Kurzstudie, Juli 2021

Durchblick im Passwortdschungel?

Digitale Benutzerauthentifizierung

Serpil Taş
Dr. Lukas Wiewiorra
Prof. Dr. Anna Schneider

HOCHSCHULE FRESENIUS
UNIVERSITY OF APPLIED SCIENCES

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

Impressum

Autorinnen und Autor der Studie:

Serpil Taş
Senior Economist | Märkte & Perspektiven
Kontakt: *s.tas@wik.org*
+49 (0)2224 92 25 96

Prof. Dr. Anna Schneider
Professorin für Wirtschaftspsychologie
Kontakt: *anna.schneider@hs-fresenius.de*
+49 (0)221 97 31 99 715

Dr. Lukas Wiewiorra
Abteilungsleiter | Märkte & Perspektiven
Kontakt: *l.wiewiorra@wik.org*
+49 (0)2224 92 25 25

Kontaktdaten der Forschungsinstitute:

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68, 53604 Bad Honnef
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
eMail: info(at)wik.org
www.wik.org

Hochschule Fresenius – Fachbereich Wirtschaft & Medien
Business School · Media School · Psychology School
Im Mediapark 4c, 50670 Köln
www.hs-fresenius.de

Geschäftsführerin und Direktorin: Dr. Cara Schwarz-Schiling
Vorsitzende des Aufsichtsrates: Dr. Daniela Brönstrup
Handelsregister: Amtsgericht Siegburg, HRB 7225
Steuer Nr.: 222/5751/0722
Umsatzsteueridentifikations Nr.: DE 123 383 795

Geschäftsführer: Prof. Dr. Tobias Engelsleben, Sascha Kappes, Kai Metzner
Handelsregister: Amtsgericht Wiesbaden HRB 19044

Bildnachweis: Titel: claudio-schwarz-purzlbaum - unsplash; S. 4: mohamed Hassan - Pixabay; S. 6/7: Surface - unsplash; S. 8: mindspace-studio - unsplash; S. 10/11: Alexander Shatov - unsplash; S. 12: Thomas Ulrich – Pixabay; S. 15/16: jessie koranteng - unsplash; S. 16 (Fingerabdruck): OpenClipart-Vectors - pixabay; S. 2-15: sabelskay - AdobeStock

Gestaltung und Layout: Karin Wagner (WIK)

Vorwort

Sicherheit steht nicht für alle Nutzer im Vordergrund

Internetnutzer sind heutzutage mit einer Vielzahl unterschiedlicher Formen der Benutzeranmeldung im Internet konfrontiert. Für immer mehr Dienste ist eine individuelle Registrierung erforderlich, während gleichzeitig die Anzahl der genutzten Dienste stetig ansteigt. All diese Anmeldedaten zu verwalten und dabei den Durchblick im Passwortdschungel zu behalten, stellt eine wachsende Herausforderung dar.

In dieser Studie hat WIK sich intensiv mit verschiedenen Anmeldeverfahren und technischen Lösungen sowie deren Nutzung und wahrgenommenen Vor- und Nachteilen beschäftigt. Die Ergebnisse zeigen, dass Internetnutzer in Deutschland häufig noch auf die klassischen Anmeldeverfahren zurückgreifen, obwohl sie bereits eine sehr hohe Anzahl verschiedener anmeldepflichtiger Dienste nutzen.

Insbesondere Single Sign-on Dienste, welche die Vielzahl unterschiedlicher Kombinationen aus Passwort und Benutzernamen oder z.B. E-Mail-Adresse vereinheitlichen können, werden noch von relativ wenigen Verbrauchern verwendet. Gerade dieses Segment wird allerdings von großen Plattformanbietern wie Facebook und Google dominiert, die mit diesen Diensten ihre Ökosysteme erweitern. Diese Anbieter nutzen ihre starke Position und die damit verbundene Nutzerbasis, um Webseitenbetreibern und Diensteanbietern eine einfache Anmeldefunktion bereitzustellen. Durch diese Funktion können sie allerdings ebenfalls weitere Einblicke in das Verhalten ihrer Nutzer über die Grenzen ihrer eigenen Dienste hinweg gewinnen und dadurch ihre Werbeprofile weiter schärfen.

