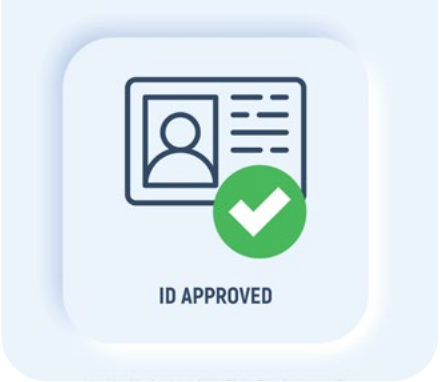


DER BESUCHER-CHECK-IN:
MANUELLES VS. DIGITALES BESUCHERMANAGEMENT

Millionen von Menschen bewegen sich täglich durch Unternehmenseinrichtungen wie Büro- und Verwaltungsgebäude, Produktionsstätten oder Logistikhallen, darunter unzählige externe Besucher – von Handwerkern und Lieferanten bis hin zu Gästen aus aller Welt. Mehr denn je stehen Unternehmen vor der Herausforderung, den Einlass von betriebsfremden Personen nicht nur effizient, sondern auch sicher und datenschutzkonform zu gestalten.

Manuelle Zutrittssysteme, bei denen das Empfangspersonal jeden Gast von Hand prüft und registriert, können mit den heutigen Anforderungen nicht mehr Schritt halten. Unternehmen setzen deshalb zunehmend auf digitale Besuchermanagement-Lösungen, um den Gebäudezutritt und die Besucherverwaltung sicher und effizient zu gestalten.

SICHERHEITSLÜCKE MANUELLES BESUCHERMANAGEMENT

Mit dem Hintergrund der Wirtschaftsspionage, Sabotageakten und Cyberattacken rückt der physische Zutritt zu Unternehmensgebäuden immer mehr in den Fokus von Sicherheitskonzepten. Um den Zutritt von unbefugten Personen zu verhindern, müssen Identitäten von Betriebsfremden und Fremddienstleistern zweifelsfrei überprüft werden. In der Praxis erfolgt dies oftmals nur durch die Sichtung eines „offiziellen“ Ausweisdokuments.

Bei manuellen Besuchermanagementsystemen obliegt diese Aufgabe den Sicherheitsmitarbeitern am Empfang. Die Prüfung eines Ausweisdokuments ist – insbesondere im internationalen Umfeld – jedoch nicht einfach (Personalausweis, Führerschein, Diplomatenpässe, Reisepässe, Aufenthaltstitel etc.). Denn der Ausweis muss nicht nur auf seine Gültigkeit, sondern auch auf Echtheit und die zweifelsfreie Identitätsübereinstimmung geprüft werden. Das ist nicht nur zeitaufwändig, sondern stellt auch eine enorme Sicherheitslücke dar, da das menschliche Auge von Natur aus nicht in der Lage ist, Ausweisdokumente auf ihre individuellen Echtheitsmerkmale wie bspw. Hologramme oder unsichtbare Sicherheitsmerkmale zu überprüfen. Auch die Kenntnis der unterschiedlichsten Sicherheits- und Erkennungsmerkmale (die steten Änderungen unterliegen) kann durch keine Person/kein Auge zuverlässig erfolgen. Das bloße Ansehen von Ausweisdokumenten reicht als Kriterium nicht aus, um einen zuverlässigen Identitätsabgleich zu erhalten, denn nur dieser bietet die Möglichkeit einer effektiven und sicheren Kontrolle.

Hinzu kommt immer auch der Abgleich, ob diese Person auch erwartet wird, weil eine Lieferung, ein Besuch oder die Durchführung einer Dienstleistung ansteht. Dies gestaltet sich mit E-Mails, mündlichen Absprachen und Notizzetteln ebenfalls schwierig. Sicherheitslücken sind da vorprogrammiert!

DIGITALE BESUCHERMANAGEMENTSYSTEME EFFEKTIV UND INDIVIDUELL NUTZEN

> DIGITALE BESUCHERMANAGEMENTSYSTEME MIT INTEGRIERTER IDENTITÄTSPRÜFUNG BIETEN EINEN DEUTLICH HÖHEREN SCHUTZ.

Digitale Zutrittsmanagementsysteme mit Identitätsprüfung verifizieren Personen nicht nur zuverlässig, sondern auch in einem Bruchteil der Zeit. Die Erstellung von Besucherkarten mit individuellen Zutrittsrechten erfolgt im Anschluss automatisch. Die Daten werden datenschutzkonform und standortübergreifend gespeichert.

Systeme dieser Art müssen immer zu den individuellen Unternehmensanforderungen passen. Themen wie „Sicherheit“ und „Effizienz“ sollten vor einer Implementierung ebenso berücksichtigt werden wie „Datenschutz“ und „Compliance“.

DIE IDENTITÄTSPRÜFUNG ERFOLGT IN 3 SCHRITTEN:

1. Ausweisverifizierung
2. Aufnahme 3D-Echtzeitportrait
3. Biometrischer Gesichtsabgleich

ERHÖHUNG DER SICHERHEIT DURCH ZUVERLÄSSIGE IDENTITÄTSPRÜFUNG

Digitale Besuchermanagementsysteme nutzen für die zuverlässige Identitätsprüfung Künstliche Intelligenz und biometrische Technologien wie bspw. einen biometrischen Gesichtsabgleich. Ausweise werden systemseitig auf ihre holographischen sowie sicht- und unsichtbaren Sicherheitsmerkmale geprüft. Sie stützen sich dabei auf 3 Komponenten: Infrarot-, UV-Licht sowie weißes Licht aus mehreren Richtungen, um bspw. Hologramme zu erkennen. Ein anschließender biometrischer Gesichtsabgleich – anhand

Biometrischer Gesichtsabgleich ©Essentry GmbH

eines Echtzeitportraits – dient dazu, die Person zweifelsfrei dem Ausweis zuzuordnen. Durch eine 3D-Tiefenkamera, die eine Lebendigkeitserkennung durchführt, lässt sich erkennen, ob beispielsweise eine Maske oder ein Foto vor die Kamera gehalten wird.

