Biometrie in Zeiten von Datenschutz und Zertifizierung

Fingerprinttechnologie für den Alltag

Der Einsatz von Fingerprinttechnologie gehört heutzutage zum normalen Alltag. Sei es beim Smartphone, in oder neben der Haustür, als Schalter, beim Tresor und Waffenschrank oder der Garage. Für alle Einsatzbereiche gibt es inzwischen, in einem immer weiter wachsenden Markt, ein vielfältiges Angebot an Systemen. Doch gerade, wenn es um Sicherheit und Datenschutz geht, zeigt sich, welch unterschiedliche Anforderungen Hersteller an ihre eigenen Entwicklungen und Produkte stellen.

Vom unsichereren Billig-Schloss bis zum Hochsicherheits-Fingerprintsystem (**Bild 1**) bietet der Markt ein breites, teils unübersichtliches, Spektrum an Sicherheitslösungen, auch wenn das ein oder andere Produkt diese Bezeichnung nicht wirklich verdient. Da lohnt es sich, zweimal hinzuschauen, bevor man sich für den Kauf und den Einsatz einer solchen Lösung entscheidet. Schließlich geht es hier um die Sicherheit und Schutz von Personen, Sachen und natürlich Daten – vor allem den eigenen.

Quelle: Wittkopp

Bild 1: *Das biometrische Hochsicherheitsschloss »Finkey« wird für die Absicherung von Tresoren und Waffenschränken eingesetzt*

Datenschutz

Datenschutz beschreibt den Schutz vor missbräuchlicher Verarbeitung personenbezogener Daten sowie die Freiheit des Einzelnen, selbst über die Verarbeitung seiner Daten zu bestimmen. Im privaten Einsatzbereich von Fingerprintsystemen stellt sich daher kein Problem dar, denn der Nutzer entscheidet ja selbst, ob er seine persönlichen Identifikationsmerkmale einem System anvertrauen will.

Im gewerblichen Bereich ist es jedoch empfehlenswert, sich die Zustimmung von Mitarbeitern und Mitarbeiterinnen einzuholen. Der Datenschutz in Deutschland wird hauptsächlich durch die Datenschutz-Grundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG) gesetzlich geregelt. Zum Datenschutz gehört natürlich auch das Verhindern von Datendiebstahl und -missbrauch. Gerade im Bereich der biometrischen Technologien, bei der äußerst sensible Daten gespeichert und abgeglichen werden, ist es essenziell, was mit den Daten eigentlich passiert und wie sie gesichert werden.

Benutzerinformationen und biometrische Erkennungsmerkmale sollten möglichst lokal im gesicherten Bereich eines Fingerprintsystems verbleiben. Diese sensiblen Daten sollten nicht in einer Cloud, dem WLAN oder einem externen Speicher wie beispielsweise einem Smartphone verlagert oder gespeichert werden. Bei App-Anwendungen empfiehlt es sich, das Smartphone als Display zur vereinfachten Bedienung eines Systems zu nutzen, nicht als Datenspeicher. Neben dem Schutz der Daten hätte dann ein verlorenes Smartphone keine negativen Konsequenzen für die Sicherheit einer Haustür oder Wertbehältnissen gleich welcher Art.

Sicherheit

Neben Funktionalität und Datenschutz ist aber der Themenkomplex »Sicherheit« für ein Fingerprintsystem ein wesentlicher Faktor. Schließlich sollen durch den Einsatz solcher Systeme Personen und Sachen vor unberechtigter Fremdeinwirkung, egal in welcher Form, geschützt werden. Der Nutzer sollte sich vor Erwerb eines Systems die Frage stellen, welche Kriterien für ihn wichtig sind, und vor allem, wo das System eingesetzt werden soll. Schließlich ist es ein elementarer Unterschied, ob sich ein System im ungesicherten Außenbereich eines Hauses befindet oder in Bereichen mit geringeren Sicherheitsansprüchen.