Auch andere verbreitete Lösungen wie Passwort-Manager und biometrische Authentifizierungsverfahren haben ihre Nachteile, bergen aber nicht die unmittelbare Gefahr, dass das individuelle Nutzungsverhalten über Dienstgrenzen hinweg verfolgt werden kann.

Dr. Cara Schwarz-Schilling

Zwischen Passwort und Fingerabdruck

Wenn Konsumenten digitale Dienste nutzen wollen, stehen sie häufig vor der Frage, wie sie sich authentifizieren möchten: Soll es „klassisch“ sein, beispielsweise mit ihrer E-Mail-Adresse und einem individuellen Passwort? Oder lieber mittels „Single Sign-on Lösungen“ von Dritten oder sozialen Netzwerken? Auch Passwort-Manager oder biometrische Merkmale, wie der Fingerabdruck, können die Anmeldung bei unterschiedlichen Diensten erleichtern. Unsere Daten zeigen: Aktuell ist (noch) die klassische Variante am verbreitetsten.

Sicherheitsexperten empfehlen, für jedes Nutzerkonto ein eigenes und eindeutiges Passwort zu verwenden, um im Fall eines Datenverlusts nicht mehrere Nutzerkonten zu gefährden. Dennoch neigen Verbraucher nicht nur dazu, einfachere und damit unsichere Passwörter zu vergeben, sondern auch für verschiedene Dienste ähnliche oder gar dieselben Passwörter zu verwenden.

Einleitung

Internetnutzer melden sich nahezu täglich bei unterschiedlichsten digitalen Diensten an, die das Anlegen eines Nutzerkontos voraussetzen – seien es Musik- oder Videostreaming-Dienste, Marktplätze, soziale Netzwerke oder andere. Mit der steigenden Anzahl an verwendeten Services steigt auch die Herausforderung, sämtliche Konten und die entsprechenden Anmeldedaten adäquat zu verwalten.

Obwohl etwa 50% der Internetnutzer angeben, ihre Passwörter zumindest gelegentlich zu vergessen, versuchen dennoch die meisten, ihre Passwörter im Gedächtnis zu behalten. Alternativ stehen Nutzern zwei grundlegende Optionen zur Verfügung: Sie können Lösungen verwenden, mit denen die Vielzahl an Anmeldedaten einfacher verwaltet werden kann, oder aber alternativ Lösungen verwenden, bei denen die Anzahl verschiedener Anmeldedaten reduziert wird.

