- Anzeige -

IT&Production
Zeitschrift für erfolgreiche Produktion

SPEZIAL

Zeit und Zutritt



Bild: PCS Systemtechnik GmbH

Zutrittskontrolle und Zeiterfassung unter neuen Vorzeichen

pcs

Anforderungen an moderne Systeme

Vier Trends bei Zutrittskontrolle und Zeiterfassung

Die Zukunft von Zeiterfassung und Zutrittskontrolle entscheidet sich nicht mehr allein an der Tür oder am Terminal. Im Mittelpunkt steht das Gesamtsystem: Integrationsfähigkeit, Sicherheitsniveau, Betriebsmodell und die Fähigkeit, mit neuen Anforderungen mitzuwachsen. Unternehmen, die diese Kriterien in ihre Investitionsentscheidungen einbeziehen, können die Basis für mehr Sicherheit, geringeren Betriebsaufwand und Investitionssicherheit schaffen.

Vor diesem Hintergrund verändert sich der Maßstab, nach dem Unternehmen solche Systeme bewerten und sich für ein Produkt entscheiden. Nicht mehr allein die Funktion einzelner Geräte entscheidet. Wichtiger wird, wie sich das Gesamtsystem in die bestehende IT-Architektur einfügt und wie sicher, effizient und langfristig es sich betreiben lässt. Integrationsfähigkeit, Cybersecurity und Lifecycle-Management rücken deshalb bei Investitionsentscheidungen in den Fokus. Dabei lassen sich die Entwicklungen in vier wesentliche Trends einordnen.

1. Vom Inselbetrieb zur vernetzten Plattform

Immer wichtiger für die Entscheidung ist die Frage der Interoperabilität. Systeme müssen sich nahtlos in bestehende IT-Strukturen integrieren lassen und offen für Erweiterungen sein. Entscheidend ist dabei auch die Vernetzung mit angrenzenden Anwendungen: So kann die Zutrittskontrolle beispielsweise mit Besuchermanagement, Gefahrenmanagement oder Videoüberwachung verbunden werden. Standardisierte REST-APIs ermöglichen zudem, Zeiterfassungsdaten an übergeordnete ERP-Systeme zu übertragen und Echtzeitdaten für die Personaleinsatzplanung bereitzustellen. Integrationsfähigkeit wird so zu einem zentralen Qualitätsmerkmal der Systeme.

2. Cybersecurity wird zum Entscheidungskriterium

Mit der Integration steigen zugleich die Anforderungen an die Sicherheit der angeschlossenen Peripheriegeräte. Gerade die Zutrittskontrolle, die dem physischen

Bilder der Doppelseite: PCS Systemtechnik GmbH





Bei einer Modernisierung von Zeiterfassung und Zutrittskontrolle sind neue Anforderungen an Vernetzung und Cybersecurity zu beachten.

Schutz von Räumen und Gebäuden dient, muss deshalb besonders robust abgesichert werden. Dadurch steigen die Anforderungen an die Härtung der Systeme und an das Risikomanagement. Ziel ist es, Manipulationen, Abhörversuche und Sabotage möglichst früh zu erkennen und zu verhindern. Dazu gehören etwa verschlüsselte Kommunikation, Firewall- und Passwortkonzepte sowie signierte Firmware und ein abgesicherter Boot-Prozess. Solche Mechanismen schaffen eine durchgängige Chain of Trust und erschweren unbefugte Eingriffe in Hard- und Software.

Gleichzeitig steigen die regulatorischen Anforderungen. Der Cyber Resilience Act rückt die IT-Sicherheit digitaler Produkte über ihren Lebenszyklus in den Fokus. Hinzu kommen Anforderungen an Datenschutz, Dokumentation und Nachweisbarkeit, die im Rahmen des Risikomanagements zu berücksichtigen sind. Aktuelle Hardwaregenerationen sind an diesen Vorgaben ausgerichtet.

3. Terminals verbinden mit Cloud-Rechenzentren

Moderne Zeiterfassungsterminals lassen sich sicher an Cloud-Applikationen anbinden und in vernetzte Systemarchitekturen integrieren. Doch Cloud-Systeme verändern nicht nur die Anwendungen rund um Zutrittskontrolle und Zeiterfassung. Auch die Hardware selbst wird Teil cloudbasierter Betriebsmodelle.

Geräte können heute über eine SaaS-Plattform initialisiert, zentral verwaltet und kontinuierlich überwacht werden. Das vereinfacht die Inbetriebnahme und reduziert den Aufwand im laufenden Betrieb. Neue Applikationen und Sicherheitsupdates lassen sich zentral ausrollen, sodass bekannte Schwachstellen schneller geschlossen werden können. Auch für Projektverantwortliche ändert sich etwas. Der Bedarf an produktspezifischem Knowhow im Unternehmen sinkt, wenn Betrieb, Monitoring und Updates zentral über die Plattform des Herstellers erfolgen. So wird Hardware als Bestandteil der digitalen Infrastruktur zentral eingebunden und kontinuierlich betreut.

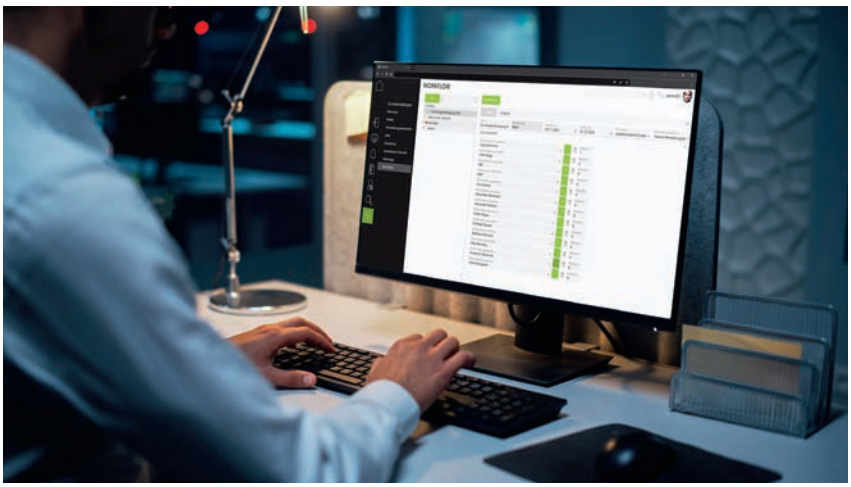
4. Identitäten auf Smartphones

Auch bei den Identmedien verändert sich der Standard. Der klassische Firmenausweis bleibt im Einsatz, wird aber zunehmend durch digitale Ausweise auf dem Smartphone ergänzt. Diese lassen sich schnell digital verteilen und bieten zugleich ein hohes Sicherheitsniveau. Besonders vorteilhaft ist das bei verteilten Standorten, mobilen Mitarbeitenden oder kurzfristig benötigten Berechtigungen. Mobile Credentials verschleißen nicht und reduzieren den Ausgabeaufwand. Gerade Wallet-Anwendungen, die mit NFC oder Bluetooth arbeiten, verbinden hier Komfort und Sicherheit. Für die Nutzung dieser Technologien sollten Zeiterfassungs- und Zutrittssysteme allerdings mit aktueller Lesertechnologie ausgestattet sein.

Modernisierung ohne Komplettaustausch

Eine Modernisierung kann neben einer erhöhten Sicherheit auch Vorteile bei Bedienbarkeit, Displaygröße und Installationsmöglichkeiten bieten. Dabei muss eine bestehende Infrastruktur nicht zwangsläufig vollständig ersetzt werden. In vielen Fällen ist ein schrittweiser Umstieg durch Kombinationen von diverser Hardware und Identmedien möglich. Kombiausweise können während der Migration sowohl ältere als auch aktuelle RFID-Technologien unterstützen. Alternativ lassen sich Lesesysteme einsetzen, die mehrere Verfahren parallel verarbeiten. So können Hardware und Identmedien nach und nach erneuert werden, ohne dass es zu organisatorischen Engpässen kommt. ■

PCS Systemtechnik GmbH
www.pcs.de

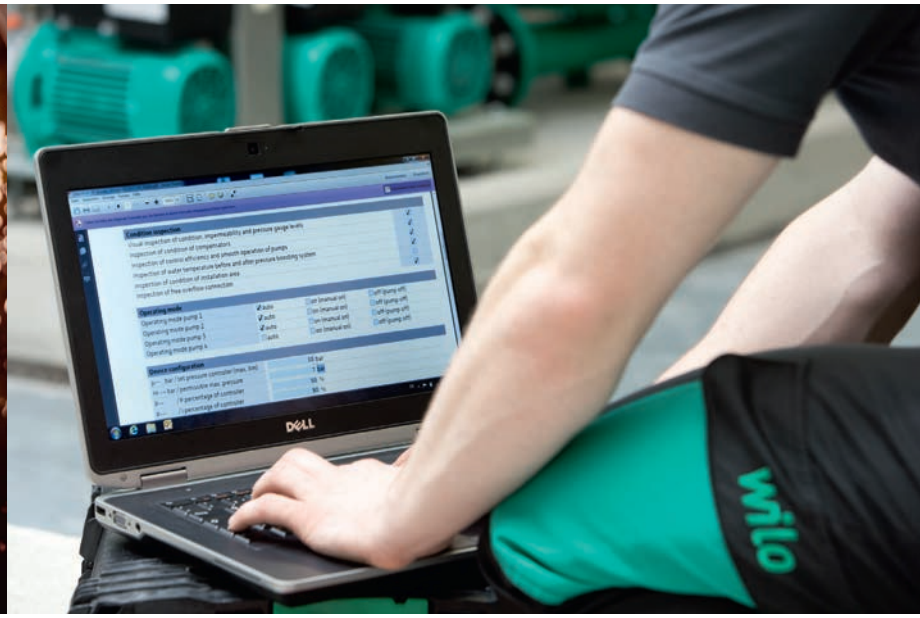


Neue Betriebsmodelle für Zeiterfassungs- und Zutrittskontrollsysteme als SaaS können kosteneffizient sein und Betriebsaufwand sparen.