Quelle: Idencom

Bild 2: *»Biokey« Fingerprinttechnologie gibt es für Auf- und Unterputzanwendungen oder für die direkte Integration in Türblätter, Rahmen und Griffe*

Material, Design, Funktionalität und Sicherheit sind alles Faktoren, die für eine Kaufentscheidung wichtig sind. Der Endanwender sollte aber für sich klare Präferenzen festlegen, bevor er sich für ein System entscheidet. Und das ist gar nicht so einfach, denn schließlich sieht der normale Nutzer ein Produkt erst einmal nur von außen. Bei dem einen Fingerprint-System zieht man den Finger über den Sensor, beim anderen legt man ihn auf – und dann geht die Tür auf, oder auch nicht.

Was aber im Hintergrund passiert, kann der Endanwender nicht wissen oder beurteilen. Also wird er sich auf Marketingaussagen

der Hersteller verlassen müssen. Das kann funktionieren – je nach Seriosität des Herstellers – muss aber nicht. Noch abenteuerlicher ist die Suche nach Antworten im Internet: Hier finden sich haufenweise User-Kommentare, vermeintlich objektive Informationen und sogar nebulöse Produkttest-Seiten, die frei jeder Fachkompetenz Empfehlungen und »Testergebnisse« verbreiten. Teilweise finden sich hier hanebüchene Aussagen zur Qualität eines Produktes.

Natürlich gibt es im Markt inzwischen ein großes Angebot an Systemen (**Bild 2**). Und da ist es gar nicht so einfach, den Überblick zu behalten. Manche sind sicher, andere sogar objektiv von Zertifizierungsstellen anerkannt, jedoch gibt es auch eine nicht gerade kleine Anzahl an Systemen, die durch eklatante Sicherheitslücken auffallen. Mal ist es eine nicht verschlüsselte Kommunikation, mal ist eine simple Manipulation des Türrelais durch einen Magneten möglich und auch der so genannte »latente Fingerabdruck«, ein Fettfilm, der auf der Oberfläche eines Sensors verbleibt, kann ein Risiko darstellen und unter Umständen kopiert und missbraucht werden.

Hilfreich und empfehlenswert ist es daher, sich auf objektivere Quellen zu verlassen. Auch wenn man in Deutschland gerne auf negative Folgen der Überregulierung schimpft, ist es beim Thema Sicherheit doch ein großer Vorteil, dass wir auf Normen und Zertifizierungsinstitute wie VdS (VdS Schadenverhütung GmbH) oder ECB-S (European Certification Body – Security) und deren Expertise und Zertifikate zurückgreifen können (**Bild 3**). Sicherheitsprodukte, die objektiv »auf Herz und Nieren« geprüft werden, helfen dem Verbraucher, Qualität, Zuverlässigkeit und Sicherheit auch bei einem Fingerprint-System besser beurteilen zu können.

Zertifizierung

Bei Waffenschränken oder Tresoren ist eine Zertifizierung, sei es ECB oder VdS, ohnehin zwingend erforderlich, um überhaupt eine Zulassung für ein Wertbehältnis zu erhalten. Der Velberter Hersteller von Hochsicherheitsschlössern Carl Wittkopp GmbH hat mit seiner »Finkey«-Serie die VdS-Zertifizierung Klasse 1 und 2 bereits im Jahr 2015 umgesetzt. Das »Finkey«-Produktportfolio ist seit Jahren im Markt der Tresorhersteller und Händler etabliert. Den gleichen Weg ist auch GU/BKS gegangen und hat sein Haustürkonzept um zertifizierte (Klasse A +B) Sets mit Fingerprint-Systemen ergänzt.

Die zertifizierten Serien beider Unternehmen basieren auf der »Biokey«-Technologie des Berliner Unternehmens Idencom Germany GmbH. Idencom ist seit über 20 Jahren für seine patentierte Erkennungs-Software bekannt und findet sich, neben dem eigenen »Biokey«-Portfolio, in vielen Produkten der Elektro-, Schloss-, Beschlags- und Türindustrie wieder.