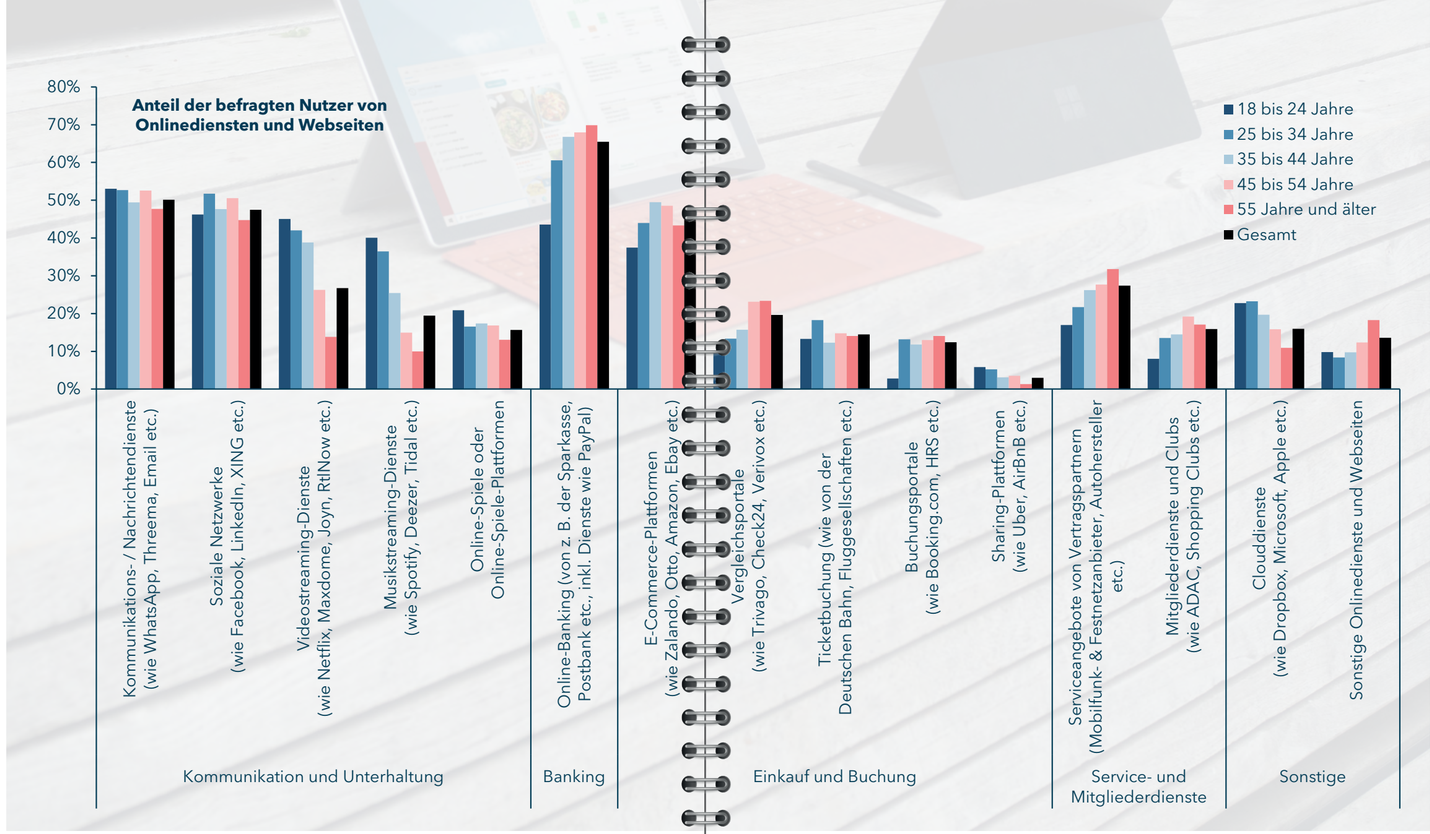
Doch welche Authentifizierungsverfahren und Lösungen verwenden Internetnutzer und welche sind für sie weniger relevant? Um diese Frage zu beantworten, kombiniert die vorliegende Studie Ergebnisse aus einer quantitativen, repräsentativen Umfrage mit mehr als 3.000 Teilnehmern in Deutschland mit den Ergebnissen einer tiefgreifenden qualitativen Erhebung mit 12 Konsumenten.

Der Log-in Alltag

Internetnutzer verwenden heutzutage eine Vielzahl an unterschiedlichen digitalen Diensten und täglich kommen neue hinzu.

Laut unserer Befragung nutzen etwa 48% der Internetnutzer in Deutschland wöchentlich 4 – 12 Dienste. 12% der Befragten verwenden wöchentlich sogar bis zu 30 Dienste aus unterschiedlichen Bereichen.

Digitale Dienste, in den Kategorien Kommunikation und Unterhaltung, verzeichnen die höchste Anzahl an Nutzern. Hierzu zählen soziale Netzwerke, Kommunikationsdienste wie E-Mail, WhatsApp oder Threema, aber auch Streaming-Dienste für Musik oder Video sowie Online-Spiele.



Die Daten basieren auf der jährlichen Online-Befragung des WIK. Daten im Text: N=3016. Daten für die Abbildung: N=2344. Auswertung ohne Berücksichtigung fehlender Antworten („keine Angabe"/"weiß nicht").