Integrated Workplace Management-Systeme

Gebäudemanagement bei Wilo





Energiekosten, komplexe Anlagen und Nachhaltigkeitsanforderungen machen Gebäudemanagement zum Wettbewerbsfaktor. IWMS-Plattformen helfen dabei, Effizienzziele zu erkennen und zu erreichen.

Während Fertigungsprozesse oft digital gesteuert werden, besteht beim Gebäudemanagement häufig noch Nachholbedarf. Wartungen werden manuell koordiniert, Störungen reaktiv bearbeitet und Informationen liegen in unterschiedlichen Systemen vor. Dabei lassen sich gerade im technischen Gebäudebetrieb oft erhebliche Potenziale erschließen, was Resilienz, Effizienz, Nachhaltigkeit, Kontinuität und Betriebskosten betrifft. Voraussetzung dafür ist, dass relevante Daten auf einer Plattform zusammenlaufen. Integrated Workplace Management-Systeme (IWMS) bündeln Informationen zu Flächen, technischen Anlagen, Wartungsprozessen und Services und schaffen die Grundlage für datenbasierte Entscheidungen.

Das Beispiel Wilo

Wilo Group ist ein international tätiger Wassertechnologiekonzern mit Hauptsitz in Dortmund. Mit dem Aufbau seines neuen Unternehmenscampus entstand ein Standortkonzept mit Smart Factory, Verwaltungsgebäuden sowie Forschungs- und Begegnungszentren. Dabei stand auch das Gebäudemanagement im Fokus. 2019 entschied sich das Unternehmen, das bisher eingesetzte CAFM-System durch ein IWMS von Planon zu ersetzen. Zunächst wurde es On-Premises installiert. Im täglichen Betrieb zeigte sich jedoch, dass etwa der Aufwand für Hardware, Softwarepflege und Updates viele Ressourcen kostete. Gleichzeitig wuchsen die Anforderungen an mobile Anwendungen sowie an die künftige Einbindung von IoT-Sensorik und weiterer internationaler Standorte. Schließlich wurde in einem dreimonatigen Projekt auf die cloudbasierte Plattform des Anbieter gewechselt.

Zentral und verzahnt

Heute nutzt Wilo das System vor allem für Ticketmanagement, Wartungsplanung und Flächenmanagement. Gleichzeitig werden Daten aus der Gebäudeleittechnik und angeschlossenen IoT-Sensoren zentral erfasst und ausgewertet. Dadurch entsteht ein deutlich transparenteres Bild über den Zustand der technischen Infrastruktur. Administrativ hat sich auch einiges geändert. Software-Updates erfolgen automatisiert, mobile Endgeräte lassen sich leichter integrieren und durch den Wegfall mehrerer lokaler Server wurde die IT-Infrastruktur verschlankt. Gleichzeitig schafft die cloudbasierte Architektur die Voraussetzungen, weitere internationale Standorte auf derselben Plattform abzubilden – ein Pilotprojekt wird gerade umgesetzt. Auch für die Anbindung zusätzlicher Anwendungen wie Business Intelligence-Software oder für weitergehende Automatisierungen in der Gebäudeleittechnik sind die Weichen nun gestellt. n

Nancy Hartmann
Customer Success Managerin
Planon GmbH
www.planonsoftware.com

Bilder: Wilo Group

Kein Mittelmaß in der Sicherheit

Zutrittskontrollsysteme machen den Unterschied

Der deutsche Mittelstand hat es nicht einfach: Die Investitionsbereitschaft ist laut aktueller DZ BANK/BVR-Umfrage (August 2026) auf einen neuen Tiefstand gefallen. Folglich prüfen viele Unternehmen Investitionen besonders kritisch. Die Sorge vor Fehlinvestitionen, umfangreichen Projekten und möglichen Beeinträchtigungen des laufenden Betriebs führt dazu, dass notwendige Modernisierungsvorhaben häufig verschoben werden.



Bild: Interflex Datensysteme GmbH

Mit den kabellosen Schließkomponenten von Opendor lassen sich auch selten genutzte Zugänge ohne Mehraufwand in ein Sicherheitskonzept einbinden.

Irrglaube hemmt Investitionen

Davon betroffen sind auch Sicherheits- und Zutrittskonzepte. Denn in vielen Unternehmen prägen noch manuelle Prozesse, eine punktuelle Schlüsselverwaltung und fehlende Transparenz über Zuständigkeiten und Berechtigungen den Alltag. Grund hierfür: HR und Facility Management arbeiten oft mit getrennten Zuständigkeiten und unklaren Abstimmungen. Zudem erhöhen regulatorische Anforderungen wie NIS2 sowie steigende Prüf- und Nachweispflichten bei vielen Unternehmen den Druck, Sicherheitsprozesse transparent und nachvollziehbar zu dokumentieren.

Viele Mittelständler wissen, dass Zutrittskontrollsysteme ein elementarer Bestandteil moderner Sicherheitsarchitekturen sein sollten. Dennoch setzen sie auf veraltete Insellösungen, die nicht nur einen administrativen Mehraufwand, sondern auch schwer erkennbare Sicherheitslücken nach sich ziehen. Grund hierfür ist der Trugschluss, dass ein vernetztes Zutrittskontrollsystem den Komplettumbau oder die aufwendige Verkabelung bestehender Türen bedingt.

IF-6040: Für mehr Übersicht im Unternehmen

Das muss nicht der Fall sein: Bestehende Strukturen lassen sich schließlich gezielt weiterentwickeln. Entscheidend ist hierbei nicht die teuerste Technik, sondern dass jede Tür Teil einer zentralen Zutrittsstrategie ist. Eine wichtige Grundlage hierfür bildet die Management- und Systemplattform IF-6040 von Interflex.

Die zentrale Steuerungssoftware für rollenbasierte Zutrittsberechtigungen erleichtert die Administration auf beiden Seiten: Ändert die HR-Abteilung die Rolle eines Mitarbeitenden, ändern sich die betreffenden Zutrittsrechte automatisch. Das senkt den manuellen Mehraufwand und schafft Klarheit darüber, wer wo und warum Zutritt erhält. Kurzum: Berechtigungen lassen sich nachvollziehbar dokumentieren, Abstimmungen und Audits leichter vorbereiten.

Skalierbarkeit leicht gemacht

Die Modernisierung der eigenen Zutrittskontrolle lässt sich schrittweise und anforderungsgerecht angehen – angefangen bei den kritischen Unternehmensbereichen. Hier verfolgt Interflex einen klaren Ansatz:

- Analysieren, wo Übersicht und Kontrolle fehlen.
- Priorisieren, welche Zugänge zuerst gesichert werden sollen.
- Erweitern, indem bestehende Strukturen genutzt und Lücken gezielt geschlossen werden.

Sicherheit schrittweise erweitern

Die kabellosen Opendor-Komponenten erweitern die zentrale Zutrittsorganisation bis in jene Bereiche, die bislang nur mit hohem Aufwand integrierbar waren. Dazu zählen beispielsweise abgelegene Bereiche oder selten genutzte Zugänge. Unternehmen können diese Bereiche in ihre Sicherheitsorganisation einbinden und organisatorische Lücken gezielt schließen, ohne umfangreiche Baumaßnahmen oder zusätzliche Verkabelung. So wird aus einer fragmentierten Zutrittslandschaft Schritt für Schritt eine durchgängige und skalierbare Zutrittsorganisation.

Mehr Informationen

interflex
UPGRADES YOUR WORK

Kontakt

Interflex Datensysteme GmbH
Epplestraße 225 (Haus 3) • 70567 Stuttgart
Tel.: +49 711 1322-0
interflex.info@allegion.com
www.interflex.com

CNC-Spezialist Hundegger setzt auf Interflex-Software

Zutritt für 600 Mitarbeitende zentral administriert



Mit einem neuen Zutrittskontrollsystem in Verbindung mit einem visualisierbaren Berechtigungsmanagement hat der CNC-Spezialist Hans Hundegger seine Sicherheitstechnik modernisiert. Wo früher viel Verwaltungsarbeit nötig war, läuft heute vieles automatisiert und transparenter ab.

