Information des DIN-Verbraucherrates

DIGITALE SICHERHEIT - Biometrische Erkennungssysteme

Einleitung mit Anwendungsbeispielen

Biometrische Erkennungssysteme, die zunächst vorrangig im hoheitlichen Kontext (u. a. im Bereich der Grenzkontrollen) genutzt wurden, halten zunehmend Einzug in Alltags- und kommerzielle Anwendungen (z. B. Smartphone- bzw. PC-Freigabe, Zutrittsfreigabe für Wohnraum / Büro / Labor, Authentifizierung im Zahlungsverkehr gemäß Richtlinie (EU) 2015/2366 über Zahlungsdienste im Binnenmarkt). Biometrische Erkennungsverfahren werden in diesem Kontext entweder als ein Faktor einer Zwei-Faktor-Authentifikation oder als einziger Faktor der Authentifikation genutzt.

Dieses Dokument betrachtet algorithmengestützte Verfahren, die sich auf verschiedene biometrische Charakteristiken beziehen. Dabei werden entweder natürliche körperliche Eigenschaften oder Verhaltensmuster zu einer automatisierten Erkennung genutzt. Die biometrischen Charakteristiken „Gesicht“ und „Fingerabdrücke“ werden derzeit bei den in der Öffentlichkeit gängigsten Verfahren verwendet. Die Venenerkennung in Fingern und Handflächen wird im asiatischen Raum stark genutzt, da dort kontaktlose Verfahren bevorzugt werden; allerdings spielt sie im europäischen Raum nur eine nachrangige Rolle. Auch die Charakteristik Stimme wird zukünftig zunehmend Bedeutung erlangen. Zum Beispiel im Smart Home-Bereich kann es sinnvoll sein, dass nur bestimmte Personen ein Gerät bedienen oder gar mit ihrer Stimme eine Tür öffnen. Als weitere biometrische Charakteristiken können Iris bzw. Netzhaut, Unterschrift und Gang, oder auch DNA genannt werden.

Die biometrischen Referenzdaten (Proben, Referenzmuster - sog. Templates oder Modelle), welche bei dem biometrischen Enrolment (Einlernphase) entstehen, können auf einem Authentisierungsgerät (z. B. einem Smartphone), einem Token (z.B. eine Chipkarte), einem Server oder einem sogenannten Client (mobiles oder stationäres Endgerät) gespeichert sein. Der Vergleich der biometrischen Referenzdaten mit den biometrischen Probedaten (also beispielsweise dem Bild, das die Kamera des Smartphones zur Erkennung erzeugt) kann auf einem Server, einem Token, einem Authentisierungsgerät oder einem Client durchgeführt werden.

Aus der Verbraucherrats-Studie „Biometrische Erkennungssysteme – Nutzen und Hemmnisse im Verbraucheralltag“ wird ersichtlich, dass Verbraucher häufig denken, ihre Daten seien sicherer, wenn sie die biometrische Anwendung mit einem Gerät in ihrem Zugriff (ihr Smartphone) nutzen. Jedoch kann es auch hier sein, dass der Datenvergleich auf einem kommerziellen Server stattfindet und die Referenzdaten nicht auf dem verwendeten Gerät abgelegt sind.

Verbraucheranforderungen an biometrische Systeme

Mindestanforderungen aus Verbrauchersicht betreffen im Wesentlichen den Datenschutz bzw. die Datensicherheit, die Sozialverträglichkeit und die Zugänglichkeit sowie Gebrauchstauglichkeit. Anhand der VR-Leitwerte konnten viele Mindestanforderungen an biometrische Systeme bereits in die Normung eingebracht werden. Diese finden sich insbesondere in der ISO/IEC 24714 „Informationstechnik - Rechtssystemübergreifende und gesellschaftliche Aspekte für biometrische Anwendungen“ (zurzeit in Erarbeitung aus ISO/IEC TR 24714-1:2008). Aber auch in konkrete Projekte zum Beispiel zu kontaktlosen Anwendungen (ISO/IEC TS 22604 „Biometric recognition of subjects in motion in access related systems - General information“ in Erarbeitung) oder zur Erkennung von Angriffsversuchen (Normenreihe ISO/IEC 30107 „Informationstechnik - Biometrische Manipulationsabwehr“) werden Verbraucheranforderungen eingebracht.

