77500

ISSN 1866-2420

SECURITY INSIGHT

FACHZEITSCHRIFT FÜR UNTERNEHMENSSICHERHEIT UND WIRTSCHAFTSSCHUTZ

TITELTHEMA

BRICS – eine unberechenbare Erfolgsgeschichte

Mai/Juni
03/2021
EPr. 15,– €

www.prosecurity.de

dass er einen neuen mobilen Schlüssel erhalten hat und für welche Türen er berechtigt ist. Er muss dann nur noch das Smartphone vor den elektronischen Beschlag, Zylinder oder Wandleser halten und via App die Kommunikation starten.

450 Zutrittspunkte

Derzeit sind auf dem gesamten Campus 450 Zutrittspunkte in die Lösung eingebunden. „An rund 20 Eingängen befinden sich SALTO Online-Wandleser samt Türsteuerungen. Etwa 380 Türen, vor allem Innentüren, sind mit elektronischen Beschlägen ausgestattet, davon ca. 70 mit XS4 One Beschlägen und rund 310 mit XS4 Original Beschlägen. Die meisten XS4 One Beschläge sind über BLUEnet funkvernetzt und für SVN-Flex aktiviert. Damit werden sie zugleich als kabellose Aktualisierungspunkte im SVN genutzt, was der Schule zusätzliche Flexibilität und Sicherheit bietet“, führt Didier Kauer aus. Darüber hinaus sind noch etwa zehn elektronische SALTO GEO Zylinder an Glasschiebetüren und auf den Parkplätzen sowie zehn elektronische Spindschlösser XS4 Locker an Schlüsselschränken (z.B. für die Campus-Busse) im Einsatz.

Als Identifikationstechnologie fungiert MIFARE DESFire EV1. Die Badges dienen parallel zur Zutrittskontrolle auch für die Kopierer und das Bibliothekssystem.

Für das Management der Zutrittsrechte von Schülern, Angestellten und Externen verwendet das College die Software ProAccess SPACE von SALTO. „Um die komplexen Strukturen abzubilden, haben wir sechs Türpartitionen und sieben Nutzerpartitionen eingerichtet. Damit können wir neben internen Zuständigkeiten der Mitarbeiter auch die unterschiedlichen Nutzungsszenarien während der Schulzeit und während der Ferien abbilden. Während unserer ‚Summer School‘ befinden sich z.B. wesentlich mehr externe Personen auf unserem Campus als sonst. Für die Internatsgebäude gelten dann ebenfalls andere Berechtigungen als während der Schulzeit, weil ja keine Schüler da sind“, erläutert John Gerhardt. Die Zutrittsrechte werden nach einem festen internen Prozess über mehrere Ebenen zugewiesen, geprüft und freigegeben und regelmäßig einer Revision unterzogen.