Während die Beschäftigten der Hans Hundegger AG ihrer täglichen Arbeit in der hochpräzisen Fertigung nachgehen, sorgt im Hintergrund eine neue Zutrittskontrolle für Sicherheit. Denn als beim Allgäuer Hersteller von Holzbearbeitungsmaschinen die Erneuerung eines älteren und störungsanfälligen Zutrittssystems anstand, haben die Verantwortlichen den Markt sondiert und sich schließlich für ein System von Interflex entschieden.

„Mit unserer bisherigen Zutrittskontrolle stießen wir zunehmend an Grenzen: Softwaretechnisch war sie eine Insellösung, und das Gesamtsystem war instabil", erklärt Michael Stechele, Manager IT-Operations des Unternehmens. Er verweist darauf, dass beim neuen System schon die robuste Hardware Vertrauen schafft. Und mehr noch die Software, die dahintersteht. Hundegger suchte nach einer Zutrittskontrolllösung auf dem neuesten Stand der Technik. Im Pflichtenheft standen außerdem eine intuitive Benutzeroberfläche, die Anbindungsmöglichkeit an das Personalmanagement und die Option, das Berechtigungsmanagement transparent zu visualisieren. Das System sollte moderne Identifikationsmedien unterstützen und mit einem Echtzeit-Monitoring inklusive Alarmfunktion das Sicherheitsniveau in sensiblen Bereichen erhöhen.

Anbindung an HR-Systeme

Heute nutzt das Unternehmen das Interflex-System IF-6040 als zentrale Managementplattform. Am Hauptsitz im Bayerischen Allgäu beschäftigt Hundegger rund 600 Mitarbeitende. Die Plattform administriert dort mehr als 700 Datensätze und ist nahtlos über Schnitt-

Bilder der Doppelseite Hans Hundegger AG



Am Hauptsitz von Hans Hundegger arbeiten rund 600 Beschäftigte. Die Zutrittsverwaltung erfolgt über das Interflex-System IF-6040.

stellen an die bestehenden HR-Systeme angebunden. „Das nimmt der Personalabteilung sehr viel Arbeit ab", sagt Stechele, „denn bisher musste sie die Zutrittsrechte manuell verwalten. Jetzt muss nur noch bei großen organisatorischen Änderungen händisch eingegriffen werden. Standardprozesse wie Onboarding, Offboarding oder Abteilungswechsel mit Veränderung von Zutrittsrechten werden automatisiert über Schnittstellen zwischen HR-Systemen und IF-6040 abgewickelt."

Remote Monitoring und Alarmierung

„Das Monitoring-Modul des Systems ermöglicht uns jetzt die Überwachung von Zugängen rund um die Uhr. Früher sind wir über das Werksgelände gegangen und haben vor Ort geprüft, ob Tore und Türen geschlossen sind. Heute kann ich den Status online checken und bekomme beispielsweise nach Betriebsschluss oder an Wochenenden einen Alarm auf das Smartphone, wenn etwas nicht stimmt", erläutert Daniel Klemens, Leiter Gebäudemanagement bei Hundegger. Mit wenigen Klicks kann er den Status prüfen und gegebenenfalls eine Tür oder ein Tor aus der Ferne verschließen. Während der regulären Betriebszeiten unterstützt das System mit der automatisierten, zeitgesteuerten Öffnung und Schließung von Werkstoren und Zugängen den Betrieb.

Sicherheit in kritischen Bereichen

Da am Hauptsitz des Unternehmens auch die Entwicklungsabteilungen, etwa für Software und Fertigungssteuerung, angesiedelt sind, regelt und überwacht das Organigramm-basierte Berechtigungsmanagement intern den Zutritt zu sensiblen Bereichen. Die Visualisierung des Systems ermöglicht die einfache Vergabe von Zutrittsrechten. Einmal festgelegt, weist die Software den Beschäftigten ihre Zutrittsberechtigungen automatisiert zu. Wechselt eine Person im Unternehmen die Abteilung oder Funktion, passt das System die Rechte selbsttätig an.

Erweiterbares System

Das Interflex-System lässt sich flexibel erweitern. Zur Inbetriebnahme hat Hundegger 74 alte Zutrittsleser gegen Online-Terminals der Baureihe IF-800 getauscht. Diese kabelgebundenen Terminals sind an hochfrequenten Werkstoren und Gebäudezugängen installiert und werden zentral über die Software gesteuert. An geschäftskritischen Zugängen wurden sie um Pin-Pads für eine Zwei-Faktor-Authentifizierung ergänzt. Im Innenbereich der Verwaltung kommen die Zylinder IF-281, die Türbeschläge IF-241 und die Türdrücker IF-271 zum Einsatz und dienen vorrangig dem Schutz sensibler Personen- und Unternehmensdaten.

Für die kosteneffiziente Erweiterung gesicherter Bereiche setzt Hundegger auf kabellose Schließkomponenten der Interflex-Produktfamilie Opendor in der Air-Variante. Sie lassen sich an Türen nachrüsten, ohne dass Kabel gezogen oder Schlösser getauscht werden müssen.

Ergänzende Komfortfunktionen

Die Ausweismedien für die Beschäftigten wurden vom Vorgängersystem übernommen und um neue Möglichkeiten erweitert. Zutrittschips mit begrenzter Gültigkeit für Dienstleisterfirmen sorgen für mehr Transparenz und Sicherheit im Besucherverkehr. Die Geschäftsführung und die Bereichsleiter des CNC-Spezialisten nutzen zum Zutritt zusätzlich die Interflex-App 'Key' auf ihren Smartphones, die beispielsweise Features wie das Öffnen von Toren aus dem Auto heraus bietet.

„Mit Interflex als Partner haben wir die richtige Wahl getroffen", bilanziert IT-Manager Michael Stechele. „Die Software bietet uns den besten Mehrwert für unsere Anforderungen. Neben der Passgenauigkeit haben uns die reibungslose Projektumsetzung und der zuverlässige Support voll und ganz überzeugt. Nicht zuletzt unterstützt die neue Zutrittskontrolllösung uns dabei, die Anforderungen von NIS2 zu erfüllen." n

Interflex Datensysteme GmbH
www.interflex.com

Jetzt anhören!

Praxistipps: On- und Offline-Zutrittssysteme vereinen

Funkvernetzung von Mechatronik einrichten



Für hohe Sicherheitsanforderungen wird ein aktives Monitoring des Zutrittssystems empfohlen.

Moderne Zutrittskontrollsysteme bieten durch die Kombination von mechatronischen Komponenten und drahtloser Funkvernetzung flexible Möglichkeiten für die sichere Zugangskontrolle. Doch wie lassen sich On- und Offline-Zutrittssysteme vereinen? Wir geben im Beitrag Praxistipps zur Funkvernetzung von Mechatronik und zeigen Beispiele, mit denen entsprechende Systeme realisiert werden können.

Moderne Zutrittskontrolle ist vielfältig: Der Standard sind verkabelte RFID-Zutrittsleser, die von einem übergeordnetem Zutrittsmanager verwaltet werden. Weit verbreitet sind auch mechatronische Schließsysteme, die Zutrittslesemodule direkt im Türgriff oder im Zylinder integrieren. Allerdings war die Vergabe von Zutrittsrechten bisher nur mit einer Zeitverzögerung möglich. Die Aktualisierung musste entweder direkt an der mechatronischen Komponente mit Hilfe einer Masterkarte erfolgen oder über ein verknüpftes Online-Zutrittssystem, dass aktuelle Zutrittsrechte aktiv auf Zutrittsausweise schrieb. Die mechatronische Schließsysteme waren nicht in Echtzeit mit der führenden Zutrittskontrolle verbunden.

Funkvernetzung verbindet

Abhilfe für die Zeitverzögerung schafft jetzt die Nutzung von Funkvernetzung für die mechatronischen Schließsysteme. So lassen sich jetzt die Effekte eines Online-Zutrittssystems mit den Vorteilen der Mechatronik verbinden. Zutrittsprofile lassen sich in Echtzeit aktualisieren, Einzeltüröffnungen oder Permanentzutritte lassen sich über die Software steuern. Zudem werden Zutrittsereignisse in der Zutrittssoftware dokumentiert. Um die mechatronischen Komponenten in das vernetzte Zutrittssystem einzubinden, werden Funk-Gateways genutzt. Sie kommunizieren drahtlos über eine Bluetooth-Verbindung mit dem Leser an der Tür. Das Gateway selbst wird über einen Zutrittskontrollmanager mit dem führenden Zutrittssystem verbunden. Diese Technologie ermöglicht eine kosteneffiziente Vernetzung mechatronischer Komponenten, z.B. wie bei der Produktlinie Intus Flex Air von PCS Systemtechnik.

