Wiewiorra, Lukas; Liebe, Andrea; Tas, Serpil

Working Paper

Die wettbewerbliche Bedeutung von Single-Sign-On- bzw. Login-Diensten und ihre Relevanz für datenbasierte Geschäftsmodelle sowie den Datenschutz

WIK Diskussionsbeitrag, No. 462

Provided in Cooperation with:
WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Bad Honnef

WIK • Diskussionsbeitrag

Nr. 462

Die wettbewerbliche Bedeutung von Single-Sign-On- bzw. Login-Diensten und ihre Relevanz für datenbasierte Geschäftsmodelle sowie den Datenschutz

Autoren:

Lukas Wiewiorra
Andrea Liebe
Serpil Taş

Bad Honnef, Juni 2020

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

Impressum

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Deutschland
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
E-Mail: info@wik.org
www.wik.org

Vertretungs- und zeichnungsberechtigte Personen

Geschäftsführerin und Direktorin	Dr. Cara Schwarz-Schilling
Direktor Abteilungsleiter Post und Logistik	Alex Kalevi Dieke
Direktor Abteilungsleiter Netze und Kosten	Dr. Thomas Plückebaum
Direktor Abteilungsleiter Regulierung und Wettbewerb	Dr. Bernd Sörries
Leiter der Verwaltung	Karl-Hubert Strüver
Vorsitzende des Aufsichtsrates	Dr. Daniela Brönstrup
Handelsregister	Amtsgericht Siegburg, HRB 7225
Steuer-Nr.	222/5751/0722
Umsatzsteueridentifikations-Nr.	DE 123 383 795

In den vom WIK herausgegebenen Diskussionsbeiträgen erscheinen in loser Folge Aufsätze und Vorträge von Mitarbeitern des Instituts sowie ausgewählte Zwischen- und Abschlussberichte von durchgeführten Forschungsprojekten. Mit der Herausgabe dieser Reihe bezweckt das WIK, über seine Tätigkeit zu informieren, Diskussionsanstöße zu geben, aber auch Anregungen von außen zu empfangen. Kritik und Kommentare sind deshalb jederzeit willkommen. Die in den verschiedenen Beiträgen zum Ausdruck kommenden Ansichten geben ausschließlich die Meinung der jeweiligen Autoren wieder.

ISSN 1865-8997

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Zusammenfassung

Das Anlegen eines Nutzerkontos ist mittlerweile bei vielen digitalen Diensten eine Grundvoraussetzung, um diese in vollem Umfang nutzen zu können. Nutzer sind daher mit der Herausforderung konfrontiert, alle Anmeldedaten der von ihnen genutzten digitalen Dienste zu verwalten.

Single-Sign-On(SSO)-Verfahren treten mit dem Versprechen an, die Anzahl der verschiedenen Zugangsdaten zu unterschiedlichen digitalen Diensten zu reduzieren und den Registrierungsprozess bei neuen Diensten zu vereinfachen. Andererseits können Nutzer technische Hilfsmittel verwenden, um die verschiedenen Anmeldedaten komfortabler zu verwalten und zentral zu speichern (z.B. Passwort-Manager).

Die Analyse der Nachfrageseite zeigt, dass Konsumenten unabhängig von Alter und Geschlecht mehrheitlich bis zu 12 Onlinedienste in der Woche nutzen. Die Nachfrage nach SSO-Lösungen von Drittanbietern ist mit aktuell etwa 2% sehr gering. Am häufigsten werden die SSO-Dienste von digitalen Plattformprovidern (Social Logins) genutzt. Insbesondere Nutzer, die Wert auf eine Ve reinfachung des Anmeldeprozesses und eine komfortable Nutzung legen, ziehen Vorteile aus diesen Angeboten. Der Login via Facebook wird von knapp 60% der Social Login-Nutzer (ca. 7% der befragten Nutzer von Onlinediensten und Webseiten) zur Anmeldung bei Onlinediensten oder Webseiten genutzt. In der Regel verwenden die Befragten 1,2 Social Login-Dienste.

Allerdings ist der Zweifel an der Sicherheit dieser Systeme für viele Konsumenten ein wichtiger Grund, sich bei Onlinediensten oder Webseiten nicht via Facebook, Google oder durch andere (soziale) Netzwerke anzumelden.

Die verbundenen Dienstanbieter, die diese Anmeldeverfahren auf ihren Webseiten implementieren, profitieren davon, wenn sich ein Nutzer mit einem Social Login bei ihren Diensten anmeldet. Allerdings profitieren auch die Anbieter von SSO-Diensten von den Informationen, die durch die Nutzung auf verbundenen Diensten und Webseiten anfallen. Insbesondere werbefinanzierte Plattformen, die Social Logins anbieten, zielen darauf ab, die Benutzerprofile ihrer Kunden mit Informationen anzureichern, die über ihre eigene Plattform nicht direkt erhoben bzw. beobachtet werden können.

Dabei ist unklar, welche Informationen genau durch die Anbieter von Social Logins dauerhaft gespeichert werden. Während bestimmte Daten im Rahmen der technischen Bereitstellung der Funktionalität notwendigerweise übertragen werden müssen, können diese auch nach der Leistungserbringung vom Anbieter dauerhaft gespeichert und weiter verwendet werden. Darüber hinaus könnten auch Daten erhoben und dauerhaft gespeichert werden, die zur Erbringung der Leistung nicht erforderlich sind. Wie im Fall des Like-Buttons (Facebook) ist daher zu vermuten, dass die Anbieter von Social Logins nicht nur von der direkten Nutzung der Funktionalität profitieren, sondern bereits implizit von der Verbreitung der Funktionalität.

Summary

Creating a user account is a basic requirement for many digital services in order to be able to use them to their full extent. Users therefore face the challenge of managing the login data of all the digital services they use.

Single Sign-On (SSO) services aim at reducing the number login data for different digital services and simplifying the registration process for new services. On the other hand, users can use technical measures to manage the different login data more conveniently and to store them centrally (e.g. password manager).

The analysis of the demand side shows that the majority of consumers use up to 12 online services per week, regardless of age and gender. The demand for third-party SSO solutions is very low, currently around 2%. SSO services are most frequently used by digital platform providers (social logins). In particular, users who value a simplified registration process and convenient use will benefit from these offers. Login via Facebook is used by almost 60% of social login users (about 7% of the surveyed users of online services and websites) to log in to online services or websites. As a rule, the respondents use 1.2 social login services.

However, doubts about the security of these systems are an important reason for many consumers not to access online services or websites via Facebook, Google or other (social) networks.

Service providers that implement these login procedures on their websites benefit from users logging into their services with a social login. On the other hand, the providers of SSO services also benefit from the information generated by the use of connected services and websites. In particular, advertising-financed platforms that offer social logins aim to enrich the user profiles of their customers with information that cannot be directly collected or monitored via their own platform.

However, it is not clear which data is permanently stored by the providers of social logins. While certain data has to be transferred as part of the technical provision of the functionality, this data can also be permanently stored and used by the provider after the service has been delivered. Furthermore, data that is not necessary for the provision of the SSO service could also be permanently stored. As in the case of the Like-Button (Facebook), it has to be assumed that the providers of social logins do not only benefit from the direct use of the functionality, but already implicitly from the popularity of the functionality.

1 Einleitung

Das Anlegen eines Nutzerkontos ist mittlerweile bei vielen digitalen Diensten eine Grundvoraussetzung um diese in vollem Umfang nutzen zu können. Daher ist die Anmeldung mit Hilfe von z.B. Benutzername und Kennwort für viele Internetnutzer ein alltäglicher, aber auch lästiger Vorgang geworden. Durch die stetig wachsende Anzahl der alltäglich genutzten digitalen Dienste müssen Internetnutzer heutzutage eine Vielzahl verschiedener Zugangsdaten verwalten und werden dabei regelmäßig mit neuen Registrierungs- und Anmeldeverfahren konfrontiert.

Internetnutzern stehen allerdings auch technische Lösungen zur Verfügung, um ihre Login-Daten zu verwalten, beispielsweise in Form eines Passwort-Managers. Aber auch Inhalte- und Dienstanbieter stellen Nutzern Lösungen bereit, um Registrierungs- und Anmeldeprozesse zu vereinfachen und die Anzahl verschiedener Login-Daten zu minimieren. In diesem Fall kommen sogenannte Single-Sign-On(SSO)-Verfahren zum Einsatz. Durch diese Verfahren kann ein Nutzer ein bereits bestehendes Konto bei einem SSO-Betreiber für den Zugang zu anderen digitalen Diensten nutzen. Ein Nutzer hat dadurch mehrere Vorteile: Zunächst entfällt der Aufwand, bei jedem einzelnen Inhalte- und Dienstanbieter ein eigenständiges Kundenkonto mit allen notwendigen Angaben händisch zu erstellen. Darüber hinaus muss sich der Nutzer für die alltägliche Nutzung nur noch die Zugangsdaten des SSO-Betreibers merken und kann sich über das SSO-Verfahren bei allen angeschlossenen Diensten ausweisen.

Dieser Diskussionsbeitrag geht gezielt auf die Nachfrageseite ein und stellt zunächst die unterschiedlichen Verfahren und Systeme zur Authentifizierung und anschließend empirisch erhobene Daten zum Nutzungsverhalten im Kontext von Login-Verfahren und SSO-Diensten vor. Die Auswertung der im Rahmen dieser Studie durchgeführten Konsumentenbefragung gibt dazu einen detaillierten Überblick über die Nutzung verschiedener Login-Verfahren im Allgemeinen und die Akzeptanz von SSO-Verfahren im Speziellen. Darüber hinaus beleuchtet dieser Beitrag auch die Akzeptanz und Verwendung neuer biometrischer Verfahren, die mittlerweile Einzug in viele am Markt verfügbare Smartphones, Tablets und Notebooks gefunden haben.

2 Digitale Identität

Eine digitale Identität stellt die virtuelle Repräsentation einer realen Identität dar, welche in digitalen Systemen bei Interaktionen und Transaktionen genutzt wird.[1] Dabei ist zu beachten, dass diese virtuelle Repräsentation nicht notwendigerweise der realen Identität entsprechen muss. Die Übereinstimmung kann durch eine Validierung der entsprechenden Angaben überprüft werden.

Aus einer technischen Perspektive lässt sich eine digitale Identität durch die mit einem Kundenkonto verknüpften Attribute, Rechte und Informationen beschreiben. Diese Daten erlauben es einem Dienstanbieter beispielsweise, kontextspezifische Informationen zu präsentieren und die dargestellten Inhalte je nach Identität anzupassen.

Konsumenten bewegen sich in der digitalen Welt heute ebenso selbstverständlich wie in der realen. Ein wichtiges Ziel, auch aus Sicht eines Dienstanbieters, ist dabei der Schutz der persönlichen Daten der Nutzer. Daher ist es wichtig, dass ein digitaler Dienstanbieter seine Nutzer konsistent und zuverlässig über die Zeit identifizieren kann. Nur so kann er einem individuellen Nutzer Rechte einräumen bzw. Inhalte und Dienste bereitstellen und gleichzeitig seine persönlichen Informationen vor unbefugtem Zugriff schützen.

Der Vorgang bis zum Zugriff auf eine digitale Identität kann in folgende Phasen untergliedert werden:[2]

1. **Authentisierung**
   Bei der Authentisierung weist sich der Nutzer gegenüber dem Dienstanbieter aus. Dafür wird häufig eine Kombination aus Benutzername und Passwort verwendet. Andere Authentisierungsverfahren nutzen zu diesem Zweck beispielsweise eine Kombination aus E-Mailadresse oder Telefonnummer und Passwort oder einer PIN.
2. **Authentifizierung**
   In der Authentifizierungsphase prüft das System, ob die entsprechenden Daten bzw. Merkmale, mit denen sich der Nutzer gegenüber dem System ausweist, auch in der Datenbank des Dienstanbieters vorhanden sind.
3. **Autorisierung**
   Sind die vom Nutzer eingegebenen Daten korrekt und in der Datenbank vorhanden, wird der Nutzer vom System berechtigt, das Konto zu nutzen und ihm werden die damit verknüpften Berechtigungen erteilt.

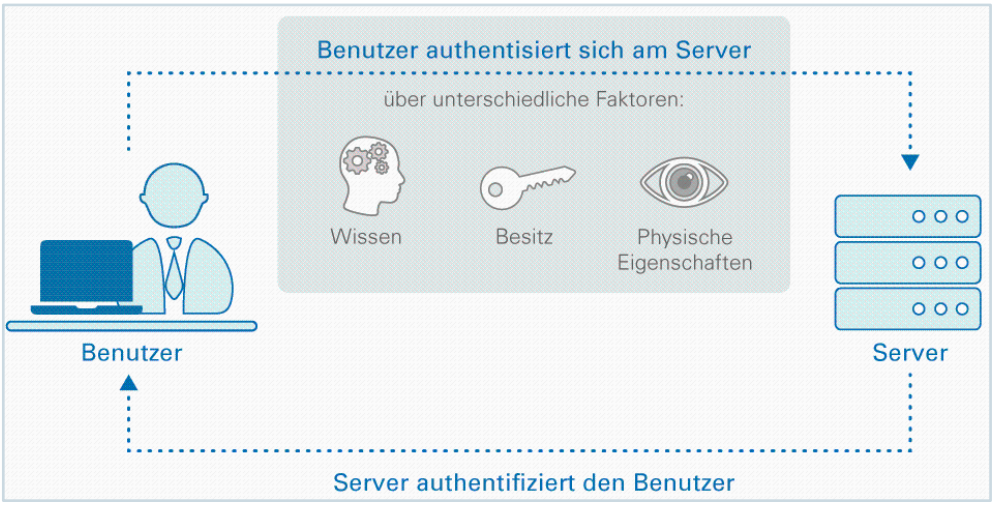
1 Vgl. Camp, J. L. (2004). Digital identity. IEEE Technology and society Magazine, 23(3), 34-41.
2 Vgl. Tsolkas, A., & Schmidt, K. (2017): Zugriffskontrolle über Authentifizierung, in: Rollen und Berechtigungskonzepte (pp. 129-160), Wiesbaden.

3 Anmeldeverfahren

3.1 Überblick und Funktionsweise

Ein Nutzer verschiedener digitaler Dienste kann innerhalb dieser Systeme unter verschiedenen Benutzernamen bzw. digitalen Identitäten gespeichert sein. Nutzer sind daher mit der Herausforderung konfrontiert, alle Anmeldedaten der von ihnen genutzten digitalen Dienste zu verwalten.[3] Dabei ist das Wissen bzw. das Erinnern an die entsprechenden Zugangsdaten das wohl gängigste Verfahren. Dieser Weg wird für Nutzer allerdings immer komplizierter, wenn die Anzahl der unterschiedlichen verwendeten digitalen Identitäten bzw. Benutzerkonten zunimmt und diese regelmäßig geändert werden.[4] Dabei bieten sich aus Nutzersicht zwei Maßnahmen an, um dieser Vielfalt Herr zu werden. Einerseits können Nutzer technische Hilfsmittel verwenden, um die verschiedenen Anmeldedaten komfortabler zu verwalten und zentral zu speichern (z.B. Passwort-Manager). Andererseits können Nutzer Anmeldeverfahren nutzen, welche die Anzahl verschiedener Anmeldedaten reduzieren (z.B. Single Sign-On).

Abbildung 3–1: Funktionsweise von Authentisierung & Authentifizierung



Quelle: https://www.tuv.com/germany/de/authentifizierung.html [letzter Abruf 02.07.2020]

3 Vgl. Chadwick, D. W., Inman, G. L., Siu, K. W., & Ferdous, M. S. (2011, October). Leveraging social networks to gain access to organisational resources. Proceedings of the 7th ACM workshop on Digital Identity Management, pp. 43-52.

4 Vgl. O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040.

3.1.1 Passwörter

Um die Stärke eines Passworts zu beschreiben, wird auf den Begriff der Entropie zurückgegriffen. Passwort-Entropie ist eine Messgröße welche beschreibt, wie unvorhersehbar ein Passwort aus statistischer Perspektive ist.[5] Diese Messgröße ist entscheidend, da sie Aufschluss darüber gibt, wie leicht ein Passwort mit gängigen Methoden erraten bzw. durch „Versuch und Fehler" automatisiert gefunden werden kann.[6] Klassische Wörterbuchattacken auf Benutzerkonten machen sich dabei häufig verwendete Wörter aus einem Wörterbuch zu Nutze, die automatisiert nacheinander nach dem Versuch und Fehler-Prinzip getestet werden. Die Entropie eines Passworts steigt daher mit der zu erwartenden Anzahl an Versuchen, die ein Unbefugter benötigt, um das korrekte Passwort zu erraten. Daher steigt die Passwort-Entropie z.B. mit der Länge eines Passworts, der Verwendung von Groß- und Kleinbuchstaben und der Nutzung von Sonderzeichen. Aus Nutzersicht besteht im Hinblick auf die Passwort-Entropie aber eine Abwägung im Hinblick auf die einfache Verwendbarkeit. Je unvorhersehbarer ein Passwort gewählt wird, desto schwieriger kann es für den Nutzer sein, sich bei dem nächsten Anmeldevorgang daran zu erinnern.[7]

3.1.2 Passwort-Manager

Die zentrale und komfortable Verwaltung aller Zugangsdaten eines Nutzers wird durch Passwort-Manager ermöglicht. Dabei handelt es sich um Softwareprodukte, die einem Nutzer eine abgesicherte Datenbank für Anmeldedaten bereitstellen. Diese Datenbank kann in einem Browser-Plug-In, einer eigenständigen Software, oder sogar in der Cloud gespeichert werden. Benutzer können in dieser Datenbank alle Anmeldedaten für unterschiedliche Dienste abspeichern sowie bei einem Login-Vorgang (z.B. auf einer Webseite) die passenden Daten aus der Datenbank abfragen und an entsprechender Stelle einfügen lassen. Passwort-Manager werden selbst geschützt, beispielsweise durch ein Passwort oder einen physischen Faktor (SmartCard, Dongle). Auf diese Weise kann ein Nutzer mit der einmaligen Authentifizierung gegenüber dem Passwort-Manager Zugriff auf alle gespeicherten Anmeldedaten erhalten. Durch die automatisierte Verwendung der gespeicherten Informationen entfällt damit die Notwendigkeit, diese Daten für die alltägliche Verwendung im Gedächtnis zu behalten. Der unbefugte Zugriff auf einen Passwort-Manager (z.B. durch Sicherheitsmängel) kann dadurch verhehrende Folgen für einen Nutzer haben.[8] Auf der anderen Seite ermöglicht ein Passwort-Manager dem Nutzer, bei einzelnen Diensten unabhängige und starke Passwörter mit

5 Vgl. Ma, Wanli, et al. "Password entropy and password quality." 2010 Fourth International Conference on Network and System Security. IEEE, 2010.

6 Vgl. Taha, M. M., Alhaj, T. A., Moktar, A. E., Salim, A. H., & Abdullah, S. M. (2013): On password strength measurements: Password entropy and password quality. In 2013 International conference on computing, electrical and electronic engineering (ICCEEE) (pp. 497-501). IEEE.

