Nutzung von Biometrie in der 2-Faktor-Authentisierung (2FA)

Ergebnisse einer Untersuchung des BSI und des vzbv

Bundesamt
für Sicherheit in der
Informationstechnik

verbraucherzentrale
Bundesverband

Inhaltsverzeichnis

1. Management Summery

Mit der 2-Faktor-Authentisierung (2FA) können Nutzerkonten im Internet einfach und effektiv geschützt werden. Dieses Verfahren mittels mehrerer Faktoren, mit denen die Nutzerin oder der Nutzer sich zusätzlich bzw. alternativ zur Passworteingabe identifizieren können, ist ein wichtiger Baustein für den Digitalen Verbraucherschutz. Im März 2022 veröffentlichten das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Verbraucherzentrale Bundesverband (vzbv) die Ergebnisse einer gemeinsamen Untersuchung zum Stand der 2FA in Deutschland.

Ein umfangreicher Markcheck zeigte, dass 72 Prozent der untersuchten Anbieter digitaler Dienstleistungen eine 2FA anboten.[1] Gleichzeitig ergab eine repräsentative Online-Befragung, dass bei Verbraucherinnen und Verbrauchern ein hohes Schutzbedürfnis vorhanden ist.[2] Dabei wurde jedoch ein deutliches Missverhältnis zwischen der Nutzungsabsicht und der tatsächlichen Nutzung einer 2FA festgestellt – und das in nahezu jeder Produktkategorie. So wollten beispielsweise zwar 44 Prozent der Befragten das eigene E-Mail-Konto mit einem zweiten Faktor absichern. Jedoch gaben nur 17 Prozent an, das auch tatsächlich zu tun.[3]

Für diese Diskrepanz konnte nicht allein das fehlende Angebot einer 2FA als Ursache herangezogen werden. Denn insbesondere die untersuchten E-Mail-Dienste boten die zusätzliche Absicherung mehrheitlich an. In 4 von 10 Fällen stand aber nur die Nutzung einer Authentisierungs-App zur Auswahl – ein Authentisierungsverfahren, das nur knapp ein Viertel der Verbraucherinnen und Verbraucher kennt (24 Prozent).[4]

Eine erneute Auswertung des vzbv im Januar 2024 von 121 digitalen Diensten ergab, dass eine Absicherung des Nutzerkontos mittels biometrischer Merkmale bei 46 Prozent der untersuchten Anbieter möglich war (ab Seite 5). Bei der Verwendung von Biometrie in der 2FA wird der Wissensfaktor (zum Beispiel PIN oder Passwort) durch biometrische Merkmale wie Fingerabdruck oder Gesichtserkennung ersetzt. So könnte jedoch laut BSI eine breitere Implementierung von biometrischen 2FA-Verfahren die Cybersicherheit der Verbraucherinnen und Verbraucher verbessern, da diese Verfahren einfach und bequem anwendbar sind. Dies hängt in hohem Maße von einer sicheren Umsetzung ab.

Wie Hersteller und Anbieter diese gewährleisten, fasst das BSI neben einer Bewertung der IT-Sicherheit für dieses Themenfeld in seinen Empfehlungen zur sicheren Implementierung zusammen (ab Seite 10). So sollten biometrische Systeme zum Beispiel mit einer Fälschungserkennung ausgestattet sein und auch eine Rückfall-Option auf einen anderen zweiten Faktor (Wissen/Besitz) anbieten. Darüber hinaus sollten die Verbraucherinnen und Verbraucher die Möglichkeit haben, unterschiedliche biometrische Charakteristiken (also beispielsweise mehrere Fingerabdrücke) zu hinterlegen, um diese für verschiedene Anwendungsfälle (Geräteentsperrung, Nutzung von Applikationen) nutzen zu können.

Die häufigsten Fragen und Antworten (ab Seite 16) sowie ein Glossar (Seite 23) zur biometrischen 2FA runden das vorliegende Ergebnisdokument ab.

2. Marktcheck und Ergebnisse von Verbraucher-befragungen

2-FAKTOR-AUTHENTISIERUNG – FOKUS BIOMETRIE

Die Untersuchung stellt eine Bestandsaufnahme der (biometrischen) 2FA dar und nähert sich dem Thema aus der Perspektive der Verbraucherinnen und Verbraucher. Wissen Verbraucherinnen und Verbraucher um die Möglichkeit einer (biometrischen) 2FA? Wo kann diese überhaupt genutzt werden? Gibt es Vorbehalte bei der Verwendung und wie sehen die Erfahrungen der Verbraucherinnen und Verbraucher aus?

Um das generelle Angebot von biometrischer 2FA zu erfassen, hat der vzbv im Januar 2024 einen Marktcheck durchgeführt. Darüber hinaus hat der vzbv in einem Verbraucheraufruf die Einstellung und eventuelle Vorbehalte der Nutzerinnen und Nutzer gegenüber biometrischer Verfahren abgefragt. In den Rückläufen zeigte sich eine Bandbreite von Problemen und Bedenken, die in einer Online-Befragung noch detaillierter untersucht wurden.

2.1 Marktcheck

Bei einem im Januar 2024 durchgeführten Marktcheck wurden die Smartphone-Anwendungen von insgesamt 121 digitalen Diensten erfasst. Hier zeigte sich, wie schon bei der letzten Erhebung im Jahr 2022, ein sehr homogenes Bild innerhalb der betrachteten Branchen, aber ein sehr heterogenes beim Vergleich der Branchen untereinander.[5] Die Mehrheit der Unternehmen versteht die 2FA offensichtlich als Stand der Technik. So bieten die Anbieter in 9 der 13 untersuchten Branchen mehrheitlich ihren Nutzerinnen und Nutzern mindestens eine Form der 2FA an. In einigen Bereichen wie Social Media, Cloud-Dienste, aber auch Gaming betrifft das sogar alle der untersuchten Dienste. Ein ganz anderes Bild zeigt sich beim Blick auf Gesundheitsdienstleistungen wie Fitness-Tracker oder Versandapotheken. Obwohl hier besonders sensible Daten verarbeitet werden, müssen die Nutzerinnen und Nutzern bei 8 von 10 beziehungsweise 9 von 10 Anbietern ganz ohne 2FA auskommen. Auch bei den untersuchten Online-Shops hat sich seit der letzten Erhebung die Situation nicht verbessert. Hier bieten weiterhin nur drei der untersuchten Online-Händler den Schutz des Kundenkontos mittels 2FA. Dem gegenüber stehen 50 Prozent der Verbraucherinnen und Verbraucher, die ihr Nutzerkonto beim Online-Shopping gerne absichern würden.[6]

Banking

Gesetzliche Vorgaben verpflichten die untersuchten Finanzinstitute zum Angebot einer 2FA. Alle Dienste bieten diese auch mit biometrischen Verfahren an.

10/10 Diensten bieten die 2FA mittels biometrischer Verfahren.

Anbieter	2FA	ohne Biometrie	mit Biometrie
Sparkasse	verpflichtend	●	●
Volksbank/Raiffeisenbank	verpflichtend	●	●
ING DiBa	verpflichtend	●	●
Postbank	verpflichtend	●	●
Deutsche Bank	verpflichtend	●	●
Commerzbank	verpflichtend	●	●
DKB	verpflichtend	●	●
Sparda Bank	verpflichtend	●	●
Comdirect	verpflichtend	●	●
Consorsbank	verpflichtend	●	●

Abb. 1

Krankenkassen

Auch Krankenkassen unterliegen einer 2FA-Pflicht. Zusätzlich zu dieser Pflicht ermöglichen alle untersuchten Krankenkassen die Authentisierung mit biometrischen Merkmalen.

10/10 Diensten bieten die 2FA mittels biometrischer Verfahren.

Anbieter	2FA	ohne Biometrie	mit Biometrie
Techniker Krankenkasse	verpflichtend	●	●
BARMER	verpflichtend	●	●
DAK	verpflichtend	●	●
Meine AOK	verpflichtend	●	●
IKKclassic	verpflichtend	●	●
KKH	verpflichtend	●	●
Knappschaft	verpflichtend	●	●
hkk	verpflichtend	●	●
mobil Krankenkasse	verpflichtend	●	●
SBK	verpflichtend	●	●

Abb. 2

Versandapotheken

Obwohl die Anbieter sensible Daten verarbeiten bietet nur eine Versandapotheke eine 2FA.

0/10 Diensten bieten die 2FA mittels biometrischer Verfahren.

