen [DIN ISO/IEC 25000:2013-01]

3.3.1.1 Genauigkeit der Zielerreichung

Beschreibung	Grad der Genauigkeit, mit der ein Nutzer bestimmte Ziele in einem bestimmten Nutzungskontext erreicht.
Quelle	DIN EN ISO 9241-11:1999-01

3.3.1.2 Vollständigkeit der Zielerreichung

Beschreibung	Grad der Vollständigkeit, mit der ein Nutzer bestimmte Ziele in einem bestimmten Nutzungskontext erreicht.
--------------	--

Projekt „Usable Security by Design“

- Qualitätsmodell auf Basis des ISO-Standards 25010
- Sammlung typischer Anwendungsfälle im Bereich betrieblicher Software

3.3 Monats-/Quartalsabschluss durchführen	
ID/Titel	Monats-/Quartalsabschluss durchführen
Beschreibung	Dieser Use Case beschreibt, wie ein Finanzbuchhalter einen Monats- bzw. Quartalsabschluss durchführt.
Akteur	Finanzbuchhalter
System	Finanzbuchhaltung
Nutzungskontext	Der Anwender ist an der Finanzbuchhaltung teil, der der Erstellung von Monats- bzw. Quartalsabschlüssen dient.
Ziel	Anwender: • Periodenabschlüsse mitsamt Kontenplan erstellt werden Geschäftsleitung: • Geschäftsdaten sind vor und nach dem Abschluss • Formale Anforderungen an den Abschluss
Vorbedingung	Alle relevanten Geschäftsvorgänge sind abgeschlossen.
Standardablauf	1. Finanzbuchhalter ruft Monats- bzw. Quartalsabschluss an. 2. System zeigt Monats- bzw. Quartalsabschluss an. 3. Finanzbuchhalter wählt Filter (Periode, Beraternummer (eigene DATEV-Nummer), Passwort für Verschlüsselung der Exportdatei). 4. System zeigt Aufträge des Kunden. 5. Finanzbuchhalter wählt Filter (z. B. best. Zeitraum). 6. System zeigt Prüfliste an. 7. Finanzbuchhalter bestätigt Prüfliste. 8. System legt Sammelrechnung an, die alle Geschäftsvorgänge aus (optional) und begleicht. 9. Finanzbuchhalter führt DATEV-Export durch. 10. System erstellt Exportdatei und speichert sie. 11. Anwender speichert Exportdatei.
Ausnahmen	–
Nachbedingung/Ergebnis	Nachbedingung: Der Periodenabschluss wurde durch den Steuerberater übergeben oder per E-Mail.
Sicherheitsrisiken	• Unsichere direkte Objektkommunikation • Sicherheitsrelevante Fehlkonfiguration • Verlust der Vertraulichkeit sensibler Daten
Gefährdung	• Unberechtigte Personen haben Zugriff auf Geschäftsdaten.
Qualitätsmerkmale	Gebrauchstauglichkeit: Fehlertoleranz, Erwartungskonformität, Steuerbarkeit, Fehlersicherheit Sicherheit: Vertraulichkeit, Integrität, Nachweisbarkeit, Zugriffskontrolle,