Funkausleuchtung ist wichtig

Zum Start der Installation empfiehlt sich unbedingt, eine Funkausleuchtung des geplanten Standorts des Gates durchzuführen, um die beste Position zu bestimmen. Bei der Funkausleuchtung wird geprüft, ob Signalqualität und -stärke ausreichend ist, um eine stabile Kommunikation zwischen Mechatronik und Gateway zu gewährleisten. Bei der Durchfüh-

Bilder der Doppelseite: PCS Systemtechnik GmbH

rung einer Funkausleuchtung sind einige Hinweise zu beachten:

- Ausleuchtungen sollten möglichst vollständig möbliert durchgeführt werden! Ein Rohbau weist andere Messergebnisse auf. Auch alle Trennwände und Türen müssen bereits verbaut sein.
- Dämpfungseigenschaften berücksichtigen: Verschiedene Materialien dämpfen Funksignale unterschiedlich stark. Wärmeschutz-Verglasungen und Stahlbeton haben z.B. eine hohe Dämpfung, während Holz und unbeschichtetes Glas eine geringe aufweisen. Auch Wände und anwesende Personen können sich als signaldämpfend erweisen.
- Elektromagnetische Störquellen identifizieren: Geräte wie WLAN Access Points, drahtlose Telefone und Mikrowellen können Interferenzen verursachen, da sie im gleichen Frequenzbereich wie Bluetooth arbeiten.
- Adaptive Frequency Hopping nutzen: Intus Flex Air kann zwischen zufälligen Kanälen wechseln, um stabile Kommunikationskanäle zu finden.
- Signalstärke überwachen: Die Signalstärke (RSSI-Wert) sollte regelmäßig überprüft werden. Werte über –80dBm sind ideal für eine stabile Verbindung.
- Aufgrund vielfältiger Einflussfaktoren und Störquellen sind die Installationsszenarien für eine funkvernetzte Mechatronik genau zu prüfen. Als batteriebetriebenes System bietet sich Mechatronik vor allem für Zutrittspunkte in Gebäuden an, die nur mäßig frequentiert werden, z.B. einzelne Büros.

Verkabelte Zutrittskontrolle

Für Zutrittspunkte mit hohen Frequentierungen und hunderten oder tausenden Zutritten pro Tag rät PCS Systemtechnik zum Einsatz verkabelter Intus-Zutrittsleser. Auch für die Absicherung der Gebäudehülle im Außenbereich empfiehlt man den Einsatz von verkabelten Zutrittslesern, da sich Temperaturschwankungen negativ auf die Batterielaufzeiten auswirken. Das gleiche gilt für Sicherheitsszenarien, die eine Echtzeit-Überwachung von Türen notwendig machen. Nur verkabelte Zutrittskomponenten erlauben eine aktive Türstatusüberwachung im Sinne einer Risikoalarmierung. Bei sicherheitskritischen Zutrittspunkten wird der Einsatz von verkabelten Zutrittslesern mit Reed-Kontakten und Verschlussüberwachungen empfohlen, um ein aktives Monitoring im Sicherheitsleitstand zu ermöglichen. Denn ein Sicherheitssystem muss im Notfall einschreiten und aktiv auf Ereignisse in der Zutrittskontrolle reagieren. PCS bietet eine Software, die bei Abweichungen oder Auffälligkeiten in der Zutrittskontrolle eine Alarmierung aktiviert. Solche Auffälligkeiten sind z.B. die Ablehnung einer unberechtigten Karte oder ein mehrfach ungenehmigter Zutrittsversuch. Im Alarmierungsfall wird z.B. ein Wachdienst über eine Email-Benachrichtigung informiert. Eine weitere Möglichkeit ist die Kombination mit einem Gefahrenmanagement-System (GMS) über die OSDP- oder eine Webservice-Schnittstelle, die z.B. Türstatus-Meldungen überwacht. Diese Standard-Schnittstellen zur Anbindung externer Systeme helfen, die Zutrittskontrolle in die Infrastrukturen und Alarmierungsstrukturen zu integrieren. ■



Mechatronische Schließsysteme eignen sich für alle genormten Türen, auch für Glas- und Rauchschutztüren.

Dominik Jensen
Produktmanager
PCS Systemtechnik GmbH
www.pcs.com



Die IT&Production berichtet über alle Aspekte der Industrie 4.0 und digitalen Transformation. Der E-Mail-Newsletter hilft Entscheidern die Herausforderungen der digitalen Produktion zu bewältigen.
Jetzt Wissensvorsprung sichern:
tedo.link/itp-newsletter

IT&Production
Zeitschrift für erfolgreiche Produktion

Gesichtserkennungssysteme absichern

Biometrische Systeme vor Täuschungen schützen

Jetzt anhören!



Bild: ©ImageFlow/stock.adobe.com

Neben der korrekten Identifikation von Personen müssen biometrische Systeme auch Betrugsversuche abwehren. Eine besondere Bedeutung hat dabei die Presentation Attack Detection (PAD). Dabei handelt es sich um Angriffe auf Zugangskontrollsysteme, etwa durch Vorhalten gefälschter biometrischer Daten. Um kamerabasierte Gesichtserkennungssysteme robuster gegen Angriffe zu machen, gibt es verschiedene Analyse-Methoden, die dieser Beitrag beschreibt.

Die IT-Sicherheitsorganisation FIDO-Allianz (Fast IDentity Online) definiert in ihren Biometric Requirements drei verschiedene Angriffsarten (Level A, B und C), die nach Zeitaufwand, der notwendigen Expertise und des Zugangs zur Quelle der biometrischen Daten geordnet sind (siehe Tabelle).

Um ein System gegen solche Angriffe zu schützen, gibt es verschiedene Ansätze. Eine Möglichkeit ist es, mit weiteren Sensoren zusätzliche Informationen zu erfassen, wie etwa Tiefeninformationen. Ein Beispiel hierfür ist das in Apples iPhones verbaute FaceID, das einen Lidar-Sensor für die dreidimensionale Abtastung des Nutzergesichts verwendet. Weitere Möglichkeiten sind Infrarot-, Wärmebild-, Lichtfeld-, Multispektral- und Stereokameras. Der Einsatz von zusätzlichen Sensoren ist jedoch oft mit hohen Kosten für Entwicklung und Material verbunden und nicht in allen Designs realisierbar. Zudem sind Verbesserungen für bestehende Systeme selten eine Optionen. Zusätzlich bedroht der Fortschritt im 3D-Druck zunehmend auch die Sicherheit von Systemen, die mit Tiefensensoren oder 3D-Kameras ausgestattet sind.

Es gibt jedoch eine Reihe von Möglichkeiten, rein kamerabasierte Gesichtserkennungssysteme robuster gegen Angriffe aller drei FIDO-Arten zu machen. Dabei wird zwischen statischer und dynamischer Analyse unterschieden. Statische Verfahren werten dabei nur ein Bild aus, dynamische Verfahren verarbeiten Informationen aus mehreren Bildern gleichzeitig.

Die statische Analyse

Statische Methoden basieren darauf, dass sie gefälschte Gesichtsdaten – etwa Masken, Bildschirme oder Papierdruck – nutzen, die sich in ihrer Qualität und ihrem Aussehen von echten Gesichtern unterscheiden. Dabei geht es um Unterschiede in der Textur, aber auch bei der Reflexion und Absorption, sowie der Streuung und Brechung des Lichts durch das betrachtete Material. Ein Nachteil ist die starke Abhängigkeit von der Qualität der Aufnahme, die vor allem durch die Kameraauflösung und die Lichtbedingungen beeinflusst wird.

Durch die sich stetig verbessernde Verfügbarkeit von Beispieldaten für diese Aufgabe und maschinellem Lernen sind die Resultate dieser Verfahren mittlerweile sehr vielversprechend. Eine Einschränkung ist, dass sie nur bei bekannten Angriffsarten unter bekann-

ten Umständen wirklich gut funktionieren.

Da ein Modell nur mit Bildern bekannter Täuschungsversuche trainiert wird, ist ein Schutz gegen alle drei Angriffsebenen zwar möglich, neue Angriffsmethoden könnten diese jedoch wieder aushebeln. Ein entsprechendes System sollte daher dauerhafte Updatefähigkeit bieten.

