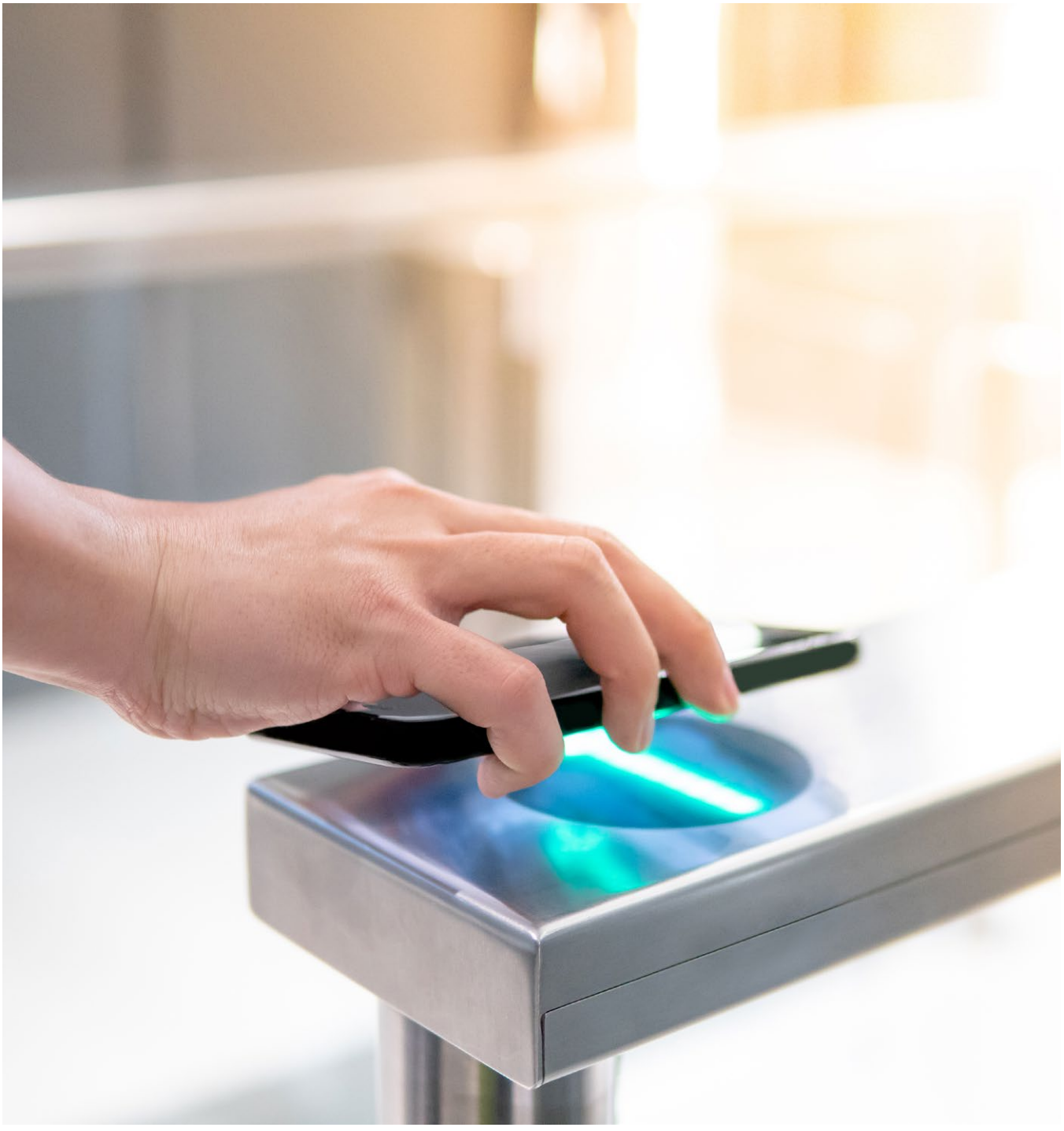