In unserem Downloadbereich haben wir weitere Informationen kostenfrei hinterlegt.

© Pixelshot - stockadobe.com

> **EIN DIGITALES BESUCHERMANAGEMENTSYSTEM KANN ANMELDEZEITEN AN REZEPTIONEN UM CA. 90 % REDUZIEREN.**

EFFIZIENTERE ABLÄUFE

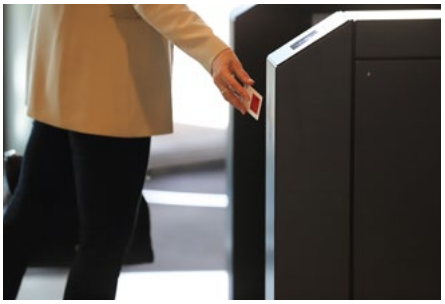
Ein manueller Check-in dauert durchschnittlich 15 Minuten, somit bietet ein digitales System auch enorme monetäre Vorteile. Empfangspersonal ist von monotonen Aufgaben befreit, Gästen werden lange Wartezeiten erspart und externe Dienstleister sind schnell einsatzbereit.

Zutrittsvoraussetzungen wie zum Beispiel Sicherheitsunterweisungen, Gesundheitsbriefings oder die Unterzeichnung von Vertraulichkeitsvereinbarungen (NDAs) können bereits vor dem Besuch digital durchgeführt und automatisch systemseitig abgelegt werden.

> **i** Die Europäische Datenschutzgrundverordnung setzt hohe Standards für die Verarbeitung personenbezogener Daten – auch dieser Thematik tragen derartige Systeme Rechnung. Bei der Wahl eines Besuchermanagementsystems sollte die gewählte Lösung höchsten Datenschutz- und Datensicherheitsstandards entsprechen.

Weiter auf der nächsten Seite. >>>

AUF EINEN BLICK: MANUELLE VS. DIGITALE PROZESSE		
ETABLIERTE UND OFTMALS MANUELLE PROZESSE	**WAS LEISTET EIN DIGITALER PROZESS?**	**WAS ERFOLGT NICHT IM RAHMEN DES DIGITALEN PROZESSES?**
Unzureichende Überprüfung des Identitätsdokuments (ID) Das menschliche Auge ist nicht in der Lage, Ausweise auf Sicherheitsmerkmale zu überprüfen.	**Lokale Verifizierung des Ausweises (ID)** Verschiedene Lichtquellen prüfen (auch internationale) Ausweise auf sichtbare und unsichtbare Sicherheitsmerkmale.	**Verifizierung des Ausweises (ID) in der Cloud** Bilder der vollständigen ID werden nicht gespeichert - weder lokal noch in der Cloud.
Manueller Gesichtsabgleich Das menschliche Auge ist bei der Durchführung von Gesichtsabgleichen wesentlich fehleranfälliger.	**1:1 Gesichtsabgleich** Der Abgleich erfolgt nur mit dem Bild auf dem Ausweis und der Person vor dem Gerät.	**Gesichtserkennung** Ein Abgleich erfolgt nur 1:1, niemals jedoch mit einer größeren Datenbank oder mit einer Vielzahl von Bildern.
Manuelle Datenverarbeitung und intransparente Aufbewahrungsrichtlinien Besucherdaten werden in mehreren Systemen oder Papierlogbüchern dokumentiert und gemeinsam genutzt. Die Aufbewahrungs- und Löschungsrichtlinien dieser Systeme sind nicht transparent.	**Erweiterte Datenschutzrechte und transparente Aufbewahrungsrichtlinien** Rechte und Aufbewahrungsrichtlinien müssen auf die Bedürfnisse der Kunden zugeschnitten sein. Nur autorisierte Personen haben Zugriff. Transparenter Überblick über die Aufbewahrungsfristen und Löschregeln.	**Gleiche Datenschutzrechte für alle und unbegrenzte Datenspeicherung** Der Informationszugriff auf Grundlage der zugewiesenen Berechtigungen muss beschränkt sein.
Intransparente Datenschutzerklärung und fehlende Einwilligungserklärung Datenschutzhinweise nur in Papierform verfügbar. Einwilligung der Benutzer wird oftmals nicht eingeholt oder nicht zentral gespeichert und ist somit nicht nachvollziehbar.	**Klare Datenschutzerklärung und Einwilligung der Benutzer** Von Beginn an wird auf die kundenspezifische Datenschutzerklärung hingewiesen. Vor der Verarbeitung sensibler Daten erfolgt die Einwilligung durch den Gast.	**Verarbeitung von sensiblen Daten ohne erteilte Einwilligung** Zu keinem Zeitpunkt dürfen sensible Daten vor der Einwilligung verarbeitet werden. Erst nach Einwilligung darf der Verifizierungsprozess eingeleitet werden.



Bildreihe: ©Essentry GmbH

Dieser Artikel ist mit freundlicher Unterstützung der Essentry GmbH, einem Anbieter von digitalen Besucher- und Zutrittsmanagementsystemen, entstanden.