Sowohl das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit BSI TR 3107 als auch die FIDO (Fast Identity Online) Allianz erarbeiten Spezifikationen bzw. Technische Berichte (TR) zur Falschübereinstimmungsrate (en: false match rate) bei biometrischen Verfahren.

Datenschutz und Datensicherheit

Hinsichtlich Datenschutz und Datensicherheit geht es aus Sicht des europäischen Verbraucherschutzes hauptsächlich um die Umsetzung der Anforderungen der Datenschutzgrundverordnung (DSGVO) und um ein frühzeitiges Gestalten der Systeme im Sinne des Privacy by Design und des Privacy by Default.

Bei einigen Anforderungen aus der DSGVO gibt es aus Verbrauchersicht Klärungsbedarf. Zum Beispiel ist ein Einblick in die Daten dem Verbraucher schwerlich zu gewährleisten, da einem Verbraucher mit Zugriff auf ein verschlüsseltes Template nicht geholfen ist.

Ein ausgesprochen wichtiges Prinzip nach der DSGVO ist das Prinzip der Zweckbindung der Nutzung biometrischer Daten. Aus biometrischen Datensätzen können Zusatzinformationen zum Beispiel über Krankheiten gewonnen werden, die bei Missbrauch erheblichen Schaden anrichten können. Es muss also bedacht werden, welche Informationen aus Datensätzen wie gespeichert werden. Würde also beispielsweise aus einem Datensatz der Sprechererkennung mit rauchiger Stimme abgeleitet, dass der Endnutzer Raucher ist und dies zu Konsequenzen bei der Krankenversicherung führen, wäre solch ein System aus Verbrauchersicht inakzeptabel. In die genormten Datenaustauschformate für biometrische Systeme dürfen solche Datenfelder also nicht aufgenommen werden.

Biometrische Daten müssen besonders geschützt werden, da sie nicht widerrufbar sind und nicht ersetzt werden können, wie beispielsweise eine PIN oder ein Passwort. Der Diebstahl biometrischer Datenbanken kann daher prinzipiell dazu führen, dass ganze biometrische Modalitäten für die betroffenen Verbraucher nicht mehr sicher nutzbar sind (vgl. 2019: Einbruch in Biostar 2-Datenbank [Suprema] mit 28 Millionen Datensätzen mit Fingerabdrücken und Gesichtsbildern). Daher müssen biometrische Datenbanken zumindest hochwertig verschlüsselt werden. Idealerweise müssen zusätzlich für alle biometrische Modalitäten sogenannte „Template-Protection“-Verfahren entwickelt werden, welche grundsätzlich verhindern, dass aus Templates die originalen biometrischen Merkmale rekonstruiert werden können. Es gibt hierzu weitreichende Normung zum Thema Schutz biometrischer Templates und kryptografischer Verfahren (z.B. ISO/IEC 24745 „Informationstechnik - Sicherheitsverfahren - Schutz biometrischer Informationen“ oder ISO/IEC 30136 „Informationstechnik - Performanztest von Template-Protection-Schemes“).

Aspekte der Barrierefreiheit

Die Zugänglichkeit von biometrischen Systemen muss für einen größtmöglichen Nutzerkreis gewährleistet werden. Teilweise können biometrische Systeme selber die Barrieren zum Beispiel für den Zugang zu einem Raum o.ä. abbauen. Bei der Nutzung einer kontaktlosen Biometrie, wie der Gesichtserkennung, hat zum Beispiel ein Rollstuhlfahrer weniger Probleme als wenn an einem (zu hohen) Terminal eine Karte eingeführt werden muss. Eine Anpassbarkeit der Kamerahöhe ist bei der Gesichtserkennung Voraussetzung.

Bei der Nutzung biometrischer Systeme können für bestimmte Nutzergruppen Barrieren entstehen, z.B. bei der Nutzung von Fingerabdruckverfahren werden Nutzer mit abgenutzten Fingerabdrücken benachteiligt.