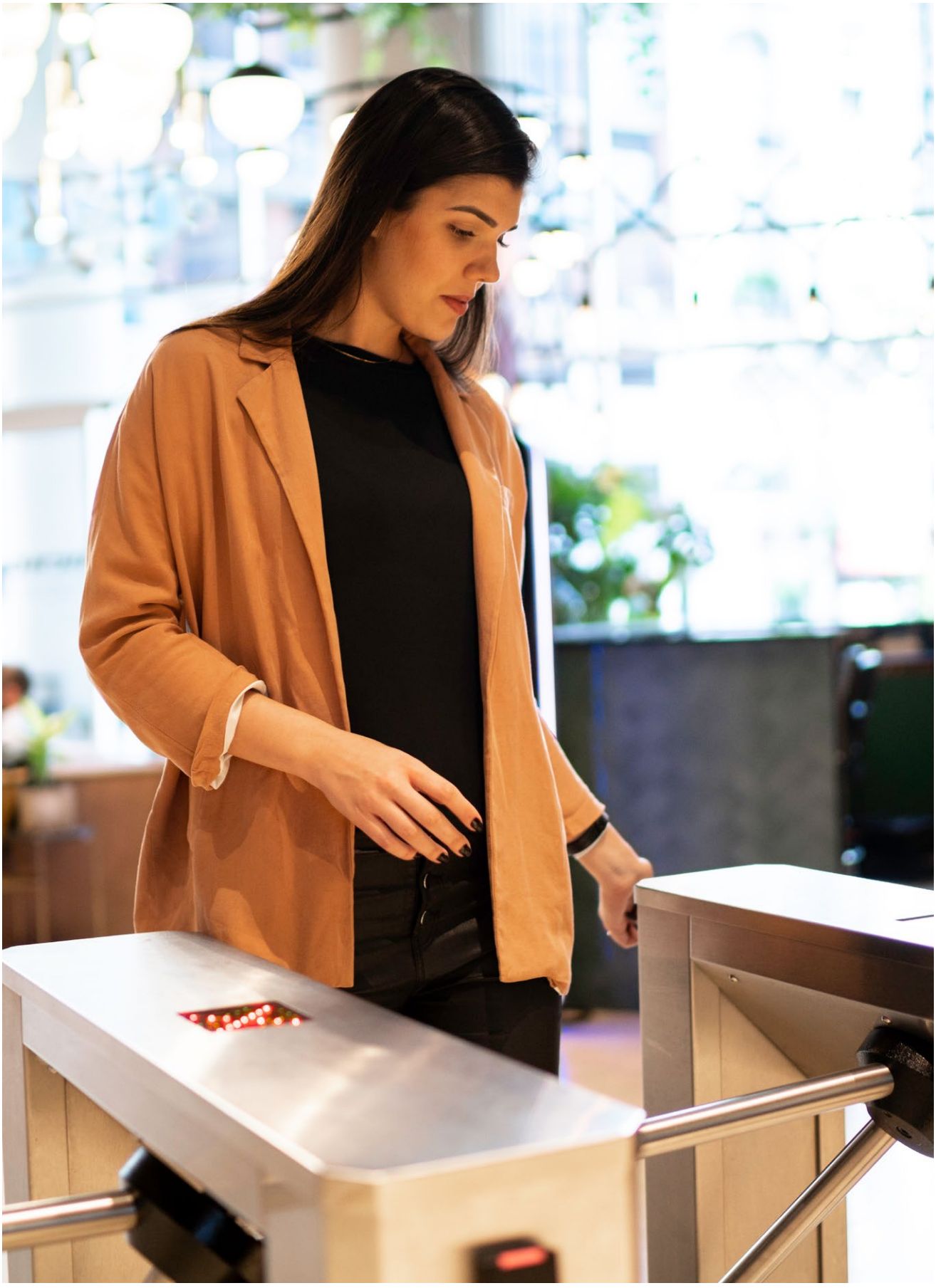
Whitepaper

