Hilfestellung zu Datensicherheit und Datenschutzkonformität bei Verwendung der biometrischen Gesichtserkennung des Kentix iDFace Max

Grundfunktionalität, Datenfluss und Sicherheitsarchitektur

Der Kentix iDFace Max verarbeitet biometrische Daten nach dem Prinzip Privacy by Design. Die gesamte Architektur des Geräts ist darauf ausgelegt, personenbezogene Daten auf das technisch notwendige Minimum zu reduzieren und ausschließlich lokal zu verarbeiten. Nachfolgend wird der vollständige Datenfluss sowie die Sicherheitsarchitektur beschrieben.

1. Erfassung und Verwaltung von Nutzerbildern in KentixONE

Administratoren und Nutzer mit entsprechender Berechtigung können in KentixONE Nutzerprofile anlegen und verwalten. Für die Nutzung der biometrischen Gesichtserkennung wird im jeweiligen Nutzerprofil ein Referenzfoto hinterlegt. Wesentliche Punkte:

- Das Hochladen eines Fotos steuert, ob ein Nutzer in die biometrische Erkennung einbezogen wird.
- Administratoren sind verantwortlich für die Einhaltung datenschutzrechtlicher Vorgaben (z. B. Nutzerzustimmung, Bildrechte, Löschfristen).
- Das Referenzfoto verbleibt ausschließlich im KentixONE-System und wird nicht automatisch an Geräte übertragen.

2. Lokale Template-Erstellung im iDFace Max

Sobald ein Nutzerfoto in KentixONE hinzugefügt oder aktualisiert wird, erhält der iDFace Max eine entsprechende Änderungsinformation. . Der iDFace Max führt anschließend folgende Schritte aus:

a. Lokale Konvertierung

Das Gerät lädt sich das entsprechende Nutzerphoto in den Arbeitspeiche, dort wird es in ein biometrisches Template umgewandelt. Dabei handelt es sich um eine mathematische Repräsentation charakteristischer Gesichtsmerkmale.

b. Lokale Speicherung des Templates

Das Template wird:

1. ausschließlich lokal im Gerät gespeichert,
2. verschlüsselt abgelegt,
3. eindeutig der Nutzerkennung zugeordnet.

Biometrische Templates werden nicht ins Netzwerk oder in die Cloud übertragen. Es erfolgt keine Rückübertragung an KentixONE. Templates werden nicht zwischen mehreren iDFace Max Geräten synchronisiert. Damit verbleiben alle biometrischen Merkmalsdaten vollständig auf dem jeweiligen Gerät.

3. Umgang mit Rohbilddaten

Standardmäßig findet auf dem iDFace Max keinerlei Speicherung von Rohbilddaten statt.

Ausnahme: Eine optionale Streaming-Funktion kann im Menü aktiviert werden. In diesem Fall können ereignisbasierte Standbilder oder Videostreams erzeugt und an autorisierte Systeme übertragen werden (z. B. Alarmereignisse). Diese Funktion ist standardmäßig deaktiviert und muss bewusst durch einen Administrator aktiviert werden.

4. Löschung von Templates

Wird das Referenzfoto eines Nutzers in KentixONE gelöscht oder das Nutzerprofil entfernt, erfolgt bei der nächsten Synchronisation der Nutzerinformationen automatisch eine vollständige Löschung des zugehörigen biometrischen Templates aus dem lokalen Speicher

Aspekte für einen datenschutzkonformen Betrieb

Rechtsgrundlage

Folgende Verfahren sind zur Schaffung des rechtlichen Rahmens für einen Betrieb üblich. Welche Verfahren im individuellen Fall zulässig sind, bestimmen nationale Gesetzgebung und ggf. anwendungsspezifischen Regelungen wie z.B. Arbeitsnehmer-Datenschutz

1. individuelle Nutzer-Einwilligung

Hier sind Aspekte zu beachten wie z.B:

- Freiwilligkeit der Einwilligung (ggf. ist eine alternative Zugangsmöglichkeit

bereitzustellen)
- Information aller Nutzer
- Widerrufbarkeit der Einwilligung

2. Berufung auf Hochsicherheit

Für den Zugang zu besonders sensiblen Bereichen (z. B. Rechenzentren, Labore) können Regelungen in Kraft gesetzt werden, die den Schutz des Bereichs über Datenschutzrechte des Nutzers stellen

3. Kollektivvereinbarung (Betriebsvereinbarung)

Unternehmen können sich für Mitarbeiter die Aspekte der Verwendung von biometrischen Daten in Betriebsvereinbarungen inkludieren. Hier müssen Aspekte wie Zweck, Datenarten, Löschfristen, Zugriffsrechte, Alternativen klar geregelt und benannt sein. In den meisten Fällen sind diese Betriebsvereinbarungen von der Mitarbeitervertretung freizugeben.

Datenschutzkonforme Aufstellung

- Kamera nur auf Zutrittsbereiche richten, nicht auf Aufenthalts- und Arbeitsbereiche, nicht auf öffentlich zugängliche Bereiche
- Sichtbare Hinweisschilder: „Video-/Biometrische Erfassung“
- Security Hardening des Geräts durchgeführt

Datenschutzkonformer Betrieb

Für biometrische Daten gelten die Regelungen für allgemeinen Datenschutz auch vollumfänglich. Aspekte wie:

- Einschränkung der Datenerfassung und -weitergabe
- Löschkonzept
- Zugriffskontrolle auf die Geräte und Datenbanken nur für Administratoren mit Need-to-Know
- Protokollierung aller Zugriffe auf die Geräte und Datenbanken
- Systemhärtung
- Regelmäßige Rechteüberprüfung
- Transparenz gegenüber Nutzern
- Dokumentation

sind zu beachten.

Biometrische Gesichtsdaten gelten nach Art. 9 DSGVO als besondere Kategorien personenbezogener Daten. Damit können zusätzliche Anforderungen aus nationaler

Gesetzgebung und/oder anwendungsspezifischen Regelungen verpflichtend sein. Diese sind vor in Betriebnahme für jeden EInzelfall zu prüfen.

Systemhärtung

Konfiguration von Software, Kommunikation und Schnittstellen des Geräts ermöglicht Anpassung auf die geltenden Richtlinien. Folgende Aspekte sind einzustellen und bei Inbetriebnahme zu konfigurieren:

- Geräte - Passwort
- Festlegung HTTPS/ HTTP
- De-/aktivierung SSH
- De-/aktivierung Web Interface
- Geräteinterne Audit Logs
- Firmware Updates
- Netzwerk Ports

Aktuellste und detaillierte Informationen zu den Möglichkeiten und der Konfiguration zur Systemhärtung finden sie hier:
https://www.controlid.com.br/manual/security-hardening-guide-en.pdf