Auch Online-Banking, Einkaufs- und Buchungsdienste oder Service- und Mitgliederdienste werden von vielen Internetnutzern verwendet. Im Gegensatz zu den Kategorien Kommunikation und Unterhaltung werden Dienste in diesen Kategorien von jungen Internetnutzern allerdings weniger stark genutzt als von Internetnutzern höherer Altersgruppen.

Für viele der verwendeten digitalen Dienste ist das Anlegen eines Nutzerkontos Grundvoraussetzung, um diese in vollem Umfang nutzen zu können.

42% der Internetnutzer nutzen nahezu täglich digitale Dienste, für die ein Log-in erforderlich ist.

So sind Log-ins zwar mittlerweile ein alltäglicher Vorgang, betreffen aber nicht alle Internetnutzer gleichermaßen und in der selben Intensität.

Gängig, aber kompliziert

Die gängigste und am häufigsten verwendete Methode der Authentifizierung ist eine Kombination aus einem Benutzernamen oder einer E-Mail-Adresse und einem Passwort bzw. einer PIN.

Etwa 86% der Internetnutzer in Deutschland greifen auf diese Methode zurück. Dieser Weg wird jedoch mit steigender Anzahl unterschiedlicher Dienste zunehmend kompliziert, falls Nutzer für jeden der Dienste unterschiedliche Zugangsdaten verwenden und diese sogar regelmäßig ändern.

Die Daten basieren auf der jährlichen Online-Befragung des WIK: N=2287.
Auswertung ohne Berücksichtigung fehlender Antworten („keine Angabe"/"weiß nicht").

Einfach, aber unüblich

Technische Lösungen wie Passwortmanager und Single Sign-on Dienste können Nutzer dabei unterstützen, der Passwortflut zu begegnen und damit auch das Sicherheitsrisiko reduzieren, welches durch den Einsatz identischer Passwörter für unterschiedliche Dienste entsteht.

Passwort-Manger erlauben dabei eine komfortable Verwaltung und zentrale Speicherung der zahlreichen Anmeldedaten.

Single Sign-on Lösungen ersetzen unterschiedliche individuelle Log-ins durch einen zentralen Anmeldedienst und sind damit darauf ausgelegt, die Anzahl verschiedener Anmeldedaten zu reduzieren.

Mindestens eine dieser beiden Lösungen, wird aktuell jedoch nur von **32%** der Befragten verwendet.

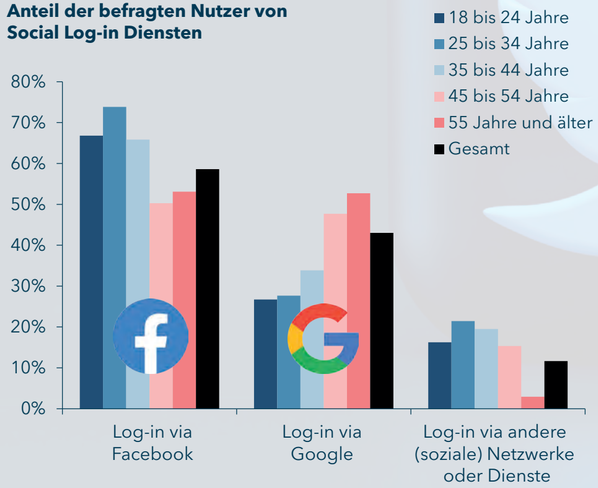
Die Daten basieren auf der jährlichen Online-Befragung des WIK: N=2287.
Auswertung ohne Berücksichtigung fehlender Antworten („keine Angabe"/"weiß nicht").
Quelle der Abbildung: https://www.tuv.com/germany/de/authentifizierung.html

Der Social Log-in

Am vergleichsweise häufigsten werden die Single Sign-on Dienste der digitalen Plattformprovider (Social Log-ins) genutzt. Insbesondere Nutzer, die Wert auf eine Vereinfachung des Anmeldeprozesses und eine komfortable Nutzung legen, betrachten diese Möglichkeit als vorteilhaft.