	Quelle der biometrischen Charakteristika	Schwierigkeit	Art des Angriffs
Level A (leicht)	Fotos aus sozialen Medien	Zeit: < 1 Tag Expertise: Laie Equipment: Standard	Bild eines Gesichts auf Papier gedruckt / auf Mobilgerät angezeigt
Level B (moderat)	Hochauflösendes Foto, Videoaufnahme der Zielperson	Zeit: < 7 Tage Expertise: Geübt Equipment: Standard + Speziell	Papiermaske, Bewegtbild des Gesichts auf Bildschirm abgespielt
Level C (schwer)	Hochauflösendes Foto, 3D-Informationen des Gesichts der Zielperson	Zeit: > 7 Tage Expertise: Experte Equipment: Speziell + maßgefertigt	Silikonmaske, Theatermaske

Dynamische Analyse

Dynamische Methoden verwenden Informationen aus mehreren Frames der Kamera. Sie basieren also auf Bewegungen, die auf eine echte Person schließen lassen. Die Methode lässt sich weiter unterteilen in passive Methoden, die auf natürliche Bewegungen der Person reagieren, und aktive Methoden, die eine bestimmte Aktion des Nutzers fordern. Für die Nutzerfreundlichkeit eines Zugangskontroll- oder besonders eines Zeiterfassungssystems sollte man sich auf Methoden beschränken, die keine bis nur minimale aktive Kooperation des Nutzers erfordern.

Ein Ansatz, der sich auf die Erkennung von Level-B- und besonders auf Level-A-Angriffen fokussiert, nutzt Optical Flow. Diese Methode untersucht, ob die sichtbare Bewegung die Pixel der Rotation einer ebenen Fläche um sich selbst entsprechen, wie es bei einem Foto der Fall wäre. Andere auf Optical Flow basierende Methoden suchen eine Korrelation zwischen der Bewegung des Gesichts und des unmittelbaren Hintergrunds. Synchrone Bewegung von Gesicht und Hintergrund, wie bei Bewegungen von handgehaltenen Fotos oder Mobilgeräten, würden so als Angriff, und die rein unkorrelierte Bewegung als echte Person klassifiziert werden. Diese Methoden er-

- Anzeige -

Aug. Winkhaus SE

Mehr Sicherheit und weniger Risiko mit blueEvo von Winkhaus

Das elektronische Schließsystem blueEvo von Winkhaus umfasst eine ganzheitliche Sicherheitsarchitektur, ein vielseitiges Komponentenprogramm und eine intuitiv bedienbare Verwaltungssoftware. Auf diese Weise erfüllt es unterschiedlichste Anforderungen in einer Vielzahl von Bereichen.

Das elektronische Schließsystem blueEvo eignet sich ideal für den Einsatz in Industrie- und Verwaltungsgebäuden, Behörden und Einrichtungen des Gesundheitswesens. Die ganzheitliche Systemplattform umfasst flächenbündige Zylinder, Türbeschläge, Zutrittsleser und robuste Identmedien.

Die ganzheitliche Sicherheitsarchitektur sorgt für eine sichere Verschlüsselung und schützt vor Hackerangriffen. Eine flexible Anbindung an Drittsysteme bietet vielseitige Einsatzmöglichkeiten. Die Verwaltungssoftware BE blueControl ermöglicht mit ihrer intuitiven Benutzeroberfläche eine einfache Einrichtung, einen effizienten Betrieb und eine schnelle Schlüsselsperrung.

Vorteile für besondere Einrichtungen

Durch die Einhaltung der NIS-2-Richtlinie ermöglicht blueEvo Einrichtungen der kritischen Infrastruktur hinsichtlich der Zutrittsorganisation, ihre Datenintegrität sicherzustellen und sich vor unbefugtem Zugriff zu schützen. Die robusten Identmedien sind nach Schutzklasse IP68 zertifiziert und beständig gegen Desinfektionsmittel – das gewährleistet Langlebigkeit auch unter schwierigen Bedienungen.



Kontakt

Aug. Winkhaus SE
August-Winkhaus-Straße 31 • 48291 Telgte
Tel.: 0251 – 49080
www.blueEvo.com



Sicherheitsmaßnahmen sollten sich an der benötigten Sicherheitsstufe der Applikation orientieren.

fordern ein gewisses Mindestmaß an Nutzerbewegung, um effektiv zu sein.

Ein weiterer Ansatz setzt auf den Fokus der Kamera. Durch leichtes Verschieben der Fokusdistanz am erkannten Gesicht vorbei, kann durch Änderung der Pixelwerte zum fokussierten Bild ein Tiefenprofil erstellt werden. Die Genauigkeit hängt dabei von der Größe des Fokusbereichs der Kamera, und damit von dessen Blende, Brennweite und Sensorgröße ab. Bei dieser Methode wird zudem davon ausgegangen, dass zwischen den beiden Bildern keine wesentliche Bewegung in der Szene stattgefunden hat.

Diese Methoden wären jedoch nur bedingt oder überhaupt nicht in der Lage, Level-C-Angriffe mittels Masken erfolgreich abzuwehren. Hierfür existieren mittlerweile Methoden, die den menschlichen Herzschlag über die leichten Farbänderungen in kurzen Bildabfolgen einer RGB-Kamera ermitteln können. Die Nachteile dieser Methode sind der negative Einfluss von Bewegung, sowie der etwa fünfsekündige Betrachtungszeitraum den das System mindestens benötigt.

Presentation Attack Detection

Die vorgestellten Methoden haben alle verschiedene Vor- und Nachteile. Es ist daher naheliegend verschiedene Ansätze dynamischer sowie statischer Analyse parallel einzusetzen, um in allen Situationen hinreichende Sicherheit und Nutzbarkeit bieten zu können. Da die Gesichtserkennung und das Presentation Attack Detection-System in der Regel parallel laufen können, ist es üblich die Ergebnisse beider Systeme in der Entscheidung über die Echtheit des Authentifizierungsversuchs zu vereinigen, was die Genauigkeit weiter verbessern kann. Dass in der Praxis ein rein kamerabasiertes System ausreichend gegen Angriffe gesichert werden kann, wurde von Google demonstriert: Das ‘Face Unlock’ des Google Pixel 8 (Pro) genügt der höchsten biometrischen Sicherheitsklasse in Android und Nutzer können sich damit in Banking Apps authentifizieren.

Level-A PAD-System nur mit Face Detector

In der Praxis muss nicht zwangsläufig jeder Anwendungsfall für Gesichtserkennung gleichermaßen sicherheitskritisch sein. Da sich Zeiterfassungssysteme meistens in zugangsbeschränkten Bereichen befinden, sollten sie etwa gegen einfache Täuschungsversuche auf Level A, beispielsweise durch Schabernack treibende Arbeitskollegen, gewappnet sein.

Mit Embedded Hardware gegensteuern

Ein Experiment soll das Potenzial von Embedded-Hardware für Gegenmaßnahme aufzeigen: Der für die Erkennung und das Alignment der Gesichter bereits benötigte Face Detector erkennt mehrere Schlüsselpunkte, wie Augen, Nase, Mund und Ohren. Das verwendete BlazeFace-Modell zur Gesichtserkennung ist also bereits dazu fähig, die Lage des Kopfes im dreidimensionalen Raum hinter der zweidimensionalen Projektionsebene des Kamerabilds zu ermitteln. Diese Information kann in einem PAD-System genutzt werden, um festzustellen, ob sich das erkannte Objekt im Raum bewegt wie ein echter Kopf oder nur wie ein zweidimensionales Abbild. Die Grundidee ähnelt der beschriebenen auf Optical Flow basierenden Methode.

Im obigen Bild (S. 62) gezeigten Beispiel wurde der virtuelle Punkt zwischen den Ohren und der Nasenspitze verwendet, um die Lage des Kopfes im Raum zu visualisieren. Da der reale Abstand zwischen Nasenspitze und Mittelpunkt beider Ohren eine bekannte konstante Größe ist, kann mithilfe trigonometrischer Funktionen der relative Lagewinkel des Kopfes zur Projektionsebene berechnet werden. Durch gezieltes Drehen des Handyfotos wird das dargestellte Gesicht zwar verzerrt, der errechnete Lagewinkel des Kopfes wird dadurch jedoch nur unwesentlich verändert. Aufgrund der leichten Fehlerkennungen des BlazeFace-Modells durch die Verzerrung treten dabei relative Winkeldifferenzen von weniger als 10° auf. Bei einem echten Kopf sind meist schon innerhalb eines kurzen Zeitraums Unterschiede von über 20° zu beobachten, die unaufgefordert durch natürliche Bewegungen entstehen.

Diese Methode bietet einen effektiven Schutz gegen einfache Foto-Angriffe, wie in Level A nach FIDO definiert. Mehr als Level A ist damit aber in keinem Fall möglich, da sich dieses System durch eine Videoaufnahme täuschen lässt. Da jedoch lediglich das bereits implementierte BlazeFace-Modell genutzt wird, ist die zusätzlich benötigte Rechenleistung geringer, besonders im Vergleich zum hohen Rechenaufwand den die Optical Flow-Methode verursachen würde.

Fazit und Ausblick

Die Entwicklung eines auf Gesichtserkennung basierenden Zutrittskontroll- oder Zeiterfassungssystems ist mit überschaubaren Ressourcen realisierbar, wobei der Aufwand im Wesentlichen vom gewünschten Sicherheitsniveau abhängt. Sobald ein höheres Sicherheitsniveau erreicht werden soll, gilt es, entsprechend mehr Aufwand in die Presentation Attack Detection zu investieren. Da Angreifer potenziell ständig neue Methoden entwickeln, um die gängigen Methoden zu umgehen, muss das System im laufenden Betrieb mit Software-Updates aktualisierbar sein, um ausreichend gewappnet zu sein. ■

TQ-Systems GmbH
www.tq-group.com

Bild: © Cphotography/stockphoto.com

Jetzt anhören!