Viele Integrationen

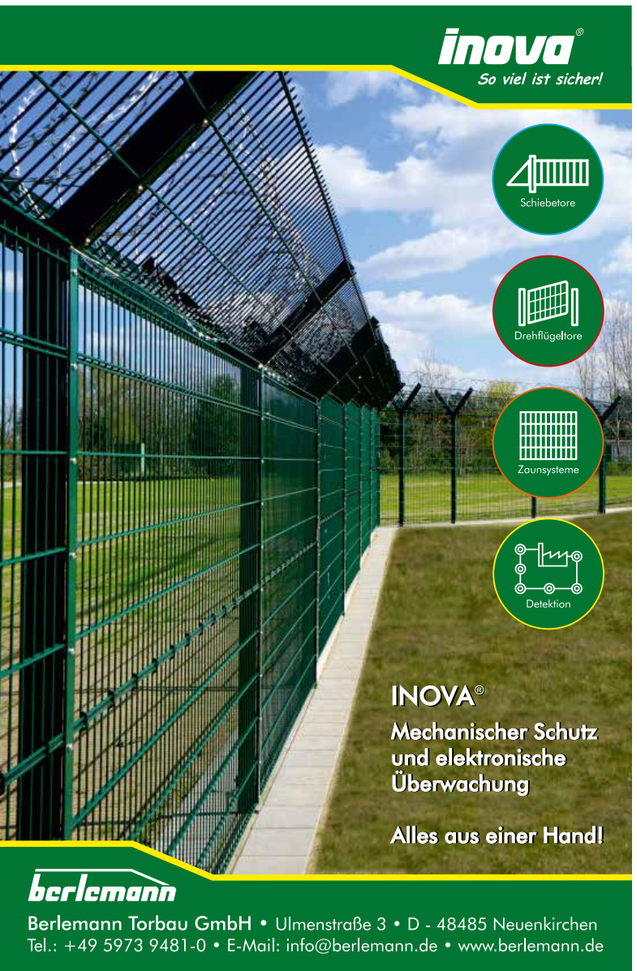
Die Software findet John Gerhardt „fantastisch, die hat letztlich den Ausschlag für die Anschaffung der SALTO Zutrittskontrolle gegeben. Und man sieht mit jedem neuen Release Fortschritte. Da werden nicht nur Fehler behoben, sondern immer neue Funktionen hinzugefügt. Obendrein läuft sie sehr stabil und bietet eine sehr gute Integrationsplattform, die wir ausgiebig nutzen“. Die Software ist mit etlichen Drittsystemen verknüpft: mit dem ERP-System für die Stammdaten, dem Active Directory für die Berechtigungsstruktur, dem Ticketsystem für Besucher und Weiteren, die z.T. Daten aus dem Zutrittssystem verwenden.

Er setzt überdies z.B. das Add-on „Alarm Events“ ein, womit ausgewählte Personen Meldungen zu bestimmten Ereignissen erhalten, u.a. bei niedrigem Batteriestand, was den Wartungsaufwand reduziert. Zu den besten Funktionen von ProAccess SPACE zählt John Gerhardt passenderweise die Integrationsmöglichkeiten. „Außerdem machen wir von den Zeitzonen reichlich Gebrauch. Denn während der Unterrichtszeiten dürfen Schüler praktisch keine anderen Räume als ihre Klassenzimmer betreten und haben während dieser Zeitfenster keine Zutrittsrechte für Räume, die sie sonst betreten dürfen.“

Zuverlässige Sicherheitslösung

Insgesamt zieht John Gerhardt ein positives Fazit zur Einführung der elektronischen Zutrittslösung: „Wir haben unsere Flexibilität sowohl IT-seitig als auch bei der Nutzung unserer Räumlichkeiten zurückgewonnen. Und es handelt sich um eine zuverlässige Sicherheitslösung, mit der wir physisch – durch differenzierte Zutrittsrechte – und digital – über die Sicherheitsarchitektur des Systems selbst – unseren Schülern, deren Eltern und unseren Mitarbeitern ein hohes Maß an Schutz bieten können. Alles Dinge, die wir als maßgeblich bei den Anforderungen angesehen haben und von denen wir jetzt profitieren.“ ●

▶ www.saltosystems.de



Was ein Schweizer Käse mit der Sicherheit beim Zutrittsmanagement zu tun hat

Wie Löcher in einem Schweizer Käse weisen heutige Zutrittsmanagementsysteme und -prozesse nachweislich Schwachstellen auf, die weitreichende Risiken für die physische Sicherheit, Daten- und Cybersicherheit darstellen. Unternehmen sollten ihre mehrschichtige Zutrittssicherheitsstrategie mit einem vollautomatischen Zutritts- und Besuchermanagement inklusive Identitätsverifikation ergänzen, um Mitarbeiter, Waren und geistiges Eigentum ohne Kompromisse zu schützen und diese Löcher zu schließen.

Spezifische Sicherheitsanforderungen an den Zutritt

Dem Zutritt als erste Verteidigungslinie für Unternehmen kommt eine besondere Bedeutung zu und muss höchsten Sicherheitsanforderungen entsprechen. Dies wird durch gesetzliche und regulatorische Vorgaben forciert, die beispielsweise den Zutritt zu Produktions-, Erzeugungsanlagen und Lagerhallen streng reglementieren sowie die Angriffsfläche für Cyberattacken über physische Schwachstellen reduzieren. Zusätzlich zeigt die Corona-Pandemie, wie anfällig Unternehmen für Betriebsunterbrechungen ohne entsprechende Maßnahmen sein können. Zwangsquarantäne von ganzen Belegschaften und Betriebsschließungen wurden real und nicht umsonst regelt der SARS-CoV-2 Arbeitschutzstandard die Anforderungen an die Dokumentation von Betriebsfremden und erforderliche Unterweisungen zu Hygienemaßnahmen und -regeln.

