Alfred Zimmermann, Alexander Rossmann (Hrsg.): Digital Enterprise Computing 2015,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 111

Identitäts- und Zugangsmanagement für Kundenportale – Eine Bestandsaufnahme

Peter Weierich[1], David Weich[2] und Sebastian Abeck[3]

Abstract: Das Identitäts- und Zugangsmanagement (engl. Identity and Access Management, IAM) entwickelt sich zu einer Schlüsseltechnologie zur Umsetzung von digitalen Transformationen und der damit einhergehenden Personalisierung. An der Interaktionsschnittstelle zum Kunden ist eine gute Benutzerfreundlichkeit gefragt, damit die Kundenakzeptanz gewährleistet werden kann. Die hier vorgestellte Studie evaluiert die Benutzerfreundlichkeit des IAM von 112 Unternehmensportalen der Branchen Banken, Versicherungen, Automobilindustrie und E-Commerce. Lösungen innerhalb einer Branche sind sich häufig ähnlich, profitieren jedoch nicht von den Erfahrungen anderer Branchen. Jedes der betrachteten Portale hat kleinere und größere Schwachstellen hinsichtlich der Benutzerfreundlichkeit.

Keywords: IAM, Consumer IAM, Kundenportale, Benutzerfreundlichkeit

1 Einleitung

Die digitale Transformation ist für viele Unternehmen derzeit hochpriorisiert, um die Kundenbindung zu erhöhen und neue Geschäftsmodelle zu entwickeln. Kunden begrüßen dies und nutzen digital verbundene Produkte und Services, um ihre Bedürfnisse zu erfüllen. Es wurde vielfach festgestellt, dass das traditionelle IAM nicht geeignet ist, um den dynamischen Anforderungen von Kunden gerecht zu werden. Dieses dient meist der Erfüllung von Compliance-Vorgaben und setzt den Fokus auf die Sicherheit. Bedienerfreundlichkeit ist in vielen Fällen nicht relevant, da die IAM-Systeme vor allem in stark regulierten Branchen – z.B. bei Banken – vor allem als lästige „Pflichtübung" betrachtet werden. Im kundenorientierten IAM (Consumer IAM) dagegen ist die Benutzerfreundlichkeit der IAM-Prozesse ein kritischer Faktor für erfolgreiche Kundenportale. Sicherheitssysteme müssen so gestaltet sein, dass sie gleichzeitig sicher und benutzbar sind. Beispielsweise muss die Registrierung eines Interessenten so einfach und effizient sein, dass die Einstiegsbarriere so niedrig wie möglich liegt. Auch Anmeldeprozesse über Passworteingabe, soziale Medien oder andere Authentisierungswege müssen möglichst einfach und unempfindlich gegen das Vergessen von Zugangsdaten sein. Trotzdem verlangt der Kunde, dass sowohl Datenschutz und Sicherheit seiner Daten gewährleistet als auch sensible Geschäftsprozesse ausreichend gegen Missbrauch abgesichert sind.

[1] iC Consult GmbH, Keltenring 14, 82041 Oberhaching, peter.weierich@ic-consult.com
[2] Karlsruhe Institut für Technologie (KIT), Forschungsgruppe Cooperation & Management (C&M), Zirkel 2, 76131 Karlsruhe, david.weich@student.kit.edu
[3] Karlsruhe Institut für Technologie (KIT), Forschungsgruppe Cooperation & Management (C&M), Zirkel 2, 76131 Karlsruhe, abeck@kit.edu

In dieser Arbeit wird die Usability der IAM-Komponenten typischer Endkundenportale analysiert und verglichen. Dabei ist zu betonen, dass nach gängigen Kriterien [Ni12, La05] [ISO25010] die Funktionsvollständigkeit eine wichtige Dimension einer ganzheitlichen Usability-Bewertung darstellt. Details zu der Studie finden sich in [We15].