Insgesamt betrachtet, ist die Nutzung von Social Log-ins in Deutschland noch vergleichsweise wenig gefragt. Nur **etwa 13%** der Internetnutzer nutzen Social Log-ins. Hierbei hält Facebook den größten Marktanteil an den bestehenden Social Log-in Lösungen, gefolgt von Google, LinkedIn, Yahoo, Twitter und anderen.

Anteil der befragten Nutzer von Social Log-in Diensten



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	Contacs
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	

Pro und Contra

Aus Sicht der Anbieter ist die Installation von Social Log-ins auf der eigenen Website vorteilhaft. Von der Implementierung von Social Log-ins versprechen sich die Diensteanbieter vor allem eine höhere Konversion von Besuchern zu registrierten Kunden.

Zudem können bestimmte Attribute und Informationen des bei dem sozialen Netzwerk hinterlegten Benutzerprofils vom Diensteanbieter einfach übernommen werden. Dadurch vereinfacht sich der Anmelde- und Registrierungsprozess für neue Dienste drastisch und damit die Einstiegshürde für neue Nutzer.

Gleichzeitig bedeutet dies jedoch, dass das Verhalten der Nutzer über die Grenzen einzelner Dienste hinweg verfolgt werden kann und Daten aus unterschiedlichen Quellen miteinander kombiniert werden können.

Die Daten basieren auf der jährlichen Online-Befragung des WIK. Daten im Text: N=2287. Daten in der Abbildung: N=304. Auswertung ohne Berücksichtigung fehlender Antworten („keine Angabe"/"weiß nicht").

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

Sicherheit & Zuverlässigkeit oder Komfort?

Die wenigsten der Internetnutzer, die einen stärkeren Fokus auf Sicherheit im Vergleich zu Aspekten wie Schnelligkeit oder Einfachheit legen, verwenden einen Social Log-in.

Insbesondere Zweifel an der Sicherheit dieser Verfahren, aber auch Datenschutzbedenken werden vielfach geäußert. Ein weiterer wesentlicher Faktor ist das geringe Vertrauen in die Social Log-in Anbieter, wie Facebook oder Google.

Nutzer von Social Log-ins sind von dem Komfort der Lösung überzeugt. Die Anmeldung und Registrierung bei digitalen Diensten ist durch den Social Log-in in der Regel bequemer, einfacher und schneller und macht das Merken neuer Passwörter obsolet.

„Also da ist die Frage wie seriös die dann mit deinen Daten umgehen. Weil die ja jetzt theoretisch deinen Facebook Log-in haben." (Willi, 19)

„Man hat ja das Gefühl, man spinnt so ein Spinnennetz an Informationen. Und irgendwie fühlt es sich für mich nicht so an, als würde ich das wollen." (Nils, 23)

„Man denkt nicht groß drüber nach, sondern geht halt einfach den (…) Weg des geringsten Widerstandes und geht dann halt einfach auf Facebook, weil es ja für einen selber auch angenehmer ist, weil es schneller geht." (Anna, 25)

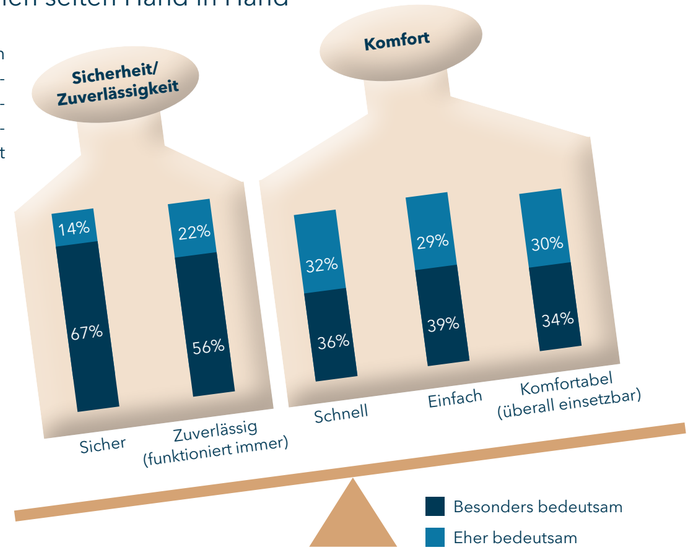
„Weil des Öfteren schon in der Öffentlichkeit bekannt wurde, dass Facebook die Daten auch an Drittanbieter weitergibt." (Maximilian, 30)

