Benutzerfreundliche IT-Sicherheit: Prozessintegration und Werkzeuge (UPA-Arbeitskreis Usable Security & Privacy)

Hartmut Schmitt[1], Edna Kropp[2]

HK Business Solutions GmbH[1]
akquinet AG[2]

Zusammenfassung

Gängige Sicherheitsfeatures von interaktiven Systemen und Technikprodukten sind für viele Anwender und Anwenderinnen zu komplex. Sie sind zeitaufwändig in der Bedienung, für Nichtexperten schwer verständlich und werden daher falsch bedient oder gleich komplett umgangen. Der Arbeitskreis Usable Security & Privacy beschäftigt sich aus diesem Grund mit Ansätzen und geeigneten Konzepten, um sicherheits- und privatheitsfördernde Verfahren und Technologien stärker an den Zielen und Aufgaben der Anwenderinnen und Anwender auszurichten. Im Workshop „Benutzerfreundliche IT-Sicherheit: Prozessintegration und Werkzeuge“ werden gemeinsam mit den Teilnehmenden Erfahrungen diskutiert, wie Usability Engineering und Security Engineering stärker miteinander verzahnt werden können. Hierbei werden unter anderem diese Fragestellungen betrachtet: Wie können Methoden, Tools und Erkenntnisse aus dem Bereich (Usable) Security & Privacy in den User-Centered-Design-Prozess integriert werden? Und welche Evaluationsmethoden und -werkzeuge können für den Bereich Usable Security & Privacy genutzt werden?

1 Nutzerzentrierte Gestaltung von Sicherheitsfeatures

Der Schutz sensibler digitaler Daten wird immer wichtiger. Technikprodukte und interaktive Systeme, mit denen solche Daten erzeugt oder verwaltet werden, sollten daher mit Sicherheitsfeatures ausgestattet sein, die für möglichst alle verständlich und benutzbar sind – und zwar sowohl im beruflichen wie im privaten Bereich (Holz et al., 2016). Damit dies gelingt, bedarf es eines interdisziplinären Ansatzes, der Methoden und Werkzeuge des Security Engineerings mit Modellen der Psychologie und Erkenntnissen aus der Mensch-

Veröffentlicht durch die Gesellschaft für Informatik e. V. und die German UPA e. V. 2017 in
S. Hess, H. Fischer (Hrsg.):
Mensch und Computer 2017 – Usability Professionals, 10.–13. September 2017, Regensburg.
 https://doi.org/10.18420/muc2017-up-0115

Maschine-Interaktion und der Designforschung zusammenführt. Dieser Ansatz wird seit einigen Jahren unter dem Schlagwort „Usable Security & Privacy“ diskutiert.

Ein oft angeführtes, aber bislang noch ungelöstes Beispiel in diesem Themenfeld ist die vertrauliche E-Mail-Kommunikation: Obwohl das Thema seit etwa 20 Jahren erforscht wird (Whitten & Tygar, 1999), sehen auch heute noch 70 % der Teilnehmenden einer Studie (Nguyen & Lo Iacono, 2016) Bedarf an gebrauchstauglichen Lösungen für die E-Mail-Verschlüsselung. Es gibt also eine große Nachfrage nach verwertbaren Erkenntnissen aus der Forschung, aber auch nach praktischen Empfehlungen für deren Umsetzung in benutzerfreundliche IT-Sicherheitsfeatures und -lösungen. Im Workshop sollen bisherige Erkenntnisse und Erfahrungen über die Integration in die Entwicklung interaktiver Systeme und mögliche Evaluationsmethoden ausgetauscht werden.