Anbieter	2FA	ohne Biometrie	mit Biometrie
Docmorris.de	nicht verfügbar		
shop-apotheke.com	nicht verfügbar		
medpex.de	nicht verfügbar		
medikamente-per-klick.de	nicht verfügbar		
mayd.com	optional	●	
apodiscounter.de	nicht verfügbar		
aponeo.de	nicht verfügbar		
mycare.de	nicht verfügbar		
Volksversand.de	nicht verfügbar		
sanicare.de	nicht verfügbar		

Abb. 3

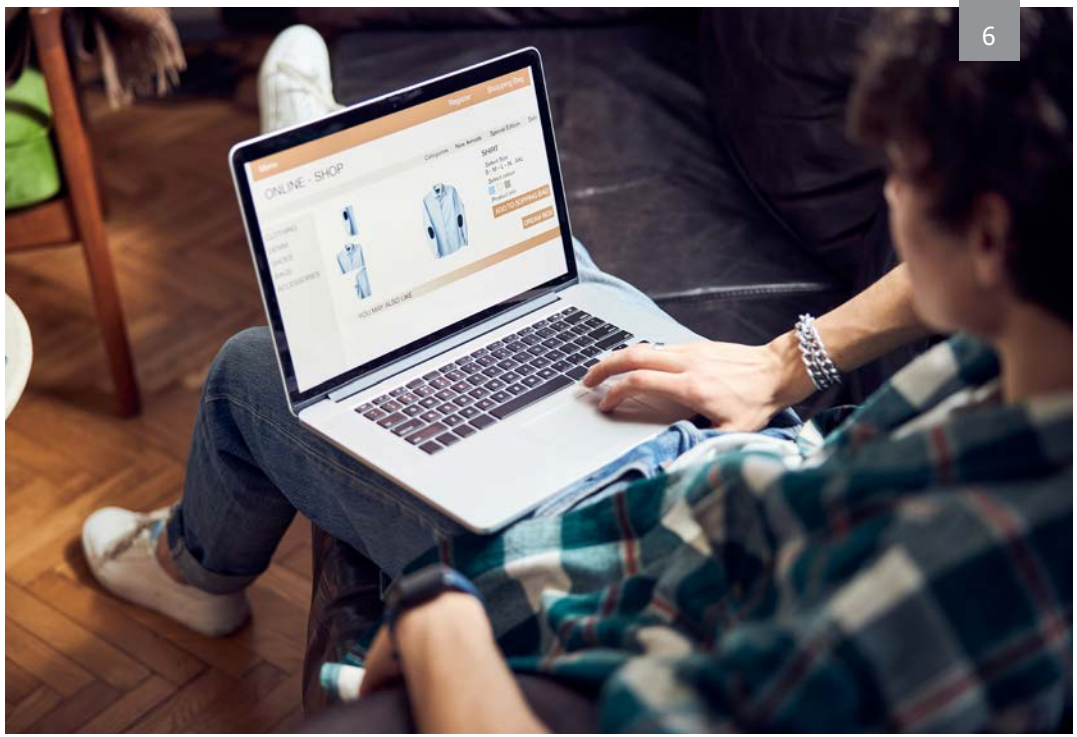
Online-Shopping

Nur wenige Online-Shops bieten die Absicherung per 2FA. Dann ist aberauch die Nutzung biometrischer Merkmale möglich.

3/10 Diensten bieten die 2FA mittels biometrischer Verfahren.

Anbieter	2FA	ohne Biometrie	mit Biometrie
amazon.de	optional	●	●
hm.com.de	nicht verfügbar		
otto.de	nicht verfügbar		
zalando.de	nicht verfügbar		
ikea	nicht verfügbar		
saturn	nicht verfügbar		
mediamarkt	nicht verfügbar		
apple	verpflichtend	●	●
ebay	optional	●	●
lidl.de	nicht verfügbar		

Abb. 4



Insgesamt bieten zum Zeitpunkt der Untersuchung von allen erfassten Diensten 73 Prozent der Anbieter die Absicherung mit einem zweiten Faktor an. Die Erhebung des Angebots biometrischer 2FA zeigt, dass eine Authentisierung mit Fingerabdruck oder Gesichtsscan nur bei 46 Prozent der Anbieter möglich ist.

Interessanterweise konzentriert sich das Angebot biometrischer 2FA auf die Branchen, in denen die Unternehmen verpflichtet sind eine Form der 2FA anzubieten. Dies betrifft Finanzinstitute und Krankenkassen, von denen alle untersuchten Dienste auch die Authentisierung mittels Biometrie ermöglichen.

Die Unternehmen machen keinerlei Angaben zu den eingesetzten Verfahren oder zugrundliegenden Standards, so dass der vzbv eine Unterscheidung der einzelnen Verfahren (wie beispielsweise zweidimensionaler oder dreidimensionaler Scan des Fingerabdrucks) in diesem Marktcheck nicht erfassen konnte. Dies bedeutet auch, dass es für Verbraucherinnen und Verbraucher nicht möglich ist, eine hinreichende Sicherheitsabwägung zu den angebotenen Verfahren vorzunehmen.

2.2 Verbraucheraufruf

In einem Aufruf des vzbv äußerten die Verbraucherinnen und Verbraucher Bedenken beim Einsatz von 2FA mittels biometrischer Merkmale. Diese beziehen sich im Wesentlichen auf drei Aspekte:

Sicherheit/Datenschutz:

„Grundsätzlich sorge ich mich um meine biometrischen Daten, gerade diese sollten nicht in die falschen Hände geraten."

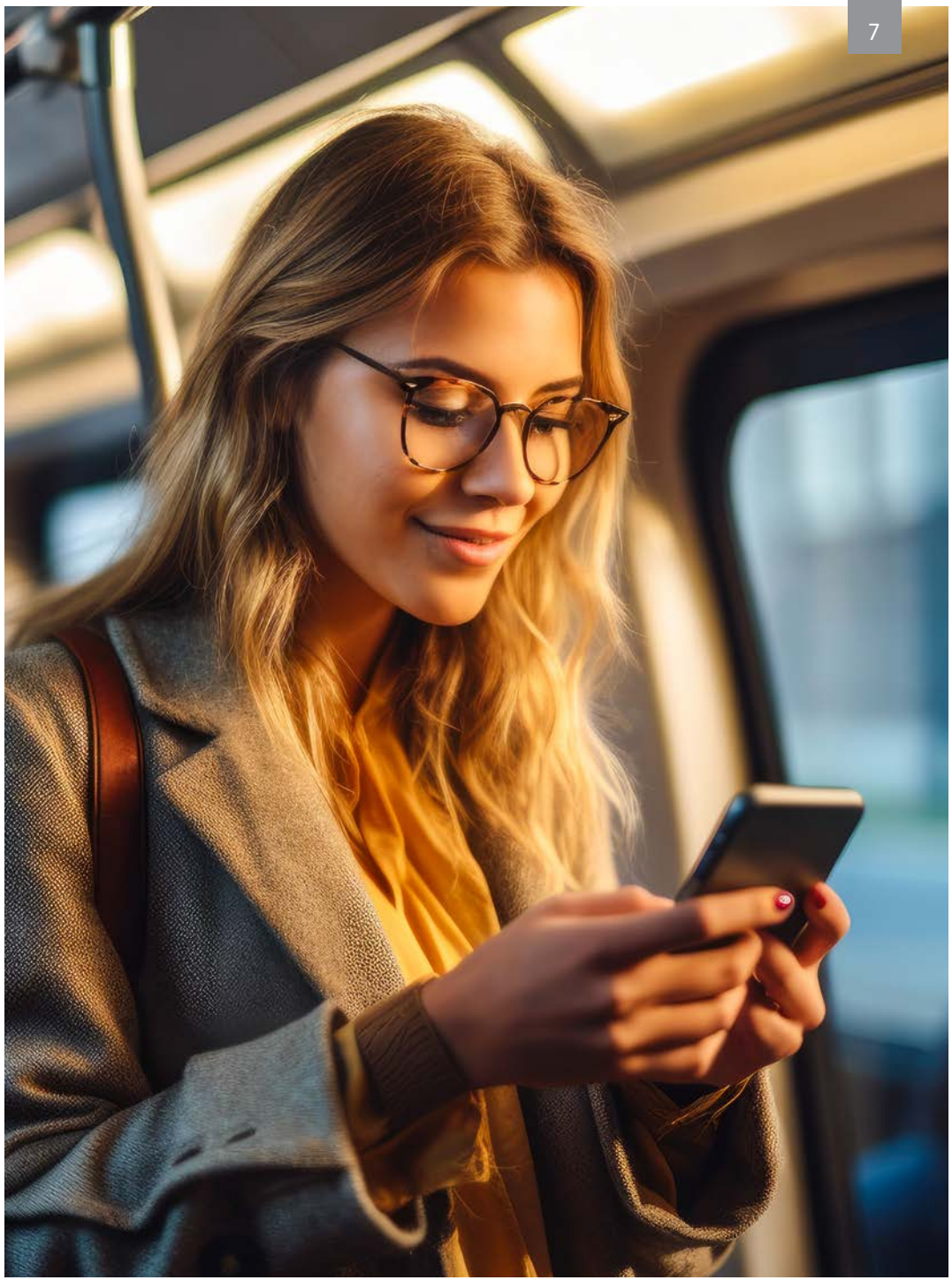
Usability:

„Das Problem war, dass ich durch das häufige Benutzen der Fingerabdrucksperre die PIN andauernd vergesse."

Funktion:

„Die Fingerabdrücke funktionieren nicht immer, obwohl ich mehrere Scans auf meinem Smartphone hinterlegt habe. Zum Beispiel werden meine Fingerabdrücke bei trockener Haut nicht erkannt. Ein Login darüber ist mir daher oft nicht möglich."

Immer wieder äußerten sich die Teilnehmerinnen und Teilnehmer beim Thema Usability aber auch positiv.