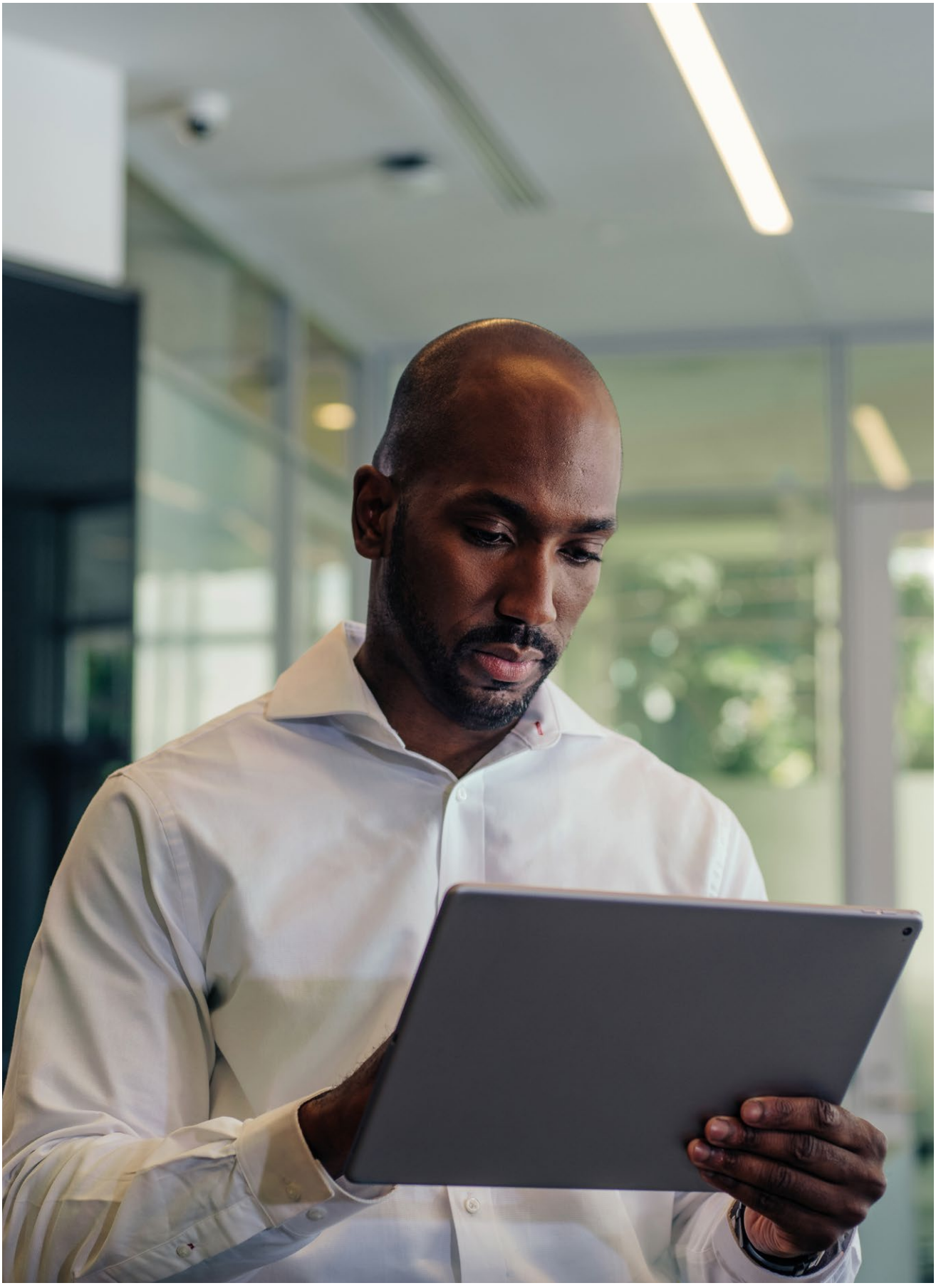
Überlegungen und bewährte Methoden zur Migration zu einem IP-basierten Zutrittskontrollsystem