7 Vgl. O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040.

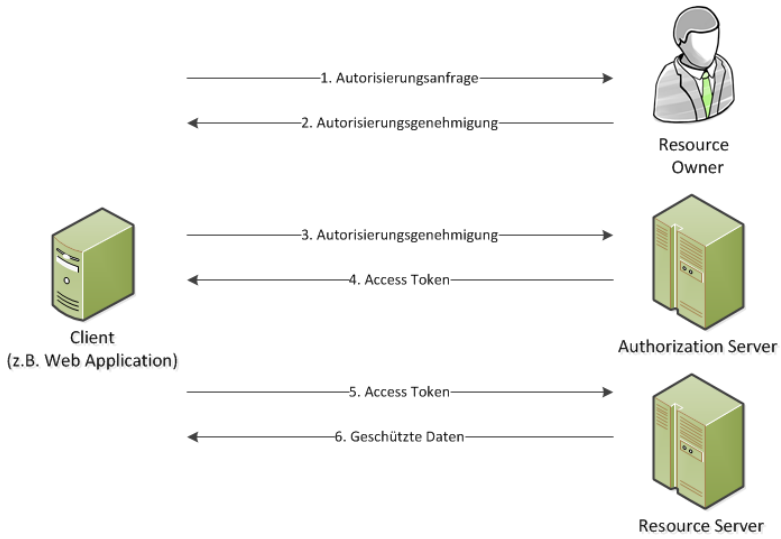
8 Vgl. Gasti, P., & Rasmussen, K. B. (2012, September). On the security of password manager database formats. In *European Symposium on Research in Computer Security* (pp. 770-787). Springer, Berlin, Heidelberg.

hoher Entropie zu wählen, da er sich selbst nicht mehr an einzelne Passwörter erinnern muss. Durch einen Passwort-Manager wird allerdings nicht der Aufwand reduziert, ein Kundenkonto bei einem neuen Dienstanbieter anzulegen. Eine Registrierung bzw. das Anlegen neuer Nutzerkonten ist weiterhin notwendig, bevor die regelmäßige Anmeldung durch einen Passwort-Manager vereinfacht werden kann.

3.1.3 Single Sign-On (SSO)

Im Gegensatz zu einer zentralen Verwaltung verschiedener Anmeldedaten führen SSO-Verfahren zu einer Reduzierung der Anzahl unterschiedlicher Anmeldedaten. Ziel von SSO-Systemen ist es, dass sich ein Nutzer nur einmalig gegenüber dem SSO-Betreiber ausweisen muss (federated identity). Danach bestätigt der SSO-Betreiber gegenüber den verbundenen (unabhängigen) Diensten die Identität des Nutzers. Dabei verwenden viele SSO-Dienste sogenannte „Tokens“, einen zeitlich begrenzten digitalen Autorisierungsschlüssel.[9] Viele Anbieter basieren ihre Systeme auf offenen Protokollen (z.B. OAuth) mit teilweise dezentralen Architekturen (z.B. OpenID).

Abbildung 3–2: Protocol Flow von OAuth 2.0



wik

Quelle: https://de.wikipedia.org/wiki/OAuth [letzter Abruf 02.07.2020].

Durch dieses Verfahren kann ein Benutzer mit SSO-Diensten Zugriff auf seine digitale Identität gewähren, ohne dabei die Details seiner Zugangsberechtigung mit Dritten zu teilen. Ein SSO-Dienst ist also nicht vergleichbar mit einem Passwort-Manager in der Cloud oder mit der (nicht empfehlenswerten) Vorgehensweise, bei verschiedenen Diensten die gleichen Anmeldedaten zu verwenden.

9 Vgl. De Clercq, J. (2002, October). Single sign-on architectures. In International Conference on Infrastructure Security (pp. 40-58). Springer, Berlin, Heidelberg.

Ein weiterer wichtiger Unterschied zu einem Passwort-Manager liegt in der Möglichkeit, Attribute eines SSO-Nutzerprofils mit verbundenen Diensten auszutauschen. Diese Funktionalität ermöglicht es einem Nutzer nicht nur, Zugriff auf einen verbundenen Dienst zu erhalten, sondern auch zu entscheiden, welche Informationen aus seiner digitalen Identität bei einem SSO-Anbieter an den verbundenen Dienst weitergegeben werden. Dadurch reduziert sich aus Nutzersicht nicht nur der Aufwand bei der regelmäßigen Anmeldung, sondern auch der Aufwand bei der (erstmaligen) Registrierung bei neuen Diensten. In einem konkreten Beispiel kann dies bedeuten, dass ein Nutzer bei der erstmaligen Verwendung eines neuen Dienstes nach der Eingabe seiner SSO-Anmeldedaten nur noch bestätigen muss, welche Informationen (z.B. Name, Adresse, Alter) er aus seinem SSO-Nutzerprofil übertragen möchte. Dadurch entfällt der übliche händische Aufwand bei der Erstellung eines neuen Nutzerkontos.

3.1.4 Biometrische Verfahren

Auch biometrische Verfahren können eingesetzt werden, um Nutzer gegenüber einem Dienst oder einer Anwendung zu authentisieren. Biometrische Verfahren verwenden dazu üblicherweise individuelle Körpercharakteristika (z.B. Fingerabdruck, Gesichtsgeometrie, Iris). Um mit diesen Verfahren eine Identifizierung von Nutzern mit einer geringen Fehlerrate vornehmen zu können, ist es entscheidend, möglichst einmalige Kriterien zu verwenden, die bei möglichst jeder Person vorkommen und konstant messbar sind.[10]

Der Durchbruch dieser Verfahren wurde aber erst durch die Verbreitung entsprechender Sensoren ermöglicht. Viele der heute vermarkteten Smartphones sind mit Fingerabdrucksensoren oder mit Infrarotmatrixprojektoren und -sensoren zur Erkennung der Gesichtsgeometrie bestückt. Durch diese Entwicklung sind biometrische Verfahren heute jedermann zugänglich und finden Einsatz im täglichen Gebrauch von Endgeräten.[11]

Dabei ist anzumerken, dass biometrische Verfahren bisher nicht direkt zur Anmeldung bei internetbasierten Diensten verwendet werden. Die Verfahren werden meist lokal eingesetzt (z.B. zum Entsperren des Endgeräts) oder dienen als vereinfachter Zugang zu den Anmeldedaten die in einem Passwort-Manager hinterlegt sind. Da biometrische Daten einmalige körperliche Charakteristika eines Nutzers beschreiben, sind sie äußerst sensibel. Im Gegensatz zu Benutzernamen, Passwörtern oder einer PIN können diese Informationen nicht einfach vom Nutzer geändert werden. Sie sind eine digitale Beschreibung der unveränderlichen körperlichen Merkmale eines Nutzers (z.B. Fingerabdruck). Die Sicherheit dieser Verfahren kann in Abhängigkeit der jeweiligen technischen Implementierung zwischen Anbietern stark variieren. Am Massenmarkt (z.B. bei Smartphones) treibt insbesondere Apple die Verbreitung von biometrischen Verfahren.

10 Vgl. Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2013). Guide to biometrics. Springer Science & Business Media.

11 Vgl. Goode, A. (2014). Bring your own finger–how mobile is bringing biometrics to consumers. Biometric Technology Today, 2014(5), 5-9.

Dabei speichert der Hersteller die biometrischen Informationen seiner Nutzer hardwareseitig in einem speziell für diese Daten ausgelegten Chip lokal auf den jeweiligen Geräten. Diese Informationen sind damit weder für andere Softwareanwendungen auf dem Endgerät direkt zugänglich, noch sollen sie bei physischem Zugriff auf das Gerät ausgelesen werden können. Darüber hinaus werden bei diesem Ansatz die biometrischen Informationen nicht in die Cloud übertragen, sondern liegen ausschließlich lokal auf den jeweiligen Geräten vor. Dies bedeutet, dass ein Nutzer die biometrischen Informationen bei einem Gerätewechsel erneut hinterlegen muss und diese nicht übertragbar sind. Dabei entwickeln sich die am Massenmarkt verfügbaren Lösungen positiv im Hinblick auf sicherheitsrelevante Kriterien. Während gängige Fingerabdruckverfahren noch eine Falscherkennungsrate von 1 zu 50.000 aufweisen, bieten aktuelle Verfahren zur Gesichtserkennung bereits erheblich niedrigere Falscherkennungsraten von 1 zu 1.000.000.[12] Beide Verfahren erhöhen damit deutlich die Sicherheit eines Nutzers, der beispielsweise sein Smartphone anderenfalls nur mit einem vierstelligen numerischen Code schützen würde.

12 https://www.howtogeek.com/350676/how-secure-are-face-id-and-touch-id/ [Zuletzt abgerufen: 29.06.2020]

4 Marktüberblick zu SSO-Systemen

Bevor auf die ökonomischen Aspekte von SSO-Diensten und die Präferenzen von Konsumenten eingegangen wird, soll zunächst ein kurzer Marktüberblick gegeben werden. Dazu wird weiterhin zwischen Authentifizierungsverfahren basierend auf der einfacheren Verwaltung bestehender Benutzerkonten (i.e Passwort-Managern) und der Verringerung der Anzahl nötiger Zugangsdaten (i.e. SSO-Diensten) unterschieden.

4.1 Passwort-Manager

Passwort-Manager, auch Passwort-Safes oder Passwort-Tresore genannt, gibt es zum einen als Browser Plug-Ins und zum anderen als eigenständige Softwarelösungen bzw. mobile Applikationen. Teilweise werden diese um Cloud-Funktionalitäten ergänzt, welche die gespeicherten Zugangsdaten automatisch zwischen verschiedenen Geräten (z.B. Notebook, Table und Smartphone) abgleichen und auch auf anderen Endgeräten zugänglich machen. Sämtliche gängigen Browser wie Firefox, Google Chrome, Microsoft Edge, Safari etc. verfügen über solche Angebote. Sie gelten als anfälliger für Missbrauch als eigenständige Passwort-Manager-Programme.[13]

Der Markt für eigenständige Passwort-Manager ist relativ groß und dynamisch. Entsprechend ihrer Präferenzen können die Nachfrager das für sie passende Angebot auswählen. Es stellt sich jedoch die Frage, ob alle potenziell Interessierten ihre Bedürfnisse auch wirklich kennen, bzw. die zur Auswahl stehenden Angebote aus technischer Perspektive vergleichen können. Das Bundesamt für Sicherheit in der Informationstechnik gibt Hinweise darauf, welche Kriterien bei der Auswahl angelegt werden können.[14] Darüber hinaus bieten zahlreiche Computerzeitschriften und Websites, die regelmäßig Testberichte mit variierendem Fokus erstellen und die Vor- und Nachteile einzelner Angebote herausstellen, Entscheidungshilfen.[15] Die nachstehende Liste soll einen kurzen, nicht vollständigen Überblick zum umfangreichen Marktangebot geben.

---

13 Vgl. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Passwort_Manager/Passwort_Manager_node.html [letzter Abruf 23.06.2020].

14 Vgl. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Passwort_Manager/Passwort_Manager_node.html [letzter Abruf 23.06.2020].

15 Vgl. https://www.chip.de/artikel/Test-Die-besten-Passwort-Manager_182620837.html [letzter Abruf 23.06.2020]
https://www.pcwelt.de/ratgeber/Die_besten_Passwort-Manager_fuer_Android-9008619.html [letzter Abruf 23.06.2020]

Tabelle 4-1: Marktüberblick Passwort-Manager

▪ 1Password ▪ Avira Password Manager ▪ Bitwarden ▪ BlackBerry Password Keeper ▪ Dashlane ▪ HighCrypt Password Manager LT ▪ Kaspersky Password Manager - Secure Tresor ▪ Keepass	▪ Keeper ▪ LastPass ▪ My Passwords - Password Manager ▪ Myki ▪ NordPass ▪ Norton Identity Safe Password ▪ OI Safe ▪ Password Safe ▪ Password Saver	▪ Passwort Manager SafeIn-Cloud ▪ Passwort Tresor ▪ Passwort-Manager ▪ RememBear: Password Manager ▪ RoboForm ▪ Sticky password ▪ Truekey ▪ etc.

Quelle: Eigene Zusammenstellung

Die bis dato gelisteten Passwort-Manager erfüllen nach Auskunft diverser Testberichte die Mindestanforderungen an Sicherheit eines Passwort-Managers. Sie unterscheiden sich jedoch durchaus in ihren Funktionalitäten und in ihrem Ausstattungsumfang. So sind meist einfache Versionen kostenlos erhältlich und eine umfangreichere Ausstattung ist als kostenpflichtige Premiumvariante verfügbar. Alternativ werden kostenlose Varianten als Probeversion angeboten, die dann in eine werbebasierte Version überführt werden können. Manche Produkte eignen sich eher für einen Desktop-Computer, andere eher für die Anwendung auf mobilen Endgeräten.

4.2 SSO-Dienste

SSO-Dienste sind sowohl von unabhängigen Dienstleistern als auch von integrierten digitalen Plattformprovidern (z.B. Facebook, Amazon) verfügbar. Dabei basieren viele SSO-Dienste auf offenen Protokollen (z.B. OAuth) bzw. den darauf aufbauenden Authentifizierungsschichten (z.B. OpenID Connect).

Bei den Angeboten von Drittanbietern von SSO-Diensten findet sich eine recht fragmentierte Marktstruktur. Dazu soll in Form einer nicht abschließenden Aufzählung ein Überblick gegeben werden:

Tabelle 4-2: Marktüberblick SSO-Dienste

▪ Akamai ▪ CA Secure Cloud ▪ Centrify Identity Service ▪ CloudAccess SaaS SSO ▪ CloudHQ ▪ IBM Tivoli Federated Identity Manager	▪ Okta Single Sign-On ▪ OneLogin ▪ Otixo ▪ PingOne ▪ SecureAuth IdP ▪ Storage Made Easy	▪ SurePassID ▪ Symantec Identity Access Manager ▪ ZeroPC ▪ etc.

Quelle: Eigene Zusammenstellung.

Kommerzielle Lösungen von digitalen Plattformprovidern sind üblicherweise nicht mit Nutzungsgebühren verbunden. Da die digitalen Identitäten bei diesen SSO-Betreibern vornehmlich auf den Benutzerprofilen von sozialen Netzwerken basieren, werden diese SSO-Dienste auch als „Social Logins“ oder „Social IDs“ bezeichnet. Die Möglichkeit des Social Login ist mittlerweile recht verbreitet. Einen Eindruck dazu, welche digitalen Identitäten aus sozialen Netzwerken genutzt werden können, um sich auf anderen Webseiten oder für andere Dienste zu authentifizieren, soll der folgende Überblick geben.[16]

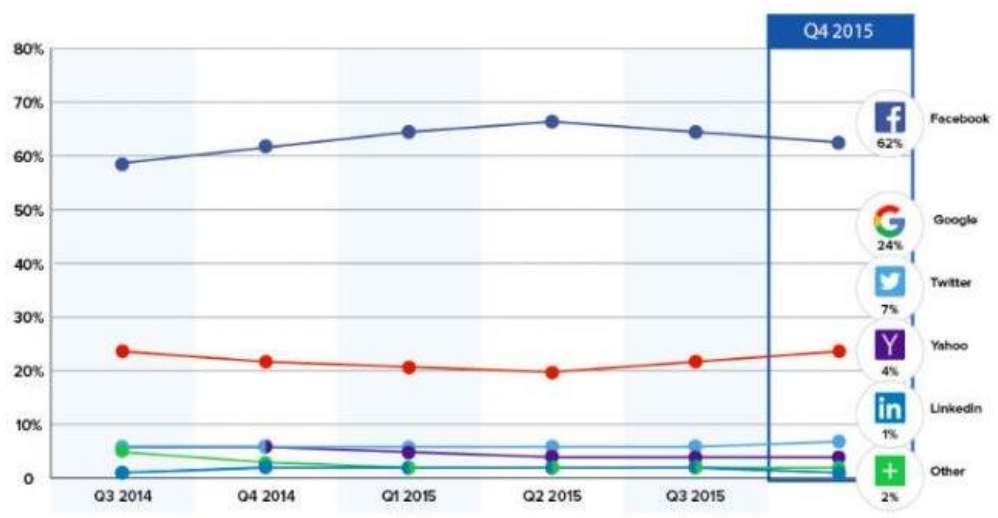
Tabelle 4-3: Marktüberblick Social Logins

▪ AOL ▪ Amazon ▪ Disqus ▪ Facebook ▪ Foursquare ▪ Google+ ▪ Hyves ▪ Instagram ▪ LinkedIn	▪ LiveJournal ▪ Meetup ▪ PayPal ▪ Plurk ▪ QQ ▪ Renren ▪ Pinterest ▪ Sina Weibo	▪ Telegram ▪ Twitter ▪ Vkontakte ▪ WeChat ▪ WordPress ▪ XING ▪ Yahoo! ▪ etc.

Quelle: Eigene Zusammenstellung.

Dabei ist festzuhalten, dass Facebook den größten Marktanteil an den bestehenden Social-Login-Lösungen hält, gefolgt von Google, Twitter, Yahoo, LinkedIn und anderen.

Abbildung 4–1: Marktanteile von Social-Login-Anbietern



Quelle: https://adage.com/article/digital/facebook-owns-social-login-scene-google-s-creeping/302407 [letzter Abruf 02.07.2020].

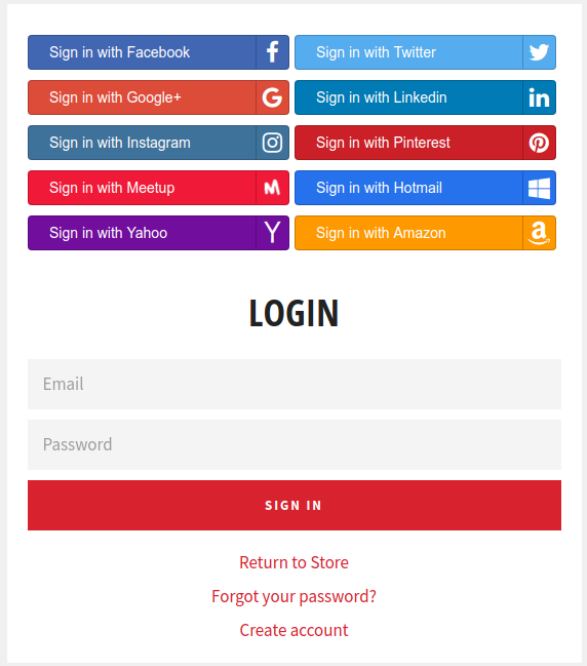
16 Liste basierend auf: https://en.wikipedia.org/wiki/Social_login [letzter Zugriff 23.06.2020].

Der Markt für biometrische Verfahren ist unmittelbar an die schnelle Entwicklung auf dem Markt für Smartphones gekoppelt. Durch die steigende Durchdringung von Smartphones mit biometrischen Technologien werden Nutzer über diese Geräte im alltäglichen Gebrauch immer intensiver mit diesen Technologien vertraut gemacht. So bieten insbesondere die Gerätehersteller von iPhone/iPad und Android-Geräten eine Identifizierung über Fingerabdrucksensoren und Gesichtserkennung an.

5 Ökonomische Aspekte

Von der Implementierung von SSO-Diensten auf ihren Webseiten versprechen sich verbundene Dienstanbieter vor allem eine höhere Konversion von Besuchern zu registrierten Kunden. Durch SSO-Dienste können Attribute und Informationen des Benutzerkontos bei einem SSO-Anbieter einfach zu einem verbundenen Dienstanbieter übernommen werden. Dadurch vereinfacht sich der Anmelde- und Registrierungsprozess für neue Dienste drastisch und damit die Einstiegshürde für neue Benutzer. Da Internetnutzer unterschiedliche Social Logins bevorzugen und die Implementierung einzelner Anbieter auf spezifischen Webseiten keinen hohen Aufwand bzw. keine hohen Kosten erzeugt, werden häufig eine Vielzahl unterschiedlicher Social Logins gleichzeitig angeboten. So kann der verbundene Dienstanbieter neuen Kunden mit unterschiedlichen sozialen Benutzerkonten einen einfachen Einstieg in sein Dienstleistungsangebot ermöglichen. Es wird aber auch deutlich, dass nicht jeder Dienst oder jede Webseite die Möglichkeit eines SSO anbietet. In aller Regel handelt es sich nicht um Bereiche mit erhöhten Sicherheitsanforderungen wie Banken oder öffentliche Stellen, die eigene Authentifizierungsverfahren erfordern.