2.3 Online-Befragung

Zwei repräsentative Online-Befragungen des vzbv von 2021 und 2023 zeigten, dass bei den Verbraucherinnen und Verbrauchern grundsätzlich ein hohes Schutzbedürfnis vorhanden ist. Auch in Branchen, in denen nur wenige Unternehmen eine 2FA anbieten, würden die Verbraucherinnen und Verbraucher ihr Nutzerkonto gerne zusätzlich absichern. So gaben beispielsweise 50 Prozent der Befragten an, dass sie eine 2FA beim Online-Shopping nutzen würden, wenn ein Angebot bestünde.[7]

Da wo eine 2FA zur Verfügung steht, wird diese regelmäßig von rund 6 von 10 (59 Prozent) der befragten Internetnutzerinnen und -nutzer genutzt. Dabei wird die SMS-TAN immer noch am häufigsten verwendet (60 Prozent der Nutzerinnen und Nutzer). Das biometrische Verfahren des Fingerabdrucks wird von gut einem Drittel (34 Prozent) verwendet, das des Gesichtsscans von gut einem Fünftel (22 Prozent). Weiter zeigt die Befragung, dass biometrische Verfahren nicht nur wegen ihrer Anwendungsfreundlichkeit beliebt sind, vielmehr sprechen die Verbraucherinnen und Verbraucher dem Verfahren auch in Punkto Sicherheit ihr Vertrauen aus.

Empfundene Datensicherheit der 2FA

Die Datensicherheit wird bei allen 2FA-Verfahren mehrheitlich als eher oder sehr hoch eingeschätzt. Die höchste Datensicherheit wird dem Fingerabdruck zugesprochen.

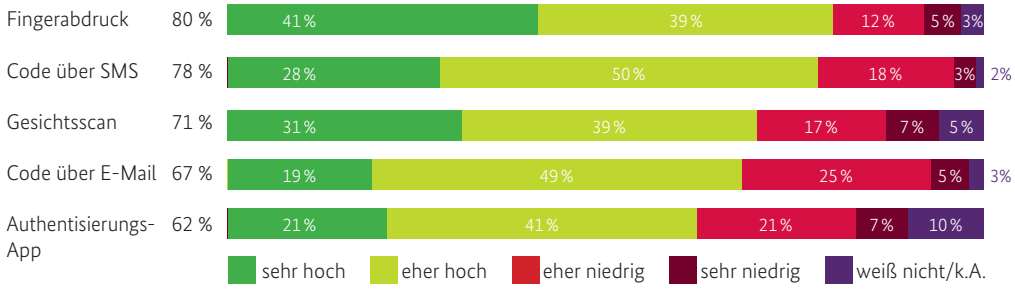


Abb. 5

Anwendungsfreundlichkeit der 2FA

Biometrische Verfahren und Codes über SMS/E-Mail werden mehrheitlich als eher oder sehr einfach bewertet. Die Authentisierungs-App ist die als am umständlichsten empfundene Variante.

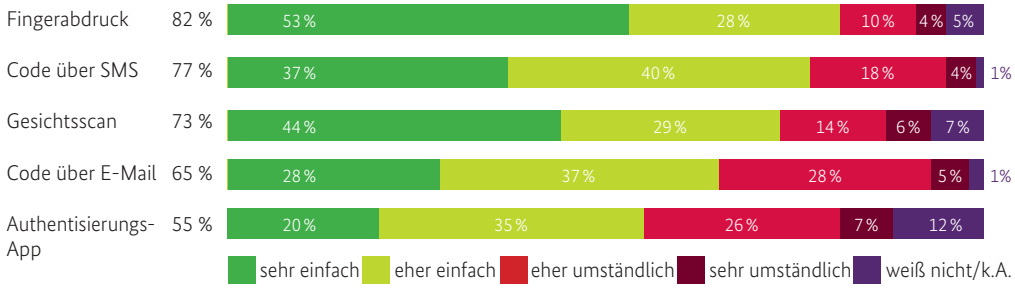


Abb. 6

2.4 Methoden

Dem Marktcheck (siehe 2.1) liegt eine eigene Erhebung des vzbv zugrunde. Untersucht wurde für insgesamt 121 Anbieter aus 13 Branchen, wie häufig digitale Dienste ihren Nutzerinnen und Nutzer eine 2FA anboten und ob diese optional/voreingestellt/verpflichtend war. Zudem wurde erfasst, ob die Anbieter in ihren Smartphone-Anwendungen (Android/iOS) die Möglichkeit einer biometrischen 2FA anboten – also der Login oder die Eingabe eines zweiten Faktors mittels Fingerabdruck oder Gesichtsscan umgesetzt werden konnte. Erhebungszeitraum: 11. bis 15. Januar 2024.

Verbraucheraufruf (siehe 2.2): Verbraucherinnen und Verbraucher meldeten über einen Kurzfragebogen auf der Website der Verbraucherzentralen ihre Erfahrungen im Umgang mit biometrischen 2FA-Verfahren. Insgesamt gingen 23 Meldungen von Verbrauchern und Verbraucherinnen ein. Erhebungszeitraum: 31. Mai bis 11. Juli 2023.

Online-Befragung im Jahr 2021 (siehe 2.3) – Grundgesamtheit: Internetnutzerinnen und -nutzer ab 16 Jahren, die bereits 2FA-Verfahren kennen. Stichprobengröße: 2.014 Befragte. Erhebungszeitraum: 27. April bis 7. Mai 2021. Statistische Fehlertoleranz: max. ± 2 Prozentpunkte in der Gesamtstichprobe. Institut: hopp Marktforschung.

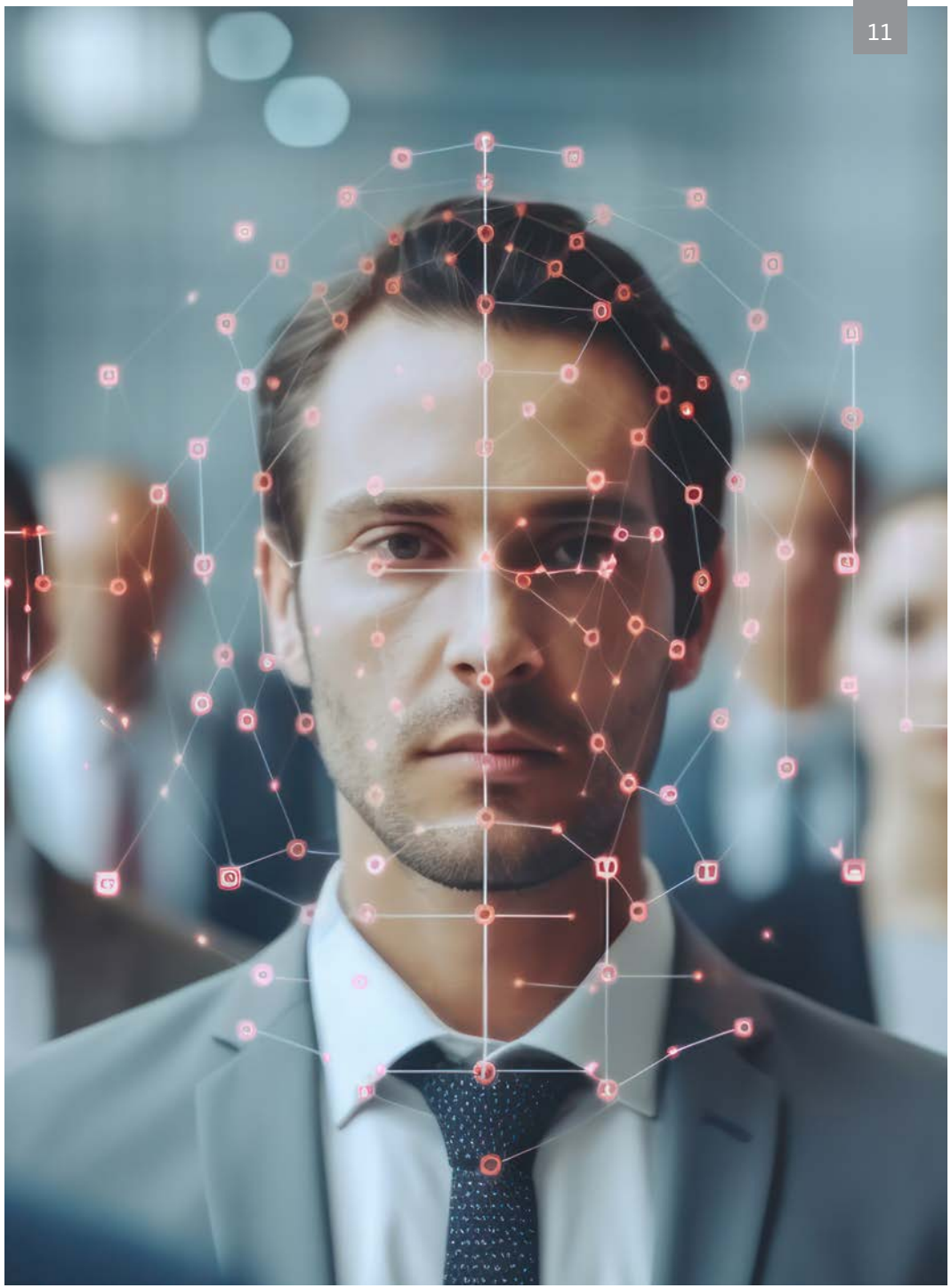
Online-Befragung im Jahr 2023 (siehe 2.3) – Grundgesamtheit: Internetnutzerinnen und -nutzer ab 16 Jahren, die aktuell eine Form der 2FA nutzen. Stichprobengröße: 1.754 Internetnutzerinnen und -nutzer / 1.007 2FA-Anwenderinnen und -Anwender. Erhebungszeitraum: 16. bis 22. Juni 2023. Statistische Fehlertoleranz: max. ± 2 Prozentpunkte in der Gesamtstichprobe. Institut: eye square GmbH.