Bei der Barrierefreiheit ist auch an Nutzergruppen zu denken, die nicht im klassischen Sinne als Gruppen mit besonderen Bedürfnissen gelten. Brillenträger beispielsweise können Probleme mit der Nutzung von Gesichtserkennungssystemen bekommen. Hier ist dann darauf zu achten, dass sich das System auf die Bedürfnisse der Nutzer einstellt (zum Beispiel durch Verwendung besserer Algorithmen oder durch Beleuchtung des Nutzungsraums), als dass der

Nutzer sich dem System anpassen muss. Die Nutzung biometrischer Systeme sollte keine Abweichung von natürlichem Verhalten erfordern und intuitiv sein. Demographische Faktoren, wie Geschlecht, Alter oder Ethnie, dürfen keine Einschränkungen erzeugen, d.h. ein System sollte die gleiche Erkennungsleistung für alle Benutzergruppen bieten. Manche biometrischen Merkmale sind dafür gegebenenfalls besser geeignet als andere; die Verwendung muss dann mit der Akzeptanz der Nutzer einhergehen (z. B. ist DNA häufig sehr gut geeignet, aber nur wenig akzeptiert).

Bei einer Umfrage des Verbraucherrats zur Nutzung von Automatisierter Grenzkontrolle im Jahr 2017 sprachen beispielsweise einige Nutzer die Problematik an, dass die "Vereinzelung" von biometrischen Zugangssystemen, also die fehlende Nutzungsmöglichkeit durch kleine Gruppen wie beispielsweise Familien für sie ein Problem und eine Diskriminierung darstellt. Der Verbraucherrat hat daraufhin gemeinsam mit ANEC die Entwicklung einer europäischen Technischen Spezifikation (TS) zur Nutzung von Zugangskontrolle durch kleine Gruppen initiiert und maßgeblich beeinflusst. Hier wird diskutiert, welche Aspekte zu betrachten und welche Hindernisse zu überwinden sind. Das Dokument CEN TS 17631 "Personal identification – Biometric group access control" wird in Kürze veröffentlicht.

Die Barrierefreiheit des biometrischen Systems sollte durch Tests und die Umsetzung von Testergebnissen in der Entwicklungsphase sichergestellt und verbessert werden.

Für Endnutzer, die das System nicht nutzen können, müssen alternative Systeme vorgehalten werden. Wichtig ist hierbei, dass solche Endnutzer nicht automatisch des unberechtigten Zugangsversuchs verdächtigt werden. Bei dauerhaften Zugangsproblemen sollte außerdem eine dauerhafte alternative Lösung gefunden werden.

Die biometrischen Systeme sollten den Endnutzern mindestens einen weiteren Versuch nach einem Fehlversuch gewähren, wenn die Sicherheitsanforderungen es erlauben. Die Zugangs- und Nutzungsprobleme können teilweise durch eine erneute Ersterfassung des (durch Wissen oder Besitz) autorisierten Nutzers vermieden werden.

Biometrische Systeme müssen einfach und intuitiv nutzbar sein. Hierdurch können Fehler der Endnutzer bei der Anwendung vermieden werden. Nutzungsfehler haben immense Auswirkungen auf die Systemperformanz z. B. hinsichtlich Erkennungsleistung aber auch Schnelligkeit der Erkennung.

Hinweise zur Nutzung können durch genormte Bilder und Symbole, aber auch durch Animationen gegeben werden. Die Normenreihe ISO/IEC 24779 „Informationstechnik - Rechtssystemübergreifende und gesellschaftliche Aspekte bei der Einführung biometrischer Technologien - Piktogramme, Bildzeichen und Symbole für die Verwendung in biometrischen Systemen“ schlägt Symbole für die Nutzung in biometrischen Anwendungen vor. Eine Nutzung genormter Symbole, aber auch wiederkehrender Prozesse in verschiedenen Systemen erhöht den Wiedererkennungswert und erleichtert die Nutzung.

Aus der Verbraucherrats-Studie „Biometrische Erkennungssysteme – Nutzen und Hemmnisse im Verbraucheralltag“ geht hervor, dass Nutzer Systeme, die sie häufig nutzen und die damit einen hohen Wiedererkennungswert besitzen, als leichter nutzbar empfinden (i.S. der Gebrauchstauglichkeit) als Systeme, die selten genutzt werden.

Kooperative Nutzung und Verbraucherakzeptanz

Ziel der Verbrauchervertretung ist es, biometrische Systeme so zu gestalten, dass sie bei den Endnutzern auf Akzeptanz stoßen. Endnutzer, die die Notwendigkeit der Anwendung eines Systems verstehen und dieses System akzeptieren, verhalten sich kooperativ und tragen so zu einem erfolgreichen Einsatz von biometrischen Systemen bei.