2 Integration von Security Engineering und User-Centered Design

Für die heute übliche Gestaltung sicherer Systeme wurde eine Vielzahl von Vorgehensmodellen und Best Practices entwickelt. Es existieren Standards zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten wie die Common Criteria (Common Criteria Maintenance Board, 2017), verpflichtende anwendungsspezifische Regelwerke für bestimmte Dienstleistungen, z. B. für die Abwicklung von Kreditkartentransaktionen (PCI Security Standards Council, 2013), und organisatorische Sicherheitsvorgaben, z. B. der IT-Grundschutz (Bundesamt für Sicherheit in der Informationstechnik, 2017). Daneben gibt es zahlreiche Handlungsempfehlungen für die Produktentwicklung wie z. B. die Development und Code Review Guides des Open Web Application Security Project (OWASP, 2013; OWASP, 2016) und außerdem vereinzelte Vorgehensmodelle wie etwa den Security Development Lifecycle von Microsoft (Microsoft Corporation, 2017). Gemeinsam ist all diesen Arbeiten allerdings, dass Usability – wenn überhaupt – nur am Rande berücksichtigt wird und dass in der Regel keine konsequente Einbeziehung der Anwender und Anwenderinnen stattfindet (Gorski & Lo Iacono, 2016; Wijayarathna et al., 2017).

In vielen anderen Bereichen der System- und Produktentwicklung dagegen ist die nutzerzentrierte Gestaltung schon lange etablierte Praxis. User-Centered Design (Norman & Draper, 1986) versteht sich als interaktiver und iterativer Gestaltungsprozess, bei dem die Anwenderinnen und Anwender des Produktes mit ihren Aufgaben, Zielen und Eigenschaften in den Mittelpunkt des Entwicklungsprozesses gestellt werden. Hauptargument für die Anwendung von User-Centered-Design-Prozessen (Deutsches Institut für Normung, 2011) ist meist die Passgenauigkeit des Produktes an die Anforderungen von Anwenderinnen und Anwendern, die durch deren Einbindung an unterschiedlichen Punkten des Gestaltungsprozesses erreicht wird. Hierdurch können Kosten vermieden werden, die andernfalls oft durch Fehlentwicklungen entstehen. Hinsichtlich Sicherheit und Usability gibt es jedoch Ziele, die einander widersprechen. Entsprechende Untersuchungen (Whitten &

Tygar, 1999) zeigen beispielsweise, dass Anwenderinnen und Anwender in ihrem Nutzungsverhalten häufig Kompromisse zwischen sicherer und gebrauchstauglicher Nutzung eingehen, um ihre Aufgaben zu erledigen. Eine Erhebung entsprechender Bedarfe ist im User-Centered Design nicht explizit vorgesehen, weshalb spezifische Anforderungen hinsichtlich Usable Security & Privacy oft weitgehend unberücksichtigt bleiben.

Dies offenbart die Notwendigkeit einer stärkeren Integration von etablierten Prozessen und Vorgehensmodellen aus den Bereichen Usability, IT-Sicherheit und Datenschutz. Für die Verantwortlichen in einem solchen integrierten Prozess bedeutet dies, für Sicherheitsinteressen und -anforderungen auf unterschiedlichen (Anwendungs-)Ebenen sensibilisiert zu sein und insbesondere in frühen Phasen interdisziplinär und organisationsübergreifend auf Schutzziele der verschiedenen Interessengruppen hinzuweisen, z. B. in der Herstellung, dem Betrieb und der Nutzung eines IT-Systems.

3 Werkzeugunterstützung für benutzerfreundliche IT-Sicherheit

Gestaltungs- und Entwurfswerkzeuge, die bereits in frühen Phasen der Entwicklung eingesetzt werden, können eine geeignete Arbeitsgrundlage darstellen, um IT-Systeme zu entwickeln, die gleichermaßen sicher und benutzerfreundlich sind. Mit solchen Werkzeugen können typische Usabilityschwächen, wie sie bei der Konzeption, dem Entwurf oder der Entwicklung von Sicherheitsfeatures auftreten, bestenfalls von Anfang an vermeiden werden. Diese Mängel müssen dann nicht erst in späteren Prozessphasen identifiziert, dokumentiert und – mit höherem Aufwand – nachträglich beseitigt werden.

Solche Entwurfs- und Gestaltungswerkzeuge dienen also zur Integration von Schutzmaßnahmen als Teil der Qualitätssicherung in frühen Projektphasen. Je nach Abstraktionsgrad können verschiedene Werkzeugarten unterschieden werden (Nehren et. al, 2017), beispielsweise

- allgemeine Grundsätze und Prinzipien, die z. B. dabei helfen, zu Beginn der Systementwicklung die richtigen Weichenstellungen vorzunehmen,
- konkrete Entwicklungsrichtlinien, die beschreiben, wie solche Prinzipien genau umgesetzt werden können, und
- bewährte, wiederverwendbare Musterlösungen, also etwa Design- oder Interaktionspatterns für bekannte, wiederkehrende Gestaltungsprobleme.