3. Bewertung der IT-Sicherheit biometrischer Verfahren in der 2-Faktor-Authentisierung

3.1 Einleitung

Die Kombination von Nutzername und Passwort ist die gängigste Authentisierungsoption zur Anmeldung bei einem Dienst im Internet. Selbst wenn Passwörter nach den empfohlenen Vorgaben gebildet und immer ein anderes je Dienst eingesetzt werden, sind damit weitere Risiken, wie z. B. Phishing verbunden. Das BSI empfiehlt deswegen seit langem, neben starken Passwörtern einen zweiten Faktor zur Absicherung der Accounts einzusetzen. In den letzten Jahren haben in Verbraucherprodukten → *biometrische Verfahren,* wie Fingerabdruck- oder Gesichtserkennung auf mobilen Endgeräten an Relevanz gewonnen. Mittels → *biometrischer Verfahren* kann in einer 2FA der Faktor Wissen (PIN oder Passwort) ersetzt werden.[8] Die folgenden Ausführungen gehen der Frage nach, wie Biometrie aus Sicht der Verbraucherinnen und Verbraucher hinsichtlich der Aspekte → *Usable Security* und IT-Sicherheit aktuell anzusehen sind und welche Empfehlungen an Anbieter und Hersteller sich daraus für einen sicheren Umgang mit Biometrie ableiten lassen.

Es existieren eine ganze Reihe an unterschiedlichen Verfahren zur biometrischen Erkennung. Nach einer Marktuntersuchung des Verbraucherzentrale Bundesverband (vzbv)[9] sind aber vorrangig die Verfahren der Fingerabdruck- und der Gesichtserkennung in der Anwendung, auf die im Folgenden fokussiert wird. Für andere → *biometrische Verfahren* sind in der Sicherheitsbewertung abweichende Ergebnisse zu erwarten; die hier gewonnenen Erkenntnisse können somit nicht 1:1 übertragen werden..



3.2 Grundsätzlicher Ablauf und Schritte biometrischer Verfahren

Das Grundprinzip der biometrischen Erkennung ist bei allen Systemen gleich. Zuerst wird der Nutzende im System registriert und die für das jeweilige → *biometrische Verfahren* relevanten Eigenschaften (z. B. Gesicht) der Person werden erfasst (z. B. mittels Kamera) und gespeichert. Die Erfassung → *biometrischer Merkmale* erfolgt sowohl bei der erstmaligen Erfassung zur Erstellung einer → *Referenz* als auch bei der späteren Erfassung zur Wiedererkennung.

Beim sogenannten Matching wird schließlich ein Vergleich zwischen der Referenz und dem Datensatz, der bei der erneuten Präsentation des → *biometrischen Merkmals* gegenüber dem biometrischen System erstellt wird, vorgenommen. Bei Übereinstimmung meldet das Gerät die Erkennung des Nutzenden. Erfassung, Auswertung und Vergleich biometrischer Merkmale sind naturgemäß mit Messfehlern behaftet, da sich die verwendeten Merkmale im Lauf der Zeit verändern.

Die tatsächliche Entscheidung über Match oder Non-Match beruht auf zuvor eingestellten Parametern („Schwellwert"), die einen Toleranzbereich bilden, in dem biometrische Daten vom System als „gleich" erkannt werden. Die biometrischen Merkmale werden nicht auf Gleichheit, sondern nur auf „hinreichende Ähnlichkeit" getestet. Dies hat zur Folge, dass biometrische Systeme nur mit systemtypischer Wahrscheinlichkeit bestimmen können, ob es sich um den Berechtigten handelt. Ein exakter Abgleich der Daten kann daher nicht erreicht werden.

Die für das → *biometrische Verfahren* benötigten Daten von Finger oder Gesicht werden, z. B. als Originalbild oder → *Template* i. d. R. bei in Deutschland angebotenen Diensten lokal auf dem Gerät gespeichert. Bei einer biometrischen 2FA über das Smartphone werden biometrische Informationen in der sogenannten secure enclave lokal gespeichert – Apps bekommen dann nur über eine Schnittstelle mitgeteilt, dass die Authentifizierung erfolgreich war und haben selbst keinen Zugriff auf die biometrischen Daten. Biometrische Daten sind nach Datenschutzgrundverordnung[10] besondere Kategorien personenbezogener Daten und müssen von daher besonders geschützt werden. Zum Beispiel, wenn nicht das Originalbild des Gesichts als → *Referenz* zum Abgleich hinterlegt wird, sondern durch Extraktion gewisser → *Merkmale* und einer mathematischen Transformation ein → *Template als* → *Referenz* erzeugt wird. Ein Schutz des → *Templates* kann durch Verwendung eines → *Templateschutzes* (en: template protection)[11] realisiert werden. Dies kann unter anderem einen direkten Zugriff auf das Originalbild und damit eine direkte Weiterverwendung verhindern. Wenn die vollständige Verarbeitung der Daten lokal und in einer gesondert gesicherten Umgebung stattfindet, können Angriffe auf eine ungesicherte Datenübertragung, Datenlecks und Angriffe auf den Serviceanbieter deutlich erschwert werden.

3.3 Wichtige Sicherheitsaspekte biometrischer Verfahren

Im Folgenden werden die → *biometrischen Verfahren* Fingerabdruck- und Gesichtserkennung auf deren Eigenschaften zur Usable Security sowie IT-Sicherheit untersucht.

3.3.1 Usable Security

Die Nutzung von Biometrie in 2FA-Verfahren kann die Gebrauchstauglichkeit und Barrierefreiheit erhöhen. Biometrische → *Charakteristiken* (z. B. Fingerabdrücke) werden im Gegensatz zu Passwörtern normalerweise weder vergessen noch gehen sie verloren. Zudem können Veränderungen der → *Charakteristiken* aufgrund von Alterung, Verletzungen, Krankheiten u.ä. durch Erzeugung einer neuen → *Referenz* kompensiert werden. Weiter ist positiv zu werten, dass die einmal entsprechend eingerichtete Biometrie für mehrere Dienste sowie ein → *biometrisches Merkmal* auch auf mehreren Geräten verwendet werden kann. Mit wenigen Ausnahmen werden Nutzerinnen und Nutzer gut durch den Implementierungsprozess geführt, so dass die Ersteinrichtung aber auch z. B. eine wiederholte Einrichtung bei Gerätewechsel i. d. R. mit wenig Aufwand verbunden ist. Nach der Ersterfassung im Gerät und insbesondere in der regelmäßigen Nutzung, sind bei entsprechenden Diensten der Aufwand und die Komplexität bei Registrierung und Verwendung gering. Voraussetzung dafür ist allerdings, dass der Dienst die Nutzung von Biometrie bereitstellt. Das Angebot ist zwar von Branche zu Branche unterschiedlich, aber insgesamt als ausbaufähig zu bewerten.

Geht der Verlust des Gerätes mit der Kompromittierung der darin gespeicherten → *Referenz* einher oder ist auch nur letzteres der Fall, so kann genau diese als → *Referenz* nicht für eine sichere Nutzung der Biometrie wiederhergestellt werden. Die Anzahl der biometrischen → *Charakteristiken* einer Person ist begrenzt (wir haben alle nur ein Gesicht und in der Regel zehn Finger), so dass nicht einfach auf ein neues Merkmal gewechselt werden kann, wie es bei Passwörtern möglich ist.

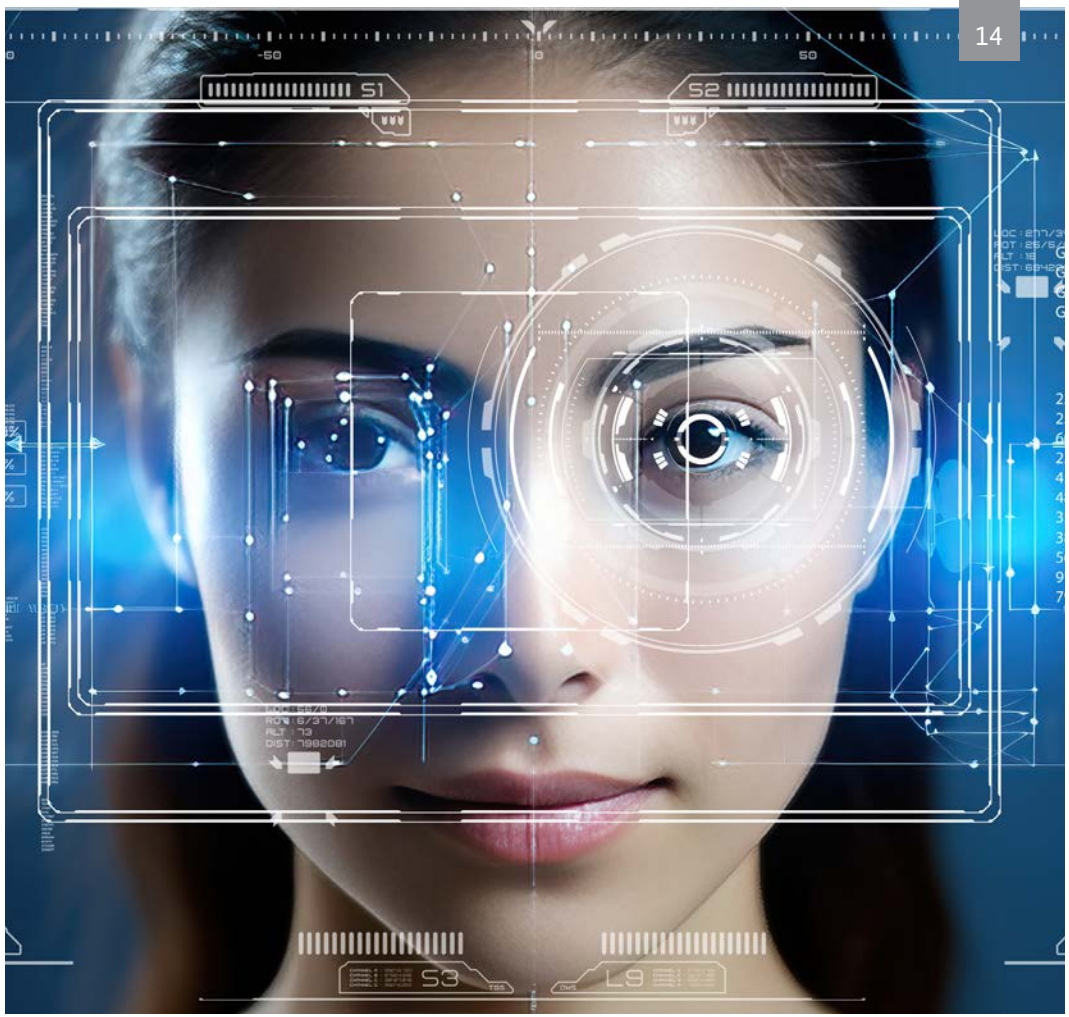
Insgesamt kann die Usable Security von Biometrie als hoch eingeschätzt werden. Dem besonderen Risiko bei Kompromittierung von biometrischen Merkmalen ist insbesondere durch hohe Anforderungen an die Sicherheit der entsprechenden Dienste und Geräte durch Hersteller und Anbieter Rechnung zu tragen.