„Weil das halt, viel, viel einfacher ist sich zu registrieren. Weil ich mir dann halt nicht die Mühe geben muss, meinen Namen mit Nachnamen zu schreiben. Das geht dann halt ganz schnell damit." (Sinem, 23)

Sicherheit und Komfort gehen selten Hand in Hand

Zusätzliche Sicherheit geht oft zu Lasten der Usability und erhöht die Komplexität für Anwender, während sehr komfortable Systeme meist Kompromissbereitschaft der Nutzer bei der Sicherheit voraussetzen.

Obwohl Internetnutzer den Aspekten „Sicherheit" und „Zuverlässigkeit" mehr Bedeutung zumessen als den Aspekten „Schnelligkeit", „Einfachheit" und „Komfort", sind auch diese jeweils für mehr als 60% der Internutzer wichtige Eigenschaften von Authentifizierungssystemen.



Die Daten basieren auf der jährlichen Online-Befragung des WIK. N=3016.
Auswertung ohne Berücksichtigung fehlender Antworten („keine Angabe"/"weiß nicht").

Konvergenz

„Also ich versuche das (Anm.: die personenbezogenen Angaben) dann schon immer irgendwie so ein bisschen zu verändern, wenn das denn geht (...). Auch was das Alter angeht (…) man wischt ja manchmal nur. Da mache ich dann einfach irgendwann Stopp." (Katharina, 23)

„Also Facebook nutze ich aktiv eigentlich gar nicht. Alleine schon, weil ich da viele Arbeitskollegen habe und ich glaube, da ist dann die Hemmung schon etwas mehr, dass man da einen seriösen Eindruck machen möchte. Also ich würde sagen, mein Account ist da cleaner. Da teile ich nichts, da poste ich nichts. Instagram ist dann doch etwas persönlicher. Da gebe ich schon meine Meinung von mir, weil ich dann schon einen gewissen Überblick habe, wer die Dinge sieht, die ich poste." (Eva, 23)

Digitale Identitäten, die bei verschiedenen internetbasierten Diensten hinterlassen werden, entsprechen nicht zwangsläufig der realen Identität der Nutzer. 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. Dies kann der Fall sein, wenn Anonymität gewünscht ist, oder wenn Bedenken bestehen, dass die digitale Identität bzw. die hier angegebenen Informationen missbraucht werden könnten. Abhängig vom Anwendungsfeld präsentieren Nutzer also verschiedene Facetten ihrer Identität, während andere eher verschleiert werden.

Jedoch kann die Bündelung von verschiedenen digitalen Identitäten ein Bild schaffen, das der realen Identität näher kommt. Auch neue biometrische Verfahren werden mitunter sehr kritisch diskutiert, da diese eine eindeutige Identifikation der Nutzer ermöglichen und so einen Rückschluss auf die reale Identität erlauben.

Biometrische Authentifizierungsverfahren

Nutzer einiger Endgeräte können alternativ auch biometrische Merkmale wie ihren Fingerabdruck oder aber auch ihr Gesicht zur Authentifizierung nutzen. Die Authentifizierung über biometrische Merkmale ist dabei **etwa 80%** der Internetnutzer in unserer Befragung bekannt.