Die Datenschutzgrundverordnung (DSGVO) stellt einen weiteren Aspekt des Zutrittsverfahrens in den Vordergrund: personenbezogene Daten. Auch knapp drei Jahre nach der Einführung der DSGVO finden sich noch viele Unternehmen, die Besucherdokumentationen mithilfe eines Klemmbretts lösen, auf dem alle Besucher an diesem Tag für jeden weiteren Besucher einsehbar sind. Die Nichteinhaltung der DSGVO kann erhebliche Geldstrafen sowie Imageschäden zur Folge haben, insbesondere wenn – beispielsweise – eine zweckgebundene Datenverarbeitung nicht eingehalten wird oder gar Daten gestohlen werden. Infolgedessen hat sich durch die DSGVO auch die Anforderung an die Datensicherheit beim Zutritt signifikant erhöht.

Status quo und involvierte Systeme

Antiquierte, manuelle und ineffiziente Prozesse prägen heutzutage das Bild beim Zutritt. Die Folge sind lange Wartezeiten für Betriebsfremde, überlastete Werkschutzmitarbeiter und hohe Prozesskosten. Durch Covid-19 kommt zusätzlich die Gefahr durch den direkten Kontakt mit potenziellen Virusträgern hinzu, der Empfangsmitarbeiter ausgesetzt sind.

Zur Beschränkung des Zutritts zu Gebäuden und Einrichtungen verfügen die meisten Organisationen über verschiedene Systeme und Prozesse. Meistens werden sowohl Zutrittskontrollsysteme, in denen Profile und Zutrittsberechtigungen verwaltet werden, als auch physische Barrieren wie z.B. Speedgates und Keycards verwendet, um den Zutritt zu kontrollieren. Die „Best Practice“ im Zutrittsmanagement von Unternehmen besteht aus einem mehrschichtigen Sicherheitsansatz, der aus mehreren Systemen besteht. Alle diese Systeme haben ihre Stärken und Schwächen. Die Schwächen werden zumeist durch die Vielzahl der anderen Systeme (Barrieren) neutralisiert bzw. gemindert. Der Status quo der Zutrittsprozesse besteht aus den folgenden Systemen:

1. Identity und Access Management (IAM)
   Mitarbeiterverzeichnisse wie z.B. Microsoft AD oder Azure AD verwalten digitale Berechtigungsprofile, um zu steuern, wer Systeme mit welchen Berechtigungsprofilen nutzen darf.
2. Besuchermanagementsystem
   Manuelle oder digitale Verwaltung des gesamten Zyklus des Besucher- und Fremdfirmenbetriebs, einschließlich Gesundheits- und Sicherheitsschulungen, um die Einhaltung von Vorschriften zu gewährleisten.