Abbildung 5–1: Shopify – One Click Social Login



Quelle: https://apps.shopify.com/one-click-social-login [letzter Abruf 02.07.2020].

Darüber hinaus erlaubt ein personalisiertes Kundenkonto und die damit verbundene eindeutige Identifizierung einem verbundenen Dienstanbieter, das Verhalten seiner Kunden über die Grenzen einzelner Dienste hinweg zu verfolgen. Dadurch kann der

Betreiber dieser Dienste z.B. eine Customer Journey-Analyse durchführen, die ihm Aufschluss über das ganzheitliche Nutzungsverhalten über alle seine Dienste gibt. Dabei profitiert der Anbieter zusätzlich davon, dass er durch den Social Login berechtigungsbasierten Zugriff auf die vorvalidierten Identitätsdaten der (neuen) Nutzer erhält. Durch die Verknüpfung dieser Identitätsdaten mit verhaltensbezogenen Nutzerdaten des eigenen Dienstes kann der Anbieter gezielter Werbung platzieren und sein Kundenerlebnis weiter personalisieren. Die folgende Tabelle gibt Aufschluss darüber, auf welche Informationen aus einem sozialen Benutzerprofil ein Dienstanbieter Zugriff erbitten kann.

Tabelle 5-1: Merkmale sozialer Benutzerprofile

Log in	Twitter	Google	Linkedin	Yahoo
First Name	First Name	First Name	First Name	First Name
Last Name	Last Name	Last Name	Last Name	Last Name
Nickname	Nickname	Nickname	Nickname	Nickname
Email Address	Country	Email Address	Email Address	Email Address
Birthday	Profile Photo	Age	State	Age
Gender	Location	Birthday	Country	Birthday
City	Follower Info	Gender	Profile Photo	Gender
State		City	Interests	Country
Country		Profile Photo	Languages	Profile Photo
Location		Education	Address	Interests
Profile Photo		Work History	Phone	Contacts
Likes		Locale	Education	Friends
Languages		Friend Info	Honors	
Education		Contacts	Publications	
Work History			Certifications	
Religion			Bio	
Political View			Industry	
Relationships			Work History	
Friends			Skills	
Friend Info			Favorites	
			Connections	

Quelle: Gigya (2015): Social Login 101: Everything You Need to Know About Social Login and the Future of Customer Identity. Whitepaper. [Abruf 02.10.2019].

Neben diesen unmittelbar geschäftsfördernden Aspekten gibt es aber auch weitere Gründe, SSO-Dienste zu implementieren. Kompromittierte bzw. durch Dritte übernommene Benutzerkonten können zu Reputationsverlust des Dienstanbieters und damit auch zu ökonomischen Verlusten führen. Durch die Vielzahl der genutzten Dienste und Internetangebote verwenden Nutzer Passwörter mehrfach, denken sich schwache Passwörter aus oder notieren ihre Anmeldedaten. Dieses Phänomen wird landläufig als „Passwortmüdigkeit“ bezeichnet und stellt ein erhebliches Sicherheitsrisiko dar.[17] SSO-Dienste reduzieren Passwortmüdigkeit, da keine Mehrfachverwendung von Passwörtern notwendig wird und der Benutzer nur ein Passwort mit hoher Entropie für den SSO-Dienst vergeben muss.

17 Pittman, J. M., & Robinson, N. (2020). Shades of Perception-User Factors in Identifying Password Strength. arXiv preprint arXiv:2001.04930.

Dennoch können gerade bei der Nutzung von SSO-Diensten sensible Daten bei einem SSO-Anbieter anfallen. Nutzer geben gegenüber einem SSO-Anbieter preis, welche verbundenen Dienste sie nutzen und wann bzw. wie häufig sie sich dort anmelden. Insbesondere für digitale Plattformprovider die ein werbefinanziertes Geschäftsmodell verfolgen, können diese Informationen daher von hoher Relevanz sein, da sie die Erstellung eines genaueren Kundenprofils zu Werbezwecken ermöglichen. Ein Plattformprovider erhält auf diesem Weg zusätzliche Informationen über seine Nutzer, insbesondere über deren Aktivitäten in den Bereichen des Internetökosystems, welche für ihn anderweitig nicht oder nur teilweise beobachtbar sind.

Inhalte- und Dienstanbieter sind also an den Profilen der großen sozialen Netzwerke und digitalen Plattformanbieter interessiert und bieten entsprechende Social Logins auf ihren Diensten an.[18] Krämer et al. (2018) fassen zusammen, dass sowohl diese Inhalte- und Dienstanbieter als auch der Anbieter eines Social Login von dieser Konstellation profitieren können. Die Verbreitung eines Social Logins kann darüber hinaus die Wohlfahrt der Konsumenten und die Gesamtwohlfahrt steigern.

Die Autoren finden allerdings auch Konstellationen, in denen sich Inhalte- und Dienstanbieter, die sich durch starken Wettbewerb untereinander zu der Implementierung eines Social Logins entscheiden, schlechter stellen. Während sich die Dienstanbieter durch die Implementierung eines Social-Logis einen Wettbewerbsvorteil versprechen, profitieren sie letztlich gleichermaßen von den Vorteilen eines Social Logins und erreichen dadurch relativ zueinander keinen Wettbewerbsvorteil. In diesem Fall entsteht ein Gefangenendilemma unter den Social Login nutzenden Unternehmen, da die unilaterale Entscheidung eines Dienstanbieters, einen Social Login zu implementieren, zwar einen Wettbewerbsvorteil verspricht, letztlich durch die gleichgerichteten Anreize der Wettbewerber aber ein schlechteres Ergebnis erzielt wird als in der Ausgangssituation (keine Implementierung eines Social Logins).

Der Anbieter des Social Logins profitiert im Gegensatz dazu auch in dieser Situation von den zusätzlichen Daten, die er über den Social Login von den beiden Unternehmen erhält, und kann sich damit durchaus einen Wettbewerbsvorteil (z.B. auf dem Werbemarkt) gegenüber diesen Unternehmen sichern.

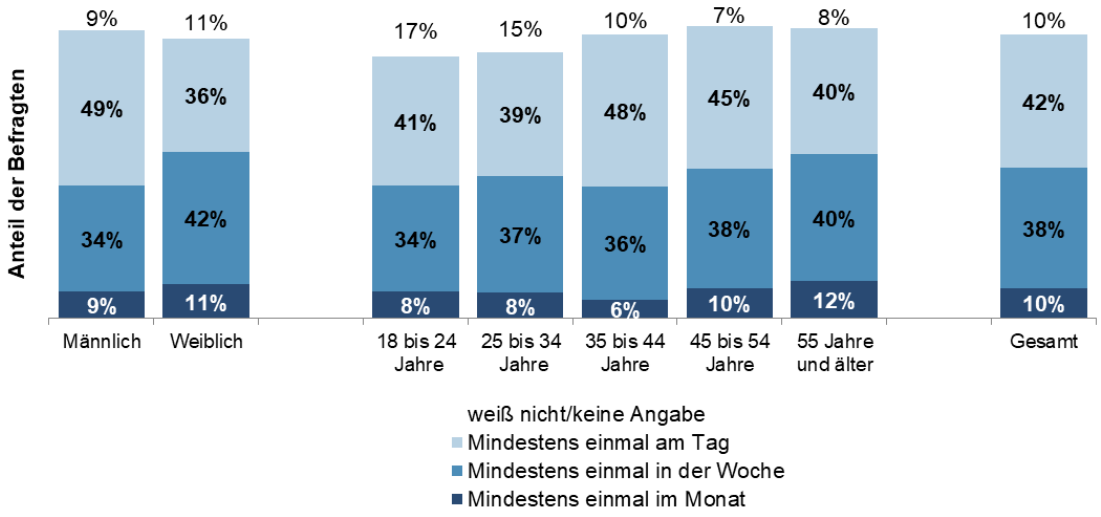
18 Vgl. Krämer, J., Schnurr, D., Wohlfahrt, M. (2018): Winners, Losers, and Facebook: The Role of Social Logins in the Online Advertising Ecosystem, in: Management Science, 2019, vol. 65, no. 4, pp. 1678–1699.

6 Analyse der Nachfrageseite

Um ein differenziertes Bild über die tatsächliche Nutzung der verschiedenen bisher diskutierten Anmeldeverfahren seitens der Konsumenten zu erhalten, führten wir eine Konsumentenbefragung durch. Im Winter 2019 wurden im Rahmen dieser Konsumentenbefragung 3016 Personen zu ihrer Nutzung von Internetdiensten mit erforderlicher Registrierung befragt. Eine nähere Beschreibung der Methodik befindet sich im Anhang dieser Publikation.

Insgesamt zeigt sich, dass 47 % der Befragten, die eine Antwort auf diese Frage gegebenen haben,[19] mindesten einmal am Tag Onlinedienste und/oder Webseiten nutzen, die eine Registrierung oder ein Login erfordern, 42 % tun dieses mindestens einmal in der Woche und 11 % nur einmal im Monat. Obwohl Männer tendenziell häufiger Dienste mit Logins nutzen als Frauen, zeigen sich keine gravierenden Unterschiede in der Nutzung zwischen den Altersgruppen. Einzig die Befragten in der Altersgruppe 35 bis 44 Jahre nutzen vergleichsweise häufiger Onlinedienste.

Abbildung 6–1: Häufigkeit der Nutzung von Onlinediensten und/oder Webseiten, die eine Registrierung oder ein Login erfordern nach Geschlecht und Alter



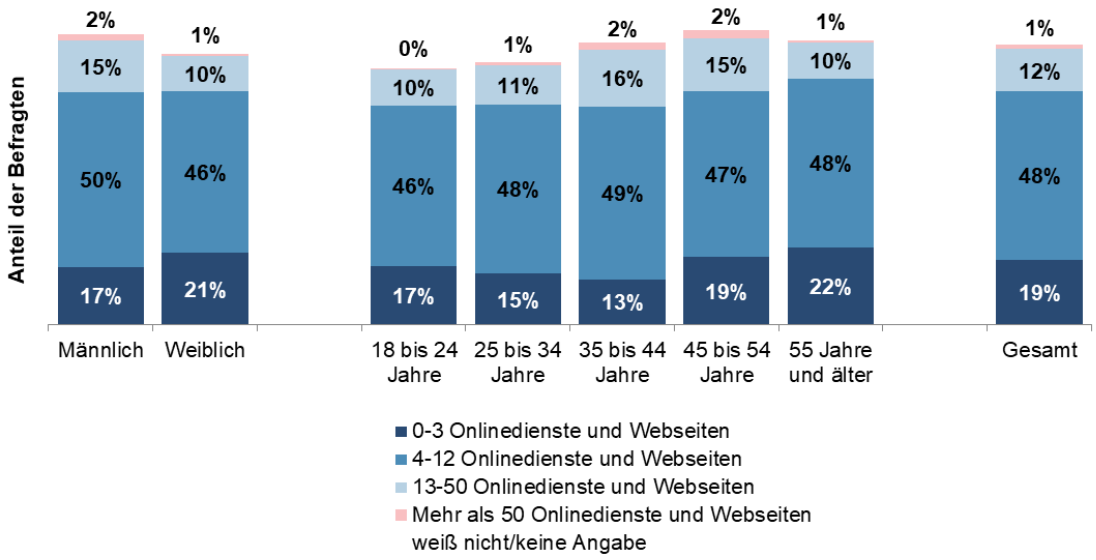
Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: N=3016. „Wie häufig nutzen Sie Onlinedienste und / oder Webseiten, für die Sie sich registrieren oder einen LogIn nutzen müssen?“.

An diesen Zahlen zeigt sich, dass Logins bei Onlinediensten mittlerweile ein alltäglicher Vorgang für einen Großteil der Internetnutzer in allen Altersschichten geworden sind und alle Internetnutzer regelmäßig betreffen.

19 Ohne Befragte, die „weiß nicht/keine Angabe“ angegeben haben.

Unabhängig von Alter und Geschlecht nutzen Konsumenten mehrheitlich bis zu 12 Onlinedienste in der Woche. Frauen nehmen dabei tendenziell etwas weniger Dienste in Anspruch als Männer und die Altersgruppen zwischen 35 und 54 Jahren scheinen etwas mehr Dienste zu nutzen als die Altersgruppen unter 35 oder ab 55 Jahren.

Abbildung 6–2: Anzahl an genutzten Onlinediensten und Webseiten innerhalb einer Woche nach Geschlecht und Alter der Befragten

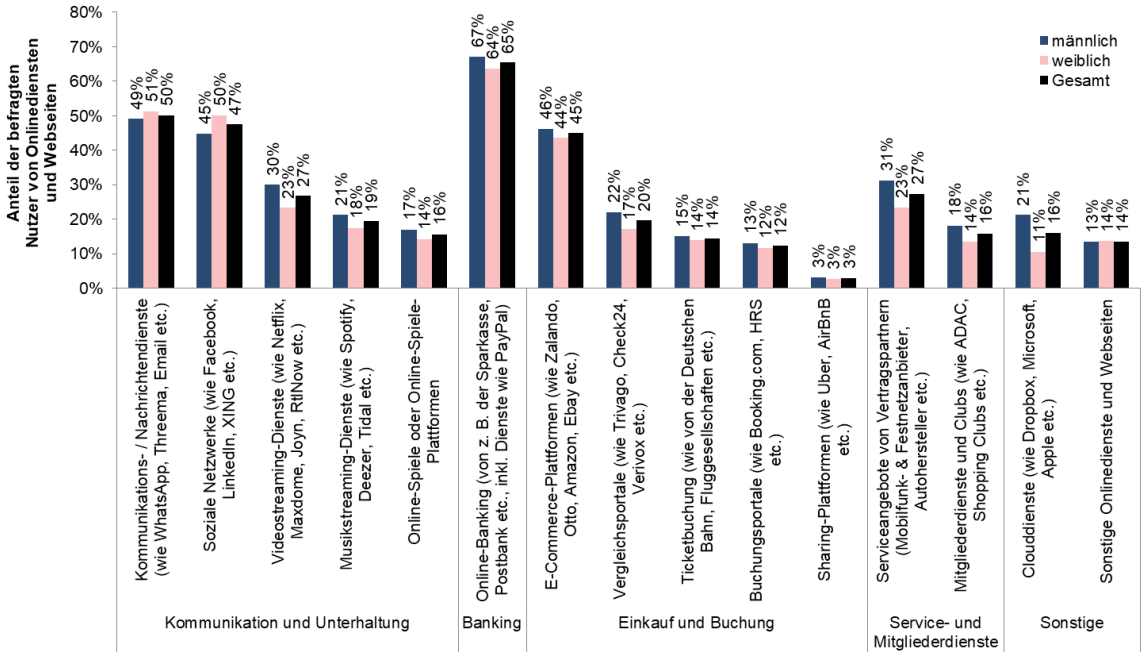


Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: N=3016. Im Durchschnitt haben etwa 20% „weiß nicht/keine Angabe“ angegeben. „Wie viele Onlinedienste und / oder Webseiten, die eine Registrierung und / oder ein Einloggen Ihrerseits erfordern, haben Sie in der letzten Woche genutzt?

6.1 Nutzung von verschiedenen Anmeldeverfahren

Um das Nutzungsverhalten weiter analysieren zu können, bedarf es Informationen dazu, welche Onlinedienste und Webseiten regelmäßig genutzt werden. Im Kontext dieser Studie wird darunter die Nutzung von Onlinediensten und Webseiten mindestens einmal in der Woche verstanden. Des Weiteren wird nach Art der Registrierung, d.h. welcher Login-Typ dabei verwendet wird, unterschieden. Darüber hinaus stellt sich die Frage, ob bestimmte Login-Typen insbesondere für bestimmte Onlinedienste verwendet werden, oder ob identische Login-Typen für verschiedenste Dienste präferiert werden. Auch soll analysiert werden, ob sich das Nutzungsverhalten nach Geschlecht oder Altersgruppen ausdifferenziert.

Abbildung 6–3: Anteil der Nutzer von Onlinediensten mit Registrierung je Art von Onlinedienst oder Webseite nach Geschlecht



wik

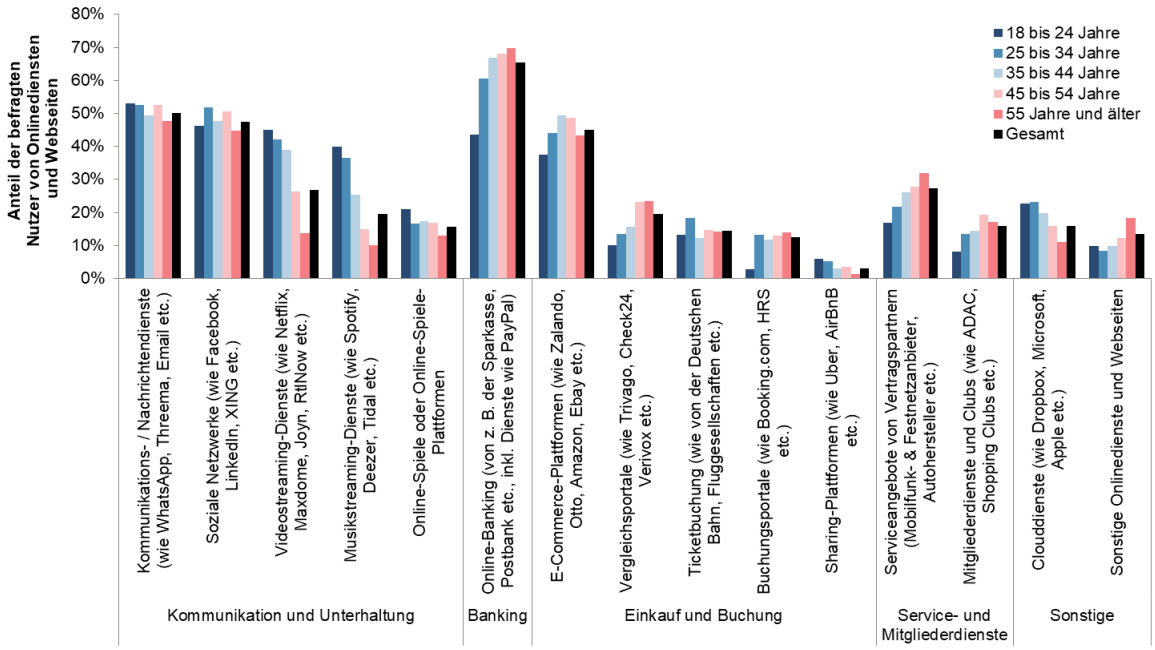
Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: N=2344. Ohne Berücksichtigung ungültiger Antworten. „Um welche Art von Onlinediensten und Webseiten handelte es sich dabei in der letzten Woche?“.

Es zeigt sich, dass Onlinebanking[20], soziale Netzwerke wie Facebook, LinkedIn, XING etc., ebenso wie Kommunikations- und Nachrichtendienste wie WhatsApp, Threema, E-Mail etc. sowie E-Commerce-Plattformen zu den meistgenutzten Onlineservices zählen. Dieses gilt zunächst einmal unabhängig vom Geschlecht. Es zeigt sich aber auch, dass mit Ausnahme von sozialen Netzwerken und Kommunikationsdiensten sämtliche Onlinedienste von Männern stärker frequentiert werden als von Frauen. Dieses gilt insbesondere für Serviceangebote von Vertragspartnern wie Mobilfunk- und Festnetzanbietern, Autoherstellern etc. sowie Cloud-Diensten von beispielsweise Dropbox, Microsoft oder Apple.

Im Folgenden wird die Nutzung von Onlinediensten und Webseiten in den verschiedenen Altersgruppen dargestellt.

20 Zum Onlinebanking sollen hier neben den Angeboten von Banken und Sparkassen auch Bezahldienste wie zum Beispiel Pay Pal, Klarna etc. gerechnet werden.