Biometrische Identifikation per Embedded-KI

Gesichtserkennung an der Maschine



Bild erstellt mit Google Gemini

Mit der Digitalisierung in der Industrie werden neue Schnittstellen zwischen Mensch und Technik möglich. Biometrische Verfahren wie Gesichtserkennung, die in Konsumgeräten und Flughäfen etabliert sind, sind nun auch in industriellen Anwendungen möglich.

Die digitale Fabrik verlangt nach neuen Schnittstellen – nicht nur zwischen Maschinen, sondern auch zwischen Menschen und der Technik. Eine besonders intuitive Form dieser Interaktion ist die biometrische Gesichtserkennung (Face Recognition). Sie ermöglicht es, Menschen eindeutig und sekundenschnell zu identifizieren – kontaktlos, sicher und effizient. Was in Smartphones und Flughäfen längst Standard ist, hält nun auch in der Industrie Einzug.

Was ist industrielle Face Recognition?

Face Recognition beschreibt die automatisierte Erkennung oder Verifikation einer Person anhand ihrer Gesichtsmerkmale. Während der Mensch visuell etwa 10 bis 20 Merkmale unterscheiden kann – Augenabstand, Kieferlinie, Nasenform –, kann ein KI-gestütztes System hunderte bis tausende mikroskopischer Marker erfassen: Porenstrukturen, Faltenmuster, Hautrelief, Symmetrieachsen. In Kombination mit KI-Algorithmen lassen sich diese Daten zu einem individuellen Face Print verarbeiten – einer Art biometrischem Fingerabdruck des Gesichts. Dieser wird mit vorhandenen Refe-

Zeit für Sicherheit.

DEXIOS

SOFTWARE FÜR GEBÄUDESICHERHEIT & ZEITERFASSUNG

MIX & MATCH

- Webbasierte Software
- Modularer Aufbau
- Offene Schnittstellen
- Intuitiv & cloudfähig

Treffen Sie uns vor Ort:
Protekt – Fachkonferenz
25.-26.11.2025
Leipzig

pcs

www.pcs.com

25 JAHRE IT&Production



Schafft Bewusstsein für IT-Sicherheit

„Seit einem Vierteljahrhundert zeigt IT&Production, wie die Kombination aus IT und industrieller Exzellenz neue Wege in der Produktion eröffnet. Von vernetzten Anlagen bis zu KI-gestützten Prozessen: Wenn Daten, Software und Maschinen gemeinsame Sache machen, wird aus Vision Alltag. Als IT-Sicherheitsfachmann weiß ich aber auch: Sicherheit ist dabei nicht Beiwerk, sondern die Voraussetzung für Qualität, Verfügbarkeit und Vertrauen. 'Security by Design', Zero-Trust-Prinzipien und gelebte Resilienz machen Produktionsumgebungen belastbar – und eröffnen Freiräume für Innovation und neue Geschäftsmodelle.

Gerade dafür braucht es starke Fachmedien. IT&Production schafft Bewusstsein für IT-Sicherheit, erklärt Hintergründe verständlich, ordnet aktuelle Entwicklungen ein und zeigt Best Practices – kritisch-konstruktiv und stets lösungsorientiert. Dieses kontinuierliche Aufklären macht Risiken beherrschbar und verwandelt Verantwortung in Wettbewerbsvorteile. Herzlichen Glückwunsch zum 25-jährigen Jubiläum! Bleiben Sie der Kompass für eine sichere, smarte und starke Industrie – auf die nächsten 25 Jahre."

Andreas Lüning
Mitgründer und Vorstand

G DATA CyberDefense AG

renzdaten abgeglichen, um Zugriffe, Berechtigungen oder Prozessschritte zu steuern.

Spezifische Anforderungen

Die industrielle Face Recognition unterscheidet sich in wesentlichen Punkten von Consumer-Lösungen. Sie muss auch unter schwierigen Lichtverhältnissen, etwa in Werkshallen, zuverlässig arbeiten und robust gegenüber Masken, Helmen oder Schutzbrillen sein. Darüber hinaus ist eine Offline-Fähigkeit bei gleichzeitig datensparsamer Verarbeitung erforderlich. Ebenso wird erwartet, dass die Technologie in sicherheitskritischen Umgebungen eingesetzt werden kann und sich zugleich problemlos in bestehende Maschinenlandschaften integrieren lässt.

Typische Anwendungsfelder

Die industrielle Gesichtserkennung eröffnet ein breites Feld an Anwendungen – überall dort, wo Sicherheit, Nachverfolgbarkeit oder Benutzerinteraktion gefragt sind. Typische Einsatzbereiche sind die Zutrittskontrolle und die Freigabe von Bereichen ebenso wie die Maschinenfreigabe und die individuelle Personalisierung von Arbeitsplätzen. Hinzu kommen Funktionen für die Zeiterfassung und Unterstützung beim Schichtwechsel. Auch die Erkennung von Emotionen zur ergonomischen Unterstützung sowie der Nachweis von Qualität und die Bereitstellung lückenloser Audit-Trails gehören zu den Anwendungsszenarien.

Wie funktioniert es technisch?

Ein typischer Ablauf bei Aitad-Systemen umfasst mehrere Schritte: Zunächst erfolgt die Gesichtserfassung, anschließend die Erkennung relevanter Merkmale. Daraufhin wird ein sogenannter Face Print erstellt, der mit den vorhandenen Einträgen in einer Datenbank abgeglichen wird. Das Ergebnis dieses Abgleichs ist entweder die Verifikation einer bekannten Identität oder die Identifikation einer Person. Optional kann zusätzlich eine Emotionserkennung integriert werden.

KI hält Daten im Haus

Viele marktübliche Systeme setzen auf Cloudverarbeitung, was mit Nachteilen verbunden sein kann: Datenschutzrisiken, Betriebsrat-Diskussionen, Abhängigkeit von Konnektivität, Latenzzeiten und schwer kalkulierbaren Betriebskosten. Bei Systemen des Anbieters Aitad erfolgt die Verarbeitung am Ort des Geschehens – auf einem Sensorboard, das oft kleiner ist als eine Visitenkarte. Ein Internetzugang ist dafür nicht erforderlich, was die Technologie auch für sensible Produktionsumgebungen geeignet machen soll. Keine personenbezogenen Daten verlassen die Anlage. Gleichzeitig sorgt der geringe Energieverbrauch dafür, dass die Systeme auch in IoT-Umgebungen und mobilen Einheiten eingesetzt werden können. Die Reaktionszeiten sind bis zu millisekundenschnell. Der Anbieter setzt auf integrierte Sensorsysteme, bei denen Kamera, Recheneinheit,



KI kann auch für den Mensch schwer unterscheidbare Personen wie z.B. Zwillinge zuverlässig erkennen.

Bilder der Doppelseite erstellt mit Google Gemini



Bei der Emotionserkennung wird ein 1:n-Vergleich durchgeführt: die aktuelle Aufnahme wird gegen viele verschiedene Aufnahmen abgeglichenen.

Speicher und Schnittstellen auf einer Platine gebündelt sind.

Warum das Ganze?

Aus welchen Faktoren sich der Return on Investment (ROI) ergeben kann: die Reduktion von Produktionsausfällen, etwa durch die Vermeidung von Maschinenmissbrauch, sowie Effizienzgewinne bei Zugängen und Freigaben. Hinzu kommen die Verringerung des Risikos von Compliance-Verstößen, eine erhöhte Arbeitssicherheit und der Wegfall physischer Zutrittsmedien. Gerade in Zeiten von Personalmangel, Digitalisierungsschub und wachsendem Sicherheitsdruck kann ein automatisiertes Identifikationssystem zum integralen Bestandteil der Produktion werden. ■

Aitad GmbH
www.aitad.de

Anzeige



Zuverlässige Zutrittskontrolle für den optimalen Schutz

- **IF-6040 Software-System:** Modular, skalierbar und cloudfähig. Unterstützt Anforderungen nach NIS2, KRITIS-DG & CRA.
- **Identitäts- und Berechtigungsmanagement**: Volle Kontrolle durch lückenlose, DSGVO-konforme Zutrittsreports.
- **Vielfältige Zutrittskomponenten:** Moderne Sicherheitstechnologien nach Stand der Technik für nachhaltigen Investitionsschutz.
- **Inhouse-Services:** Komplettlösungen von Beratung bis Wartung – alles aus einer Hand.

Hier mehr erfahren!

Interflex Datensysteme GmbH · 07 11 / 13 22-0 · www.interflex.com

BlueEvo von Winkhaus für kritische Infrastrukturen

Zutrittssystem als SINGLE SOURCE OF TRUTH

Höre was Du siehst!

