Durch die stark wachsende Digitalisierung findet eine wichtige Veränderung in allen Lebensbereichen statt. Die mittlerweile selbstverständlich gewordene Nutzung von sozialen Netzwerken, steigender Mobilität, Cloud-Technologien und die Explosion an digital verfügbaren Informationen (Big Data) verändert die Bedarfe, Ansprüche und das Verhalten von Kunden und erschließt gleichzeitig neue Geschäftsfelder für viele Unternehmen. Voraussetzung für all das ist aber eine bestmögliche Absicherung von Rechenzentren, in den alle oben genannten Aspekte ihren Ursprung haben.

Einsatz von Handvenenscannern im Rechenzentrum

#biometrie #handvenen #zugangskontrolle

Die Herausforderung

Rechenzentren, die mit ihren Servern, Storages und Netzwerken oft Unmengen von Terrabyte an Daten beherbergen, zählen zu den kritischen Infrastrukturen. Oft haben sie eine besondere Bedeutung für das Funktionieren des Gemeinwesens, der Wirtschaft und des öffentlichen Lebens. Man stelle sich nur einmal vor, im Frühjahr 2020 während der Coronakrise, wäre ein Rechenzentrum durch einen unbefugten Zutritt lahmgelegt worden. Die ständig steigende Nachfrage, durch die sich immer mehr verstärkende Digitalisierung, führt dazu, dass immer mehr Daten - häufig auch aus dem privaten Sektor - auf den Servern in den Rechenzentren liegen und gut geschützt werden müssen.

Betreiber von Rechenzentren sind für den funktionalen Rahmen eines Rechenzentrums verantwortlich und hierbei bedarf schon der Eingang besonderer Schutzmaßnahmen. Für den Zutritt zu Rechenzentren sind strukturierte Abläufe aus Sicherheitsaspekten unerlässlich. Dabei sollte die Zugangskontrolle über mehrere, parallel eingesetzte Verfahren geregelt werden. Hierfür bieten sich die Kriterien **Besitz** (zum Beispiel ID-Karte), **Wissen** (zum Beispiel PIN-Code) und **Eigenschaften** (zum Beispiel biometrische Merkmale) an. Alle Vorgänge - erfolgreiche wie nicht erfolgreiche - sind zu protokollieren, die Protokolle aufzubewahren. Aus Datenschutzgründen wird sehr häufig in den Rechenzentren auf das Verfahren „Template on Card“ gesetzt. Dies bedeutet, das das eingelesenen HandvenenMuster beim Enrollment auf den Mitarbeiterausweis gespeichert wird. Es erfolgt keine Speicherung in einer zentralen Datenbank, sodass jeder Nutzer seine biometrischen Daten immer bei sich trägt.

Wichtig ist zudem, neben dem Zugang, auch das Verlassen des Rechenzentrums zu erfassen, um temporäre Zugangsberechtigungen zu widerrufen und bei einer nicht regelkonformen Abmeldung den erneuten späteren Zutritt verweigern zu können. Die Risikominimierung und das Absichern der Rechenzentren für Notfallsituationen sowie das Einhalten gesetzlicher Compliance-Regelungen oder länderspezifische Audit-Regulierungen, verlangen von den Verantwortlichen eines Rechenzentrums eine enge Verbindung zwischen IT- und physischer Sicherheit der Gebäude zu schaffen.

Gesetzliche Vorgaben / Orientierungshilfen

Betreiber kritischer Infrastrukturen (KRITIS) sind laut §8a BSIG in der Pflicht, nachzuweisen, dass ihre IT-Sicherheit auf dem neuesten Stand der Technik ist. Viele Systeme, auf die wir uns verlassen, laufen zunehmend digital oder zumindest digital unterstützt ab. Das macht Infrastruktur zwar intelligenter, schneller und präziser, aber eben auch verwundbarer. Deshalb sind laut Bundesamt für Sicherheit in der Informationstechnik (BSI), Betreiber kritischer Infrastruktur in der Pflicht, diese bestmöglich abzusichern.
Auch aus Sicht des Datenschutzes muss sichergestellt werden, dass personenbezogene Daten sicher vor Missbrauch und nicht frei zugänglich aufbewahrt werden.

iCOGNIZE GmbH
Justus-von-Liebig-Straße 9
63128 Dietzenbach

+49 (0) 6074 310 3600

https://www.icognize.de
info@icognize.de

Zur Orientierung für Betreiber von Rechenzentren wurde mit der Europäischen Norm EN50600 ein Standard für die Einrichtung und Infrastruktur von Rechenzentren geschaffen. Diese Europäische Norm spezifiziert Anforderungen an und gibt Empfehlungen für die in EN 50600-1 definierten Rechenzentrumsbereiche, und die in diesen Bereichen eingesetzten Sicherungssysteme hinsichtlich des Schutzes gegen:

a) unautorisierten Zugang, indem sie konstruktionsbedingte, organisatorische und technologische Lösungen aufzeigt
b) Feuer innerhalb der Rechenzentrumsbereiche
c) andere umgebungsbedingte Ereignisse, ausgenommen Brände, aber einschließlich Gefährdungen durch elektromagnetische Beeinflussung, Vibration, Überflutung, Gas und Staub, welche
- innerhalb der Rechenzentrumsbereiche;
- außerhalb der Rechenzentrumsbereiche