Abbildung 6–4: Anteil der Nutzer von Onlinediensten mit Registrierung je Art von Onlinedienst oder Webseite nach Alter



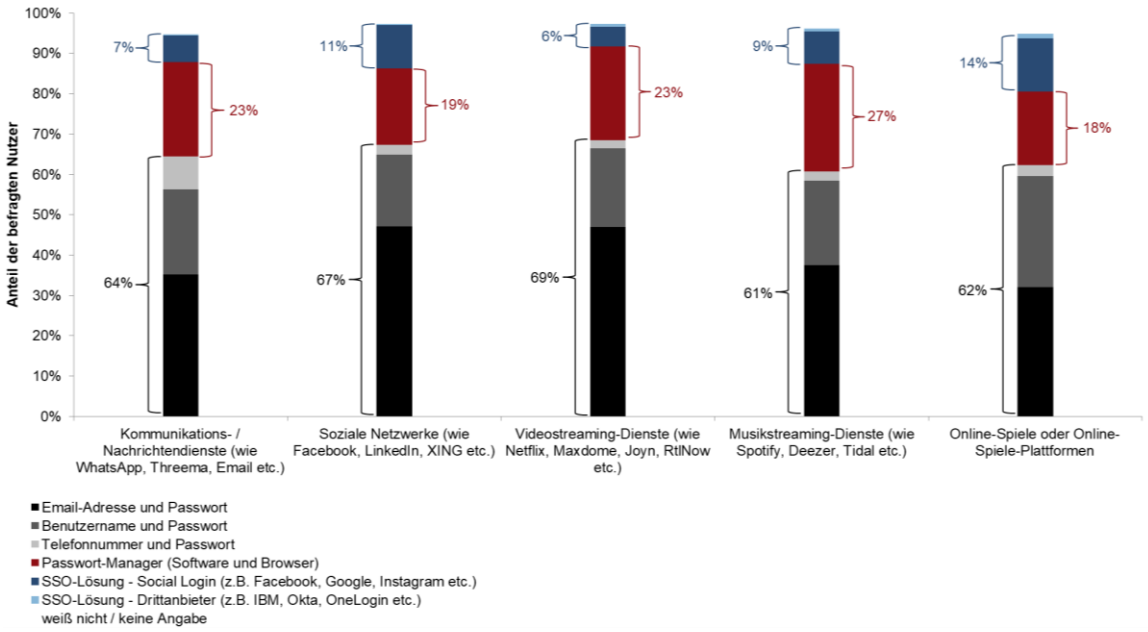
Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: N=2344. Ohne Berücksichtigung ungültiger Antworten. „Um welche Art von Onlinediensten und Webseiten handelte es sich dabei in der letzten Woche?“.

Die Betrachtung der Nutzung von Onlinediensten und Webseiten mit Registrierung getrennt nach Altersgruppen zeigt, dass das Nutzungsverhalten der jüngeren Konsumenten sich von dem Nutzungsverhalten der Älteren deutlich unterscheidet. Besonders auffällig sind die Unterschiede zwischen den Altersgruppen bei der Inanspruchnahme von Onlinebanking und Streaming-Diensten. Während ein Anteil von 46% der 18- bis 24-Jährigen regelmäßig Onlinebanking nutzt, sind es bei den ab 55-Jährigen bereits 71%. Umgekehrt nutzen 43% bzw. 45% der 18- bis 24-Jährigen Musik- bzw. Videostreaming-Dienste, wohingegen lediglich 10% bzw. 15% der Gruppe der ab 55-Jährigen dieses tun. Des Weiteren steigt das Interesse an Serviceangeboten von Vertragspartnern und Vergleichsportalen mit dem Alter. Ein extrem niedriges Interesse haben 18- bis 24-Jährige an Buchungsportalen, wohingegen das Interesse der Altersgruppe ab 55 an Sharing-Plattformen besonders niedrig ist.

Im Folgenden steht die Nutzung der verschiedenen Anmeldeverfahren für verschiedene Dienste und Webseiten beim letzten Login im Mittelpunkt des Interesses. Die in der Befragung berücksichtigten Anmeldeverfahren lassen sich in vier Gruppen einsortieren: 1) Klassische Anmeldeverfahren (z.B. Passwort und E-Mail-Adresse, Telefonnummer oder Benutzername), 2) Passwort-Manager, 3) SSO-Lösungen durch Drittanbieter (z.B. IBM, Okta, OneLogin, Verimi, NetID etc.) und 4) SSO-Dienste, die durch soziale Netz-

werke bereitgestellt werden (i.e. Social Logins von z.B. Facebook, Google, LinkedIn etc.).

Abbildung 6–5: Nutzung von Login-Typen für verschiedene Onlinedienste und Webseiten – Kommunikation und Entertainment

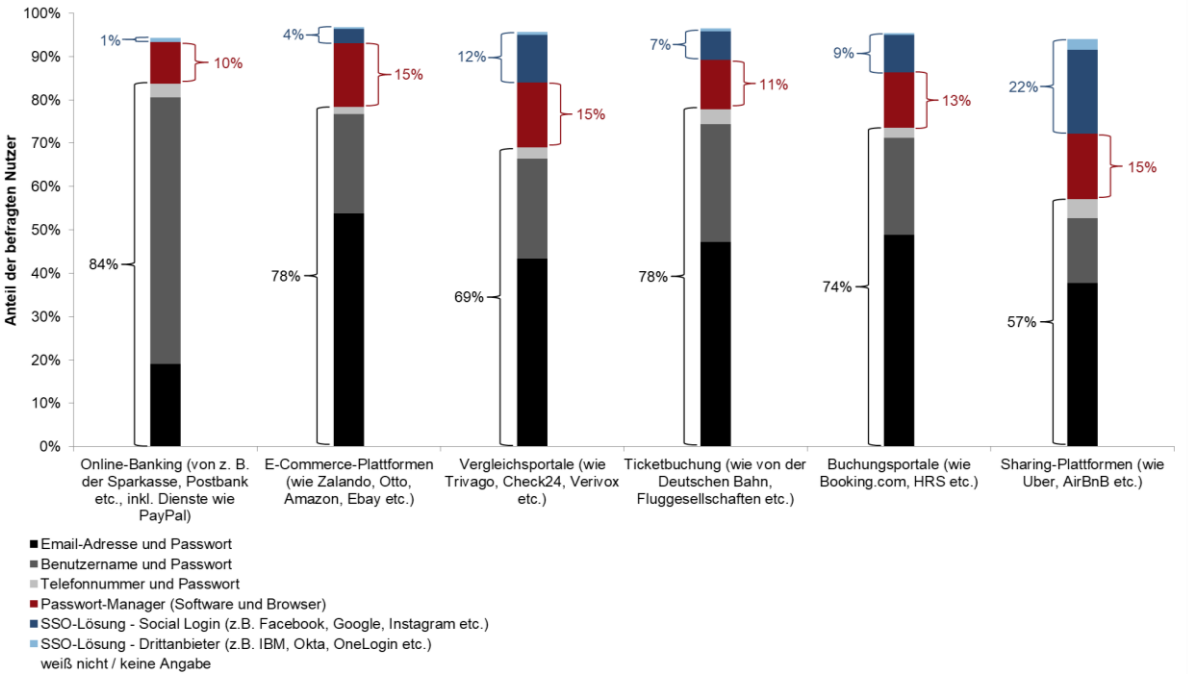


wik

Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: Stichprobe von links nach rechts: N= 1125, 1063, 596, 427, 348. „Wie sind Sie bei dem letzten Login bei den von Ihnen verwendeten Onlinediensten und Webseiten vorgegangen?“

Bei der Gruppe von Onlinediensten und Webseiten, die der Kategorie Kommunikation und Entertainment zuzuordnen sind, zeigt sich deutlich, dass im Allgemeinen die klassischen Anmeldeverfahren aus Kombination von E-Mail-Adresse, Benutzername oder Telefonnummer und Passwort bzw. Pin die am intensivsten genutzten Login-Typen sind. Die zweitgrößte Gruppe der genutzten Anmeldeverfahren machen die Passwort-Manager mit einem Nutzeranteil von gerade einmal 18-27% je nach Dienst aus. SSO-Lösungen finden hingegen kaum Verwendung. Für die Registrierung und das Einloggen bei Kommunikations- bzw. Entertainmentdiensten und -webseiten nutzen je nach betrachtetem Dienst 6-14% SSO-Lösungen. Mehr als 90% von diesen verwenden jedoch vor allem die Social Logins von z.B. Facebook, Google und LinkedIn. SSO-Lösungen von Drittanbietern wie Centrify, IBM, Okta etc. finden bei den allerwenigsten Befragten Anwendung, unabhängig davon, bei welchem Onlinedienst oder welcher Webseite sich die Befragten anmelden.

Abbildung 6–6: Nutzung von Login-Typen für verschiedene Onlinedienste und Webseiten – Banking, Einkauf und Buchung

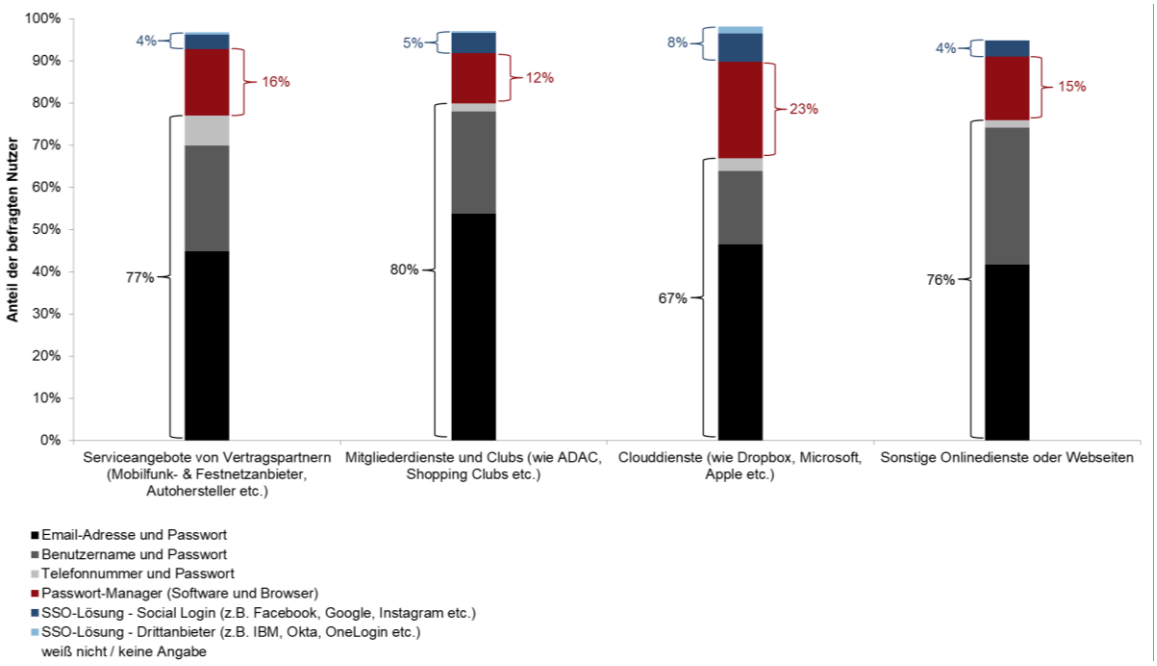


Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: Stichprobe von links nach rechts: N= 1473, 1008, 457, 333, 291, 66. „Wie sind Sie bei dem letzten Login bei den von Ihnen verwendeten Onlinediensten und Webseiten vorgegangen?“.

Bei den Onlinediensten und Webseiten der Kategorie Banking, Einkauf und Buchung ergibt sich ein ähnliches Bild wie zuvor. Die Mehrheit der Konsumenten verwendete beim letzten Login die klassischen Anmeldeverfahren. Ein etwas geringerer Anteil an Befragten gibt hingegen an, Passwort-Manager zur Anmeldung verwendet zu haben. Hier sind es nur noch 10-15% der Befragten, die diesen Login-Typ auswählen. Insgesamt geringer fällt auch der Anteil der Nutzer von SSO-Lösungen aus. Hier sind es in der Regel 1-12% der Nutzer, die dieses Anmeldeverfahren nutzen. Aus diesem Muster fällt jedoch die Nutzung von Sharing-Plattformen wie Uber oder Airbnb heraus. Hier gaben 22% der Nutzer an, SSO-Lösungen zu verwenden.

Die nachfolgende Abbildung zeigt die Nutzung von Anmeldeverfahren für weitere Onlinedienste und Webseiten wie Service- bzw. Mitgliederdienste und Cloud-Dienste. Die Nutzungsmuster von Anmeldeverfahren aus den obigen Kategorien scheinen sich hier zu wiederholen.

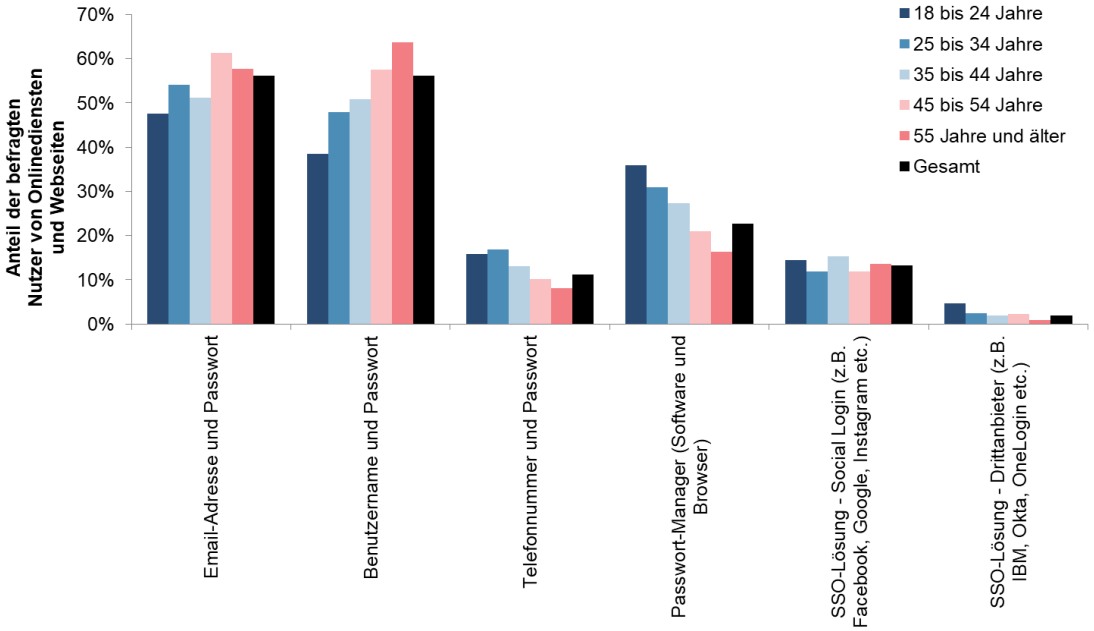
Abbildung 6–7: Nutzung von Login-Typen für verschiedene Onlinedienste und Webseiten – Service-/Mitglieder- und sonstige Dienste



Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: Stichprobe von links nach rechts: N= 631, 369, 353, 314. „Wie sind Sie bei dem letzten Login bei den von Ihnen verwendeten Onlinediensten und Webseiten vorgegangen?“.

Insgesamt lässt sich festhalten, dass nach der Anmeldung via E-Mail-Adresse, Benutzername oder Telefonnummer in Kombination mit einem Passwort oder Pin, ein Passwort-Manager – sei es als eigenständige Softwarelösung oder im Browser integriert – bevorzugt von Konsumenten verwendet wird. Der Markt für SSO-Lösungen fällt heute noch sehr klein aus und ist dort vor allem von Social Logins dominiert. Dies verdeutlicht auch die nachfolgende Abbildung.

Abbildung 6–8: Nutzung von Login-Typen für verschiedene Onlinedienste und Webseiten – Service-/Mitglieder- und sonstige Dienste



Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: N=2344. Ohne Berücksichtigung ungültiger Antworten. „Wie sind Sie bei dem letzten Login bei den von Ihnen verwendeten Onlinediensten und Webseiten vorgegangen?“.

Die Kombination E-Mail-Adresse und Passwort sowie Benutzername und Passwort wird von der Mehrheit der Befragten verwendet, obgleich letzteres Verfahren weniger stark von den Befragten in den unteren Altersgruppen genutzt wird als in den oberen Altersgruppen. Passwort-Manager – sei es als eigenständige Softwarelösung oder im Browser integriert – scheinen bei jüngeren Befragten größeren Anklang zu finden als bei älteren Befragten. Die Nutzeranteile sinken in den höheren Altersgruppen. Die Nutzung von SSO-Lösungen hingegen gestaltet sich relativ gleichmäßig in allen Altersgruppen.

Insgesamt zeigen die Ergebnisse der Befragung, dass die Teilnehmer im Schnitt etwa 1,6 verschiedene Anmeldeverfahren bei ihren Onlineaktivitäten verwenden.[21]

6.2 Nutzung von SSO-Diensten

Im vorherigen Kapitel konnte festgehalten werden, dass nur eine geringe Anzahl der Befragten angegeben haben, bei ihrem letzten Login SSO-Systeme verwendet zu haben, unabhängig davon, bei welchem Onlinedienst oder welcher Webseite sie sich anmelden. Die klassischen Anmeldeverfahren scheinen daher immer noch von den Kon-

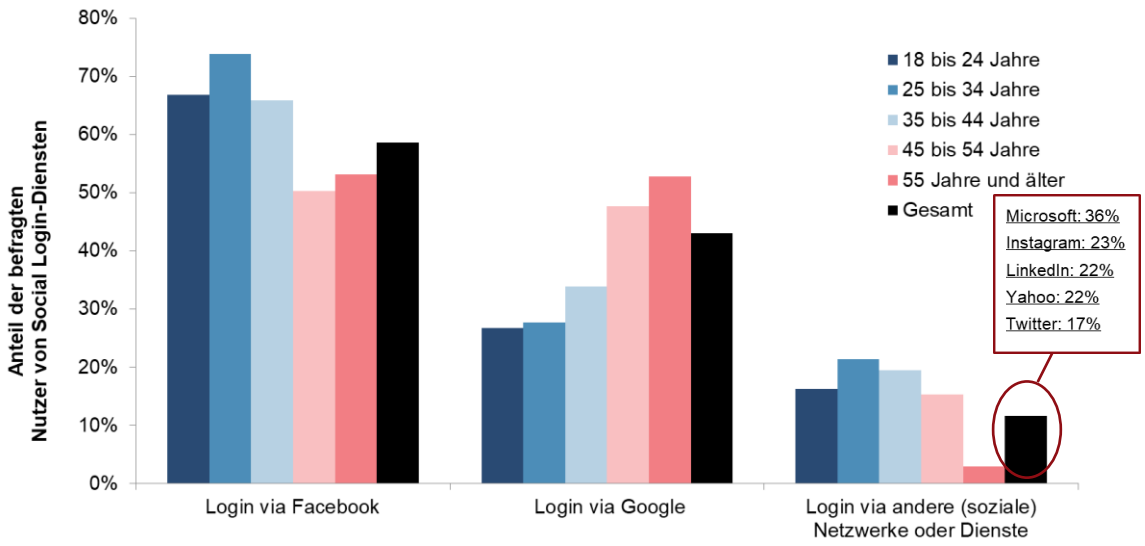
21 1,6 von 5 Verfahren. Berücksichtigt wurden 1) E-Mail-Adresse und Passwort, 2) Benutzername und Passwort, 3) Telefonnummer und Passwort, 4) Passwort-Manager (Software und Browser) und 5) SSO-Lösungen (inkl. Social Login).

sumenten bevorzugt zu werden. Unter allen Befragten, die sich in den letzten vier Wochen vor der Befragung bei einem Onlinedienst oder bei einer Webseite angemeldet haben, gaben lediglich etwa 14% an, mindestens eine SSO-Lösung (inkl. Social Login) zur Anmeldung bei Onlinediensten oder Webseiten verwendet zu haben. Demgegenüber stehen 83% der Befragten, die angaben, mindestens eins der traditionellen Anmeldeverfahren verwendet zu haben und 15% die angaben, entweder einen Passwort-Manager genutzt oder das Passwort im Browser gespeichert zu haben.

Auch wenn nur ein geringer Anteil an Konsumenten SSO-Lösungen zur Anmeldung verwendet, gilt es die Nutzung von SSO-Lösungen genauer zu analysieren.

Die nachfolgende Abbildung zeigt, welche Social Logins bei welcher Altersgruppe relevant sind. Am häufigsten wird ein Login via Facebook durchgeführt an, sich via diesem sozialen Netzwerk bei einem Onlinedienst oder bei Webseiten anzumelden. Vor allem Befragte bis 44 Jahre nutzen dies Verfahren. Beim Login via Google zeigt sich, dass dieses eher bei Befragten in den Altersgruppen 35+ Verwendung findet als in der Altersgruppe 18 bis 34 Jahre.

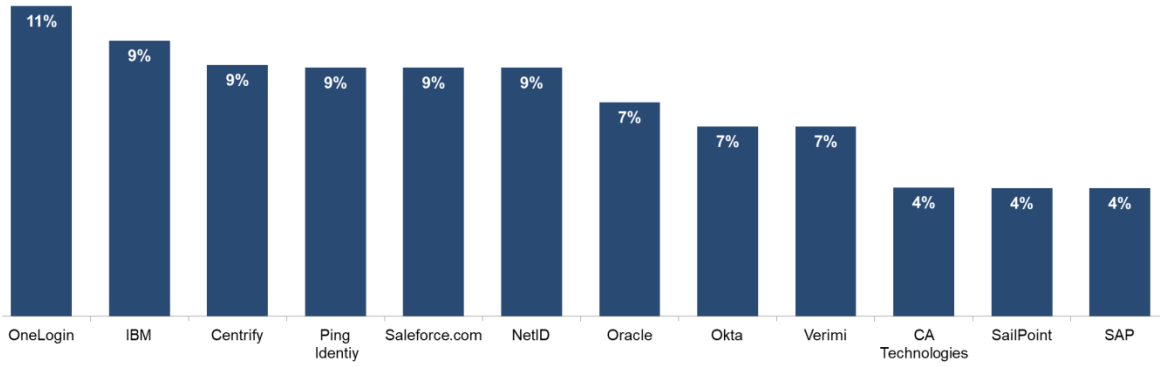
Abbildung 6–9: Nutzung von Social-Login-Lösungen



Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: N=304. Ohne Berücksichtigung ungültiger Antworten. „Wie sind Sie bei dem letzten Login bei den von Ihnen verwendeten Onlinediensten und Webseiten vorgegangen?“ und „Welche sonstigen Login-Lösungen verwenden Sie üblicherweise?“.

In der Regel verwenden die Befragten 1,2 Social-Login-Dienste.[22] Die Nachfrage nach SSO-Lösungen von Drittanbietern ist derzeit noch sehr gering. Wie im vorherigen Kapitel gezeigt, verwenden aktuell etwa 2% der Befragten SSO-Lösungen von Anbietern wie Okta, OneLogin, IBM, Centrify etc. Die nachfolgende Abbildung zeigt, welche Dienste diese Befragten im Speziellen verwenden.

Abbildung 6–10: Nutzung von Social-Login-Lösungen



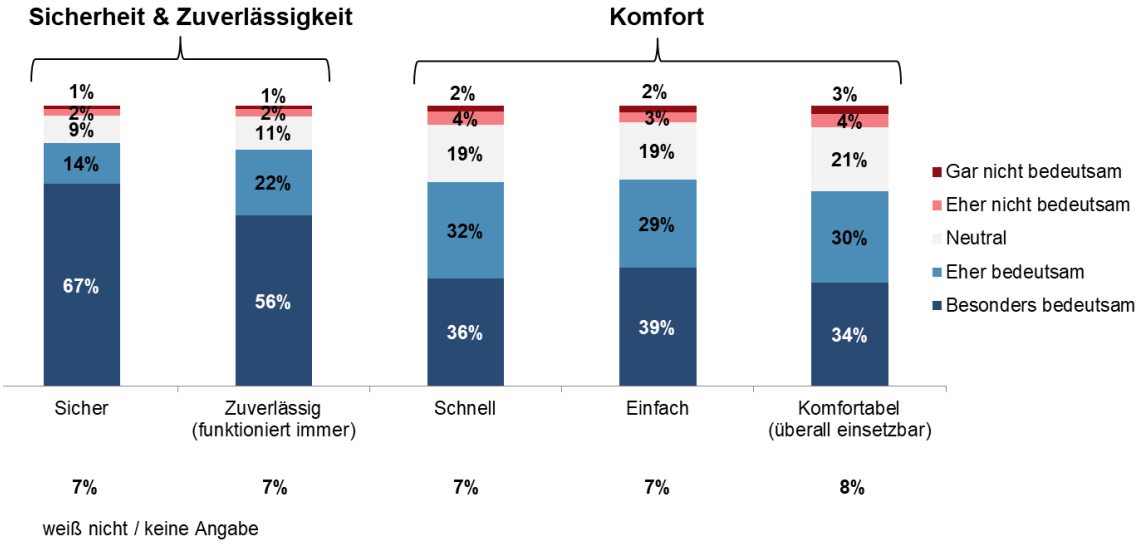
Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: N=40. „Welche sonstigen Login-Lösungen verwenden Sie üblicherweise?“.

6.3 Gründe für die Nutzung bzw. Nicht-Nutzung von SSO-Lösungen

Eine nähere Betrachtung der Gründe für die Nutzung von SSO-Systemen zeigt, dass für die Konsumenten vor allem die Aspekte Sicherheit und Zuverlässigkeit eine wichtige Rolle bei der Auswahl des Anmeldeverfahrens spielen. Etwa 72% der Konsumenten geben an, dass der Sicherheitsaspekt für sie sehr bedeutsam ist. Etwa 61% geben das gleiche in Bezug auf die Zuverlässigkeit an. Auch Komfort spielt eine Rolle. Die Anmeldung sollte schnell, einfach und komfortabel sein. Im Vergleich zu den anderen beiden Aspekten haben diese jedoch für die Konsumenten eine etwas geringere Bedeutung.

22 1,2 von 7 Verfahren. Berücksichtigt wurden 1) Facebook, 2) Google, 3) LinkedIn, 4) Twitter, 5) Microsoft, 6) Yahoo und 7) Instagram.

Abbildung 6–11: Eigenschaften von Authentifizierungssystemen für Onlinedienste und Webseiten



Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: N=3016. „Für zahlreiche Onlinedienste und Webseiten ist es heute notwendig, ein Nutzerprofil anzulegen und sich entsprechend für die Nutzung einzuloggen bzw. zu authentifizieren. Welche Eigenschaften sollten solche Authentifizierungssysteme für Onlinedienste und Webseiten Ihrer Meinung nach erfüllen? (Bitte ordnen Sie die folgenden Eigenschaften jeweils Ihre Bedeutung zu, von besonders bedeutsam (1) bis gar nicht bedeutsam (5).)“

Die beiden Eigenschaftsgruppen – Sicherheit und Zuverlässigkeit sowie Komfort – spiegeln sich auch in den meisten Antworten der Konsumenten wieder, warum sie SSO-Systeme und Social Logins nutzen oder nicht nutzen. Um die genauen Beweggründe zu erfahren, wurde den Befragten durch eine offene Frage im Fragebogen die Möglichkeit geboten zu begründen, warum sie gewisse Anmeldeverfahren nutzen oder warum sie dieses nicht tun.

Mit Blick auf Abbildung 6–11 wird offensichtlich, dass mangelnde Sicherheit bzw. der Zweifel an der Sicherheit der Systeme für viele Konsumenten ein wichtiger Grund sind, sich bei Onlinediensten oder Webseiten nicht via Facebook, Google oder durch andere (soziale) Netzwerke anzumelden.[23] Oft gehen damit auch Aussagen der Konsumenten einher, in denen ein Mangel an Vertrauen in Bezug auf ihre Daten bei der Nutzung von Social Logins bekundet wird. Weitaus mehr als die Hälfte der Befragten, die sich nicht via Google bei Onlinediensten oder Webseiten anmelden, nennen als Grund für dieses

23 Ähnlich schlussfolgern auch Sun et al (2013). Die Autoren argumentieren, dass „current implementations of web SSO solutions impose a cognitive burden on web users, and raise significant security and privacy concerns. Moreover, web users do not perceive an urgent need for SSO, and many would only use a web SSO solution on RP websites that are familiar or trustworthy.” (p.32) Sun, S.; Pospisil, E; Muslukhov, I & Nuray Dindar (2013). “A Investigating User’s Perspective of Web Single Sign-On: Conceptual Gaps, Alternative Design and Acceptance Model.” ACM Trans. On Internet Technology 13 (1), 2:1-2:35.

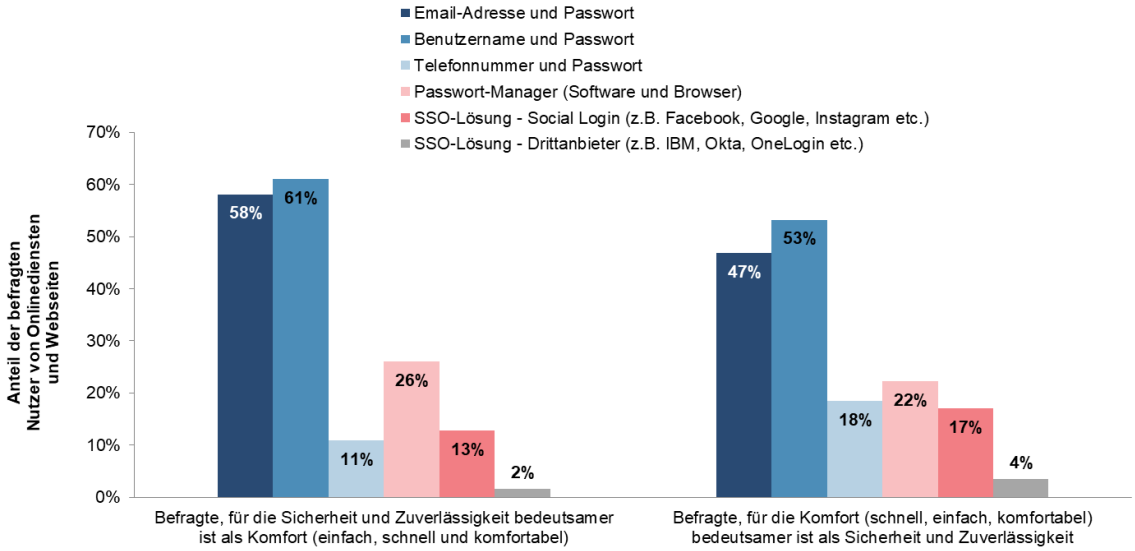
Verhalten den Aspekt der Sicherheit. Bei Facebook und anderen (sozialen) Netzwerken trifft dies auf knapp die Hälfte der erfassten Aussagen zu. Weitere häufig genannte Gründe für die Nichtnutzung von Social Logins sind schlicht das mangelnde Interesse, aber auch die Ansicht, dass diese Variante des Logins umständlich im Handling ist. Auch unter den Nutzern gibt es nur wenige, die von der Sicherheit dieser Systeme überzeugt sind. Sicherheitsaspekte sind nach Auskunft der Befragten nämlich in aller Regel kein Grund, eines der genannten Verfahren zu nutzen. Vielmehr tritt hier die Einfachheit der Nutzung in den Vordergrund. Die Befragten scheinen für ein unkompliziertes, schnelles und einfaches Verfahren ihre Sicherheitsbedenken hinten an zu stellen.[24] Dies korrespondiert genau dazu, dass Sicherheitsaspekte dann als Grund für eine Nichtnutzung angeben werden, wenn auch das Handling als kompliziert eingestuft wird und das Interesse an einem Verfahren folglich gering ist. Dies ist ein interessantes Muster im Nutzungsverhalten.

Im Hinblick auf SSO-Dienste wie die von IBM, Okata, Onelogin etc. erhalten wir ein etwas differenzierteres Bild, was die Gründe für die Nutzung bzw. Nichtnutzung betrifft. Unter den Nichtnutzern befinden sich nur wenige, die angeben, diese Dienste aus Sicherheits- oder Datenschutzbedenken nicht zu nutzen. Hauptgrund für die Nichtnutzung scheinen hier eher ein mangelndes Interesse oder mangelnde Kenntnis des Systems und dessen Handlings zu sein. Bei den Nutzern finden sich immerhin mehr als 40%, die diese Dienste als sicher einstufen und deswegen nutzen. Ein weiterer Grund für die Nutzung ist aus Sicht der Konsumenten die einfache Handhabung. Es zeigt sich also, dass die Nutzer, die aus Sicherheitsaspekten das Login über Drittanbieter auswählen und sich damit vertraut machen, das Handling nicht als hinderlich oder kompliziert bewerten.

Wird die Gruppe von Befragten, die Sicherheit und Zuverlässigkeit eines Authentifizierungsverfahrens als wichtiger bzw. bedeutsamer einstufen, mit der Gruppe von Befragten verglichen, die Komfort stärker wertschätzen, lässt sich erkennen, dass letztere eher dazu neigen, SSO-Lösungen (inkl. Social Logins) zu verwenden als die erste Gruppe von Befragten.

24 So fanden beispielsweise auch Gafni & Nissim (2014) heraus, dass „Individuals who actually use Social Login in order to access into relying Websites, […] are less inhibited by the security and privacy factors than those who do not use the mechanism. […]they appreciate the familiarity and convenience factor more than those who do not use it." (p.72). Gafni, R., & Nissim, D. (2014). To social login or not login? - Exploring factors affecting the decision. Issues in Informing Science and Information Technology, 11, 57-72.

Abbildung 6–12: Anforderungen an Authentifizierungssysteme für Onlinedienste und Webseiten



Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: Stichprobe von links nach rechts: N=1247, 227. „Für zahlreiche Onlinedienste und Webseiten ist es heute notwendig, ein Nutzerprofil anzulegen und sich entsprechend für die Nutzung einzuloggen bzw. zu authentifizieren. Welche Eigenschaften sollten solche Authentifizierungssysteme für Onlinedienste und Webseiten Ihrer Meinung nach erfüllen? (Bitte ordnen Sie die folgenden Eigenschaften jeweils Ihre Bedeutung zu, von besonders bedeutsam (1) bis gar nicht bedeutsam (5).)“. und „Wie sind Sie bei dem letzten Login bei den von Ihnen verwendeten Onlinediensten und Webseiten vorgegangen?“.

6.4 Konvergenz digitaler Identitäten

Digitale Identitäten werden für unterschiedliche Anwendungen genutzt. Sie sind erforderlich für die digitale Kommunikation via E-Mail, das Login in das eigene soziale Profil, für Internethandelsgeschäfte oder auch Online-Bankgeschäfte etc.[25]

Fakt ist, dass Internetnutzer verschiedene Logins in verschiedenen Anwendungsszenarien verwenden. Es muss sich also nicht zwangsläufig eine Konvergenz der digitalen Identität mit der realen Identität entwickeln. Es ist durchaus möglich und auch verbreitet, dass Nutzer verschiedene digitale Identitäten verwenden und diese jeweils nur einen Teilbereich der realen Identität abbilden oder sogar mit falschen Angaben befüllt werden. Dieses kann zum einen immer dann der Fall sein, wenn Anonymität gewünscht ist (zum Beispiel auf Spieleplattformen etc.) oder wenn Bedenken bestehen, dass die digitale Identität bzw. deren Informationen missbraucht werden könnten.

25 Vgl. https://www.bundesdruckerei.de/de/Themen-Trends/Magazin/Was-ist-eine-digitale-Identitaet [letzter Abruf 23.06.2020].

Gleichwohl gibt es Anwendungsbereiche, in denen die digitale Identität zwingend konvergent zur realen Identität ist. Dieses gilt zum Beispiel für öffentliche Bereiche oder auch das Onlinebanking. Hier werden dann wiederum Verfahren eingesetzt, die die Identität zweifelsfrei klären (Post-Ident-Verfahren, Digitale Signaturen etc.). Es ist zu vermuten, dass eine solche Identität dann von den Konsumenten nicht gerne als SSO eingesetzt wird, wenn gegenüber einem verbundenen Dienst oder der Webseite Bedenken hinsichtlich der Sicherheit bestehen.[26]

Es lässt sich die These aufstellen, dass je sicherer ein Authentifizierungsverfahren ist, desto eher besteht Konvergenz zwischen digitaler und realer Identität und je schützenswerter die übermittelten Daten, desto wichtiger bewertet ein Nutzer die Sicherheit eines Authentifizierungsverfahrens.

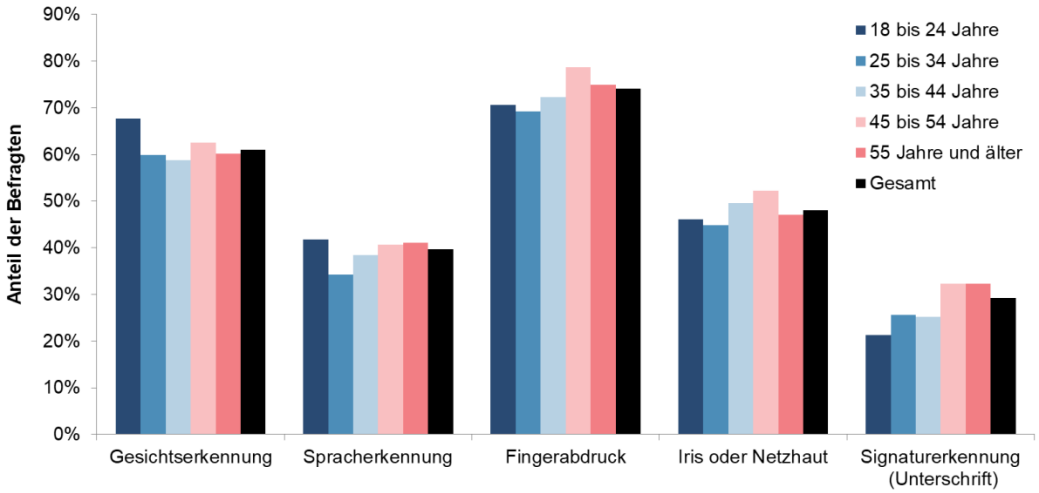
6.5 Biometrische Authentifizierungsverfahren

Die Authentifizierung über biometrische Merkmale findet immer mehr Anwendung im Alltag der Menschen, sei es im Austausch mit Behörden, beim Online-Banking oder gar beim Einschalten des eignen Smartphones. Den allermeisten Befragten sind biometrische Authentifizierungsverfahren bekannt. Mehr als 50% der Befragten sind dabei unabhängig vom Alter zwei Authentisierungsverfahren bekannt, namentlich die Gesichtserkennung und die Erkennung über den Fingerabdruck.

Die Spracherkennung und die Erkennung über Iris- oder Netzhautscan ist knapp 40% bzw. knapp 50% der Befragten bekannt. Die Erkennung über den Fingerabdruck und über den Iris- oder Netzhautscan ist mit 79% bzw. 52% der Befragten jeweils in der Altersgruppe 45 bis 54 Jahre das bekannteste Verfahren. Gesichtserkennung und Spracherkennung hingegen sind eher Verfahren, die der jüngeren Altersgruppe der 18 bis 24-Jährigen bekannt sind.

26 Vgl. zu den Gefahren gestohlener digitaler Identitäten https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Schutzmassnahmen/id-dieb_schutz_node.html [letzter Abruf 23.06.2020].

Abbildung 6–13: Anteil der Kenner von biometrischen Authentifizierungsverfahren nach Alter



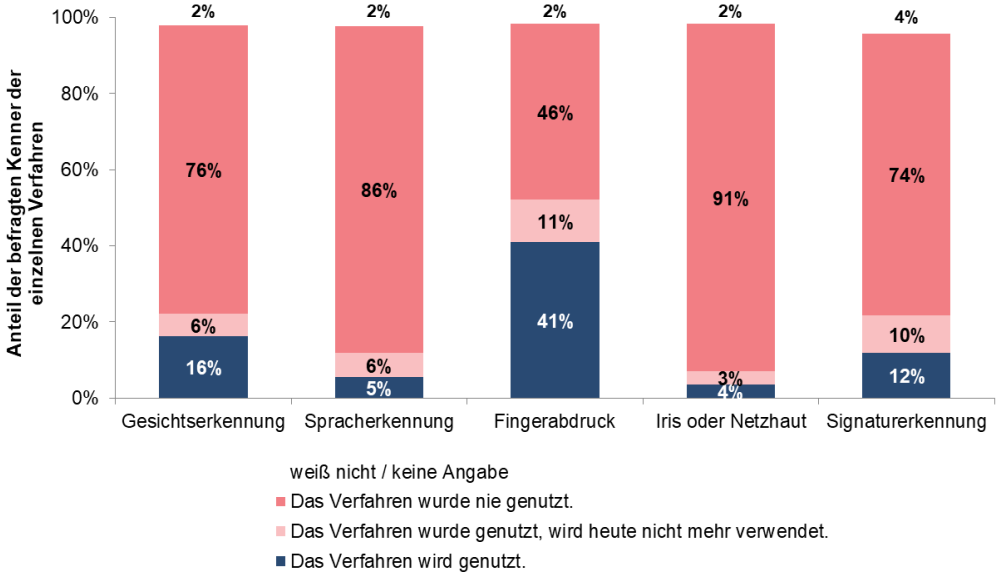
Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: N=3016. "Von welchen der folgenden Authentifizierungsverfahren haben Sie schon einmal gehört?".

Es zeigt sich, dass das bekannteste Verfahren, das Fingerabdruckverfahren, auch von den meisten Befragten genutzt wird. Auf diese Gruppe entfallen 40% der Befragten. Die meistgenannte Aussage für jedes zur Auswahl stehende Verfahren ist jedoch, dass es noch nie genutzt worden ist.

Es kann festgehalten werden, dass die meisten Verfahren nicht sonderlich intensiv genutzt werden. Die größere Bekanntheit und relativ verbreitete Nutzung des Fingerabdruckverfahrens lässt sich durch die Verbreitung dieser Technologie in Smartphones erklären. Das Marktforschungsunternehmen Statista gibt an, dass in 2018 bereits 80% aller verkauften Smartphones mit biometrischen Technologien ausgeliefert wurden, mit steigender Tendenz.[27] Daher ist es äußerst wahrscheinlich, dass Konsumenten, die bis dato andere biometrische Verfahren nicht genutzt haben (z.B. Gesichtserkennung), dieses in naher Zukunft beispielsweise nach einem Wechsel auf ein neueres Smartphone tun werden.

27 https://de.statista.com/infografik/11117/weltweiter-absatz-anteil-von-geraeten-mit-biometrischen-technologien/ [letzter Abruf 29.06.2020].

Abbildung 6–14: Nutzung verschiedener biometrischer Authentifizierungsverfahren

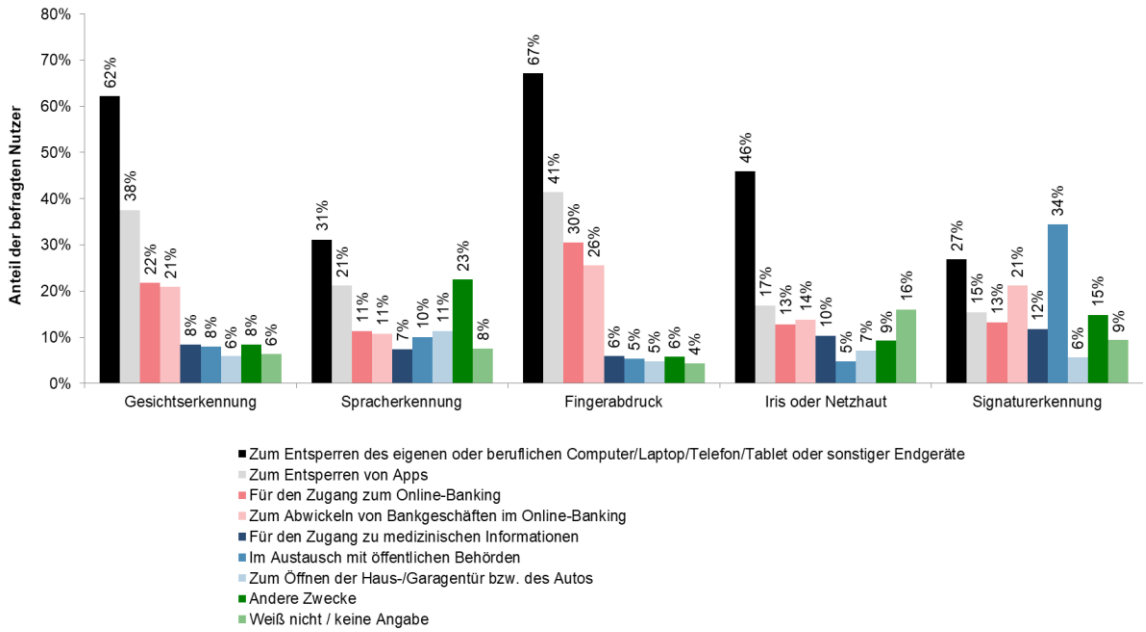


Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019. Stichprobe von links nach rechts: N=1837, 1186, 2234, 1438, 886.“ Bitte sagen Sie uns, was für Sie persönlich bei den einzelnen Authentifizierungsverfahren zutrifft.“

Die nachfolgende Abbildung stellt die Anwendungsfälle der verschiedenen biometrischen Verfahren dar, die von den Befragten genutzt werden. Es fällt auf, dass fast unabhängig vom Verfahren die biometrische Authentifizierung von den Befragten vor allem zur Entsperrung von Endgeräten wie Computer, Laptops oder Smartphones oder zur Entsperrung von Apps verwendet werden. Der jeweils größte Anteil der Nutzer von Spracherkennung, Gesichtserkennung, Iris- oder Netzhautscan und der Authentifizierung durch den Fingerabdruck verwendet die Methoden für diese Zwecke. Bei der Signaturerkennung liegt das Hauptanwendungsfeld jedoch im Austausch mit der öffentlichen Verwaltung.[28]

28 German & Suzanna (2018) untersuchten ebenfalls die gleichen und andere Anwendungsfelder. Für nähere Informationen siehe: German, Rachel L. & Barber K. Suzanna. (2018). Consumer Attitudes About Biometric Authentification. *The University of Texas at Austin. Center for Identity. UT CID Report No. 18-03.*

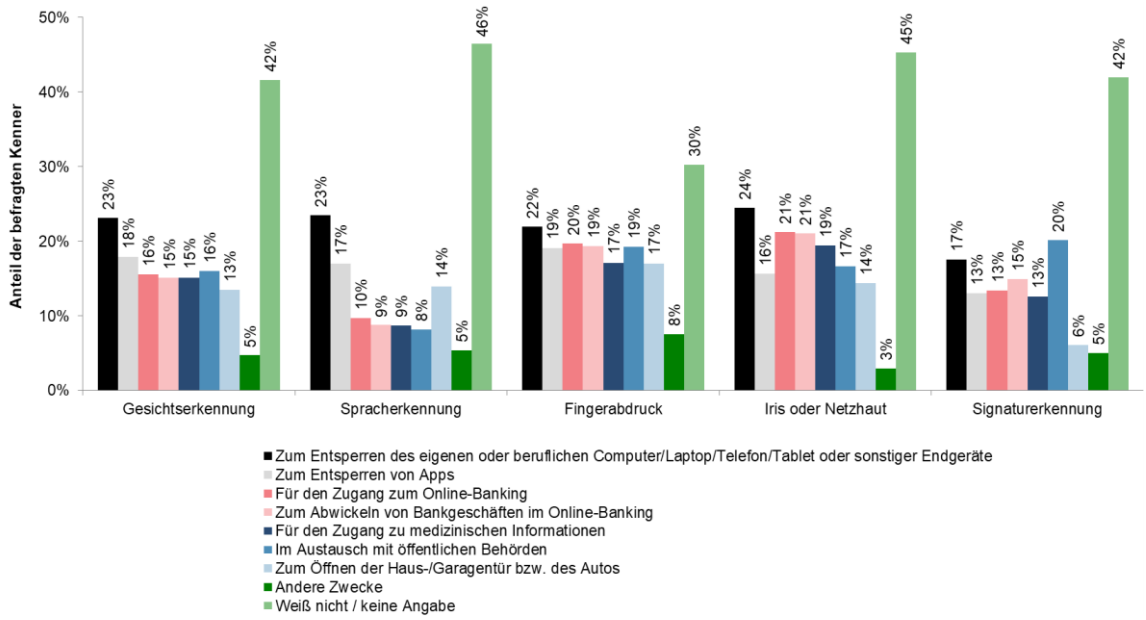
Abbildung 6–15: Nutzung verschiedener biometrischer Authentifizierungsverfahren nach Anwendungsfällen



Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: N=390, 137, 1148, 95, 191. „Bitte geben Sie an, zu welchen Zwecken Sie die Authentifizierungsverfahren verwenden bzw. verwendet haben.“

Die Vorstellungskraft der Befragten, für welche Anwendungen einzelne biometrische Verfahren, die bis dato noch nicht genutzt wurden, potenziell interessant sein könnten, ist relativ gering. Über alle Verfahren hinweg war die Antwort „weiß nicht“ bzw. „keine Angabe“ die meistgegebene auf die Frage nach potenziellen Anwendungsfällen verschiedener biometrischer Authentifizierungsverfahren. Die meisten Chancen werden letztlich den Verfahren von Iris-/Netzhautscan und Fingerabdruck zugestanden. Interessanterweise hat sich nach der Erkennung des Fingerabdrucks die Gesichtserkennung als zweites dominantes und im Massenmarkt für Smartphones verbreitetes biometrisches Verfahren etabliert. Dies legt nahe, dass Nutzer eher auf die Verfügbarkeit dieser Technologien reagieren, als deren zukünftigen Nutzen im Alltag und deren Relevanz frühzeitig zu antizipieren.

Abbildung 6–16: Potenzielle Einsatzmöglichkeiten verschiedener biometrischer Verfahren nach Anwendungsfällen



Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: Stichprobe von links nach rechts: N=1834, 1185, 2224, 1437, 885. “Bitte geben Sie an, zu welchem Zweck / welchen Zwecken Sie das folgende Authentifizierungsverfahren (noch) verwenden würden, falls dieses entsprechend verfügbar wäre.“

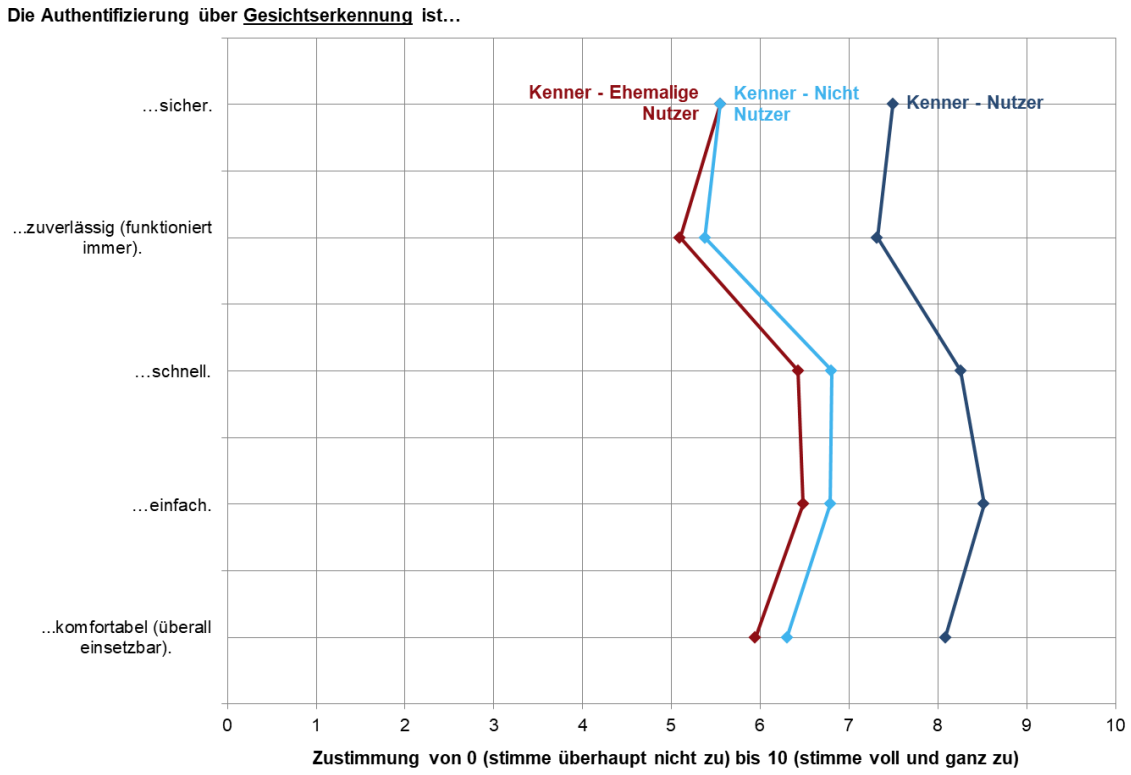
Assoziationen, die die Befragten mit den einzelnen biometrischen Verfahren verbinden, sind relativ ähnlich. Sie gelten durchweg als einfach und komfortabel in der Anwendung. Allerdings fällt auch auf, dass bei den Befragten im Hinblick auf keines der Verfahren eine starke Überzeugung zu bestehen scheint. Grundsätzlich gilt jedoch, dass die Nutzer die einzelnen biometrischen Authentifizierungsverfahren im Hinblick auf Sicherheit, Zuverlässigkeit, Einfachheit, Schnelligkeit und Komfort höher bewerten als Nichtnutzer oder gar diejenigen, die mit der Nutzung der Verfahren aufgehört haben. Nichtsdestotrotz werden in nahezu allen Fällen Sicherheit und Zuverlässigkeit geringer eingestuft als die anderen Aspekte.

Die Authentifizierung über den Fingerabdruck, also das Verfahren, das die meisten der Befragten bereits verwenden, ist mit den positivsten Assoziationen verbunden. Die Gesichtserkennung, die ebenfalls von vielen der Befragten bereits verwendet wird, gilt zwar als einfach, schnell und komfortabel, allerdings wird ihr Zuverlässigkeit und Sicherheit abgesprochen.

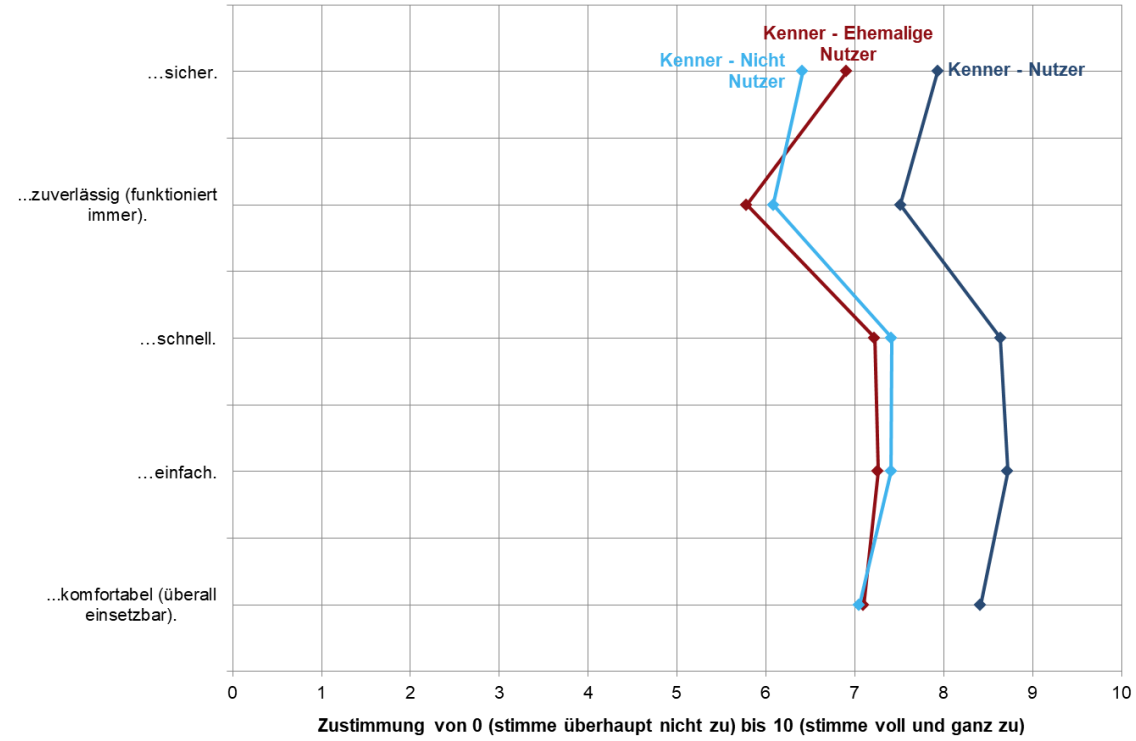
Dieser Zusammenhang lässt sich auf den folgenden Grafiken für unterschiedliche biometrische Verfahren nachvollziehen. Dazu werden auf der Y-Achse der Grafiken die unterschiedlichen Eigenschaften der biometrischen Verfahren abgetragen und auf der

X-Achse die Zustimmung der Befragten zu diesen Eigenschaften. Die Antworten der Befragten, die biometrische Verfahren kennen, werden dabei getrennt nach den Gruppen „Nicht-Nutzer“, „Ehemalige Nutzer“ und „Nutzer“ in diesem Diagramm verortet. Dabei zeigt sich, dass ehemalige Nutzer diese Verfahren tendenziell schlechter bewerten als Nicht-Nutzer, also Befragte, die diese Verfahren zwar kennen, aber selbst noch nie genutzt haben. Einzig bei der Signaturerkennung bewerten ehemalige Nutzer das Verfahren eindeutig besser als Nutzer, die das Verfahren bisher noch nicht genutzt haben.