Idealerweise sollten solche Entwurfs- und Gestaltungswerkzeuge möglichst einfach auch in etablierte Entwicklungsprozesse integriert werden können. Neben diesen Werkzeugen sollten in Entwicklungsprojekten aber stets auch Methoden und Tools eingesetzt werden, mit denen im Anschluss an die Implementierung die tatsächlich erreichte Qualität überprüft bzw. gemessen werden kann. Hierbei kann unterschieden werden zwischen analytischen Evaluationsverfahren, bei denen die Bewertung durch einen oder mehrere Experten erfolgt,

und empirischen Evaluationsverfahren, bei denen Probanden herangezogen werden. Bislang liegen nur wenige Arbeiten vor, die sich mit der Usability-Evaluation von Sicherheitsfeatures beschäftigten (u. a. Egelmann et al., 2008; Jaferian, 2011; Kainda et al., 2010). Dadurch gibt es nur wenige Anhaltspunkte, ob bzw. welche Besonderheiten in Bezug auf die Rahmenbedingungen zu beachten sind, welche Usabilitymetriken und -indikatoren für eine Usable-Security-Evaluation geeignet sind und ob bzw. welche (etablierten) Usabilitywerkzeuge für Usable-Security-Evaluationen geeignet sind und leicht in bestehende Systementwicklungsprozesse integriert werden können.

4 Agenda des Workshops

Den Schwerpunkt des 90-minütigen Workshops bilden Diskussionen mit den Teilnehmenden zu den oben beschriebenen Aspekten. Insbesondere wird ein Erfahrungsabgleich zu folgenden Themen angestrebt:

- Integration von (Usable) Security & Privacy in bestehende Vorgehensmodelle, insbesondere den User-Centered-Design-Prozess,
- Berücksichtigung von Erkenntnissen aus der Usable-Security-Forschung,
- Integration von Methoden und Tools (Patterns, Guidelines, Best Practices u. ä.) aus dem Bereich Usable Security & Privacy,
- Anwendbarkeit bekannter Usability-Evaluationsmethoden und -werkzeuge auf den Bereich Usable Security & Privacy und
- möglicher Bedarf nach Anpassungen bzw. Erweiterungen dieser Methoden und Werkzeuge.

Außerdem werden im Rahmen des Workshops der Arbeitskreis, seine Themen, Ziele und handelnde Personen sowie seine Fachschrift kurz vorgestellt. Zudem wird auf die Ergebnisse des Arbeitskreis-Workshops bei der Usability Professionals 2016 (UP16) zurückgeblickt. Die Ergebnisse des Workshops werden im Nachgang aufbereitet und den Teilnehmenden zur Verfügung gestellt.

5 Der UPA-Arbeitskreis „Usable Security & Privacy“

Der Arbeitskreis Usable Security & Privacy der German UPA bietet seit 2015 ein Forum für den Gedankenaustausch und die interdisziplinäre Zusammenarbeit rund um das Thema benutzerfreundliche Informationssicherheit. Er beschäftigt sich mit Ansätzen und Konzepten, die sicherheits- und privatheitsfördernde Verfahren und Technologien stärker als bisher an den Zielen und Aufgaben der Anwenderinnen und Anwender ausrichten. Ziel des Arbeitskreises ist es, sowohl bei Usability- und UX-Professionals als auch im privaten und geschäftlichen Umfeld im Allgemeinen ein stärkeres Bewusstsein für das Thema Usable Security & Privacy

zu schaffen. Um die Arbeit der Usability- und UX-Professionals zu unterstützen, wird das vorhandene Fachwissen aus Forschung und beruflicher Praxis zusammengeführt und es werden Brücken zwischen der Arbeit der Usability- und UX-Professionals und anderen Disziplinen, beispielsweise dem Security-Engineering, geschlagen. Mit gemeinsamen Veranstaltungen bietet der Arbeitskreis zudem eine Plattform, um Erfahrungen und Wissen gezielt auszutauschen.

Danksagung

Die Autoren danken den übrigen Mitgliedern des Arbeitskreises „Usable Security & Privacy“. Teile dieser Arbeit sind im Rahmen des Forschungsprojektes USecureD (BMWi-Förderkennzeichen 01MU14002) entstanden.