2 Methodik

Analytische Methoden sind in der Usability-Forschung weit verbreitet und sind weniger aufwändig als Usability Tests mit vielen Testusern. Gerade bei Sicherheitssystemen ist eine „schöne" Benutzeroberfläche allein nicht ausreichend, um die Benutzerfreundlichkeit sicherzustellen, da Verständnisprobleme trotzdem zu einer fehlerhaften Bedienung führen können. Für die hier durchgeführte Studie wurde eine Checkliste mit 50 unterschiedlich priorisierten Einzelkriterien entwickelt, um auch die Sicherheitseigenschaftenabzudecken.

Als Grundlage der Checkliste dienen Anforderungen an benutzbare Sicherheitssysteme aus den Arbeiten [CO+06], [SF05], [WT99] sowie [DD08]. Mithilfe dieser Grundlage wurden Dimensionen für die Checkliste abgeleitet und den Qualitätseigenschaften Bedienbarkeit und Zugänglichkeit aus [ISO25010] zugeordnet. Es wurde darauf geachtet, dass die Dimensionen objektiv bewertbar sind. Eine Darstellung aller Dimensionen ist in Tab. 1 zu finden.

Bedienbarkeit	
Effektivität	Sind alle Benutzerziele bezüglich IAM online erreichbar?
Bedienbarkeitsbarrierefreiheit	Ist die Bedienung des IAM-Systems frei von Bedienbarkeitsbarrieren?
Fehlertoleranz und Benutzerführung	Wird der Benutzer während der Bedienung entlastet sowie vor Fehlern bewahrt?
Umsetzung von Self-Service	Ist es dem Benutzer möglich, Änderungen seiner digitalen Identität selbst durchzuführen?
Zugänglichkeit	
Verständlichkeit von Eingaben	Ist dem Benutzer ersichtlich und verständlich, was wo einzugeben ist?
Unterstützung des Benutzers	Werden zusätzliche Informationen zum Vollenden einer Aufgabe bereitgestellt?
Reduzierung kognitiver Barrieren	Ist die Bedienung des IAM-Systems frei von kognitiven Barrieren?
Darstellung	Ist das IAM-System sinnvoll gestaltet?

Tab. 1: Dimensionen der Checkliste zur Beurteilung von IAM-Systemen

3 Ergebnisse

Durch die Analysen hat sich herausgestellt, dass die Branchen in unterschiedlichen Qualitätsdimensionen Schwächen und Stärken besitzen. So bieten die IAM-Systeme von Banken und Versicherungen regelmäßig zu wenige Funktionen im Self Service. Automotive und E-Commerce dagegen haben ihre Schwächen eher in der Zugänglichkeit.

Effektivität (6 Einzelkriterien): Kunden haben den Anspruch, auf allen Kanälen ihre Ziele erreichen zu können. Das bedeutet, dass Kunden sowohl über das Internet, Telefon oder durch Präsenz die gleichen Möglichkeiten geboten werden. Mängel existieren häufig im Bereich der Registrierung und Löschung von Kundenzugängen. Auch die Rücksetzung des Kennwortes ist häufig nicht ohne weiteres möglich.

Bedienbarkeitsbarrierefreiheit (5 Einzelkriterien): Um eine bessere Konversionsquote zu erreichen, sollten die Einstiegshürden und Barrieren so niedrig wie möglich sein. Der E-Commerce setzt dies am besten um. Häufige Mängel in anderen Branchen: Die Registrierung ist häufig nur Bestandskunden vorbehalten, Interessenten wird kein Zugang gewährt. Aber selbst den Bestandskunden werden Captchas, langsame Reaktionszeiten und mehrstufige Registrierungsprozesse zugemutet.

Fehlertoleranz/Benutzerführung (9 Einzelkriterien): Das häufigste Problem ist, dass Eingaben nicht validiert werden. So ist es regelmäßig möglich, ungültige Zeichen in Felder einzutragen oder nicht existente Adressen zu hinterlegen. Auch bei komplexeren Eingaben wie bei Kontoeröffnungen oder Angebotsberechnungen von Versicherungen, fehlen Plausibilitätsprüfungen. So kann der Kunde kurz nach seinem Geburtsdatum schon in seinen Beruf eingetreten sein, obwohl das in der Realität nicht möglich ist.