Die »Biokey«-Technologie wurde in puncto Datenschutz, Sicherheit und Funktionalität so entwickelt, dass sie die Anforderungen der relevanten Normen problemlos erfüllt und auch Grundlage als elektronisches Steuerelement für die DIN EN 16867 (mechatronische Türbeschläge) und der DIN EN 1627 (einbruchhemmende Bauteile) sein kann. Grundsätzlich ist zu beachten, dass ein gutes Sicherheitssystem aus aufeinander abgestimmten Komponenten bestehen sollte. Neben dem Steuerelement (wie Fingerprint) ist u. a. auch die mechanische Sicherheit von elementarer Bedeutung. Das gilt für Haustüren gleichermaßen wie für Tresore und Wertschutzräume.

Richtungsweisendes Urteil

Neben den vorgenannten Normen gibt es nun zusätzlich ein richtungsweisendes Urteil des Oberverwaltungsgerichts (OVG) NRW (Urt. V. 30.08.2023, Az. 20 A 2384/20), das das Interesse an zertifizierten Fingerprint-Systemen als Verschluss eines Waffenschranks spürbar steigern wird. Das OVG hat in seinem Urteil die Anforderungen an die Aufbewahrung von Schlüsseln zu Waffenschränken festgelegt – und die sind streng.

Laut OVG sind mechanische Schlüssel zu einem Waffenschrank nun in einem Behältnis aufzubewahren, das seinerseits den gesetzlichen Sicherheitsstandards an die Aufbewahrung der im Waffenschrank befindlichen Waffen und Munition entspricht. Mit dem »biometrischen Schlüssel«, also dem eigenen Finger, stellt sich dieses Problem jedoch nicht. Zertifizierte Fingerprint-Systeme gelten nun noch mehr als interessante Alternative zum herkömmlichen Schlüsselschloss und werden weitere Marktanteile erobern können.

Fazit und Empfehlung

Wer die Wahrscheinlichkeit erhöhen möchte, dass ein Fingerprintsystem neben Komfort auch Sicherheit und Mindeststandards beim Datenschutz garantiert, sollte nicht blind auf jede Werbeaussage vertrauen. Es ist sicher kein Fehler, Produktangaben auf Plausibilität zu überprüfen oder sich bei Zertifizierungsstellen Informationen zu zertifizierten Lösungen einzuholen.

Quelle: GU/BKS

Bild 3: *Das Haustürkonzept von GU/BKS bietet u. a. zertifizierte Komplettsets für die VdS-Klassen A und B*

Darüber hinaus ist es für den Nutzer sinnvoll, bei seiner Hausratsversicherung nachzufragen, wie es beim Einsatz von innovativen Zutrittssystemen mit Fingerprint um den Versicherungsschutz bestellt ist. Gerade bei Haus-, Keller- oder Nebeneingangstüren mit elektronischen Öffnungssystemen besteht nun mal die Gefahr, dass bei einem Einbruch oder einer Manipulation der Elektronik der Nachweis darüber nicht erbracht werden kann. Da die meisten Versicherungen in ihren AGBs aber den Nachweis von Einbruchsspuren verlangen, kann sich im Schadensfall ein Problem für den Geschädigten ergeben, nämlich dann, wenn die Versicherung den Ausgleich des Schadens verweigert. Hilfreich ist hier, Systeme einzusetzen, die über einen Ereignisspeicher verfügen, die im Schadensfall von Polizei und Versicherung überprüft werden können.

Zusammenfassend ist die Fingerprinttechnologie eine vielfältig einsetzbare Technologie mit vielen Vorteilen. Angesichts der beschriebenen Risiken empfiehlt es sich aber, möglichst objektive Informationen einzuholen, bevor man sich für ein System entscheidet.

Autor:
Ekkehard Gram,
COO, Idencom Germany GmbH, Berlin