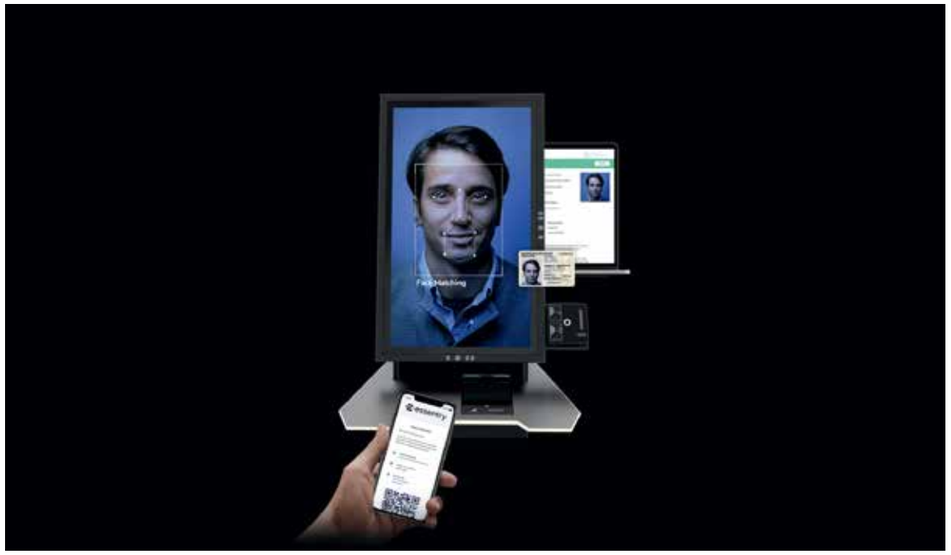


Bild: Essentry

3. Zutrittskontrollsystem
   Das Zutrittskontrollsystem generiert eine RFID- oder NFC-Karte mit vordefinierten Zutrittsrechten, die dem Karteninhaber den Zutritt ermöglicht. Neuere Systeme ermöglichen darüber hinaus bereits den Zutritt über QR-Codes oder Bluetooth-Technologie.
4. Rezeptions- und Sicherheitspersonal
   Das Personal prüft, ob eine Autorisierung für den Besuch bzw. Zutritt vorliegt, erstellt die Zutrittskarten und Besucherausweise und benachrichtigt die Gastgeber beim Eintreffen.

Das Problem der nicht verifizierten Identität

Bei näherer Betrachtung dieses Setups wird jedoch klar, dass keines der involvierten Systeme die Identität der Person verifiziert. Eine Schwachstelle, die Unternehmen durch zusätzliches Personal zu lösen versuchen - die manuelle Personen- und Identitätskontrolle durch den Werkschutz oder Empfangsmitarbeiter. Aber auch hier werden Kompromisse in Bezug auf die Sicherheit eingegangen, wenn Ausweisdokumente lediglich einer Sichtprüfung unterzogen und nicht technologisch auf Echtheit überprüft sowie ein manueller Abgleich mit der Person durchgeführt werden.

Sowohl Zutrittskontroll- als auch Besuchermanagementsysteme haben diese Schwachstelle der nicht-verifizierten Identitäten gleichermaßen und Personenkontrollen gehen mit zusätzlichem Personaleinsatz einher. Die Kosten, Personalknappheit sowie kurzen Verweildauern auf diesen Positionen erschweren das Zutrittsmanagement zusätzlich.

Mit künstlicher Intelligenz die Sicherheitslücken nachhaltig schließen und Prozesse automatisieren

Mit Hilfe von künstlicher Intelligenz kann die Identitätsverifikation automatisiert und Ausweisdokumente (Personalausweise, Reisepässe, Führerscheine, etc.) auf Echtheit geprüft und mit der einzulassenden Person mittels biometrischem Gesichtsabgleich vollautomatisch abgeglichen werden. Die Echtheit von Ausweisdokumenten kann nur mit speziell dafür vorgesehenen Scannern, die mit verschiedenen Lichtquellen (infrarotes, ultraviolettes und weißes Licht) ausgestattet sind, um alle Sicherheitsmerkmale zu erkennen, überprüft werden. Darüber hinaus sollten zum biometrischen Gesichtsabgleich nur 3D-Kameras eingesetzt werden. Diese 3D-Kameras identifizieren die Höhen und Tiefen des Gesichts einer Person, um nicht durch ein gedrucktes Bild getäuscht zu werden.

Sofortige Vorteile durch Einsatz dieser Technologien

Die beschriebenen Technologien erhalten bereits Einzug in vielen Situationen des täglichen Lebens. Daher ist bereits die Mehrheit der adressierten Personengruppen mit den Anwendungen dieser Technologien (z.B. an Flughäfen) vertraut und wissen intuitiv, wie diese zu bedienen sind. So lässt sich der voll automatisierte Registrierungsprozess an einem Self-Service Kiosk mit einem