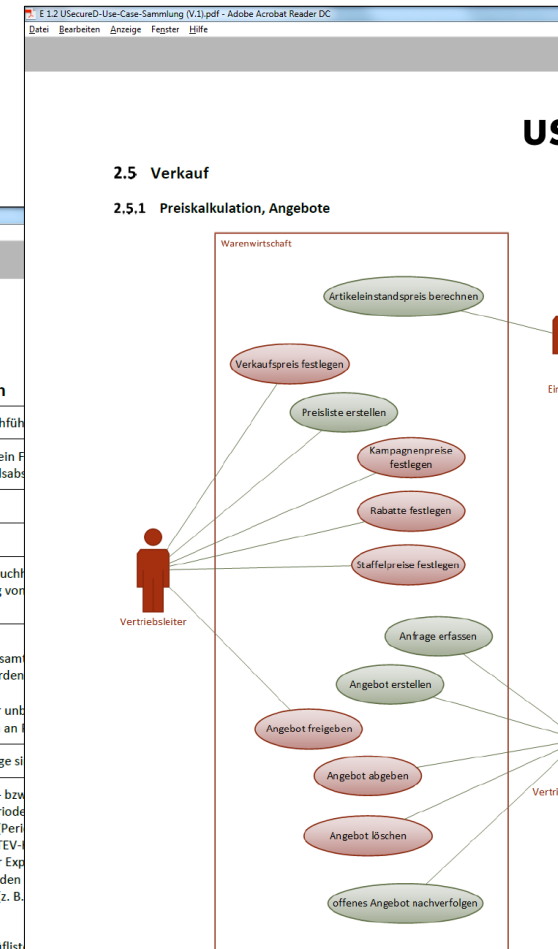
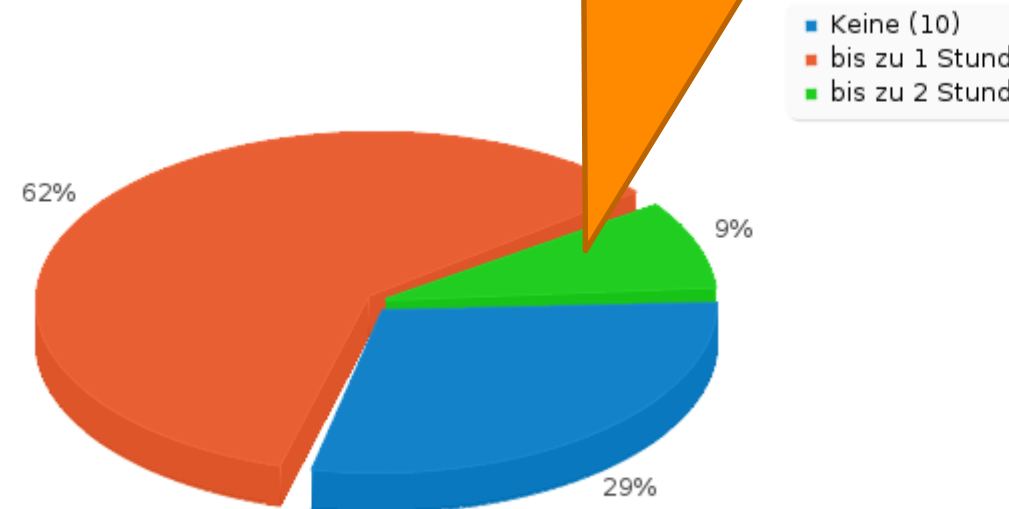


Abbildung 5: Use Cases Preiskalkulation, Angebote

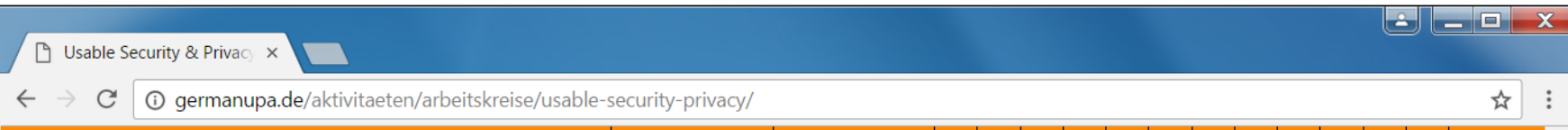
Projekt „Usable Security by Design“

- Qualitätsmodell auf Basis des ISO-Standards 25010
- Sammlung typischer Anwendungsfälle im Bereich betrieblicher Software
- Onlinestudie (+ Benutzerinterviews, Expertenworkshops):
 - > Verständnis und Stellenwert
 - > Umsetzungsgrad
 - > aktuelle Schwierigkeiten

für Sicherheitsmechanismen
aufgewendete Zeit:
bei 9 % der Anwender täglich
zwischen 1 und 2 Stunden