Dies geschieht durch das Setzen und Einhalten von Mindestanforderungen an biometrische Systeme hinsichtlich Datenschutz, Sicherheit, Barrierefreiheit etc. wie sie oben beschrieben werden.

Die biometrische Anwendung muss dem Endnutzer einen Zusatznutzen im Vergleich zu bereits angewendeten und dem Endnutzer vertrauten Systemen bieten. Bei biometrischen Systemen ist dies häufig die Schnelligkeit und Bequemlichkeit der Nutzung. Die Sicherheit von Systemen, die aus Verbraucherschutzsicht ein wesentlicher Faktor ist, scheint aus Verbrauchersicht nicht unbedingt originäres Ziel zu sein. Häufig werden unsichere Systeme genutzt, weil sie präsent und bequem sind.

Transparenz und Verbraucherinformation sind wichtige Maßnahmen zur Schaffung von Akzeptanz. Viele Verbraucherängste sind subjektiv und beruhen teilweise darauf, dass Informationsdefizite bestehen und dass die Anwendung mancher biometrischer Verfahren noch unbekanntes Terrain ist. Den Verbraucherängsten und -problemen muss angemessen begegnet werden, ohne sie zu bewerten oder gar als unbegründet abzuwerten.

Aus der Studie des Verbraucherrates lassen sich verschiedene Informationsdefizite erkennen. Besonders bei älteren Generationen scheinen Ängste bei der Nutzung sehr stark ausgeprägt sein. Hier hilft es Möglichkeiten und Chancen der sicheren Nutzung biometrischer Verfahren aufzuzeigen. Im Gegensatz hierzu scheint bei den jüngeren Verbrauchern kaum Bewusstsein hinsichtlich möglicher Gefahren der Nutzung biometrischer Verfahren vorzuliegen. Auch hier sind Ratschläge zur sicheren Nutzung hilfreich. Das Thema der Usable Security, also der einfachen sicheren Nutzung, ist für alle Verbrauchergruppen wesentlich.

Normung zu biometrischen Systemen

Verbrauchern sollte eine grundsätzlich sichere Nutzung biometrischer Erkennungssysteme im Sinne des Security-by-Design-Ansatzes ermöglicht werden.

Die Studie des Verbraucherrates deckt hier Lücken in der Normung von Technologien zur Verbesserung des Privatsphärenschutzes (Privacy-Enhancing-Technologies) auf.

Es sollten Normen mit Anforderungen an Template-Protektion erstellt werden. Auch der Matchingprozess (Vergleich der aktuell präsentierten mit den zuvor abgespeicherten Daten) soll durch Einsatz von Maßnahmen zur Erkennung von Angriffen und zur Manipulationsabwehr noch weiter geschützt werden.

Besonders für den Einsatz von biometrischen Verfahren im Bereich von maschinellem Lernen sollte ein Fokus auf der Verwendung diskriminierungsfreier und transparenter Algorithmen, z. B. bei der Qualitätsbewertung von Gesichtsbildern, gelegt werden. So können Leistungsunterschiede der biometrischen Verfahren hinsichtlich demographischer Gruppen vermieden werden.

Empfehlungen zur Nutzung (bestimmter) biometrischer Technologien

Die Studie des Verbraucherrates empfiehlt Verbrauchern so weit möglich die Nutzung biometrischer Erkennungssysteme, bei denen die biometrischen Daten auf einem Gerät oder Sicherheitstoken unter ihrer Kontrolle erfasst, in einem Trusted Execution Environment (sichere bzw. vertrauenswürdige Laufzeitumgebung für Applikationen) verarbeitet werden und vor unbefugtem Auslesen geschützt sind.

Sie sollten nur Systeme verwenden, die eine Widerstandsfähigkeit gegen die gängigen Präsentationsangriffe bieten.

Anforderungen an biometrische Systeme besonders hinsichtlich Sicherheit, Datenschutz und Barrierefreiheit sollten durch unabhängige Evaluierungsstellen bestätigt werden.

Zusätzlich zu biometrischen Verfahren müssen immer gleichermaßen benutzerfreundliche und sichere Rückfalllösungen vorhanden sein.