Self-Service (4 Einzelkriterien): Der Self-Service ist meist nur teilweise umgesetzt. Bei Banken und Versicherungen ist es häufig nicht möglich, das Kennwort über das System zurückzusetzen. Dies muss über einen anderen Kanal geschehen. Die Löschung des Kundenzuganges ist nur bei den Automobilherstellern möglich. Auch Stammdatenänderungen sind oft nicht möglich.

Verständlichkeit von Eingaben (7 Einzelkriterien): Branchenübergreifend ist die Verständlichkeit der Systeme gut. Trotzdem gibt es auch hier Probleme: So werden teilweise Passwortrichtlinien nicht angezeigt, erst nach Bestätigung der Registrierung Fehler gemeldet. Weiterhin werden häufig viele Daten abgefragt, deren Zweck unklar ist.

Unterstützung des Benutzers (6 Einzelkriterien): Die kognitive Unterstützung ist meist unzureichend umgesetzt. Fehlermeldungen geben häufig nur an, dass ein Fehler vorliegt. Außerdem bekommt der Benutzer meist erst eine Rückmeldung zu seinen Eingaben, wenn er den aktuellen Schritt abschließen möchte.

Reduzierung kognitiver Barrieren (9 Einzelkriterien): Diese Dimension wurde von keiner Branche ausreichend erfüllt. Es werden häufig Passwortrichtlinien verwendet, die keine Sicherheitsvorteile bringen oder den Benutzer zu stark einschränken. Außerdem

bieten nicht einmal 10 % der betrachteten Portale die Möglichkeit des "bring-your-own-identity", z.B. über die Nutzung eines Social Media Login wie Facebook und Google.

Darstellung (4 Einzelkriterien): Die Darstellung der IAM-bezogenen Formulare und Informationseinblendungen sind häufig nicht im Design der restlichen Seite gestaltet. Viele Anbieter nutzen Overlays und Popups, um Informationen darzustellen oder abzufragen statt das IAM-System in das Portaldesign zu integrieren.

4 Fazit

Keines der betrachteten Portale ist frei von Makeln, das heißt die Unternehmen nutzen bei weitem noch nicht die Möglichkeiten aus um in Kundenportalen Geschäftsbeziehungen zu vertiefen bzw. Neugeschäft zu generieren. So sehen wir insbesondere das "Social Login", als wertvollen Lösungsbaustein. Zukünftig bietet sich ebenfalls der Einsatz von Biometrie an, da diese durch moderne Betriebssysteme unterstützt wird. Am besten stehen aktuell E-Commerce Portale da. An Stelle zwei und drei stehen die Bereiche Automotive und Banken. An hinterster Stelle folgen Versicherungen, hauptsächlich weil nur 45 % der betrachteten Versicherungsportale überhaupt ein IAM-System aufweisen.

Literaturverzeichnis

[DD08] Dhamlia, R.; Fusseault, L.: The Seven Flaws of Identity Management – Usability and Security Challenges, IEEE Security & Privacy, 2008.

[CO+06] Chiasson S.; Oorschot, P.C; Biddle R.: A Usability Study and Critique of Two Password Managers, Proceedings of the 15th USENIX Security Symposium, 2006.

[ISO25010] ISO/IEC25010: Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models.

[La05] Lauesen, S.: User interface design – a software engineering perspective; Addison-Wesley, 2005.

[Ni12] Nielson J.: Usability 101: Introduction to Usability, http://www.nngroup.com/articles/usability-101-introduction-to-usability/, (Abgerufen am 23.03.2015).

[SF05] Sasse, A.; Flechais, I.: Usable Security - Why Do We Need It? How Do We Get It?, Security and Usability, O'Reilly Verlag, 2005.

[We15] Weich, D.: Untersuchung der Identitäts- und Zugriffsmanagementsysteme von Endkundenportalen in ausgesuchten Branchen. Masterarbeit, KIT, Cooperation und Management, 2015.

[WT99] Whitten, A.; Tygar, J. D.: Why Johnny Can't Encrypt – A Usability Evaluation of PGP 5.0, Proceedings of the 8th USENIX Security Symposium, 1999.