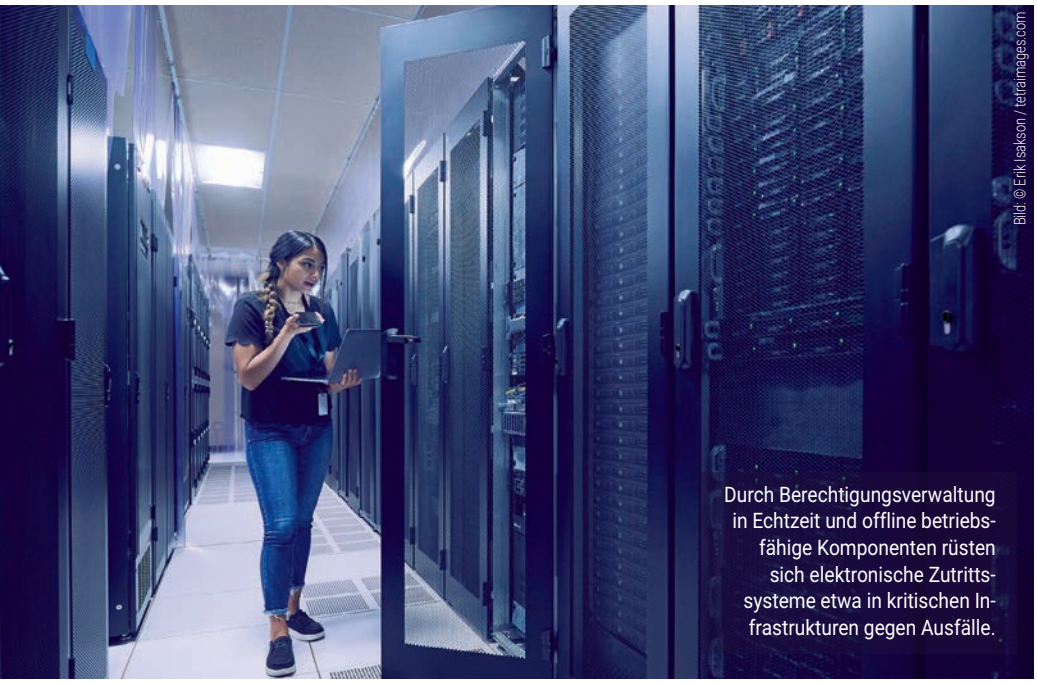


Bild: © Erik Isakson / tetraimages.com

Durch Berechtigungsverwaltung in Echtzeit und offline betriebsfähige Komponenten rüsten sich elektronische Zutrittssysteme etwa in kritischen Infrastrukturen gegen Ausfälle.

Systeme mit zentraler Datenquelle – einer Single Source of Truth – beschleunigen Prozesse und reduzieren Fehler. Das gilt auch für elektronische Schließsysteme wie BlueEvo von Winkhaus. Das System ist granular konfigurierbar, bis hin zum passenden Schutzniveau für kritische Infrastrukturen. Im Kern steht die flexible und effiziente Rechtevergabe, aber sowohl NIS-2 als auch DSGVO lassen sich mit dem System abbilden.

Technische Systeme lösen administrative Routineaufgaben automatisch, während sich Menschen komplexeren Fragen widmen. Ein Beispiel dafür sind elektronische Schließsysteme, bei denen IT-Systeme oft Aufgaben des Schließanlagenverwalters übernehmen. War das Vergeben und Entziehen von Schließberechtigungen früher Handarbeit, ist es heute großteils automatisiert. Der Verwalter konzentriert sich auf Sonderfälle und die physische Ausgabe von Schließmedien. Dabei müssen elektronische Zutrittssysteme zahlreichen Anforderungen gerecht werden. Wichtig ist die Möglichkeit, in der Verwaltungssoftware Nutzerrollen mit abgestuften Berechtigungen anzulegen. So hat der Administrator umfassenden Zugriff, während Vertreter nur Rechte wie das Sperren und Neuausgeben von Schließmedien erhalten. Gerade im Vertretungsfall ist die Nutzerfreundlichkeit der Software sehr wichtig. Sie reduziert potenzielle Anwendungsfehler und ist somit sicherheitsrelevant.

Maschinenbetrieb abgesichert

In modernen Zutrittssystemen lassen sich Stammdaten und Berechtigungen zentral verwalten. Diese werden durch die Fachabteilungen IT oder Personal gepflegt und automatisch mit dem Schließsystem synchronisiert. Dadurch können Zutrittsrechte zu Spezialräumen wie Labore automatisch spezifischen Nutzergruppen, in diesem Fall Mitarbeitenden der Entwicklungsabteilung, zugeordnet und bei Bedarf entzogen werden. Auch die Vergabe von Maschinenberechtigungen kann über die Einträge im zentralen Stammdatenverzeichnis geregelt werden. In Form einer Präsenzberechtigung, also einer Echtzeitabfrage des berechtigten Identmediums an der Maschine zur Laufzeit der Bedienung, wird sichergestellt, dass nur berechtigte Personen Maschinen einrichten, während andere diese ausschließlich bedienen können – ein wichtiger Beitrag zur Produktionssicherheit. Zeitlich begrenzte Schließberechtigungen bieten zusätzlichen Schutz: So können Zutrittsrechte über die Einstellung individueller Zeitprofile automatisch zu definierten Zeitintervallen aktiviert werden, etwa für externe Dienstleister oder Praktikanten. Auch zeitlich eingeschränkte Berechtigungen von Reinigungskräften lassen sich abbilden. In der Software lässt sich nachvollziehen, wer wann welche Bereiche betreten hat.

Sensible Bereiche im Blick

Das Zutrittssystem BlueEvo von Winkhaus nutzt Mifare Desfire EV3-Transponder als Basis für verschlüsselte Datenkommunikation von Identmedien. Der Einsatz einer Middleware erleichtert die Kommunikation mit Drittsystemen und ermöglicht die Verwaltung von Berechtigungen für Zutritt, aber auch Drucker und Fertigungsmaschi-

nen. Über die Restful-API der Middleware lassen sich je nach Berechtigung Buchungsdaten auslesen und der Zustand der Türen in sicherheitsrelevanten Bereichen wie Laboren ausgeben. Neue Türen können integriert werden, ohne die systemeigene Software öffnen zu müssen. Das JSON-Dateiformat sorgt für Interpretierbarkeit der Daten.

Für kritische Infrastruktur

Das Schließsystem kann On-Premise, auf Internet-verbundenen sowie abgekapselten PCs, Servern und virtualisierten Servern betrieben werden. Die Betriebsart von gekapselten Servern nutzen Unternehmen mit sehr hohem Schutzbedarf. Besondere Anforderungen bestehen in kritischen Infrastrukturen, die durch die NIS-2-Richtlinie geregelt sind. Krankenhäuser, Energieversorger und Rechenzentren etwa müssen weitreichende Maßnahmen zum Schutz ihrer Zugänge ergreifen, um auch bei Katastrophen zu funktionieren. BlueEvo ist auf diese Anforderungen ausgerichtet. Berechtigungen lassen sich in Echtzeit ändern und durch die Möglichkeit, Alarme auszugeben und kritische Bereiche zu überwachen, wird ein hohes Maß an physischer Sicherheit erreicht.

Vor Angriffen geschützt

Mifare Desfire EV3 in allen Komponenten, kryptografische Schlüssel und verschlüsselte Datenübertragung sind nur Teile des Schutz vor Cyberangriffen. Zusätzlich verfügen insbesondere flächenbündige Elektronikzylinder über den höchstmöglichen Schutz vor mechanischer Manipulation, gleichzeitig aber auch gegen Vandalismus und vor Verletzung, da keine Teile überstehen, die beispielsweise in einem Krankenhaus oder einer Schule Angriffsfläche für Verletzungen bieten könnte. Die Stabilität des Systems wird durch eine verschlüsselte Datenkommunikation zwischen Lese- und Steuereinheiten sichergestellt. Sogenannte Virtual Network Hubs, zu Deutsch Aufbuchleser, dienen der Informationsverteilung im virtuellen Netzwerk. Dieses wird zwischen der Verwaltungssoftware BE BlueControl, den Virtual Network Hubs und den Offline-Türkomponenten (Elektronikzylinder, Doppelknaufzylinder, Türbeschläge und Offline-Zutrittsleser) aufgebaut und nutzt die Identmedien zur Übertragung von Informationen und Befehlen. So werden Batteriestatusinformationen und Türbuchungen mit jedem Präsentieren eines Identmediums am Virtual Network Hub, der auch eine Türfunktion haben kann, im Hintergrund übertragen. Dabei erfolgt die Prüfung der Berechtigung und die Verlängerung eines aus Sicherheitsgründen möglichst kurzen Berechtigungsintervalls. Virtual Network Hubs können bis zu einen Monat ohne Serververbindung programmierte Zutrittsrechte an Identmedien aufbuchen. Batteriemonitoring und optional verfügbare Notstromversorgungen bieten zusätzlichen Schutz. Wartungsfreie, robuste Identmedien ohne Batterien sorgen für Langlebigkeit.



