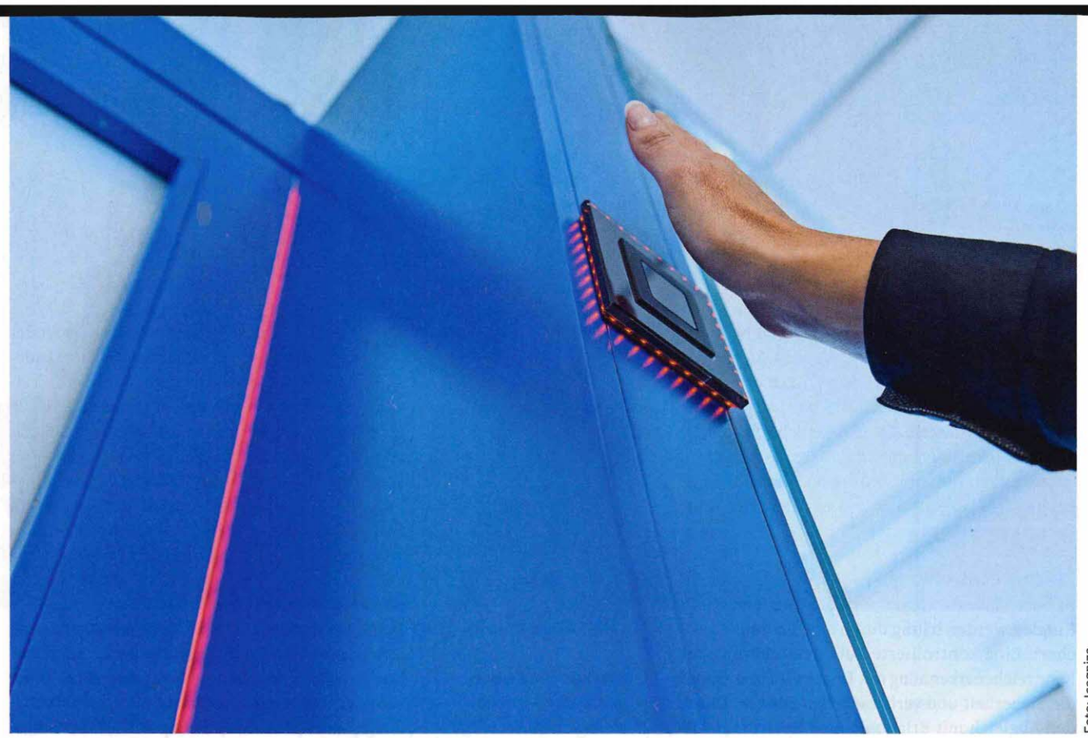

Foto: Icognize

Handvenenscanner sind als Authentifizierungslösung in Rechenzentren gut geeignet.

Per Venenscan ins Data-Center

Rechenzentren sind das Herzstück der Informationsinfrastruktur und müssen mit entsprechender Authentifizierung gesichert sein.

Für die physische Sicherung des Rechenzentrums bedarf es eines mehrschichtigen Sicherheitskonzepts, das auf die sichere Authentifizierungen von Berechtigten setzt. In Rechenzentren werden hochsensible Unternehmensdaten gespeichert und vernetzte Technologien, beispielsweise zur Steuerung der Verkehrsleittechnik oder zur Stromversorgung, beherbergt. Sie gehören damit klar zu Kritis mit vielfältigen Bedrohungsszenarien und den daraus resultierenden weitreichenden Folgen. Hinzu kommt, dass ein Rechenzentrum oft auf der „grünen Wiese" steht, ohne eine personelle Besetzung.

3-fach Authentifizierung für Rechenzentren

Höchsten Schutz bieten hierbei parallele Verfahren, die den Zugang nach verschiedenen Kriterien regeln:

„Ein mehrstufiges Kontrollsystem mit biometrischen Sicherheitsmerkmalen braucht viel Know-how von verschiedenen Seiten."

- Besitz – zum Beispiel durch eine ID-Karte
- Wissen – zum Beispiel durch einen PIN-Code
- Eigenschaften – zum Beispiel durch biometrische Merkmale

Die Erfahrung zur Umsetzung dieser Kriterien war auch bei der Vergabe für die Sicherung eines großen Rechenzentrums in Hessen ausschlaggebend. Den Zuschlag erhielt TAS Sicherheits- und Kommunikationstechnik, Spezialist für vernetzte Sicherheitssysteme, Übertragungstechnik und automatische Alarmierung.

Carsten König, Bereichsverantwortlicher für das bundesweite Errichtergeschäft der TAS, hat bereits einige Projekte mit biometrischen Zugangsverfahren realisiert, bei weiteren Rechenzentren genauso wie bei Finanzdienstleistern und selbst bei Privathäusern für Personen mit einem besonderen Risikoprofil.

Fälschungssicheres Verfahren: Handvenen

Bei der biometrischen Zutrittskontrolle wird der Handvenenscanner des Unternehmens Icognize eingesetzt, der durch seine gängigen Hardware-Schnittstellen problemlos in die Sicherheitsarchitektur eingebunden werden kann. Ausgestattet mit einem Radarsensor, können Bewegungen aus zwei bis drei Meter vor dem Scanner erkannt werden. Dieser schaltet dann auf Betriebsbereitschaft.