3.3.2 IT-Sicherheit

Eine sicherheitstechnische Betrachtung von → *biometrischen Verfahren* beginnt bei der Erkennungsgenauigkeit. Wie beschrieben, vergleicht das biometrische System (z. B. Smartphone) ein aktuelles → *Template* mit einer zuvor gespeicherten → *Referenz* und bestimmt einen Vergleichswert. Mit einem Schwellwert wird eingestellt, ab welchem Vergleichswert es sich um eine positive oder negative Vergleichsentscheidung handelt. Ein höherer Schwellwert fordert eine größere Ähnlichkeit und kann eine erhöhte Sicherheit bedeuten, führt aber gegebenenfalls vermehrt zu Falschabweisungen, was die Gebrauchstauglichkeit beeinträchtigt. Umgekehrt führt ein geringerer Schwellwert zu einer besseren Gebrauchstauglichkeit, senkt aber gleichzeitig die Sicherheit des Systems. Wie bereits festgestellt, sollten beim Einsatz biometrischer Daten hohe Ansprüche an die IT-Sicherheit gelten. Auf Grund der Vielfältigkeit biometrischer Verfahren und ihrer Umsetzung in unterschiedlichen Produkten ist eine generelle Sicherheitsbewertung aber nicht möglich.

Einige allgemeingültige Punkte zur IT-Sicherheit lassen sich jedoch aus unterschiedlichen Angriffsszenarien (Massenangriffe) ableiten. Haben Angreifende bei einem Dienst mit dem Abgreifen biometrischer Daten entsprechend Erfolg und liegen diese dann unverschlüsselt als Klarbild vor, dann können diese biometrischen Daten beim selben Dienst missbräuchlich verwendet werden. Sollen die erbeuteten Daten dann bei einem anderen Dienst zu Einsatz kommen oder es werden umfangreich Bilddaten aus vorhandenen Datenbanken, wie z. B. aus Social Media eingesetzt, dann ist die Erfolgsaussicht umso größer, wenn keine Fälschungserkennung zum Einsatz kommt.

Die für das biometrische Verfahren und zum Abgleich benötigten Daten von Finger oder Gesicht sollten daher immer so gespeichert werden, dass mittels → *Template* und → *Templateschutz* nicht auf das Originalbild zugriffen werden kann. Wichtig ist außerdem, wie gut die Verfahren Fälschungen und Angriffe, wie bspw. der Versuch mit einer Fotografie des Besitzers auf ein Gerät zuzugreifen, erkennen. Eine → *Fälschungserkennung* (en: presentation attack detection)[12] ist somit ein wichtiger Faktor, um biometrische Verfahren sicher zu gestalten. Das Schadenspotenzial von Angreifenden (insbesondere für massenhaftes Abgreifen von biometrischen Daten) sinkt, wenn biometrische Daten im Gegensatz zu Online-/Cloud-basierten biometrischen Diensten/Prozessen lokal auf dem Gerät gespeichert sind.



Die für eine Sicherheitseinschätzung notwendigen Informationen sind für Verbraucherinnen und Verbraucher aber nicht zugänglich.

Der Fall, dass Nutzende gewaltsam zur Abgabe biometrischer Daten gezwungen werden, ist ein gezielter Angriff auf die Person in Echtzeit. Allerdings ist dies kein Angriff auf die Biometrie und damit den zweiten Faktor und fällt damit aus dem Untersuchungsbereich heraus. Dennoch ist von Anbieterseite zu bedenken, dass dies häufig eine große Sorge von Verbraucherinnen und Verbrauchern ist, welche die Akzeptanz des Verfahrens beeinflussen kann.

3.4 Empfehlungen

Die Bewertung der → *Usable Security* zeigt, dass biometrische Verfahren als 2. Faktor von Verbraucherinnen und Verbrauchern im Allgemeinen sicher um- und eingesetzt werden können. Das ist eine gute Voraussetzung für einen echten Sicherheitsgewinn. Nicht beeinflussen können Verbraucherinnen und Verbraucher die Verbreitung und die Implementierung der biometrischen Verfahren. Sie sind von einer sicheren Umsetzung abhängig und müssen hierzu auf Hersteller und Anbieter in großem Maß vertrauen. Aus der durchgeführten Betrachtung zur IT-Sicherheit werden daher zusammengefasst folgende Maßnahmen für Hersteller und Anbieter empfohlen:

- → *Referenzen* sollten nicht als Originalbild, sondern nur als → Template gespeichert werden.
- Dieses → *Template* sollte durch → *Templateschutz vor Angriffen* geschützt werden.
- Das biometrische System sollte mit einer → *Fälschungserkennung* ausgestattet sein, um Angriffe und unbefugten Zugriff zu erkennen und abzuwehren.
- Standardisierte Verfahren sollten verwendet werden; wo noch keine standardisierten Verfahren entwickelt wurden, sollte die Fachcommunity diese Lücke im offenen Austausch und Konsens füllen.
- Verkürzen des Angriffsfensters, z. B. auf ein bestimmtes Zeitintervall oder eine maximale Anzahl von Versuchen.
- Auch bei erfolgreichen Authentifikationsversuchen ist es empfehlenswert Maßnahmen zu treffen, wie den Rückfall auf einen anderen Faktor (Wissen/Besitz). Dies kann in regelmäßigen Abständen erfolgen oder als Option für die Nutzenden angeboten werden.

Bei der Gestaltung von mobilen Geräten sind von Technologiehersteller und -anbieter folgende Maßnahmen zu beachten:

- Die Nutzung unterschiedlicher → *Charakteristiken* sollte angeboten werden. Insbesondere sollte die Möglichkeit bestehen selbst zu bestimmen, welche zur Geräteentsperrung und welche zur Nutzung von Applikationen verwendet werden sollen. Im Zweifelsfall sollten verschiedene → *Charakteristiken* oder verschiedene → *Instanzen* genutzt werden.
- Es sollte Transparenz hergestellt werden, ob die biometrischen Daten in einer Cloud oder lokal gespeichert werden.

4. FAQ

1. Was ist Biometrie?

Biometrie ist die Wissenschaft der Vermessung von Lebewesen. Biometrische Informationen sind also jegliche Art von Messdaten über Charakteristika von zum Beispiel Menschen. Dazu können die Form des Kopfes, die Fingerabdrücke, die Körpertemperatur oder die Beschaffenheit des Auges zählen.

2. Wann kommt Biometrie zum Einsatz?

Ziel einer biometrischen Erkennung ist stets, die Identität einer Person zu ermitteln (Identifikation) oder die behauptete Identität zu bestätigen oder zu widerlegen (Verifikation). Das heißt, biometrische Identifizierungsverfahren kommen dort zum Einsatz, wo sich Personen eindeutig authentisieren müssen. Dabei kann das Abtasten biometrischer Merkmale, beispielsweise eines Fingerabdrucks, alleine verwendet werden, um etwa ein Telefon zu entsperren oder eine gesicherte App zu öffnen. Oder aber biometrische Verfahren werden als zweiter Faktor neben etwa einer Kombination aus Benutzernamen und Passwort genutzt, zum Beispiel um das Onlinebanking zu schützen oder um das E-Mail-Konto abzusichern.[13]

3. Welche biometrischen Verfahren gibt es?

Theoretisch lässt sich jedes körperliche Merkmal biometrisch verwerten. Ausschlaggebend hierfür ist die zugrundeliegende Technik. Die Bekanntesten Beispiele sind Scanner für Fingerabdrücke, Iris, Handvenen oder das Gesicht. Man kennt die Technologien zum Beispiel vom Smartphone, PC oder Sicherheitsschlössern. Die häufigsten sind laut Marktüberblick des vzbv mit Stand 01/2024 die Verfahren der Fingerabdruck- und der Gesichtserkennung.[14]

4. Welche Vorteile bringt Biometrie mit sich?

Körperliche Merkmale sind in der Regel untrennbar mit dem Körper der Person verbunden und müssen daher nicht erst dem Berechtigten künstlich zugeordnet werden, wie beispielweise die Kombination aus Benutzername und Passwort. Körperliche Merkmale können in der Regel auch nicht verloren gehen, im Gegensatz zu Passwörtern oder Smartphones. An ein körperliches Merkmal muss sich der Merkmalsträger nicht erinnern, er trägt es untrennbar stets bei sich. Biometrische Verfahren bieten also die Möglichkeit einer Identifizierung und sind zugleich bequem in der Anwendung für die Nutzerinnen und Nutzer.[15]

5. Welche Nachteile bringt Biometrie mit sich?

Das körperliche Charakteristikum kann im Allgemeinen nicht geheim gehalten werden. Im Gegenteil liegen viele der für eine biometrische Erkennung verwendeten körperlichen Merkmale, wie Gesicht und Finger, offen. Deshalb müssen biometrische Erkennungssysteme auch prüfen, ob der Anfragende am Leben ist – damit wird erschwert, dass Systeme z. B. nicht mit einem Foto getäuscht werden. Biometrische Charakteristiken können schließlich nicht übertragen oder weitergegeben werden.

Zudem können einmal gestohlene Daten über biometrische Eigenschaften dazu führen, dass dieses Merkmal nicht mehr zur Sicherung von Diensten eingesetzt werden sollte. Ist der Fingerabdruck einmal bekannt, können Kriminelle diesen bei jedem Dienst missbrauchen, bei dem der Abdruck hinterlegt ist – der Abdruck lässt sich nicht wechseln oder ändern. Passwörter können dagegen beliebig oft gewechselt und zurückgesetzt werden. Wenn Ihre biometrischen Daten gestohlen werden oder verloren gehen, könnten sie dauerhaft gefährdet und nicht mehr sicher nutzbar sein.[16]

6. Wie funktioniert Biometrie?

Biometrische Erkennung erfolgt anhand messbarer, individueller Körpermerkmale. Erkannt wird der Nutzer oder die Nutzerin anhand seiner individuellen Merkmale, z. B. der einmaligen Geometrie der Hände. Damit die biometrischen Daten auch nützlich sind, müssen sie erfassbar, einzigartig und beständig sein. Das Grundprinzip der biometrischen Erkennung ist bei allen Systemen gleich. Zuerst wird der Anwender oder die Anwenderin im System registriert. Danach wird die Eigenschaft, die für das jeweilige Verfahren relevant ist, gespeichert. Zum Beispiel das Gesicht einer Person mittels einer Kamera. Sowohl bei der erstmaligen Erfassung zur Erstellung des sog. Referenzdatensatzes als auch bei jeder späteren Erfassung zur Wiedererkennung, wird das biometrische Merkmal erfasst.

Beim Matching wird schließlich ein Vergleich zwischen dem gespeicherten Abbild und dem Datensatz vorgenommen, der bei dem erneuten Scan des Merkmals gegenüber dem biometrischen System erstellt wird. Bei Übereinstimmung meldet das Gerät die korrekte Erkennung. Die Software nimmt jedes Mal einen Abgleich der Eingabe mit den Daten vor, die in der Datenbank gespeichert wurden. Ändern sich z. B. die Mess-Situationen (wie Beleuchtung) oder die biometrischen Merkmale selbst, etwa durch Alter oder einen Unfall, kann es zu Messfehlern oder Problemen mit dem Abgleich der Datensätze kommen.

Die tatsächliche Entscheidung über Match oder Non-Match beruht auf zuvor durch Hersteller oder Anbieter eingestellten Parametern („Schwellwert“), die einen Toleranzbereich bilden, in dem biometrische Daten vom System als „gleich“ erkannt werden. Die biometrischen Merkmale werden also nicht auf Gleichheit, sondern nur auf „hinreichende Ähnlichkeit“ getestet. Dies hat zur Folge, dass biometrische Systeme nur mit einer gewissen Wahrscheinlichkeit bestimmen können, ob es sich um den wahren Berechtigten handelt. Die Position des Fingers, z. B. auf einem Fingerabdrucksensor oder der Blickwinkel des Gesichts ändern sich bei jeder Nutzung geringfügig. Dies hat zur Folge, dass zwei digitale Abbilder eines biometrischen Merkmals niemals identisch sind und ein exakter Abgleich der Daten nicht möglich ist.[17]

7. Wie zuverlässig sind biometrische Identifizierungsverfahren?

Eine generelle Einschätzung ist auf Grund der Vielfältigkeit biometrischer Verfahren und ihrer Umsetzung in unterschiedlichen Produkten nicht möglich. Die tatsächliche Entscheidung über Match oder Non-Match beruht auf zuvor eingestellten Parametern („Schwellwert"), die einen Toleranzbereich bilden, in dem biometrische Daten vom System als „gleich" erkannt werden. Die biometrischen Merkmale werden nicht auf Gleichheit, sondern nur auf „hinreichende Ähnlichkeit" getestet. Dies hat zur Folge, dass biometrische Systeme nur mit systemtypischer Wahrscheinlichkeit bestimmen können, ob es sich um den wahren Berechtigten handelt.

Ein höherer Schwellwert fordert dabei eine größere Ähnlichkeit und kann eine erhöhte Sicherheit bedeuten. Gegebenenfalls führt er aber häufiger dazu, dass das Merkmal nicht erkannt wird, was die Gebrauchstauglichkeit beeinträchtigt. Umgekehrt führt ein geringerer Schwellwert zu einer besseren Gebrauchstauglichkeit, senkt aber gleichzeitig die Sicherheit des Systems.[18]

8. Ist der Einsatz von Biometrie für mein Gerät oder meinen Dienst möglich?

Um biometrische Verfahren einsetzen zu können, muss das Gerät oder der Dienst grundsätzlich dafür geeignet sein. Das heißt, entsprechende Hard- und Software, wie z. B. eine Kamera für die Gesichtserkennung, werden vorausgesetzt. Aktuelle Geräte bringen diese Funktionalitäten oft mit. Sind diese technischen Bedingungen gegeben, muss noch der Dienst die Nutzung

eines biometrischen Verfahrens anbieten. Viele Dienste haben die Funktion standardmäßig deaktiviert, bieten sie aber dennoch an. Eine Überprüfung der Log-In-Verfahren kann sich lohnen.[19]

9. Was hat Biometrie mit einer 2FA zu tun?

Die 2FA gibt es in zahlreichen Varianten: Einige ergänzen das zuvor eingegebene Passwort um einen zusätzlichen Faktor, andere ersetzen das Passwort komplett durch eine direkte Kombination zweier Faktoren. Faktor eins ist meist ein Passwort. Das heißt, der Nutzende weiß etwas, das andere nicht wissen. Faktor zwei kann dann z. B. ein Fingerabdruck sein. Der Nutzende besitzt also etwas oder weist eine biometrische Eigenschaft auf, die sie oder ihn eindeutig identifiziert. Erst die Kombination der beiden Faktoren führt zum Login. Wichtig ist, dass die Faktoren aus verschiedenen Kategorien stammen, also eine Kombination der Faktoren Wissen, Besitz und Biometrie darstellen. Erbeuten Kriminelle beispielsweise das Passwort, können sie sich trotzdem nicht in ein entsprechend gesichertes Benutzerkonto einloggen, weil ihnen z. B. der zugehörige Fingerabdruck fehlt.

10. Wie verbreitet sind biometrische Verfahren und wo können sie genutzt werden?

Gemäß Marktüberblick des vzbv bieten mit Stand 01/2024 56 von 121 untersuchten Diensten biometrische Verfahren an. Allerdings sind die Unterschiede zwischen den Branchen groß. So bieten alle untersuchten Finanzinstitute eine Zwei-Faktor-Authentisierung mittels Biometrie, aber beim Online-Shopping, bei Fitness-Trackern und Versandapotheken müssen Verbraucherinnen und Verbraucher bei den meisten untersuchten Anbietern sogar gänzlich auf den Schutz einer 2FA verzichten.[20]

11. Wie richte ich Biometrie sicher ein?

Der genaue Ablauf der Einrichtung ist abhängig vom eingesetzten Gerät bzw. Dienst. Grundsätzlich werden Nutzerinnen und Nutzer für die sichere Einrichtung vom Anbieter bzw. Hersteller durch den Prozess geführt.[21]

12. Was passiert, wenn Biometrie mal nicht „funktioniert"?

Funktioniert die biometrische Authentisierung kurzfristig bzw. einmalig nicht, wird in der Regel das vorher hinterlegte Passwort oder eine PIN abgefragt. Funktioniert das biometrische Verfahren dauerhaft nicht, so kann es sich lohnen, die Biometrie neu anzulegen oder ein – wenn möglich – anderes Charakteristikum (z. B. Finger statt Gesicht oder ein anderer Finger) einzusetzen. Alternativ kann ein anderes Verfahren für den zweiten Faktor gewählt werden. Gemäß einer Marktuntersuchung des vzbv bieten mit Stand 01/2024 alle untersuchten Dienste, die einen zweiten Faktor mittels Biometrie anbieten, alternativ auch immer ein anderes Verfahren wie beispielsweise die SMS-TAN oder die Verifikation mittels Authenticator-App an.[22]

13. Wo werden meine biometrischen Daten gespeichert?

Die für das biometrische Verfahren benötigten Daten von z. B. Finger oder Gesicht werden lokal auf dem Gerät oder in einer Cloud gespeichert. Bei den in Deutschland angebotenen Diensten wird zumeist eine lokale Speicherung genutzt.[23]

14. Was wird von meinen biometrischen Daten gespeichert?

Was gespeichert wird kann sich innerhalb der Verfahren und von Anbieter zu Anbieter unterscheiden. So ist beispielsweise nicht ausgeschlossen, dass Originalbilder gespeichert werden und nicht eine Liste an Merkmalen (z. B. nur bestimmte Maße oder Abstände) in Form eines Templates. Ein solches Template sollte darüber hinaus über einen Templateschutz geschützt und verschlüsselt abgelegt werden. Leider tätigen laut Marktüberblick des vzbv (Stand 01/2024) die Dienste keinerlei Aussage zu den eingesetzten Verfahren oder zugrundeliegenden Standards. Dies bedeutet auch, dass es für Verbraucherinnen und Verbraucher nicht möglich ist, eine Sicherheitsabwägung zu den angebotenen Verfahren vorzunehmen.[24]

15. Wie sicher ist der Einsatz von Biometrie?

Die Frage nach der Sicherheit biometrischer Verfahren lasst sich nicht pauschal beantworten. Sie setzt sich zusammen aus der biometrischen Zuverlässigkeit, der Überwindungs-/Fälschungssicherheit sowie der sicheren Speicherung und Verarbeitung biometrischer Daten. Die Sicherheit von Biometrie ist demnach in hohem Maße davon abhängig, wie diese durch den Hersteller implementiert wird.[25]

16. Gibt es Unterschiede bei den Verfahren? Ist z.B. eine Gesichtserkennung immer gleich standardisiert?

Ja, die Verfahren unterscheiden sich. Beispielsweise bietet eine 3D-Gesichtserkennung grundsätzlich einen höheren Schutz als eine 2D-Gesichtserkennung. Laut Marktüberblick des vzbv (Stand 01/2024) tätigen die Dienste keinerlei Aussage, wie die eingesetzten Verfahren umgesetzt werden oder zu zugrundeliegenden Standards, sodass eine Unterscheidung nicht ohne Weiteres möglich ist. Dies bedeutet auch, dass es für Verbraucherinnen und Verbraucher nicht möglich ist, die angebotenen Verfahren nach ihrer Sicherheit auszuwählen.

17. Benötige ich mit Biometrie kein Passwort mehr bzw. kann ich nun ein einfaches Passwort immer wieder verwenden, weil es nicht mehr wichtig ist?

Das Passwort ist auch in Verbindung mit Biometrie weiter ein wesentlicher Faktor für den Schutz von Online-Diensten, z. B. bei einer Zwei-Faktor-Authentisierung. Kein Faktor kann für sich einen hundertprozentigen Schutz gewährleisten, aber in der Kombination bieten starke Passwörter und Biometrie in der Regel einen ausreichend guten Schutz.

Wie werden sichere Passwörter erstellt?

Wie sicher sind die verschiedenen Verfahren der 2FA?

18. Wie können biometrische Verfahren sicher genutzt werden, wenn z.B. meine biometrischen Daten in die falschen Hände geraten oder das mobile Gerät verloren geht?

Die Bewertung des BSI zeigt auf, wie biometrische Systeme gesichert werden können. Idealerweise u. a. so, dass die gespeicherten Informationen für Dritte nicht direkt nutzbar sind (Speicherung als Template mit Templateschutz), die Verfahren nicht (z. B. mit Fotos bei der Gesichtserkennung) getäuscht werden können (durch standardisierte Verfahren zur Fälschungserkennung) und die Speicherung der Daten dezentral und lokal auf mobilen Geräten erfolgt.

Wenn Kriminellen biometrische Merkmale in die Hände fallen, dann sind diese Merkmale nicht mehr sicher zu verwenden. Ab diesem Zeitpunkt kann nicht ausgeschlossen werden, dass Dritte ebenfalls den Fingerabdruck verwenden können. In diesem Fall kann auf alternative Merkmale, wie einen anderen Finger oder einen Gesichtsscan, zurückgegriffen werden. Wenn etwa das Mobilgerät verloren geht, kann es häufig aus der Ferne gesperrt und/oder die Daten gelöscht werden. Dann ist zumeist davon auszugehen, dass die gespeicherten biometrischen Merkmale nicht missbraucht wurden.[26]

19. Wenn die Biometrie mal nicht funktioniert, werde ich aufgefordert meine PIN oder Passwort zu verwenden. Wie vermeide ich, dass ich die PIN/das Passwort vergesse?

Soweit es das Gerät oder der Dienst zulässt, ist die Nutzung eines Passwortmanagers zu empfehlen. Ansonsten empfehlen wir Anbietern eine regelmäßige Überprüfung der PIN/des Passworts sicherzustellen, das durch die Biometrie ersetzt wird. Das sollte anlassbezogen nach z. B. 3-mal falschem Datenabgleich stattfinden und auch regelmäßig nach einer bestimmten Zeit oder nach einer bestimmten Anzahl erfolgreicher Datenabgleiche, um das Vergessen des Passworts/der Pin auszuschließen. Auch als Nutzer kann i. d. R. von biometrischer Authentisierung auf Authentisierung per PIN/Passwort leicht umgestellt und in regelmäßigen Abständen das alternative Verfahren genutzt werden.[27]

5. Quellen

1. Management Summery

[1] vzbv: „Anbieter und Hersteller zu IT-Sicherheit verpflichten“, 2022, https://www.vzbv.de/pressemitteilungen/anbieter-und-hersteller-zu-it-sicherheit-verpflichten

[2] Vgl. ebd.: Frage an 2.014 Kenner des 2FA-Verfahrens: „In welchen Bereichen würden Sie die Zwei-Faktor-Authentisierung nutzen, wenn sie angeboten werden würde?“ (Mehrfachnennungen möglich)

[3] Vgl. ebd.: Frage an 2.014 Kenner des 2FA-Verfahrens: „Und bei welchen der folgenden digitalen Dienste melden Sie sich selbst mittels Zwei-Faktor-Authentisierung (2FA) an?“ (Mehrfachnennungen möglich)

[4] Vgl. ebd.: Frage an 2.014 Kenner des 2FA-Verfahrens: „Welche Verfahren der Zwei-Faktor-Authentisierung (2FA) kennen Sie – und sei es nur dem Namen nach?“ (Mehrfachnennungen möglich)

2. Marktüberblick und Ergebnisse von Verbraucherbefragungen

[5] vzbv: „Anbieter und Hersteller zu IT-Sicherheit verpflichten“, 2022, https://www.vzbv.de/pressemitteilungen/anbieter-und-hersteller-zu-it-sicherheit-verpflichten

[6] Vgl. ebd.: Frage an 2.014 Kenner des 2FA-Verfahrens: „In welchen Bereichen würden Sie die Zwei-Faktor-Authentisierung nutzen, wenn sie angeboten werden würde? (Mehrfachnennungen möglich)“

[7] Vgl. ebd.: Frage an 2.014 Kenner des 2FA-Verfahrens: „In welchen Bereichen würden Sie die Zwei-Faktor-Authentisierung nutzen, wenn sie angeboten werden würde?“ (Mehrfachnennungen möglich)

3. Bewertung der IT-Sicherheit biometrischer Verfahren in der 2FA

[8] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Biometrie/BiometrischeVerfahren/biometrischeverfahren_node.html

[9] Marktcheck des vzbv → siehe Seite 9

[10] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

[11] ISO/IEC 30136:2018: Information technology — Performance testing of biometric template protection schemes

[12] Normenreihe ISO/IEC 30107 Information technology — Biometric presentation attack detection

4. FAQs

[13] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Biometrie/AllgemeineEinfuehrung/allgemeineeinfuehrung_node.html

[14] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Biometrie/BiometrischeVerfahren/biometrischeverfahren_node.html

[15] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Biometrie/AllgemeineEinfuehrung/allgemeineeinfuehrung_node.html

[16] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Biometrie/AllgemeineEinfuehrung/allgemeineeinfuehrung_node.html

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

[17] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Biometrie/AllgemeineEinfuehrung/allgemeineeinfuehrung_node.html

[18] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Biometrie/AllgemeineEinfuehrung/allgemeineeinfuehrung_node.html

[19] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

[20] Marktcheck des vzbv → siehe Seite 9

[21] BSI-Untersuchung „Bewertung der IT-Sicherheit biometrischer Verfahren in der Zwei-Faktor-Authentisierung“

[22] Marktcheck des vzbv → siehe Seite 9

[23] BSI-Untersuchung „Bewertung der IT-Sicherheit biometrischer Verfahren in der Zwei-Faktor-Authentisierung“

[24] BSI-Untersuchung „Bewertung der IT-Sicherheit biometrischer Verfahren in der Zwei-Faktor-Authentisierung“

[25] BSI-Untersuchung „Bewertung der IT-Sicherheit biometrischer Verfahren in der Zwei-Faktor-Authentisierung“

[26] BSI-Untersuchung „Bewertung der IT-Sicherheit biometrischer Verfahren in der Zwei-Faktor-Authentisierung“

[27] BSI-Untersuchung „Bewertung der IT-Sicherheit biometrischer Verfahren in der Zwei-Faktor-Authentisierung“

Abbildungen

Abb. 1: vzbv-eigene Untersuchung des 2FA-Angebots geprüft am 13. Januar 2024. Erfasst wurden maximal zehn relevante Anbieter auf folgender Datengrundlage: Statista Consumer Insights Global Umfrage 2023 (https://de.statista.com/prognosen/999886/deutschland-beliebteste-geldinstitute-fuer-das-privatkonto)

Abb. 2: Quelle: vzbv-eigene Untersuchung des 2FA-Angebots geprüft am 13. Januar 2024. Erfasst wurden maximal zehn relevante Anbieter auf folgender Datengrundlage: Größte gesetzliche Krankenkassen in Deutschland nach der Versichertenzahl im Jahr 2023 – krankenkasse.de (https://de.statista.com/statistik/daten/studie/856392/umfrage/groesste-gesetzliche-krankenkassen-in-deutschland-nach-der-versichertenzahl/)

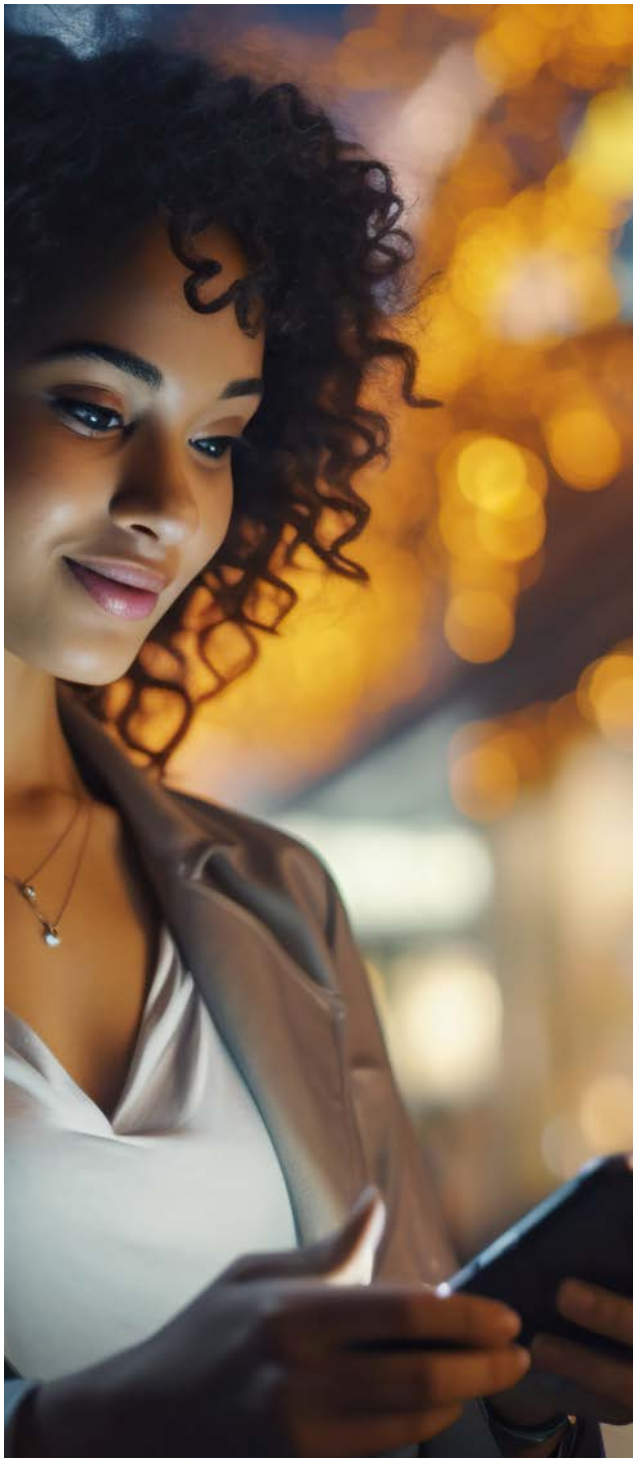
Abb. 3: vzbv-eigene Untersuchung des 2FA-Angebots geprüft am 11. Januar 2024. Erfasst wurden maximal zehn relevante Anbieter auf folgender Datengrundlage: Statista Consumer Insights 2022 (https://de.statista.com/statistik/daten/studie/1359497/umfrage/bekannteste-online-apotheken-in-deutschland/)

Abb. 4: vzbv-eigene Untersuchung des 2FA-Angebots geprüft am 11. Januar 2024. Erfasst wurden maximal zehn relevante Anbieter auf folgender Datengrundlage: ecommerceDB.com; EHI Retail Institute, E-Commerce Markt Deutschland 2022 (https://de.statista.com/statistik/daten/studie/170530/umfrage/umsatz-der-groessten-online-shops-in-deutschland/)

Abb. 5: Basis: 1.007 Internetnutzerinnen und -nutzer, die 2FA nutzen **Frage:** Wie hoch oder niedrig schätzen Sie persönlich die Sicherheit Ihrer Daten beim Einsatz der folgenden Varianten der Zwei-Faktor-Authentisierung (2FA) ein?

Abb. 6: Basis: 1.007 Internetnutzerinnen und -nutzer, die 2FA nutzen **Frage:** Wie einfach oder umständlich empfinden Sie die Anwendung der folgenden Varianten der 2FA?

6. Glossar



biometrisches Verfahren = Ein biometrisches Verfahren ist ein auf biometrischer Erkennung basierender Mechanismus zur Authentisierung eines Menschen aufgrund seiner persönlichen, biologischen Eigenschaften mittels entsprechender Erkennungsgeräte.

biometrischen System = Unter einem biometrischen System ist ein kombiniertes Hard- und Software-Gefüge zur biometrischen Identifikation oder biometrischen Verifikation der Identität zu verstehen, das unter Verwendung biometrischer Verfahren arbeitet. (z. B. Smartphone)

biometrische Charakteristik = biologische und verhaltensbasierte Charakteristiken eines Individuums zur wiederholbaren automatisierten Erkennung (z. B. Gesicht, Fingerabdruck)

biometrische Instanz = es besteht die Möglichkeit der Verwendung unterschiedlicher Instanzen, welche z. B. durch die zur Verfügung stehenden Finger gebildet werden. Entsprechend ist für das Gesicht keine weitere Instanz möglich.

biometrisches Sample = analoge oder digitale Repräsentation biometrischer Charakteristiken (z. B. Aufnahme des Gesichts)

biometrisches Merkmal = wird aus dem biometrischen Sample gewonnen und wird zum biometrischen Vergleich verwendet (z. B. aus der Aufnahme des Gesichts werden die individuellen „Merkmale“ des Gesichts extrahiert – z. B. unterschiedliche Abmessungen im Gesicht)

Referenz = kann durch mehrere biometrische Samples, biometrischen Merkmalen oder generierten biometrischen Modellen erzeugt werden (z. B. wird gespeichert und für die Erkennung abgeglichen)

Template = Merkmalsliste, die aus biometrischen Merkmalen erzeugt wird (→ Merkmalsliste kann als Referenz abgespeichert werden; i. d. R. werden für die Erkennung dann Templates miteinander abgeglichen)

Templateschutz = Verfahren zum Schutz von biometrischen Templates

Fälschungserkennung (en: Presentation Attack Detection (PAD)) = Prozess der Erkennung einer Fälschung in einem biometrischen System

Man-in-the-Middle (MitM)-Angriffe = unbemerktes, in eine Kommunikation zwischen zwei oder mehr Partnern Einschleichen mit dem Ziel, beispielsweise Daten mitzulesen oder zu manipulieren

Usable Security = Usable Security hat die größtmögliche IT-Sicherheit digitaler Technologien in der praktischen Nutzung zum Ziel. Sicherheitsmechanismen müssen so gestaltet sein, dass sie im Nutzungsalltag gut umsetzbar und in die Lebenswelt und die Handlungsabläufe der Anwendenden integrierbar sind. So kann ein hohes Maß an praktischer IT-Sicherheit gewährleistet werden. Usable Security ist als Qualitätsmerkmal von IT-Sicherheit zu verstehen, welches durch Gebrauchstauglichkeit, Zugänglichkeit und Barrierefreiheit sowie Transparenz und einem positiven Nutzungserlebnis zu mehr Nutzungsakzeptanz für Anwendende digitaler Technologien führt und damit zu einer Erhöhung der IT-Sicherheit in der tatsächlichen Nutzungspraxis beiträgt.

Impressum

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: 0800 274 1000
bsi@bsi.bund.de
www.bsi.bund.de

Verbraucherzentrale Bundesverband e.V.
Rudi-Dutschke-Str. 17
10969 Berlin
Tel.: +49 30 258000
info@vzbv.de
www.vzbv.de

Gestaltung: BSI
Stand: März 2024
Bildnachweise: Titel: AdobeStock © kitinut, Seite 2: AdobeStock © basiczto, Seite 3: AdobeStock © martina, Seite 4: AdobeStock © muse studio, Seite 6: dobeStock © Yakobchuk Olena, Seite 7: AdobeStock © MVProductions, Seite 8: AdobeStock © Friends Stock, Seite 9: AdobeStock © EUDPic, Seite 10: AdobeStock © pixcel3d Seite 11: AdobeStock © olga_demina, Seite 12: AdobeStock © tippapatt, Seite 13: AdobeStock © bonnontawat, Seite 14: AdobeStock © FrankBoston, Seite 15: AdobeStock © BOONJUNG, Seite 16: AdobeStock © Aspct-Style, Seite 17: AdobeStock © Dilok, Seite 18: AdobeStock © Koto Amatsukami , Seite 19: AdobeStock © Stavros, Seite 20: AdobeStock © Iryna, Seite 23: AdobeStock © ippapatt, Seite 24: AdobeStock © iridescentstreet