> **„Antiquierte, manuelle und ineffiziente Prozesse prägen heutzutage das Bild beim Zutritt. Die Folge sind lange Wartezeiten für Betriebsfremde, überlastete Werkschutzmitarbeiter und hohe Prozesskosten.“**

großen und - auf das Corporate Design des Unternehmens - angepassten Touchscreen so bequem wie möglich gestalten, um sowohl das Besuchererlebnis als auch die Wahrnehmung des

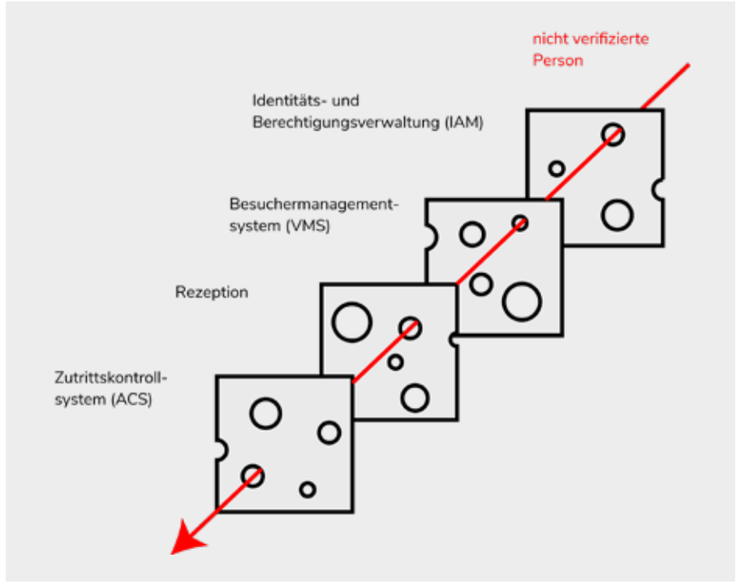
gastgebenden Unternehmens zu steigern. Durch diesen Self-Service Kiosk können bis zu 90% der Prozesszeit eingespart werden und auch unbemannte Rezeptionen können realisiert werden. Integriert in bestehende Zutrittskontrollsysteme kann der Self-Service Kiosk Namensschilder oder RFID-Karten mit vordefinierten Rechten ausgeben, um sicherzustellen, dass der Zutritt nur zu autorisierten Bereichen gewährt wird.

Fazit

Sowohl Zutrittskontroll- als auch Besuchermanagementsysteme bieten heute keine automatisierte Identitätsverifikation, was zu erhöhtem Personaleinsatz führt und weitreichende Risiken für die Sicherheit eines Unternehmens darstellen kann. Mit künstlicher Intelligenz und biometrischer Technologie können diese Risiken signifikant reduziert werden. Daher empfiehlt essentry die Erweiterung des mehrschichtigen Ansatzes des Zutrittsprozesses bestehend aus IAM, VMS und ACS durch die Verifizierung von Identitäten, um einen sicheren, effizienten und komfortablen Zutritt für Ihre Zutrittsberechtigten ohne Kompromisse zu ermöglichen.

Die daraus resultierenden Vorteile:

- Unfallverhütung und Reduzierung der Haftungsrisiken
- Compliance mit gesetzlichen und branchenspezifischen Regulationen (z.B. DSGVO, SARS-COV-2 Arbeitsschutz-standard)
- Maximale Sicherheit auf Grenzkontrollniveau reduziert die Angriffsfläche für Industriespionage und bildet ein solides Fundament für die Cybersicherheit
- Businessprozessautomatisierung für Operational Excellence
- Erster Eindruck, der innovativ und komfortabel ist



In den Zutrittsprozess involvierte Systeme bilden ein mehrschichtiges Sicherheitskonzept, doch keines der Systeme verifiziert physische Identitäten der Besucher mit ausreichender Sicherheit. Die Lösung eine zusätzliche Schicht der automatischen Identitätsverifikation in einem Self-Service auf Grenzkontrollniveau.

▶ www.essentry.com

Zeiterfassung im Home-Office

Mit prime WebTime Arbeitszeiten schnell und einfach erfassen und Daten zuverlässig weiterleiten – mit nur wenigen Klicks web-basiert oder per MobileApp.

25 Years of Excellence
1995 2020

primion
AZKOYEN Time & Security Division

www.primion.de