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (2017): *IT-Grundschutz*. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Common Criteria Maintenance Board (2017): *Common Criteria*. Verfügbar unter: https://www.commoncriteriaportal.org/

Deutsches Institut für Normung (2011): Ergonomie der Mensch-System-Interaktion – Teil 210: Prozess zur Gestaltung gebrauchstauglicher interaktiver Systeme (ISO 9241-210:2010); Deutsche Fassung EN ISO 9241-210:2010

Egelman, S., Cranor, L. F., Hong, J. (2008): You've been warned: an empirical study of the effectiveness of web browser phishing warnings. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1065–1074.

Gorski, P. L. & Lo Iacono, L. (2016): Towards the Usability Evaluation of Security APIs. *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, 252-265.

Holz, T., Pohlmann, N., Bodden, E., Smith, M., Hoffmann, J. (2016): *Human-Centered Systems Security: IT-Sicherheit von Menschen für Menschen*. Verfügbar unter: https://www.ptj.de/lw_resource/datapool/_items/item_7794/strategiepapier_it-sicherheit.pdf

Jaferian, P. (2011): Heuristics for Evaluating IT Security Management Tools. *Symposium on Usable Privacy and Security (SOUPS) 2011*

Kainda, R., Flechais, I., Roscoe, A. W. (2010): *Security and Usability: Analysis and Evaluation*. Oxford: Oxford University Computing Laboratory

Microsoft Corporation (2017): *Security Development Lifecycle*. Verfügbar unter: https://www.microsoft.com/en-us/sdl/

Nguyen, H. V. & Lo Iacono, L. (2016): *USecureD – Auswertung der Online-Studie: Deliverable E 1.3*. Verfügbar unter: https://www.usecured.de/UseWP/wp-content/uploads/2015/04/USecureD-Anforderungsanalyse-Online-Studienergebnisse-V.1.pdf

Nehren, P., Schmitt, H., Lo Iacono, L. (2017): Usable Security – Werkzeuge für Entwickler. *Wissenschaft trifft Praxis 6*, 14–20. Bad Honnef: Begleitforschung Mittelstand-Digital

Norman, D. A. & Draper, S. W. (1986): *User Centered System Design: New Perspectives on Human-Computer Interaction*. Boca Raton: CRC Press

OWASP Foundation (2013): *OWASP Development Guide*. Verfügbar unter: https://www.owasp.org/index.php/Projects/OWASP_Development_Guide

OWASP Foundation (2016): *OWASP Code Review Project*. Verfügbar unter: https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project

PCI Security Standards Council (2013): *Payment Card Industry (PCI) Datensicherheitsstandard: Anforderungen und Sicherheitsbeurteilungsverfahren Version 3.0*. Verfügbar unter: https://de.pcisecuritystandards.org/_onelink_/pcisecurity/en2de/minisite/en/docs/PCI_DSS_v3.pdf

Wijayarathna, C., Arachchilage, N. A. G., Slay, J. (2017): A Generic Cognitive Dimensions Questionnaire to Evaluate the Usability of Security APIs. *19th International Conference on Human-Computer Interaction (HCII)*

Whitten, A. & Tygar, J. D. (1999): Why Johnny can't encrypt, a Usability Evaluation of PGP 5.0. *Security and Usability: Designing secure systems that people can use*, 679–702.

Autoren

Schmitt, Hartmut

Hartmut Schmitt ist Koordinator für Forschungsprojekte bei der HK Business Solutions GmbH. Er ist seit 2006 in Verbundvorhaben im Umfeld Mensch-Computer-Interaktion, Usability/User Experience und Software-Engineering aktiv. Hartmut Schmitt leitet bei der German UPA den Arbeitskreis Usable Security & Privacy und ist Mitglied des Arbeitskreises User Research.

Kropp, Edna

Edna Kropp arbeitet als Usability-Beraterin und forscht zum Thema Usability in der Software-Entwicklung an der Freien Universität Berlin. Ein Schwerpunkt ihrer Arbeit ist die Integration von Human-Centered-Design in Software-Entwicklungsprozesse. Sie ist im Organisationsteam des World Usability Day Berlin.