Moderne Identmedien mit verschlüsselter Kommunikation sorgen für eine sichere und flexible Zutrittskontrolle ohne Batteriewechsel.

Bilder: Aug. Winkhaus GmbH & Co. KG

Whitepaper zur NIS-2-Richtlinie

Im kostenlosen Whitepaper erläutert der Systemanbieter Winkhaus die Anforderungen an die physische Sicherheit, die sich aus der NIS-2-Richtlinie für Unternehmen und öffentliche Einrichtungen ergeben. Eine Checkliste, um potenzielle Risiken zu finden, ist enthalten. Zudem werden Ansätze dargestellt, um die Zutrittsorganisation NIS-2-konform zu gestalten.

https://tedo.link/XftBl



Die Komponenten sind auf den Schutz gegen Vandalismus und vor mechanischen und elektronischen Angriffen ausgerichtet.

Verfügbarkeit und Datenschutz

Im Sinne der Investitionssicherheit sollten Entscheider bei der Wahl des Zutrittssystems auf eine langfristige Verfügbarkeit von Türkomponenten und Identmedien sowie Ersatzteilen und zuverlässigen Support achten. Daher verspricht Winkhaus weitreichende Unterstützung und lange Verfügbarkeiten. Das BlueEvo-Schließsystem lässt sich zudem DSGVO-konform betreiben. Aufzeichnungen wie Türbuchungen und Änderungen lassen sich automatisiert regelmäßig löschen oder die Aufzeichnung von Türbuchungen für bestimmte Bereiche, etwa das Betriebsratsbüro oder einzelne Identmedien in einer Anlage, ausschließen. Zudem sind Sicherheitsmechanismen wie eine 4- oder 6-Augen-Anmeldung verfügbar, um den Zugriff auf sensible Daten zu kontrollieren. ■

Dr. Volker Brink
Leiter Produktmanagement Zutrittsorganisation
Aug. Winkhaus SE & Co. KG
www.winkhaus.com

Ratgeber zur Systemwauswahl

Digitale Identitäten verwalten und schützen

Höre, was Du siehst!



Für Cyberkriminelle sind digitale Identitäten ein begehrtes Ziel. Für Unternehmen gilt es daher, diese bestmöglich zu schützen. Dabei helfen Managementsysteme. Worauf es bei der Auswahl der Software ankommt, erläutert dieser Beitrag.

Digitale Identitäten sind zum begehrten Ziel von Cyberkriminellen geworden, die damit auf Unternehmensnetzwerke zugreifen. Durch die Übernahme der digitalen Identität eines Angestellten erlangen sie weitreichende Berechtigungen, die sie oft sogar noch erweitern können. Auch Produktionsbetriebe, die mittels digitaler Identitäten den Zugriff auf sensible Systeme regeln, stehen im Fokus der Angriffe. Egal, ob sich eine Designerin in ihr CAD-System einloggen will, der Buchhalter in die Finanzsoftware oder die Mitarbeiterin an der CNC-Fräse Zugriff auf die Vorlagen für die nächste Charge benötigt: Immer ist eine digitale Identität gefragt.

Identitäten schützen

Verwaltungssysteme unterstützen das Management sowie die Sicherung digitaler Identitäten. Moderne Systeme versprechen flexible Nutzerverwaltung, die sowohl die Integration lokaler Verzeichnisse als auch die Anbindung externer Systeme über standardisierte Schnittstellen erlaubt. Gerade dies ist bei Produktionsunternehmen von großer Bedeutung, weil Systeme oft über veraltete Schnittstellen verfügen.

Ein Managementsystem sollte die granulare Steuerung von Zugriffsrechten auf Ressourcen und Anwendungen sichern und die Möglichkeit bieten, Admi-

Bild: ©David Martinez/stock.adobe.com

nistratorenrollen zu definieren und Berechtigungen zu delegieren. So lässt sich das Prinzip der minimalst möglichen Berechtigung effektiv umsetzen. Hierbei erhält jeder Mitarbeiter nur genau die Berechtigungen, die er zur Erfüllung seiner Aufgaben benötigt.

Heutige Systeme bieten die Möglichkeit, individuelle Sicherheitsrichtlinien zu definieren und unterstützen deren Durchsetzung. Auch eine revisionssichere Protokollierung aller Aktionen im Zusammenhang mit der Verwaltung von Identitäten und Berechtigungen ist erforderlich. Darüber hinaus sollte die Software mit einer wachsenden Anzahl von Nutzern, Anwendungen und Daten skalieren. Die Unterstützung offener Standards und Schnittstellen zahlt wiederum auf die Integration in bestehende IT-Landschaften ein.

Multi-Faktor-Authentisierung

Die Kontrolle und Authentifizierung digitaler Identitäten sind weitere kritische Aspekte. Wegen menschlicher Gewohnheiten, wie der Verwendung schwacher Passwörter, darf die Sicherheit nicht den Einzelnen überlassen bleiben. Multi-Faktor-Authentisierung (MFA) kann hier helfen. Auch eine gänzlich passwortlose Anmeldung, etwa mithilfe einer Hardware-Komponente ist eine akzeptable Praxis. Dies ermöglicht nicht nur eine Anmeldung auf verschiedenen Plattformen, ohne sich mehrere Passwörter merken zu müssen, sondern sorgt für ein möglichst sichere Authentisierung.

Ohne zusätzliche Sicherheitsfaktoren im Rahmen einer MFA bleiben Passwörter eine potenzielle Schwachstelle. Allerdings würde die Implementierung von MFA für jede Anwendung die gewonnene Benutzerfreundlichkeit wieder zunichtemachen und der Aufwand wäre enorm und teilweise technisch nicht machbar.

Zusätzliche Sicherheit

Die Kombination eines Single-Sign-On-(SSO-) Systems mit MFA bietet ein hohes Maß an Sicherheit. Da der zweite Faktor bei SSO nur einmalig abgefragt wird, hält sich die Beeinträchtigung des Nutzungserlebnisses in Grenzen. Heutige SSO-Tools bieten Unternehmen eine breite Palette integrierter Authentifizierungsverfahren – von Einmalpasswörtern (OTP) über Hardware-Token nach WebAuthN-Standard bis hin zu passwortlosen Verfahren wie Passkeys. Letztlich werden sich nur solche Authentifizierungssysteme langfristig als praktikabel erweisen, die sowohl für Nutzer komfortabel sind als auch IT-Verantwortlichen ein einfaches Management und umfassende Kontrolle ermöglichen.

Fehler vermeiden

Eine letzte Eigenschaft, die eine solche Software aufweisen sollte, wurde erst kürzlich durch das Crowdstrike-Desaster ins Bewusstsein der Öffentlichkeit gerufen. Zur Erinnerung: Am 19. Juli 2024 sorgte ein fehlerhaftes Konfigurationsupdate von Crowdstrike bei Windows-Systemen für massive Probleme. Rund um den Globus kam es zu Systemabstürzen. Betroffene Rechner konnten nicht mehr oder nur unvollständig gestartet werden.

Dieser Vorfall zeigt, wie gefährlich es sein kann, sich (freiwillig) in die Abhängigkeit von wenigen Anbietern zu begeben. Open-Source-Software (OSS) und offene Standards bieten eine Alternative.

Open-Source-Software bietet unterschiedliche Möglichkeiten: Die Überprüfbarkeit des Quellcodes durch eine breite Community unterstützt die Sicherheit und ermöglicht die Anpassung an spezifische Bedürfnisse. Zudem verringert der Einsatz die Abhängigkeit von einzelnen Anbietern. Allerdings sollte das 'Viele-Augen-Prinzip' beachtet werden, sodass nicht nur ein einzelner Maintainer die Kontrolle hat.

OSS stellt Unternehmen auch vor Herausforderungen. Dazu gehören fehlender Kundendienst, aufwändige Eigenentwicklungen und oft mangelnde Benutzerfreundlichkeit. Hierfür gibt es SSO-Anbieter, die Produkte auf Open-Source-Basis sowie die dazugehörigen Service-Leistungen im Portfolio haben. Zu guter Letzt zählt bei der Anbieter-Auswahl die Verfügbarkeit der Software sowie die Einhaltung von BSI-Vorgaben. ■

Elmar Eperiesi-Beck
Management – Vertrieb & Strategie
Bare.ID GmbH
www.bare.id/de

Zeit für Sicherheit.



SOFTWARE FÜR
GEBÄUDESICHERHEIT
& ZEITERFASSUNG

MIX & MATCH

- Webbasierte Software
- Modularer Aufbau
- Offene Schnittstellen
- Intuitiv & cloudfähig

PCS Systemtechnik
Von der Beratung über die Umsetzung bis zur Wartung.

pcs

www.pcs.com