Interner Bereich

GERMAN UPA
Berufsverband der Deutschen Usability
und User Experience Professionals

Start | Aktuelles

Aktivitäten »

Berufsfeld Usability »

Zertifizierung »

National Experts »

Arbeitskreise »

Wie gründe ich einen Arbeitskreis? »

User Research »

Barrierefreiheit »

Nachwuchsförderung »

In-house »

Qualitätsstandards »

Usability in der Medizintechnik »

ROI UX »

Usable Security & Privacy

1. Über den Arbeitskreis
2. Motivation und Ziele
3. Aktivitäten
4. Arbeitskreisleitung
5. Aktive Mitglieder
6. Kontakt und Mitarbeit
7. Termine des Arbeitskreises

Über den Arbeitskreis

Der Arbeitskreis Usable Security & Privacy bietet UPA ein Forum für den Gedankenaustausch und Zusammenarbeit rund um das Thema benutzerspezifische Informationssicherheit. Der Arbeitskreis beschäftigt sich mit Konzepten, die sicherheitsfördernde Verfahren für Produkte stärker an den Zielen und Aufgaben der Anwender dafür sorgen, dass Funktionsweisen von Sicherheitsprodukten für Nichtexperten verständlich sind.

Motivation und Ziele

Bei der Anschaffung von Software und Technik ist die Usability eines der zentralen Auswahlkriterien. Jedoch werden diese Produkte oft Sicherheitslücken aufweisen, die durch eine schlechte Usability entstehen.

Usable Security | XING

XING AG [DE] | <https://www.xing.com/communities/groups/usable-security-1072338>

XING

Gruppen > Usable Security

Usable Security

Gedankenaustausch zwischen Praxis und Wissenschaft rund um das Thema Usable Security (gebrauchstaugliche Informationssicherheit)

Beiträge Über diese Gruppe Events Gruppen-Mitglieder

Beiträge aus allen Foren

 **Hartmut Schmitt**

Im Forum Veranstaltungen - 03.11.2016, 11:06

Reminder: Usable-Security-Vortrag beim WUD Würzburg (10. November 2016)

World Usability Day Würzburg 2016

Zusammenfassung

Security Engineering und Usability Engineering sind (immer noch) weitgehend voneinander entkoppelt.

- Folge: Sicherheitsmechanismen werden falsch angewendet, umgangen oder ignoriert.

Es besteht Handlungsbedarf.

- interdisziplinäre Zusammenarbeit: IT-Security, Usability, Mensch-Computer-Interaktion, Design, Psychologie ...
- bessere Lösungen, dadurch Risikominimierung, Effizienzsteigerung ...

Es gibt i. d. R. keine allein seligmachenden Lösungen.

- aber: Es gibt Werkzeuge, die bei der Umsetzung unterstützen.

Ansprechpartner:

Hartmut Schmitt

HK Business Solutions GmbH

Mellinweg 20

66280 Sulzbach

Telefon: +49 6897 99904-24

Fax: +49 6897 99904-10

E-Mail: schmitt@hk-bs.de

Projekt-Webseite: www.usecured.de

- 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.
- Der Förderschwerpunkt unterstützt gezielt kleine und mittlere Unternehmen (KMU) sowie das Handwerk bei digitalen Transformation sowie der Entwicklung und Nutzung moderner Informations- und Kommunikationstechnologien (IKT). „**Mittelstand-Digital**“ setzt sich zusammen aus den Förderinitiativen „**Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse**“, „**eStandards: Geschäftsprozesse standardisieren, Erfolg sichern**“ und „**Einfach intuitiv – Usability für den Mittelstand**“.
- Weitere Informationen finden Sie unter www.mittelstand-digital.de.