Lösungen von iCOGNIZE

Zum Sicherheitskonzept eines Rechenzentrums gehört eine mehrstufige, biometriegestützte Zugangskontrolle. Hier kann die iCOGNIZE GmbH mit ihren Produkten und Lösungen einen wichtigen Baustein zur Umsetzung eines ausgereiften Sicherheitskonzeptes liefern.

Die Berührungslose Zutrittskontrolle mittels Handvene.

Der **Manuscan-Handvenenscanner** wird in einer Standard-Unterputzdose verbaut – so entsteht kaum mehr Aufwand als beim Einbau eines handelsüblichen Lichtschalters. Die Versorgung findet über Ethernet (PoE) statt. Die Leser sind an eine hutschienenfähige Authentication Unit (AU) angeschlossen, die in einem gesondert gesicherten IT-Raum im 19“ Rack betrieben wird. Er ist durch alle gängigen Hardware-Schnittstellen bestmöglichst auf die einfache Integration in bestehende Sicherheitsinfrastrukturen vorbereitet und gewährleistet durch die integrierten Soft- und Hardware Backupsysteme eine maximale Systemverfügbarkeit.

Bei positiver Authentifizierung (durch Scan der Handvenen in Verbindung mit RFID und/oder optional Eingabe eines PIN-Codes) wird den bestehenden Zutrittskontroll- und Protokollierungssystemen ein kompatibles Signal als Rückmeldung gegeben.

„Wir können auf diesem Wege sensible Türen mit Handvenenscannern sichern, ohne die gesamte Zutrittskontrollinfrastruktur austauschen zu müssen.“ – Dr. Alexander W. Lenhardt, CEO iCOGNIZE

Durch das einzigartige biometrische Merkmal „Handvenen“ bietet dieses System dem Anwender nicht nur maximale Sicherheit, sondern gleichzeitig höchsten Nutzerkomfort. Denn der ManuScan Indoor Handvenenscanner arbeitet kontaktlos und nichtinvasiv und sorgt mit seinem einzigartigen optischen Handpositionierungssystem für eine intuitive Nutzung und hohe Nutzerakzeptanz.

Vorteile der **ManuScan Indoor Handvenenscanner**

- RGB-LED Benutzerführung
- Sicherer als Irisscan-Verfahren
- FAR < 0,00008% (False Acceptance Rate)
- FRR < 0,01% (False Rejection Rate)
- Sabotagedetektion (Kontakt, Erschütterung)
- Ansteuerung von Rack-Schlössern, zum Beispiel Fath Mechatronics
- Einfache Integration in bestehende Systeme
- Integrierter PIN-Code-Leser
- Zertifiziert nach CE, BSI (Komponenten)

Die **Outdoorversion** unseres Handvenenscanners ist die erste Handvenenerkennungslösung für den Außeneinsatz und erfüllt sogar militärische EMV- und EMP-Anforderungen. Das aus V2A gefertigte Gehäuse ist allwetter- und sogar salzwasserbeständig, äußerst robust und mit einem integrierten thermischen Management für Temperaturen von -35° bis +85° geeignet.

Vorteile der **ManuScan Outdoor Handvenenscanner**

- In nahezu jeder Umgebung einsetzbar
- Hohe Benutzerfreundlichkeit
- Sicherer als Irisscan-Verfahren
- FAR < 0,00008% (False Acceptance Rate)
- FRR < 0,01% (False Rejection Rate)
- Einfache Integration in bestehende Systeme
- IP68 Standard
- Zertifiziert nach CE, BSI (Komponenten)

Vorteile beim Einsatz beider Produkte

- Pin-Codes können ausgespäht oder weitergegeben werden, dies kann mit den berührungslosen Zugangssystemen von iCOGNIZE nicht passieren.
- Die berührungslosen Scanner sind auch mit Hygienehandschuhen zu benutzen und schaffen so einen hohen Hygiene Standard.
- Eine Wartung muss nur einmal jährlich erfolgen.

Referenzen

Unsere Produkte sind im Internet-Knoten in Frankfurt am Main, den gemessen am Datendurchsatz Größten der Welt, in großer Zahl installiert und tragen dadurch zur Sicherheit dieser kritischen Infrastruktur in nicht unerheblichen Maße bei. Für weiter Informationen sprechen Sie uns jederzeit gern an.

iCOGNIZE GmbH
Justus-von-Liebig-Straße 9
63128 Dietzenbach

+49 (0) 6074 310 3600

https://www.icognize.de
info@icognize.de