Aktiv verwendet werden die Verfahren jedoch lediglich von **46%** der Befragten. Dabei handelt es sich vor allem um die Authentifizierung über den Fingerabdruck (41%) und die Gesichtserkennung (16%). Als ein Treiber dieser Entwicklung zählt vor allem die Verbreitung biometrischer Authentifizierungsverfahren in modernen Endgeräten, wie dem Smartphone.

Während bei vielen neuen Technologien oder Diensten vor allem jüngere Konsumenten Vorreiter bei der Nutzung sind, gilt dies hier nicht. Vor allem Konsumenten in den höheren Altersgruppen scheinen von diesen Verfahren Gebrauch zu machen.

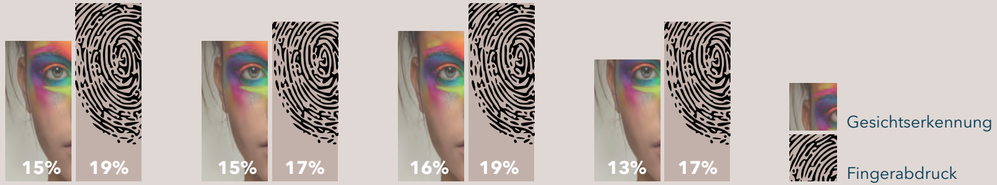
Die Daten basieren auf der jährlichen Online-Befragung des WIK. N=3016.
Auswertung ohne Berücksichtigung fehlender Antworten („keine Angabe"/"weiß nicht").

Heute und Morgen

Die Verbraucher nutzen biometrische Verfahren wie die Gesichtserkennung und den Fingerabdruck hauptsächlich zur Entsperrung von Endgeräten wie Computern, Laptops oder Smartphones. Aber auch die Nutzung einiger Apps, oder die Anmeldung beim Online-Banking ist Anlass für die Verwendung biometrischer Verfahren zur Authentifizierung.

Zukünftig können sich Konsumenten vorstellen, auch im Kontext des Zugangs zu medizinischen Information, für den Austausch mit Behörden und im Smart-Home-Bereich ihr Gesicht oder den Finger zu Authentifizierung zu nutzen.

Mögliche zukünftige Anwendungsfälle aus Sicht der Konsumenten[1]



Zum Abwickeln von Bankgeschäften im Online-Banking

Für den Zugang zu medizinischen Informationen

Im Austausch mit öffentlichen Behörden

Zum Öffnen der Haus-/Garagentür bzw. des Autos

Die Daten basieren auf der jährlichen Online-Befragung des WIK: N=3016.
Auswertung ohne Berücksichtigung fehlender Antworten („keine Angabe"/"weiß nicht").
1 Basis: Befragte, denen biometrische Authentifizierungsverfahren bekannt sind.

Ausblick

Obwohl Single Sign-on Lösungen die Handhabung von Log-in Daten durchaus vereinfachen und die Anmeldung auf digitalen Plattformen komfortabler gestalten, halten sich die Verbraucher bei der Nutzung zurück. Vor allem gegenüber Social Log-ins äußern Verbraucher Bedenken bezüglich der Sicherheit und Zuverlässigkeit der Systeme. Darüber hinaus ist der Gedanke durch die Verwendung von Social Log-ins den großen Plattformbetreibern weitere Daten über sich selbst zur Verfügung zu stellen, ein häufig genannter Grund die die Nutzung abzulehnen. Auch aus Sicht der Betreiber von Webseiten und digitalen Diensten sind Social Log-ins ein zweischneidiges Schwert. Auf der einen Seite ermöglichen diese den Nutzern eine einfachere und schnellere Anmeldung und den Betreibern Zugriff auf bestehende Nutzerinformationen. Auf der anderen Seite können die weitreichende Einbindung in die Ökosysteme großer Plattformanbieter und die darüber erfassbaren Informationen den Plattformanbietern in die Hände spielen und zu einem Wettbewerbsvorteil auf dem Werbemarkt gegenüber den Betreibern der eingebundenen Webseiten und Diensten führen.