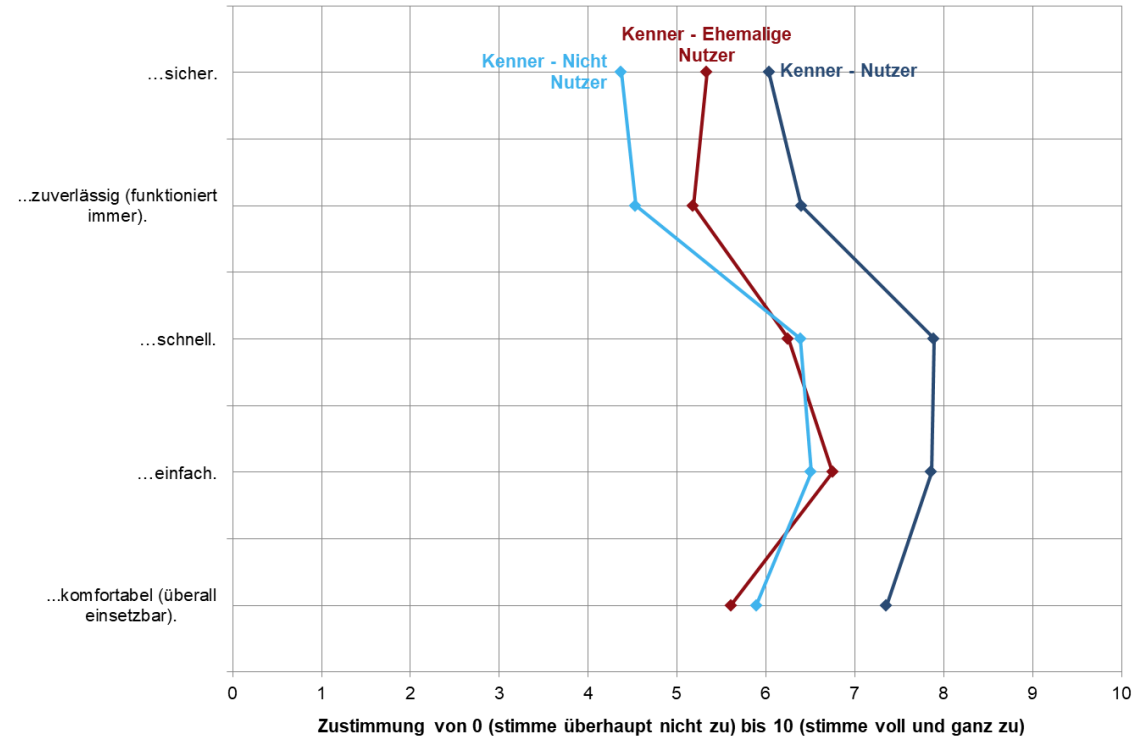
Abbildung 6–17: Assoziationen/Einschätzungen zu verschiedenen biometrischen Verfahren



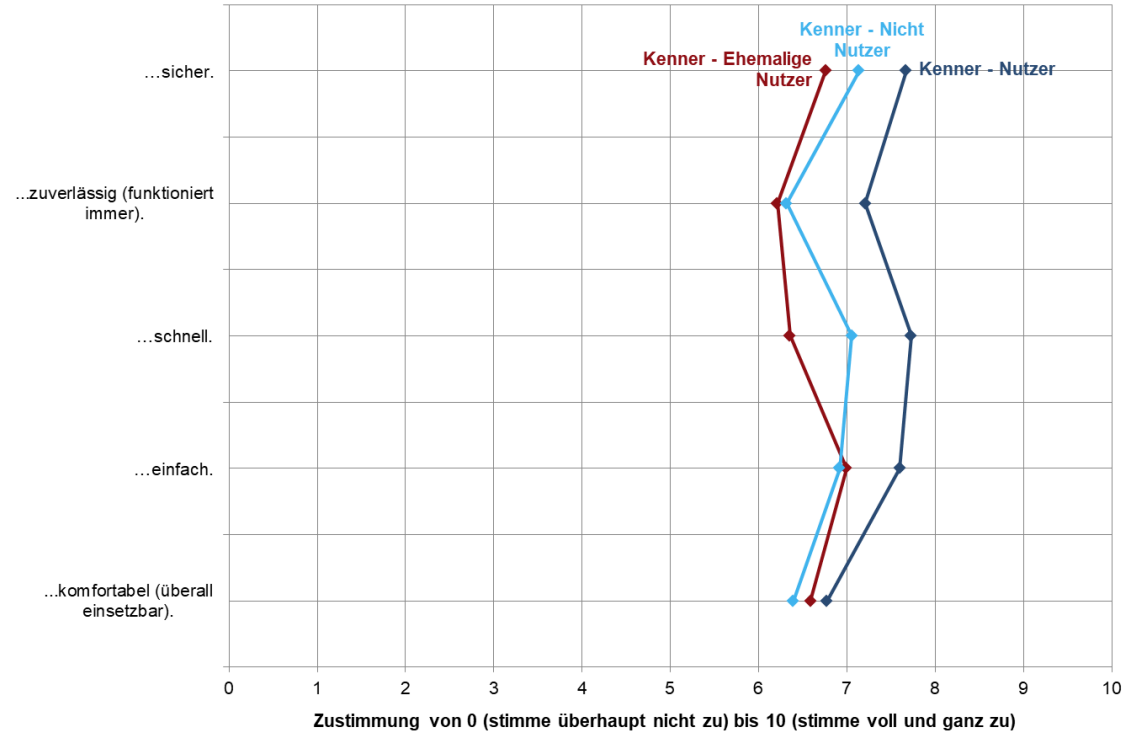
Die Authentifizierung über Fingerabdruck ist…



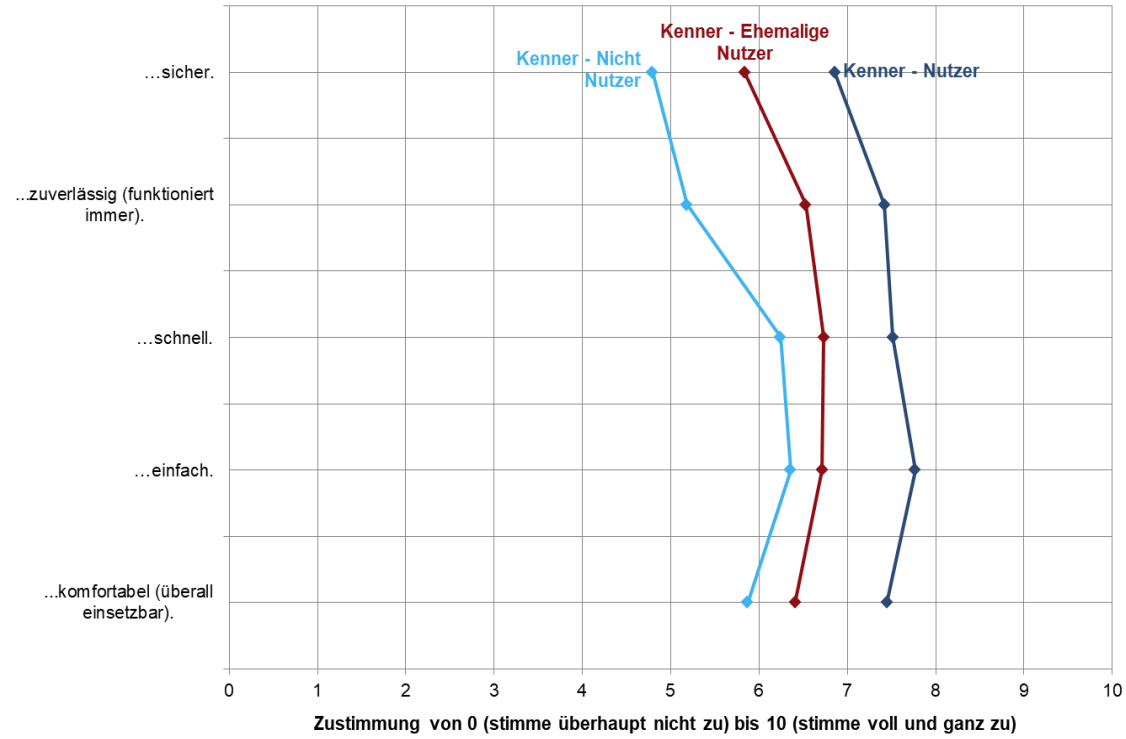
Die Authentifizierung über Spracherkennung ist…



Die Authentifizierung über die Iris oder Netzhaut ist…



Die Authentifizierung über Signaturerkennung ist…



wik

Quelle: Eigene Darstellung; Daten stammen aus der Online-Umfrage des WIK in 2019: Stichprobe von oben nach unten: N=1837, 1186, 2234, 1438, 886. Ohne Berücksichtigung der Befragten, die „weiß nicht / keine Angabe“ angegeben haben. “Inwiefern stimmen Sie den folgenden Aussagen in Bezug auf die Authentifizierung über Gesichtserkennung zu? Die Authentifizierung über Gesichtserkennung/Spracherkennung/Fingerabdruck/die Iris oder Netzhaut/Signaturerkennung ist...“.

7 Schlussfolgerungen & Ausblick

Single-Sign-On-Verfahren treten mit dem Versprechen an, die Anzahl der verschiedenen Zugangsdaten zu unterschiedlichen digitalen Diensten zu reduzieren und den Registrierungsprozess bei neuen Diensten zu vereinfachen. Drittanbieter konnten sich dabei insbesondere in einem institutionellen und geschäftlichen Kontext etablieren, während die Social Logins digitaler Plattformbetreiber wie beispielsweise Facebook und Google den Massenmarkt für Privatanwender dominieren. Insbesondere Nutzer, die Wert auf eine Vereinfachung des Anmeldeprozesses und eine komfortable Nutzung legen, profitieren dabei von diesen Angeboten. Aber auch die verbundenen Dienstanbieter, die diese Anmeldeverfahren auf ihren Webseiten implementieren, profitieren davon, wenn sich ein Nutzer mit einem Social Login bei ihren Diensten anmeldet. Durch die mögliche Übertragung vorvalidierter Informationen aus sozialen Benutzerprofilen können diese Anbieter bereits bestehende Informationen mit verhaltensbezogenen Daten der Nutzung ihrer Dienste verbinden. Dadurch entstehen reichhaltigere Nutzerprofile, welche wiederum personalisierte Dienste und Werbung ermöglichen, was sich positiv auf den Umsatz dieser Unternehmen auswirkt.

Allerdings erhalten auch die Anbieter von SSO-Diensten Informationen über die Nutzung verbundener Dienste und Webseiten. Insbesondere werbefinanzierte Plattformen, die Social Logins anbieten, zielen darauf ab, die Benutzerprofile ihrer Kunden mit Informationen anzureichern, die über ihre eigene Plattform nicht direkt erhoben bzw. beobachtet werden können. Über Social Logins erhalten diese Anbieter also einen Einblick in die Interessen und das Nutzungsverhalten ihrer Kunden in Bereichen des Internetökosystems, die anderweitig für sie nicht direkt quantifizierbar sind. Dadurch wird es auch diesen Unternehmen möglich, ihre Angebote und Werbekampagnen stärker zu personalisieren und damit höhere Umsätze pro Kunde zu erwirtschaften.

Abschließend lässt sich festhalten, dass die Implementierung insbesondere von Social Logins aus Sicht digitaler Inhalte- und Dienstanbieter keine nennenswerten Kosten verursacht. Es ist also nicht aufwendig, möglichst viele Social Logins zu unterstützen, um so möglichst vielen unterschiedlichen Kunden eine einfache Anmeldung und regelmäßige Nutzung ohne zusätzlichen Aufwand zu ermöglichen. Da es trotz Bedenken gegenüber diesen Diensten auch weiterhin Internetnutzer mit einer stärkeren Präferenz für Komfort gibt, werden diese Verfahren am Markt voraussichtlich Bestand haben.

Allerdings bleibt in diesem Kontext die Frage offen, ob Dienstanbieter, die Social Logins auf ihren Webseiten implementieren, langfristig von diesen Lösungen profitieren können. Während Social Logins die Konversion von Besuchern zu aktiven Benutzern steigern und darüber initial zusätzliche Informationen über neue Nutzer gewonnen werden können, ist es Dienstanbietern mit diesen Lösungen nicht notwendigerweise möglich, einen Wettbewerbsvorteil gegenüber anderen Dienstanbietern zu erzielen, die ebenfalls Social Logins implementieren. Darüber hinaus stärken Social Logins gleichzeitig die Marktposition der Social Login-Anbieter durch die bei der Nutzung anfallenden Daten.

Dabei ist unklar, welche Informationen genau durch die Anbieter von Social Logins dauerhaft gespeichert werden. Während bestimmte Daten im Rahmen der technischen Bereitstellung der Funktionalität notwendigerweise übertragen werden müssen, können diese auch nach der Leistungserbringung vom Anbieter dauerhaft gespeichert und weiter verwendet werden. Darüber hinaus könnten auch Daten erhoben und dauerhaft gespeichert werden, die zur Erbringung der Leistung nicht erforderlich sind. Im Gegensatz zu Social Logins wurde beispielsweise der Like-Button von Facebook im Hinblick auf Datenschutzgesichtspunkte bereits viel diskutiert. Ebenso wie der Social Login lässt sich ein Like-Button ohne großen Aufwand in ein bestehendes Webangebot einbinden. Allerdings werden dadurch bereits beim Laden der Webseite, ohne weitere Interaktion des Nutzers mit dem Button, die IP-Adresse, Browser Informationen und eventuell vorhandene Cookies an den Plattformprovider übertragen.[29] Es ist daher zu vermuten, dass die Anbieter von Social Logins nicht nur von der direkten Nutzung der Funktionalität profitieren, sondern bereits implizit von der Verbreitung der Funktionalität. Daher werden die Implikationen von Social Logins auch im Zusammenhang mit dem Digital Services Act der EU Kommission unter den Gesichtspunkten Schutz der Anwender und Sicherstellung des Wettbewerbs weiter diskutiert werden.

Im Gegensatz dazu erscheint die Zukunft biometrischer Verfahren erheblich vorhersehbarer. Mit sinkenden Kosten für biometrische Sensoren und der weiteren Durchdringung des Massenmarkts mit diesen Technologien (insb. Smartphones) wird die Akzeptanz und Nutzung dieser Verfahren immer weiter zunehmen. Smartphone-Nutzer setzen diese Verfahren bereits in immer neuen Kontexten ein, beispielsweise um kontaktlose Zahlungen zu autorisieren. Da Smartphones regelmäßig erneuert werden ist davon auszugehen, dass diese Verfahren in Zukunft immer mehr Verbreitung im Alltag finden.

29 Court of Justice of the European Union, PRESS RELEASE No 206/18, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-12/cp180206en.pdf [Zuletzt abgerufen: 02.07.2020]

Literaturverzeichnis

Bauer, N. & J. Blasius (2019). Handbuch Methoden der empirischen Sozialforschung. VS Verlag für Sozialwissenschaften.

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2013). Guide to biometrics. Springer Science & Business Media

Camp, J. L. (2004). Digital identity. IEEE Technology and society Magazine, 23(3), 34-41.

Chadwick, D. W., Inman, G. L., Siu, K. W., & Ferdous, M. S. (2011). Leveraging social networks to gain access to organisational resources. Proceedings of the 7th ACM workshop on Digital Identity Management, pp. 43-52

Court of Justice of the European Union, PRESS RELEASE No 206/18, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-12/cp180206en.pdf [Zuletzt abgerufen: 02.07.2020]

De Clercq, J. (2002, October). Single sign-on architectures. In International Conference on Infrastructure Security (pp. 40-58). Springer, Berlin, Heidelberg.

Gafni, R., & Nissim, D. (2014). To social login or not login? - Exploring factors affecting the decision. Issues in Informing Science and Information Technology, 11, 57-72

Gasti, P., & Rasmussen, K. B. (2012, September). On the security of password manager database formats. In European Symposium on Research in Computer Security (pp. 770-787). Springer, Berlin, Heidelberg.

German, R. L. & Suzanna, B. K. (2018): Consumer Attitudes About Biometric Authentification. The University of Texas at Austin. Center for Identity. UT CID Report No. 18-03.

Gigya (2015): Social Login 101: Everything You Need to Know About Social Login and the Future of Customer Identity. Whitepaper.

Goode, A. (2014). Bring your own finger–how mobile is bringing biometrics to consumers. Biometric Technology Today, 2014(5), 5-9.

https://adage.com/article/digital/facebook-owns-social-login-scene-google-s-creeping/302407 [letzter Abruf 02.07.2020].

https://en.wikipedia.org/wiki/Social_login [letzter Zugriff 23.06.2020].

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Passwort_Manager/Passwort_Manager_node.html [letzter Abruf 23.06.2020].

https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Schutzmassnahmen/id-dieb_schutz_node.html [letzer Abruf 23.06.2020].

https://www.bundesdruckerei.de/de/Themen-Trends/Magazin/Was-ist-eine-digitale-Identitaet [letzter Abruf 23.06.2020].

https://www.chip.de/artikel/Test-Die-besten-Passwort-Manager_182620837.html [letzter Abruf 23.06.2020]

https://www.pcwelt.de/ratgeber/Die_besten_Passwort-Manager_fuer_Android-9008619.html [letzter Abruf 23.06.2020]

https://www.shopify.de/ [letzer Abruf 02.07.2020]

https://www.tuv.com/germany/de/authentifizierung.html [letzter Abruf 02.07.2020].

Pittman, J. M., & Robinson, N. (2020). Shades of Perception-User Factors in Identifying Password Strength. arXiv preprint arXiv:2001.04930.

Krämer, J., Schnurr, D., Wohlfahrt, M. (2018): Winners, Losers, and Facebook: The Role of Social Logins in the Online Advertising Ecosystem, in: Management Science, 2019, vol. 65, no. 4, pp. 1678–1699.

Koch, J., Gebhardt, P., & F. Riedmüller (2016). Marktforschung. Berlin, Boston: De Gruyter Oldenbourg;

Siddique, K., Akhtar, Z., & Kim, Y. (2017). Biometrics vs passwords: A modern version of the tortoise and the hare. Computer Fraud & Security, 2017(1), 13-17.

Sun, S.; Pospisil, E; Muslukhov, I & Nuray Dindar (2013). “A Investigating User’s Perspective of Web Single Sign-On: Conceptual Gaps, Alternative Design and Acceptance Model.” ACM Trans. On Internet Technology 13 (1), 2:1-2:35.

Taha, M. M., Alhaj, T. A., Moktar, A. E., Salim, A. H., & Abdullah, S. M. (2013): On password strength measurements: Password entropy and password quality. In 2013 Internatinal conference on computing, electrical and electronic engineering (ICCEEE) (pp. 497-501). IEEE.

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040.

Tsolkas, A., & Schmidt, K. (2017): Zugriffskontrolle über Authentifizierung, in: Rollen und Berechtigungskonzepte (pp. 129-160), Wiesbaden.

Wagner, P. & Linda Hering.(2014) "Online-Befragung." In: Handbuch Methoden der empirischen Sozialforschung. Springer VS, Wiesbaden, 661-673.

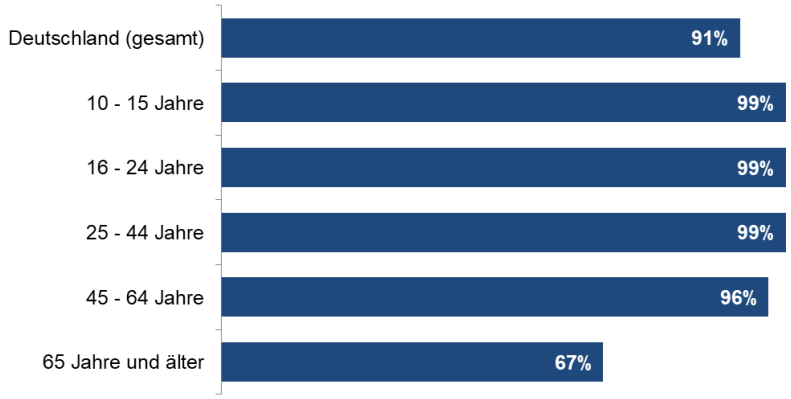
Anhang: Befragungsmethodik[30]

Die in dieser Arbeit verwendeten Primärdaten stammen aus einer im November/Dezember 2019 durchgeführten Online-Verbraucherbefragung des WIK. Anhand dieser wurde die Verwendung verschiedener Anmeldeverfahren, wie Passwort-Manager, Single-Sign-On-Lösungen, biometrische Verfahren etc., bei der Nutzung von Onlinediensten untersucht. Die Befragung wurde mit Computer Aided Web Interviewing (CAWI) erfasst. Die Stichprobengröße lag bei 3016 Befragten.

Um eine bevölkerungsrepräsentative Zusammenstellung der Stichprobe für die deutsche Bevölkerung ab 18 zu gewährleisten, wurden Quoten für Alter, Geschlecht und Region basierend auf der Verteilung der Bevölkerung in Deutschland festgelegt. Somit handelt es sich hier um eine Quotenstichprobe und keine reine Zufallsstichprobe.

Grundsätzlich decken Befragungen, die online durchgeführt werden, wie bei der CAWI-Methode, nur den Teil der Bevölkerung ab, der das Internet nutzt bzw. Zugang zu diesem hat. Dies sind die Internetnutzer. Zu den Internetnutzern zählen in Deutschland laut des Statistischen Bundesamts etwa 91% der Bevölkerung. 9% der Bevölkerung können demnach mit dieser Methode nicht erreicht werden. Vor allem unter der Altersgruppe 65+ befinden sich ein relativ hoher Anteil an Individuen, die nicht zu den Internetnutzern gehören. Die Anteile der Nutzer nach Altersgruppen sind in Abbildung A-1 zusammengefasst. Hier wird ferner ersichtlich, dass nahezu alle Personen bis 44 Jahre in Deutschland das Internet benutzen. In der Altersgruppe 45 bis 64 Jahre sind es immerhin noch 96%. Lediglich Personen älter als 65 Jahre nutzen das Internet weniger. Nur 67% von diesen nutzen es.

Abbildung A-1: Internetnutzung nach Altersgruppen (2019)

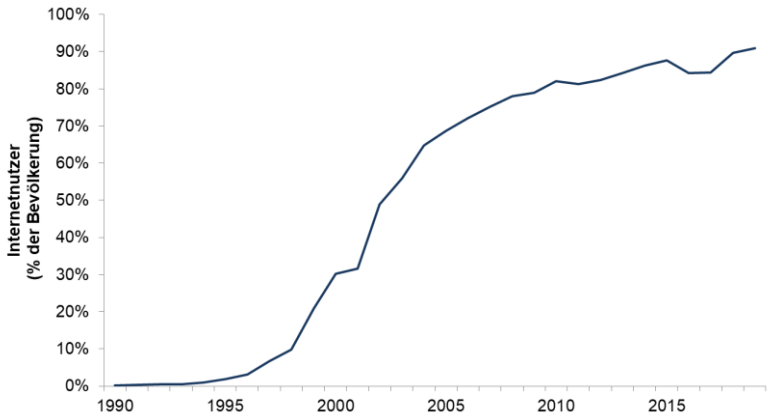


Quelle: Eigene Darstellung basierend auf Daten von Statistisches Bundesamt (Destatis) (2020).

30 Zusätzliche Information zu Befragungsmethoden finden sich bei Koch, J., Gebhardt, P., & F. Riedmüller (2016). Marktforschung. Berlin, Boston: De Gruyter Oldenbourg; Bauer, N. & J. Blasius (2019). Handbuch Methoden der empirischen Sozialforschung. VS Verlag für Sozialwissenschaften.

In unserer Online-Befragung können wir daher mit Hilfe der Quotenstichprobe die Nutzung verschiedener Anmeldeverfahren zumindest für die Altersgruppe bis 64 Jahre bevölkerungsrepräsentativ abbilden. Bei den Ergebnissen der Altersgruppe 65+ besteht die Möglichkeit, dass eine gewisse Überschätzung in den Nutzungsmustern und den Nutzeranteilen vorliegt.

Abbildung A-2: Entwicklung der Internetnutzung in Deutschland – Bevölkerungsanteil



Quelle: Eigene Darstellung; Daten stammen von der Weltbank (2020) und dem Statistischen Bundesamt (2020).

Die Verteilung der Stichprobe im Vergleich zur Verteilung der Grundgesamtheit (deutsche Bevölkerung ab 18 Jahren) ist in der nachfolgenden Tabelle zusammengefasst.

Tabelle A-1: Stichprobe und Grundgesamtheit – Verteilung

Geschlecht, Alter, Nielsengebiete		Stichprobe in der Befragung	Grundgesamtheit (deutsche Bevölkerung ab 18 Jahre)
Geschlecht	weiblich	53,7%	51,1%
	Männlich	46,3%	48,9%
Alter	18-24 Jahre	7,5%	9,0%
	25-34 Jahre	13,8%	15,2%
	35-44 Jahre	14,9%	14,7%
	45-54 Jahre	20,3%	17,2%
	55+ Jahre	43,4%	43,9%
Nielsen-gebiete	1: Bremen, Hamburg, Niedersachen, Schleswig-Holstein	16,7%	16,1%
	2: Nordrhein-Westfalen	22,4%	21,5%
	3a: Hessen. Rheinland-Pfalz, Saarland	14,3%	13,7%
	3b: Baden-Württemberg	12,2%	13,3%
	4: Bayern	13,7%	15,8%
	5: Berlin	4,4%	4,4%
	6: Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt	8,2%	7,7%
	7: Sachsen, Thüringen	8,1%	7,5%

Quelle: Eigene Darstellung basierend auf Daten von Statistisches Bundesamt (Destatis) (2020) und der Online-Umfrage des WIK (ungewichtete Werte).

Als "Diskussionsbeiträge" des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste sind zuletzt erschienen:

Nr. 385: Franz Büllingen, Annette Hillebrand, Peter Stamm:

Die Marktentwicklung für Cloud-Dienste - mögliche Anforderungen an die Netzinfrastruktur, April 2014

Nr. 386: Marcus Stronzik, Matthias Wissner:

Smart Metering Gas, März 2014

Nr. 387: René Arnold, Sebastian Tenbrock:

Bestimmungsgründe der FTTP-Nachfrage, August 2014

Nr. 388: Lorenz Nett, Stephan Jay:

Entwicklung dynamischer Marktszenarien und Wettbewerbskonstellationen zwischen Glasfasernetzen, Kupfernetzen und Kabelnetzen in Deutschland, September 2014

Nr. 389: Stephan Schmitt:

Energieeffizienz und Netzregulierung, November 2014

Nr. 390: Stephan Jay, Thomas Plückebaum:

Kostensenkungspotenziale für Glasfaseranschlussnetze durch Mitverlegung mit Stromnetzen, September 2014

Nr. 391: Peter Stamm, Franz Büllingen:

Stellenwert und Marktperspektiven öffentlicher sowie privater Funknetze im Kontext steigender Nachfrage nach nomadischer und mobiler hochbitratiger Datenübertragung, Oktober 2014

Nr. 392: Dieter Elixmann, J. Scott Marcus, Thomas Plückebaum:

IP-Netzzusammenschaltung bei NGN-basierten Sprachdiensten und die Migration zu All-IP: Ein internationaler Vergleich, November 2014

Nr. 393: Stefano Lucidi, Ulrich Stumpf:

Implikationen der Internationalisierung von Telekommunikationsnetzen und Diensten für die Nummernverwaltung, Dezember 2014

Nr. 394: Rolf Schwab:

Stand und Perspektiven von LTE in Deutschland, Dezember 2014

Nr. 395: Christian M. Bender, Alex Kalevi Dieke, Petra Junk, Antonia Niederprüm:

Produktive Effizienz von Postdienstleistern, November 2014

Nr. 396: Petra Junk, Sonja Thiele:

Methoden für Verbraucherbefragungen zur Ermittlung des Bedarfs nach Post-Universaldienst, Dezember 2014

Nr. 397: Stephan Schmitt, Matthias Wissner:

Analyse des Preissetzungsverhaltens der Netzbetreiber im Zähl- und Messwesen , März 2015

Nr. 398: Annette Hillebrand, Martin Zauner:

Qualitätsindikatoren im Brief- und Paketmarkt , Mai 2015

Nr. 399: Stephan Schmitt, Marcus Stronzik:

Die Rolle des generellen X-Faktors in verschiedenen Regulierungsregimen, Juli 2015

Nr. 400: Franz Büllingen, Solveig Börnsen:

Marktorganisation und Marktrealität von Machine-to-Machine-Kommunikation mit Blick auf Industrie 4.0 und die Vergabe von IPv6-Nummern, August 2015

Nr. 401: Lorenz Nett, Stefano Lucidi, Ulrich Stumpf:

Ein Benchmark neuer Ansätze für eine innovative Ausgestaltung von Frequenzgebühren und Implikationen für Deutschland, November 2015

Nr. 402: Christian M. Bender, Alex Kalevi Dieke, Petra Junk:

Zur Marktabgrenzung bei Kurier-, Paket- und Expressdiensten, November 2015

Nr. 403: J. Scott Marcus, Christin Gries, Christian Wernick, Imme Philbeck:

Entwicklungen im internationalen Mobile Roaming unter besonderer Berücksichtigung struktureller Lösungen, Januar 2016

Nr. 404: Karl-Heinz Neumann. Stephan Schmitt, Rolf Schwab unter Mitarbeit von Marcus Stronzik:

Die Bedeutung von TAL-Preisen für den Aufbau von NGA, März 2016

Nr. 405: Caroline Held, Gabriele Kulenkampff, Thomas Plückebaum:

Entgelte für den Netzzugang zu staatlich geförderter Breitband-Infrastruktur, März 2016

Nr. 406: Stephan Schmitt, Matthias Wissner:

Kapazitätsmechanismen – Internationale Erfahrungen, April 2016

Nr. 407: Annette Hillebrand, Petra Junk:

Paketshops im Wettbewerb, April 2016

Nr. 408: Tseveen Gantumur, Iris Henseler-Unger, Karl-Heinz Neumann:

Wohlfahrtsökonomische Effekte einer Pure LRIC - Regulierung von Terminierungsentgelten, Mai 2016

Nr. 409: René Arnold, Christian Hildebrandt, Martin Waldburger:

Der Markt für Over-The-Top Dienste in Deutschland, Juni 2016

Nr. 410: Christian Hildebrandt, Lorenz Nett:

Die Marktanalyse im Kontext von mehrseitigen Online-Plattformen, Juni 2016

Nr. 411: Tseveen Gantumur, Ulrich Stumpf:

NGA-Infrastrukturen, Märkte und Regulierungsregime in ausgewählten Ländern, Juni 2016

Nr. 412: Alex Dieke, Antonia Niederprüm, Sonja Thiele:

UPU-Endvergütungen und internationaler E-Commerce, September 2016
(in deutscher und englischer Sprache verfügbar)

Nr. 413: Sebastian Tenbrock, René Arnold:

Die Bedeutung von Telekommunikation in intelligent vernetzten PKW, Oktober 2016

Nr. 414: Christian Hildebrandt, René Arnold:

Big Data und OTT-Geschäftsmodelle sowie daraus resultierende Wettbewerbsprobleme und Herausforderungen bei Datenschutz und Verbraucherschutz, November 2016

Nr. 415: J. Scott Marcus, Christian Wernick:

Ansätze zur Messung der Performance im Best-Effort-Internet, November 2016

Nr. 416: Lorenz Nett, Christian Hildebrandt:

Marktabgrenzung und Marktmacht bei OTT-0 und OTT-1-Diensten, Eine Projektskizze am Beispiel von Instant-Messenger-Diensten, Januar 2017

Nr. 417: Peter Kroon:

Maßnahmen zur Verhinderung von Preis-Kosten-Scheren für NGA-basierte Dienste, Juni 2017

Nr. 419: Stefano Lucidi:

Analyse marktstruktureller Kriterien und Diskussion regulatorischer Handlungsoptionen bei engen Oligopolen, April 2017

Nr. 420: J. Scott Marcus, Christian Wernick, Tseveen Gantumur, Christin Gries:

Ökonomische Chancen und Risiken einer weitreichenden Harmonisierung und Zentralisierung der TK-Regulierung in Europa, Juni 2017

Nr. 421: Lorenz Nett:

Incentive Auctions als ein neues Instrument des Frequenzmanagements, Juli 2017

Nr. 422: Christin Gries, Christian Wernick:

Bedeutung der embedded SIM (eSIM) für Wettbewerb und Verbraucher im Mobilfunkmarkt, August 2017

Nr. 423: Fabian Queder, Nicole Angenendt, Christian Wernick:

Bedeutung und Entwicklungsperspektiven von öffentlichen WLAN-Netzen in Deutschland, Dezember 2017

Nr. 424: Stefano Lucidi, Bernd Sörries, Sonja Thiele:

Wirksamkeit sektorspezifischer Verbraucherschutzregelungen in Deutschland, Januar 2018

Nr. 425: Bernd Sörries, Lorenz Nett:

Frequenzpolitische Herausforderungen durch das Internet der Dinge - künftiger Frequenzbedarf durch M2M-Kommunikation und frequenzpolitische Handlungsempfehlungen, März 2018

Nr. 426: Saskja Schäfer, Gabriele Kulenkampff, Thomas Plückebaum unter Mitarbeit von Stephan Schmitt:

Zugang zu gebäudeinterner Infrastruktur und adäquate Bepreisung, April 2018

Nr. 427: Christian Hildebrandt, René Arnold:

Marktbeobachtung in der digitalen Wirtschaft – Ein Modell zur Analyse von Online-Plattformen, Mai 2018

Nr. 428: Christin Gries, Christian Wernick:

Treiber und Hemmnisse für kommerziell verhandelten Zugang zu alternativen FTTB/H-Netzinfrastrukturen, Juli 2018

Nr. 429: Serpil Taş, René Arnold:

Breitbandinfrastrukturen und die künftige Nutzung von audiovisuellen Inhalten in Deutschland: Herausforderungen für Kapazitätsmanagement und Netzneutralität, August 2018

Nr. 430: Sebastian Tenbrock, Sonia Strube Martins, Christian Wernick, Fabian Queder, Iris Henseler-Unger:

Co-Invest Modelle zum Aufbau von neuen FTTB/H-Netzinfrastrukturen, August 2018

Nr. 431: Johanna Bott, Christian Hildebrandt, René Arnold:

Die Nutzung von Daten durch OTT-Dienste zur Abschöpfung von Aufmerksamkeit und Zahlungsbereitschaft: Implikationen für Daten- und Verbraucherschutz, Oktober 2018

Nr. 432: Petra Junk, Antonia Niederprüm:

Warenversand im Briefnetz, Oktober 2018

Nr. 433: Christian M. Bender, Annette Hillebrand:

Auswirkungen der Digitalisierung auf die Zustelllogistik, Oktober 2018

Nr. 434: Antonia Niederprüm:

Hybridpost in Deutschland, Oktober 2018

Nr. 436: Petra Junk:

Digitalisierung und Briefsubstitution: Erfahrungen in Europa und Schlussfolgerungen für Deutschland, Oktober 2018

Nr. 437: Peter Kroon, René Arnold:

Die Bedeutung von Interoperabilität in der digitalen Welt – Neue Herausforderungen in der interpersonellen Kommunikation, Dezember 2018

Nr. 438: Stefano Lucidi, Bernd Sörries:

Auswirkung von Bündelprodukten auf den Wettbewerb, März 2019

Nr. 439: Christian M. Bender, Sonja Thiele:

Der deutsche Postmarkt als Infrastruktur für europäischen E-Commerce, April 2019

Nr. 440: Serpil Taş, René Arnold:

Auswirkungen von OTT-1-Diensten auf das Kommunikationsverhalten – Eine nachfrageseitige Betrachtung, Juni 2019

Nr. 441: Serpil Taş, Christian Hildebrandt, René Arnold:

Sprachassistenten in Deutschland, Juni 2019

Nr. 442: Fabian Queder, Marcus Stronzik, Christian Wernick:

Auswirkungen des Infrastrukturwettbewerbs durch HFC-Netze auf Investitionen in FTTP-Infrastrukturen in Europa, Juni 2019

Nr. 443: Lorenz Nett, Bernd Sörries:

Infrastruktur-Sharing und 5G: Anforderungen an Regulierung, neue wettbewerbliche Konstellationen, Juli 2019

Nr. 444: Pirmin Puhl, Martin Lundborg:

Breitbandzugang über Satellit in Deutschland – Stand der Marktentwicklung und Entwicklungsperspektiven, Juli 2019

Nr. 445: Bernd Sörries, Marcus Stronzik, Sebastian Tenbrock, Christian Wernick, Matthias Wissner:

Die ökonomische Relevanz und Entwicklungsperspektiven von Blockchain: Analysen für den Telekommunikations- und Energiemarkt, August 2019

Nr. 446: Petra Junk, Julia Wielgosch:

City-Logistik für den Paketmarkt, August 2019

Nr. 447: Marcus Stronzik, Matthias Wissner:

Entwicklung des Effizienzvergleichs in Richtung Smart Grids, September 2019

Nr. 448: Christian M. Bender, Antonia Niederprüm:

Berichts- und Anzeigepflichten der Unternehmen und mögliche Weiterentwicklungen der zugrundeliegenden Rechtsnormen im Postbereich, September 2019

Nr. 449: Ahmed Elbanna unter Mitwirkung von Fabian Eltges:

5G Status Studie: Herausforderungen, Standardisierung, Netzarchitektur und geplante Netzentwicklung, Oktober 2019

Nr. 450: Stefano Lucidi, Bernd Sörries:

Internationale Vergleichsstudie bezüglich der Anwendung und Umsetzung des Nachbildbarkeitsansatzes, Dezember 2019

Nr. 451: Matthias Franken, Matthias Wissner, Bernd Sörries:

Entwicklung der funkbasierten Digitalisierung in der Industrie, Energiewirtschaft und Landwirtschaft und spezifische Frequenzbedarfe, Dezember 2019

Nr. 452: Bernd Sörries, Lorenz Nett:

Frequenzmanagement: Lokale/regionale Anwendungsfälle bei 5G für bundesweite Mobilfunknetzbetreiber sowie für regionale und lokale Betreiber unter besonderer Betrachtung der europäischen Länder sowie von China, Südkorea und den Vereinigten Staaten von Amerika, Dezember 2019

Nr. 453: Martin Lundborg, Christian Märkel, Lisa Schrade-Grytsenko, Peter Stamm:

Künstliche Intelligenz im Telekommunikationssektor – Bedeutung, Entwicklungsperspektiven und regulatorische Implikationen, Dezember 2019

Nr. 454: Fabian Eltges, Petra Junk:

Entwicklungstrends im Markt für Zeitungen und Zeitschriften, Dezember 2019

Nr. 455: Christin Gries, Julian Knips, Christian Wernick:

Mobilfunkgestützte M2M-Kommunikation in Deutschland – zukünftige Marktentwicklung und Nummerierungsbedarf, Dezember 2019

Nr. 456: Menessa Ricarda Braun, Christian Wernick, Thomas Plückebaum, Martin Ockenfels:

Parallele Glasfaserausbauten auf Basis von Mitverlegung und Mitnutzung gemäß DigiNetzG als Möglichkeiten zur Schaffung von Infrastrukturwettbewerb, Dezember 2019

Nr. 457: Thomas Plückebaum, Martin Ockenfels:

Kosten und andere Hemmnisse der Migration von Kupfer- auf Glasfasernetze, Februar 2020

Nr. 458: Andrea Liebe, Jonathan Lennartz, René Arnold:

Strategische Ausrichtung bedeutender Anbieter von Internetplattformen, Februar 2020

Nr. 459: Sebastian Tenbrock, Julian Knips, Christian Wernick:

Status quo der Abschaltung der Kupfernetzinfrastruktur in der EU, März 2020

Nr. 460: Stefano Lucidi, Martin Ockenfels, Bernd Sörries:

Anhaltspunkte für die Replizierbarkeit von NGA-Anschlüssen im Rahmen des Art. 61 Abs. 3 EKEK, März 2020

Nr. 461: Fabian Eltges, Gabriele Kulenkampff, Thomas Plückebaum, Desislava Sabeva:

SDN/NFV und ihre Auswirkungen auf die Kosten von Mobilfunk und Festnetz im regulatorischen Kontext, März 2020

Nr. 462: Lukas Wiewiorra, Andrea Liebe, Serpil Taş

Die wettbewerbliche Bedeutung von Single-Sign-On- bzw. Login-Diensten und ihre Relevanz für datenbasierte Geschäftsmodelle sowie den Datenschutz, Juni 2020

ISSN 1865-8997