Warum ein Venenscan und nicht ein anderes biometrischen Verfahren wie ein Iris-Scan, Fingerprint oder die Gesichtsfelderkennung? „Venen sind nun mal eindeutig, daher hat die Handvenenerkennung den Vorteil, dass sie fälschungssicher und damit ein hochsicheres Authentifizierungssystem ist. Zudem ist sie weniger fehleranfällig als andere biometrische Verfahren, braucht weniger Zeit zur Identifikation im Vergleich zu einem Iris-Scan und ist – da kontaktlos – hygienischer als ein Fingerprint", so König.

Die Authentifizierung in Verbindung mit RFID und der Eingabe des Pin-Codes wird dem Zutrittskontrollsystem in Form eines Signals als Rückmeldung gegeben. Neben dem Zugang wird auch das Verlassen des Rechenzentrums erfasst, um bei einer nicht regelkonformen Abmeldung den erneuten späteren Zutritt verweigern zu können. Für das Projekt werden sowohl Handvenenscanner des Unternehmens Icognize als auch Multifunktionsterminals von Autec für Zutrittskontrolle und Zeiterfassung eingesetzt, da nur an zentralen Zutrittspunkten ein biometrisches Verfahren notwendig ist.

DSGVO-konforme Sicherung von biometrischen Daten

Für die Identifikation einer Person vergleicht das Handvenen-Erkennungssystem das zuvor aufgenommene Venenmuster mit allen gespeicherten Venen-Templates. Aus Datenschutzgründen wird dabei das eigene Handvenen-Muster auf dem Mitarbeiterausweis gespeichert. Durch diese „Template on Card" Verfahren trägt der Nutzer seine biometrischen Daten immer bei sich.

Im Projekt ist man bei der Sicherung der Daten noch einen Schritt weitergegangen und hat hier ein von Icognize zum Patent angemeldetes „Split-Template-Verfahren" eingesetzt, das im Übrigen nicht an biometrische Systeme gebunden ist. Es nutzt das Beste aus den Verfahren „Template in der Datenbank" und „Template on Card".

„Venen sind nun mal eindeutig, daher hat die Handvenenerkennung den Vorteil, dass sie fälschungssicher und damit ein hochsicheres Authentifizierungssystem ist."

Carsten König, Bereichsverantwortlicher für das bundesweite Errichtergeschäft der TAS

Zunächst werden kritische Datenblöcke in zwei oder mehr Datenanteile gespalten. Die einzelnen Teile werden anschließend auf unterschiedlichen Medien und an verschiedenen Orten gespeichert, wie etwa RFID-Karte und Server innerhalb der IT-Infrastruktur. Durch die Splittung sind die erfassten biometrischen Daten nicht mehr personenbezogen im Sinne der DSGVO, da keine Rückschlüsse zum eigentlichen Datensatz möglich sind. Das Split-Verfahren verhindert zudem, dass bei Cyberattacken komplette biometrische Datensätze gestohlen werden können. Alle Daten und Wege sind mehrfach gesichert: Die Templates werden mittels BSI-zertifiziertem Sensormodul verschlüsselt und AES-256-Bit verschlüsselt sind sowohl die Datenbank als auch die Kommunikation zwischen Handvenensensor und Controller. Mehr Sicherheit geht nicht.

So ausgefeilt die Datensicherung, so komplex ist das Berechtigungskonzept: Neben einer Whitelist für Berechtigte mit einem permanenten Zugang werden auch temporäre Zugänge vergeben – sowohl personell, zeitlich als auch örtlich. Denn als Colocation-Anbieter vermietet der Betreiber des Rechenzentrums Flächen an Unternehmen und Institutionen für Server und Racks.

Echzeitüberwachung der Systeme durch Vernetzung

Das fortschrittliche Zugangskontrollsystem wird mit Überwachungskameras und einer Einbruchmeldeanlage kombiniert. Im Außenbereich kommt noch eine Perimetersicherung hinzu. Die Gewerke werden dabei über Schnittstellen an ein übergeordnetes Managementsystem angebunden, wobei das Gewerk Brandmeldeanlagen derzeit noch nicht integriert ist.

Durch die Vernetzung können die Systeme in Echtzeit überwacht, Meldungen aus unterschiedlichen Bereichen erfasst und analysiert werden, um schnell auf Bedrohungen und ungewöhnliche Ereignisse reagieren zu können. So lassen sich beispielsweise Türen automatisch verriegeln und Stromquellen abschalten. Im Rechenzentrum in Frankfurt a. Main setzt das TAS-Team auf die bewährte XMP-Babylon-Software, die weltweit im Gebäudemanagement eingesetzt wird.

Ein mehrstufiges Kontrollsystem mit biometrischen Sicherheitsmerkmalen und die Integration in ein Managementsystem braucht sehr viel Know-how von verschiedenen Seiten. Als Planer und Systemintegrator arbeitet TAS daher eng mit seinen Partnern zusammen. Das ist umso wichtiger, da IT, IoT und Physical Security in ein ganzheitlichen Sicherheitskonzept münden. ■