Im Gegensatz dazu scheint die Nutzung von biometrischen Merkmalen zur Authentifizierung vergleichsweise stärkeren Zuspruch in Deutschland zu finden. Bisher werden biometrische Merkmale wie die Gesichtsgeometrie oder der Fingerabdruck hauptsächlich für das Entsperren von digitalen Endgeräten verwendet, doch für die Zukunft können sich Verbraucher vorstellen, biometrische Merkmale auch in anderen Anwendungsfeldern zu nutzen.

Daher wird derzeit die Implementierung von biometrischen Authentifizierungsverfahren in weiteren Bereichen vorangetrieben. Anfang des Jahres stellte beispielsweise Flywallet das Produkt „Keyble" vor, ein Wearable Device mit biometrischen Authentifizierungsfunktionen, mit dem Nutzer kontaktlose Zahlungen vornehmen und digitale Tickets, Zugangskarten, Schlüssel und Signaturen verwalten und verwenden können.[1] Darüber hinaus hat Amazon im vergangen Herbst damit begonnen in seinen stationären Filialen „Amazon One" auszurollen. Amazon One ist ein Dienst, welcher es Kunden in den Amazon Go Stores ermöglicht nur mit ihrer Handfläche Zahlungen zu autorisieren. Das Amazon One-System erstellt dazu einen Scan des Handabdrucks, welcher verschlüsselt in der Cloud gespeichert und mit einer hinterlegten Kreditkarte verknüpft wird.[2] Daher wurde die Umsetzung von Amazon One, welche im Gegensatz zu der Implementierung von Apple auf einer Verarbeitung der biometrischen Informationen in der Cloud basiert, von Datenschutzexperten kritisiert.[3] Dabei ist insbesondere die Tatsache zu berücksichtigen, dass die biometrischen Merkmale eines Nutzer einmalig und unveränderlich sind und daher im Gegensatz zu einem kompromittierten Passwort nicht einfach geändert werden können.

1 Siehe hierzu https://www.techradar.com & https://www.flywalletpay.com. Ein anderes Beispiel ist auch das Armband von Deed, welches Nutzer via Gestenerkennung identifizieren kann. (siehe https://www.infineon.com)
2 Siehe https://techcrunch.com.
3 https://mashable.com.

Über die Studie:
Für die Ergebnisse wurden insgesamt 3.016 Personen Ende 2019 mittels Online-Befragung durch das internationale Marktforschungsinstitut YouGov befragt. Die Ergebnisse wurden gewichtet und sind repräsentativ für die deutsche Bevölkerung (Alter 18+). Zusätzlich wurden insgesamt 12 qualitative Interviews in den Monaten November und Dezember 2020 geführt. Die vollständigen Ergebnisse der Befragung sind im WIK-Diskussionsbeitrag Nr. 462 veröffentlicht, der unter www.wik.org elektronisch verfügbar ist.

Über das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK):
Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) in Bad Honnef berät seit mehr als 30 Jahren öffentliche und private Auftraggeber weltweit in den Bereichen Telekommunikation, Internet, Post und Energie. Zu den Schwerpunktthemen gehören Politik, Regulierung und Strategie. Weitere Informationen finden Sie unter: www.wik.org.

Über die Hochschule Fresenius:
Die Hochschule Fresenius gehört mit mehr als 17.000 Studierenden und Schülern sowie nationalen und internationalen Standorten zu den größten und renommiertesten Hochschulen in privater Trägerschaft in Deutschland. Praxisnahe, innovative und zugleich auf die Anforderungen des Arbeitsmarktes ausgerichtete Studien- und Ausbildungsinhalte, kleine Studiengruppen und namhafte Kooperationspartner sind nur einige der vielen Vorteile der Hochschule Fresenius. Mit ihrem Stammhaus in Idstein bei Wiesbaden blickt die Hochschule Fresenius auf eine mehr als 170-jährige Tradition zurück.
Weitere Informationen finden Sie unter: www.hs-fresenius.de.

HOCHSCHULE FRESENIUS
UNIVERSITY OF APPLIED SCIENCES

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste