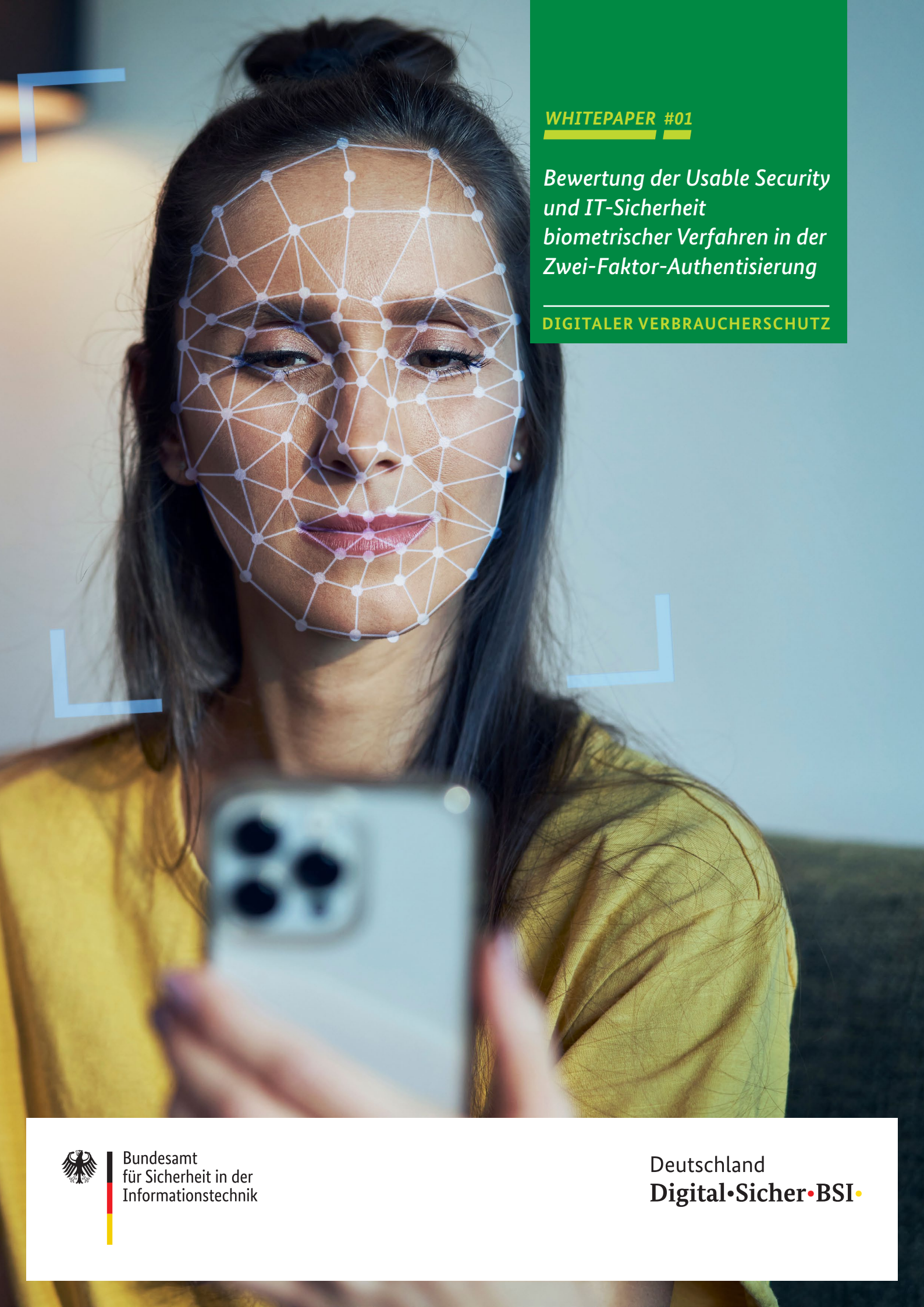

WHITEPAPER #01

Bewertung der Usable Security und IT-Sicherheit biometrischer Verfahren in der Zwei-Faktor-Authentisierung

DIGITALER VERBRAUCHERSCHUTZ

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Impressum

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

www.bsi.bund.de

Redaktion und Gestaltung: BSI

Stand: Juli 2024

Bildnachweise: Titel: AdobeStock©insta_photos; S. 2 oben: AdobeStock© sitthiphong, unten: AdobeStock© insta_photos; S. 4: AdobeStock ©Gorodenkoff; S. 8: AdobeStock©metamorworks

Inhaltsverzeichnis

Hinweis: mit „→“-markierte Begriffe im folgenden Text werden im Glossar (S. 14) näher erläutert

1. Management-Summery

Nach wie vor ist die Kombination von Nutzername und Passwort die gängigste Authentisierungsoption zur Anmeldung bei einem Dienst im Internet. Der Umgang mit Passwörtern ist jedoch mit Risiken verbunden: Datenleaks bei Diensteanbietern, Phishing, direkte Angriffe auf zu einfache Passwörter (z. B. durch → *Brute-Force-Angriffe*) oder die Mehrfachverwendung von Passwörtern bei verschiedenen Diensten *(→ Credential Stuffing)* können zu kompromittierten Onlinekonten führen. Die damit verbundenen Probleme treffen Verbraucherinnen und Verbraucher als Einzelpersonen, haben aber auch gesellschaftliche Relevanz.

Neben dem empfohlenen Einsatz von Passwörtern als Basisschutz [1] empfiehlt das BSI deswegen den Einsatz einer Zwei-Faktor-Authentisierung (2FA), sobald ein Online-Dienst dies ermöglicht [2]. In einer Untersuchung aus dem Jahr 2022 hat das BSI gängige Verfahren der 2FA aus dem Blickwinkel der Verbraucherinnen und Verbrauchern bewertet [3]. Der Fall, dass der zweite Faktor (PIN oder Passwort) einer Zwei-Faktor-Authentisierung durch Biometrie, wie Gesichts- oder Fingerabdruckerkennung ersetzt wird, wurde dort allerdings noch nicht betrachtet.

Sollte zur Authentisierung ein zweiter Faktor angeboten werden, kann man sich bei immer mehr Diensten auch für die Biometrie entscheiden. Die dafür benötigten technischen Voraussetzungen in mobilen Endgeräten, wie z. B. Smartphones, sind aktuell schon weit verbreitet. Sein Gesicht in eine Kamera halten oder mit seinem Finger einen Scanner berühren erscheint einfach und schnell – aber ist das auch im Allgemeinen sicher?

Das vorliegende Whitepaper geht daher der Frage nach, wie → *biometrische Verfahren* aus Sicht der Verbraucherinnen und Verbraucher hinsichtlich der Aspekte „Usable Security" und „IT-Sicherheit" aktuell zu bewerten sind und welche Empfehlungen an Anbieter und Hersteller sich daraus für einen sicheren Umgang mit Biometrie ableiten lassen. So liegen im folgenden biometrische Verfahren auf mobilen Endgeräten im Fokus, bei denen in einer Zwei-Faktor-Authentisierung der Faktor Wissen (PIN oder Passwort) durch Biometrie ersetzt wird [4]. Dafür kommen derzeit vorrangig die Verfahren der Fingerabdruck- und Gesichtserkennung zur Anwendung.

In Bezug auf → *Usable Security* kann die Nutzung von Biometrie in 2FA-Verfahren die Nutzerfreundlichkeit erhöhen. Gesicht oder Finger kann man im Gegensatz zu Passwörtern normalerweise weder vergessen noch verlieren. Zudem können Veränderungen aufgrund von Alterung, Verletzungen, Krankheiten u.ä. durch ein neues → *Enrolment* kompensiert werden. Beim Enrolment ist der Aufwand i. d. R. als gering und die Einsatzmöglichkeiten, sobald die entsprechende Hard- und Software zur Verfügung steht, sind als groß einzuschätzen. Einzig das Angebot für Verbraucherinnen und Verbraucher, Biometrie als 2. Faktor einsetzen zu können, ist noch ausbaufähig [5].

Eine allgemeine Bewertung der Sicherheit biometrischer Verfahren ist aufgrund der Vielfalt der Produkte und Einsatzszenarien sowie unterschiedlichster Implementierungen nicht möglich. Die Bewertung der Sicherheit ist somit einzelfallabhängig.

Beispielsweise ist die Erkennungsgenauigkeit für die Abwägung von Sicherheit und Gebrauchstauglichkeit relevant. Eine höhere Erkennungsgenauigkeit kann zwar eine erhöhte Sicherheit bedeuten, beeinträchtigt aber durch gegebenenfalls vermehrte Falschabweisungen die Gebrauchstauglichkeit. Umgekehrt führt eine geringere Genauigkeit zu einer besseren Gebrauchstauglichkeit und gleichzeitig zu einer geringeren Sicherheit des Systems.

Generell gilt: bei einer einmal kompromittierten Biometrie ist keine Wiederherstellung möglich. Daher sind hier besonders hohe Anforderungen an die IT-Sicherheit der Verfahren anzusetzen.

Zusammenfassend können folgende Empfehlungen gegeben werden: Die für das biometrische Verfahren und zum Abgleich benötigten Daten von Finger oder Gesicht sollten immer so gespeichert werden, dass mittels Template und → *Templateschutz* nicht auf das Originalbild zugriffen werden kann. Darüber hinaus sollte das → *Template* in einem sicheren Speicher abgelegt werden und die Verarbeitung der biometrischen Information soll in einem geschützten / gekapselten Ausführungsbereich stattfinden. Weiterhin ist eine → *Fälschungserkennung* (en: presentation attack detection) [11] ein wichtiger Bestandteil sicherer biometrischer Verfahren. Das heißt, wie gut die Verfahren den Zugriff auf Dienste durch Fälschungen oder auch Angriffsversuche, z. B. mittels Foto, verhindern können.

2. Szenario/ Einordnung des Themas

Das BSI empfiehlt die Absicherung der gängigen Anmeldung bei Internetdiensten über Nutzername und Passwort mit einem 2. Faktor. Im Folgenden werden dafür biometrische Verfahren betrachtet, bei denen in einer Zwei-Faktor-Authentisierung der Faktor Wissen (PIN oder Passwort) durch Biometrie ersetzt wird [4].

Biometrische Verfahren, die es Verbraucherinnen und Verbrauchern ermöglichen sich mit körperlichen → *Charakteristiken* (z. B. Gesicht) statt mit einem Wissensfaktor für einen Dienst anzumelden, sind vielfältig. Vorrangig kommen derzeit die Verfahren der Fingerabdruck- und Gesichtserkennung zur Anwendung. Gesichtserkennung kann in 2D oder in 3D stattfinden.

Andere biometrische Verfahren werden hier – aus Gründen der geringeren Verbreitung – nicht betrachtet. Für entsprechende biometrische Verfahren sind in der Sicherheitsbewertung abweichende Ergebnisse zu erwarten; die hier gewonnenen Erkenntnisse können somit nicht 1:1 übertragen werden.

Die Iriserkennung als biometrisches Verfahren ist aktuell in Verbraucherendprodukten wenig beachtet, wird aber voraussichtlich durch namhafte Geräteanbieter wieder eingeführt. Eine detaillierte Sicherheitsbetrachtung des Authentifikationsverfahrens kann an dieser Stelle nicht stattfinden.

Die für das biometrische Verfahren benötigten Daten von Finger oder Gesicht werden als Originalbild (vergleichbar mit einem Passwort im Klartext) oder Template auf dem Gerät lokal oder in einer Cloud gespeichert. Bei den in Deutschland angebotenen Diensten wird zumeist eine lokale Speicherung genutzt. Biometrische Daten werden nach Datenschutzgundverordnung (DSGVO) [6] als besonders schützenswerte personenbezogene Daten eingestuft und müssen von daher besonders geschützt werden. Dies ist z.B. der Fall, wenn nicht das Originalbild des Gesichts als → *Referenz* zum Abgleich hinterlegt wird, sondern durch Extraktion gewisser → *biometrischer Merkmale* und einer mathematischen Transformation ein Template als Referenz erzeugt wird. Ein Schutz des Templates kann durch Verwendung eines Templateschutzes (en: template protection) [9] realisiert werden. Geschützte Templates werden mittels einer Mathematischen-Einweg-Funktion erzeugt, sodass eine Rekonstruktion des ursprünglichen → *biometrischen Samples* unmöglich wird [7].

Dies kann unter anderem einen direkten Zugriff auf das Originalbild und damit eine direkte Weiterverwendung der biometrischen Daten bei anderen Diensten / bei anderen Anwendungen 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.

Eine sicherheitstechnische Betrachtung von biometrischen Verfahren darf nicht alleinig anhand z. B. der Erkennungsgenauigkeit durchgeführt werden. Wichtig ist auch, wie gut die Verfahren gegen Überwindungsversuche geschützt sind, insbesondere durch Fälschungsangriffe (en: presentation attacks) [11], wie auch bspw. der Versuch, sich mit einer Fotografie des Besitzers bei einem Dienst zu authentifizieren.

Der Prozess lässt sich – wie in Abbildung 1 schematisch dargestellt – in Enrolment und → *Verifikation* unterteilen. Während beim Enrolment die biometrischen Daten erfasst und gespeichert werden, um ein biometrisches Template als Vergleichsbasis zu erzeugen, so wird bei der Verifikation das biometrische Datum erfasst, um eine Entscheidung zu treffen. Damit 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 [9]. Wird vom biometrischen Verfahren eine größere Ähnlichkeit von einer zuvor gespeicherten Referenz im Vergleich zur authentisierenden Person gefordert, kann das eine erhöhte Sicherheit bedeuten. Da sich Menschen aber im Alltag immer etwas verändern, kann eine hohe Ähnlichkeitsschwelle auch vermehrt zu Falschabweisungen führen, was die Gebrauchstauglichkeit beeinträchtigt. Ein neues Gesichtstattoo kann schon ausreichend sein, damit ein Gesicht nicht mehr erfolgreich mit der hinterlegten Referenz verglichen werden kann [8]. Umgekehrt führt eine geringere Ähnlichkeitsschwelle zwar zu einer besseren Gebrauchstauglichkeit, senkt aber gleichzeitig die Sicherheit des Systems.

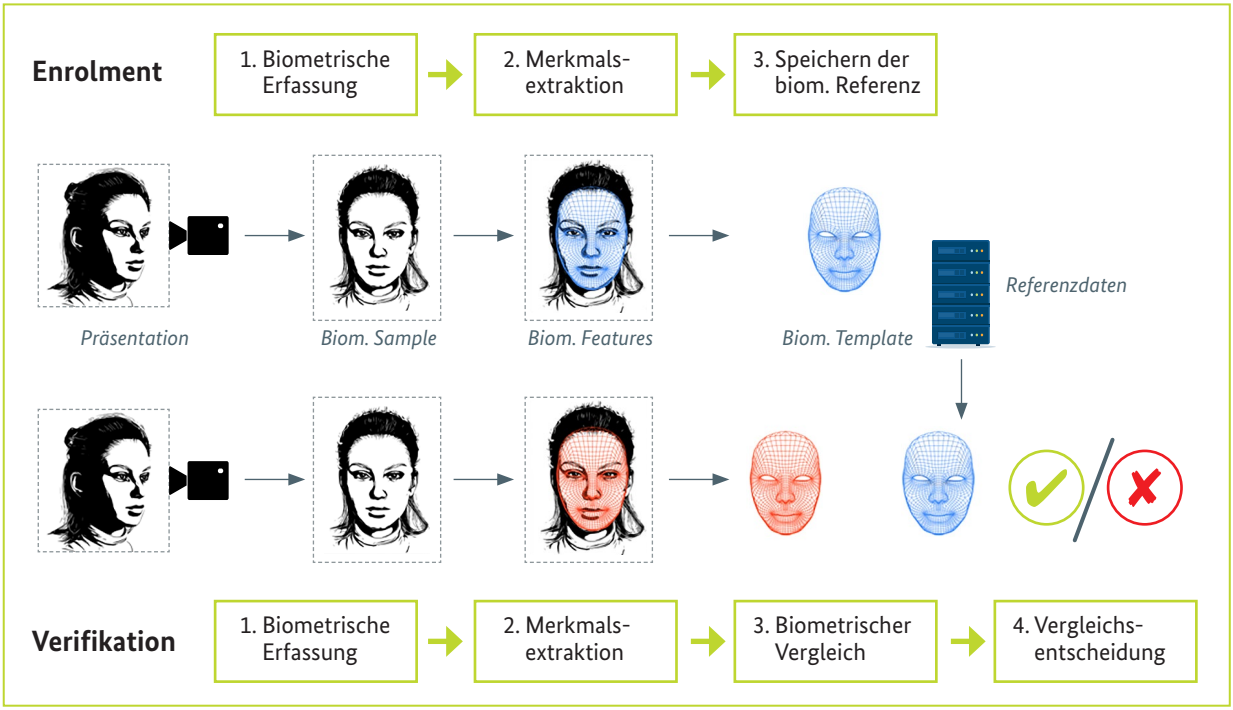

Abb. 1: Prozessdarstellung von der Erfassung bis zur Vergleichsentscheidung in einem biometrischen System

3. Usable Security

Die Nutzung von Biometrie in 2FA-Verfahren kann die Gebrauchstauglichkeit und Barrierefreiheit erhöhen. Biometrische Charakteristiken (z. B. Fingerabdrücke) kann man im Gegensatz zu Passwörtern normalerweise weder vergessen noch verlieren. Zudem können Veränderungen der Charakteristiken auf Grund von Alterung, Verletzungen, Krankheiten u.ä. durch Erzeugung einer neuen Referenz kompensiert werden.

Allerdings ist bei einmal kompromittierter Biometrie keine Wiederherstellung möglich. Es sollte dann ein neues Verfahren (z. B. Fingerabdruck statt Gesichtserkennung) oder eine andere → *biometrische Instanz* (z. B. ein anderer Finger) gewählt werden. Die Wahl(freiheit) ist auch von der zur Verfügung stehenden Hard- und Software abhängig.

In Anlehnung an die Bewertung von Verfahren der Zwei-Faktor-Authentisierung [3] stellt sich die Bewertung der Usable Security von biometrischen Verfahren wie folgt dar:

Bewertungstabelle: → Usable Security (Biometrie als 2. Faktor)

Szenarien im Einsatz biometrischer Verfahren	Bewertung
Der 2. Faktor kann bei mehreren Diensten verwendet werden.	**Ja:** Auf dem jeweiligen mobilen Endgerät ist das biometrische Verfahren meistens für alle Dienste dasselbe. Es wird dabei auch keine Unterscheidung nach dem Zweck (z. B. Entsperren eines Gerätes) oder nach unterschiedlichen Risiken eines Dienstes (z. B. für Finanzanwendungen) getroffen.
Der 2. Faktor wird zur Authentisierung bei vielen verbraucherrelevanten Diensten angeboten.	**Ausbaufähig:** Gemäß dem Marktüberblick des vzbv [5] bieten nur 56 von 121 untersuchten Diensten biometrische Verfahren an.
Der 2. Faktor kann auf unterschiedlichen Geräten bzw. mit unterschiedlichen Geräten verwendet werden. Dies bezieht sich auf Hardware, Betriebsysteme und Software.	**Ja:** Die gleiche Charakteristik kann auf verschiedenen Geräten genutzt werden, allerdings muss bei lokaler Speicherung die Referenz auf jedem Gerät separat erzeugt werden. Voraussetzung ist, dass das jeweilige Gerät entsprechende Hardware und -software mitbringt, die das jeweilige biometrische Verfahren unterstützen.
Inwieweit beeinflusst der 2. Faktor das bisherige Verhalten (1FA) der Nutzenden? Wie aufwändig ist die Nutzung des 2. Faktors (bspw. Notwendigkeit der Verfügbarkeit der Hardware, des Zugangs zur E-Mail, ...)	**Gering:** Die Nutzung von biometrischen Verfahren als 2. Faktor in der 2FA ist wenig aufwändig und beeinflusst das bisherige Verhalten der einfachen Authentisierung mittels Nutzername/Passwort (1FA) nur minimal. Voraussetzung ist die Verfügbarkeit eines mobilen Gerätes, das biometrische Verfahren unterstützt.
Aufwand und Komplexität beim erstmaligen Einrichten des 2. Faktors	**Gering:** Der Nutzende wird durch den Prozess der Referenzerzeugung geführt, der mit nur geringen Aufwand verbunden ist. Bei der Nutzerführung besteht stellenweise (anbieterabhängig) noch Verbesserungspotential.
Aufwand und Komplexität in der regelmäßigen Nutzung (Registrierung bei Diensten und Nutzung an Diensten)	**Gering:** Aufwand und Komplexität in der regelmäßigen Nutzung sind nach dem erstmaligen Einrichten der Referenz gering.
Aufwand und Komplexität der Wiederherstellung, z. B. bei Verlust oder Austausch des mobilen Endgerätes	**Gering:** Geht der Verlust des Gerätes mit der Kompromitierung der darin gespeicherten Referenz einher oder ist auch nur letzteres der Fall, so sollte genau diese als Referenz nicht für eine sichere Nutzung der Biometrie erneut verwendet werden. Die Anzahl der zur Verfügung stehenden Charakteristiken ist begrenzt. Nicht alle biometrischen Verfahren bieten zudem die gleichen Sicherheitseigenschaften oder sind verfügbar. Sofern das mobile Endgerät ein neues Charakteristikum oder eine neue Instanz zulässt, sind Aufwand und Komplexität analog zum erstmaligen Einrichten gering. Gering sind Aufwand und Komplexität ebenso bei Austausch des mobilen Endgerätes. Bei lokaler Speicherung sind die Daten auf dem nicht mehr benötigten Gerät zu löschen und auf dem neuen Gerät ist analog zum erstmaligen Einrichten vorzugehen. Bei Speicherung der biometrischen Daten in der Cloud ist keine neue Erfassung nötig.

4. IT-Sicherheit

Ein großes Risiko für die Verbraucherinnen und Verbraucher geht von Angriffen auf den zweiten Faktor (in diesem Falle die Biometrie) aus, wenn diese als Massenangriffe und automatisiert stattfinden können. Der individuelle wie auch die gesamtgesellschaftlichen Schäden sind in solchen Fällen als schwerwiegend einzuschätzen. Individuelle Angriffe können für die einzelnen Verbraucher jedoch auch weitreichende Folgen haben; für Personen des öffentlichen Interesses sind diese besonders zu beachten.

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

Auf Grund der Skalierbarkeit der IT-Sicherheit und der hohen Divergenz je nach Anwendungsfall und Implementierung, kann keine allgemeingültige Bewertung erfolgen. Stattdessen wird über die Gegenüberstellung eines Status Quo mit der Zielvorstellung aufgezeigt, wie biometrische Verfahren unter bestimmten Bedingungen sicher gestaltet werden können.

Folgende Fälle werden berachtet:

Fall 1: Abgreifen vorhandener biometrischer Daten des genutzten Dienstes und deren Verwendung (Massenangriff)

- Leaks des Dienstes

Fall 2: Abgreifen vorhandener biometrischer Daten aus anderen Diensten oder Quellen und deren Verwendung (Massenangriff)

- Leaks von anderen Diensten
- (Social Media) Photo Crawling
- Erstellung von Datenbanken
- Erstellung von synthetischen Fingerabdrücken

Fall 3: Man-in-the-Middle (MitM)-Angriffe (gezielter Angriff, ggf. auch als Massenangriff möglich)

Fall 4: Nutzen vorhandener / verfügbarer biometrischer Daten (gezielter Angriff)

- Social Media Fotos
- Fingerabdruck von Glas

Fall 1: Abgreifen vorhandener biometrischer Daten des genutzten Dienstes und deren Verwendung (Massenangriff)		
	Status Quo	**Zielvorstellung**
Fingerabdruck-verfahren	Ein automatisiertes massenhaftes abgreifen von biometrischen Daten ist dann möglich, wenn diese Daten in der Cloud gespeichert sind; in der Regel werden biometrische Daten auf dem Gerät gespeichert und sollten in dem Fall nicht automatisiert massenhaft abgreifbar sein. Eine Speicherung der Referenz kann in Form eines Originalbilds oder als Template erfolgen. Werden die Originalbilder neben oder anstatt eines Templates gespeichert, dann können die abgegriffenen Originalbilder genutzt werden.	Die biometrischen Daten sind nicht als Originalbild, sondern nur als Template in einem sicheren Speicher abgelegt. Die Verarbeitung der biometrischen Information soll einem geschützten / gekapselten Ausführungsbereich stattfinden. Eine standardisierter Templateschutz wird von allen Anbietern verwendet. 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).
Gesichts-erkennung	Ein automatisiertes massenhaftes abgreifen von biometrischen Daten ist dann möglich, wenn diese Daten in der Cloud gespeichert sind; in der Regel werden biometrische Daten auf dem Gerät gespeichert und sollten in dem Fall nicht automatisiert massenhaft abgreifbar sein. Eine Speicherung des Bildes als Originalbild ohne weiteren Schutz durch Erzeugung eines Templates ist wahrscheinlich, da für Gesichtsbilder aktuell keine allgemeinen Templateverfahren und damit Templateschutzverfahren standardisiert wurden. Wenn es durch Dritte gelingt, diese Bilder abzugreifen oder diese gehen verloren, dann können diese auch genutzt werden.	Die biometrischen Daten sind nicht als Originalbild, sondern als Template in einem sicheren Speicher abgelegt. Templateschutz auch für Gesichtsbilder ist standardisiert und etabliert und abgegriffene Bilder können nicht ohne weiteres verwendet werden. Die Verarbeitung der biometrischen Information soll einem geschützten / gekapselten Ausführungsbereich stattfinden. 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).
Fall 2: Abgreifen vorhandener biometrischer Daten aus anderen Diensten oder Quellen und deren Verwendung (Massenangriff)		
	Status Quo	**Zielvorstellung**
Fingerabdruck-verfahren	Wenn kein Templateschutz beim Dienstleister A und keine Mechanismen der Fälschungserkennung beim Dienstleister B integriert sind, können die biometrischen Daten von Dienstleister A ausreichend sein, um sich bei Dienstleister B zu authentisieren.	Die Referenzen sind nicht als Originalbild, sondern als Template in einem sicheren Speicher abgelegt. Die Verarbeitung der biometrischen Information soll einem geschützten / gekapselten Ausführungsbereich stattfinden.

Fortsetzung der Tabelle auf Folgeseite

	Status Quo	Zielvorstellung
Fingerabdruck-verfahren	Theoretisch kann auch bei bestehendem Templateschutz ohne Mechanismen der Fälschungserkennung eine Authentisierung erfolgen, wenn das biometrische System als Grundlage beider Dienste identisch ist. Hier sind noch keine Massenangriffe bekannt. Massenangriffe mittels Brute Force mit selbst erstellten Datenbanken sind möglich Die Erzeugung synthetischer Fingerabdrücke, die eine positive Vergleichsentscheidung gegen viele unterschiedliche Identitäten erzeugen können, sind ein mögliches Szenario für Massenangriffe.	Sowohl eine Fälschungserkennung als auch ein Templateschutz sind standardisiert und etabliert und werden von allen Anbietern eingesetzt. Es wird vom Dienst unterbunden, entsprechende Daten einzuspielen. 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).
Gesichts-erkennung	Bei 2D-Gesichtserkennung ist das Abgreifen vorhandener biometrischer Daten und deren Verwendung leichter, auf Grund der besseren Verfügbarkeit (z. B. bei Social Media).	Ein biometrisches Verfahren von höherer Komplexität (wie 3D-Gesichtserkennung) bietet einen höheren Schutz.
Fall 3: Man-in-the-Middle (MitM)-Angriffe (gezielter Angriff, ggf. auch als Massenangriff möglich)		
	Status Quo	**Zielvorstellung**
Fingerabdruck-verfahren Gesichts-erkennung	Mögliche → *MitM-Angriffe* bei biometrischen Verfahren: • durch Eingriff in den Kommunikationspfad zwischen Sensor und der Stelle der Auswertung (Injection) • durch Stören des Originalsignals oder durch Austausch der Referenz	Die biometrischen Daten sind nicht als Originalbild, sondern als Template in einem sicheren Speicher abgelegt. Die Verarbeitung der biometrischen Information soll einem geschützten / gekapselten Ausführungsbereich stattfinden. Templateschutz und Fälschungserkennung müssen zusätzlich zu den allgemeinen Maßnahmen, die nicht biometriespezifisch sind (z.B. Verschlüsselung), getroffen werden. 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).
Fall 4: Nutzen vorhandener/verfügbarer biometrischer Daten (gezielter Angriff)		
	Status Quo	**Zielvorstellung**
Fingerabdruck-verfahren Gesichts-erkennung	→ *Replay-Attacken* sind möglich. Gezielte Angriffe haben keine vergleichbaren globalen Auswirkungen wie Massenangriffe, haben aber eine große Relevanz für die einzelne Verbraucherin/den einzelnen Verbraucher. Beispiele sind: • Identitätsdiebstahl • Erpressung, Betrug oder Diebstahl	Die biometrischen Daten sind nicht als Originalbild, sondern als Template in einem sicheren Speicher abgelegt. Die Verarbeitung der biometrischen Information soll in einem geschützten / gekapselten Ausführungsbereich stattfinden. Eine Fälschungserkennung wird standardmäßig von allen Anbietern eingesetzt. 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).

5. Empfehlungen

Die Bewertung der Usable Security zeigt, dass biometrische Verfahren als ein Faktor in einer 2FA von Verbraucherinnen und Verbrauchern im Allgemeinen einfach 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 in einem sicheren Speicher abgelegt gespeichert werden.
- Dieses Template sollte durch Templateschutz vor Angriffen geschützt werden.
- Die Verarbeitung der biometrischen Information soll einem geschützten / gekapselten Ausführungsbereich stattfinden.
- Das biometrische System sollte mit einer, möglichst durch unabhängige Dritte zertifizierten Fälschungserkennung ausgestattet sein, um Angriffe 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, entsprechende Maßnahmen wie zum Beispiel den Rückfall auf einen anderen Faktor (Wissen / Besitz) zu treffen. Dies kann in regelmäßigen Abständen erfolgen oder als Option für die Nutzenden angeboten werden.
- Die Nutzung unterschiedlicher Charakteristiken sollte angeboten werden. Insbesondere sollten die Nutzerinnen und Nutzer die Möglichkeit haben, selbst zu bestimmen, welche Charakteristika für die Entsperrung der Geräte und welche für die Nutzung der Anwendungen verwendet werden sollen. Im Zweifelsfall sollten verschiedene Instanzen einer Charakteristik genutzt werden.
- Es sollte für die Nutzenden transparent kommuniziert werden, ob die biometrischen Daten in einer Cloud oder lokal gespeichert werden.

6. Glossar

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 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 Gesichts)

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

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).

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

Brute-Force-Angriffe = Das sind Angriffe mit dem Ziel, passwortgeschützte Zugänge durch Ausprobieren zu brechen. Meist bedienen sich Angreifende dabei einer Software um in automatisierter Abfolge verschiedene Zeichenkombinationen auszuprobieren.

Credential Stuffing = Beim Credential Stuffing werden bspw. Kombinationen aus Nutzername und Passwort aus vorangegangenen Daten-Leaks automatisiert bei verschiedenen Diensteanbietern ausprobiert, um zu testen, ob dort eine Anmeldung möglich ist. So können sich Dritte mittels zuvor abgeflossener Login-Daten getarnt als legitime Teilnehmende unberechtigt Zugang zu Diensten verschaffen.

Enrolment = Beim Enrolment werden die biometrischen Daten erfasst und gespeichert, um ein biometrisches Template als Referenz zu erzeugen.

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

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

Replay-Attacken = Angriff durch wiederholte Datenübermittlung

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

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.

Verifikation = bei der Verifikation werden die biometrischen Daten erfasst und mit der zuvor gespeicherten Referenz verglichen, um eine Entscheidung zu treffen

7. Quellen

[1] **BSI-Basisschutz: Sichere Passwörter:**
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=4

[2] **Zwei-Faktor-Authentisierung - Mehr Sicherheit für Online-Konten und vernetzte Geräte:**
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

[3] **Technische Betrachtung – Wie sicher sind die verschiedenen Verfahren der 2-Faktor-Authentisierung (2FA)?:**
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html

[4] **Biometrische Verfahren – Fingerabdruck-, Gesichts- und Iriserkennung grundsätzlich erklärt:**
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Biometrie/BiometrischeVerfahren/biometrischeverfahren_node.html

[5] **Marktcheck biometrische 2-Faktor-Authentisierung:**
https://www.vzbv.de/sites/default/files/2024-04/2024-01-15_2FA_Marktcheck_Update_Slides_QS.pdf

[6] **VERORDNUNG (EU) 2016/679 DES EUROPAISCHEN 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):
https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=de

[7] **Biometrische Template-Protection-Verfahren und Interoperabilitätsstrategien:**
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioKeys/BiometrischeTemplate-Protection-Verfahren.pdf?__blob=publicationFile&v=1

[8] **Impact of facial tattoos and paintings on face recognition systems:**
https://doi.org/10.1049/bme2.12032

[9] **ISO/IEC 30136:2018: Information technology — Performance testing of biometric template protection schemes:**
https://www.iso.org/obp/ui#iso:std:iso-iec:30136:ed-1:v1:en

[10] **Einführung in die technischen Grundlagen der biometrischen Authentisierung:**
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Technische_Grundlagen_pdf.pdf?__blob=publicationFile&v=1

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

Abruf der im Quellenverzeichnis verzeichneten URLs am 10. Juni 2024.

www.bsi.bund.de