Genetec™



Inhalt



Executive Summary

Eine Umstellung von einem bestehenden Zutrittskontrollsystem (ACS) auf ein IP-basiertes Zutrittskontrollsystem hilft Unternehmen dabei, ihre physische Zutrittskontroll-Infrastruktur einfacher zu betreiben, zu erweitern und anzupassen.

Für eine erfolgreiche Umrüstung sind jedoch sorgfältige Planung und Überlegungen notwendig. Es ist zunächst wichtig, sich klare Ziele zu setzen. Bevor eine Migration geplant wird, müssen Unternehmen ihr bestehendes System evaluieren, um Kosten und Zeitaufwand des Vorgangs bestimmen zu können.

Abschließend sollten Unternehmen zusammen mit einem Systemintegrator die Umstellung Schritt für Schritt durchführen, damit eine nahtlose Integration zu erreicht werden kann.

1

Gründe für eine Migration

Die Umstellung von einem alten zentralisierten oder verteilten Zutrittskontrollsystem (ACS) auf ein IP-basiertes Zutrittskontrollsystem erlaubt es Unternehmen, ihr System bei neuen Anforderungen einfach anzupassen, was sowohl bessere Sicherheit als auch einen höheren Return of Investment bedeutet.

Ein offenes, flexibles und IP-basiertes ACS erlaubt es Unternehmen:

- IP-Technologie zur Standardisierung ihrer Zutrittskontroll-Infrastruktur zu nutzen und proprietäre Ausstattung zu ersetzen
- zukünftige Erweiterungen und Anpassungen der Infrastruktur zu vereinfachen und so den Total Cost of Ownership (TCO) zu reduzieren
- alle Sicherheitsvorkehrungen, Zutrittskontrolle und Videoüberwachung auf einer vereinheitlichten Plattform mit einer einzigen Schnittstelle zu integrieren
- mit über das Ver- und Entriegeln von Türen hinausgehenden Einsatzmöglichkeiten einen höheren Return of Investment zu erzielen

Unternehmen können mit einer IP-basierten Lösung auch von neuen Funktionen profitieren, die in traditionellen Systemen nicht zur Verfügung stehen. Daher sollte bedacht werden, welche neuen ACS-Funktionen durch IP-basierte Lösungen umgesetzt werden können, wie etwa:

- verbesserte Multi-Site-Überwachung und -Verwaltung
- Skalierung auf eine höhere Anzahl von Türen über ein Netzwerk
- bessere Cybersicherheit dank End-to-End-Verschlüsselung und erweiterter Authentifizierung
- globale Kartenhalterverwaltung für die Verwendung einer einzelnen Karte über mehrere Standorte hinweg

Überdies wird die Instandhaltung klassischer physischer ACSs immer kostenintensiver. Die Kosten für die Wartung solcher Systeme oder für die Suche nach Ersatzteilen steigen, wenn alte ACS-Komponenten obsolet werden.

Mit neuen, gegen Cyberattacken schützenden ACS-Technologien können Unternehmen die Sicherheit ihres Systems und ihrer Abläufe sowie Schutz vor Cyberattacken gewährleisten.

Zudem können klassische ACSs vielen modernen Cyberattacken nicht standhalten. Sie verwenden veraltete Technologien, die sie anfällig für Cyberattacken machen. Mit neuen, gegen Cyberattacken schützenden ACS-Technologien können Unternehmen die Sicherheit ihres Systems und ihrer geschäftlichen Abläufe sowie Schutz vor Cyberattacken gewährleisten.

Außerdem sind klassische Systeme meist teurer, weil sie jedes Kartenlesegerät und jedes Schloss einzeln mit Strom versorgen. Eine offene, flexible und IP-basierte ACS-Lösung nutzt PoE, um die IP-basierten Türsteuerungen, Lesegeräte und Türschlösser zu vernetzen und zu betreiben.

2

Ziele einer Migration

Wenn sich Unternehmen entschieden haben, von einem älteren System auf ein offenes, flexibles und IP-basiertes ACS umzusteigen, sollten sie bei der Suche nach einem Lösungsanbieter folgende Punkte berücksichtigen:

2.1. Ein System mit langer Lebensdauer wählen

Beim Einschätzen der Lebensdauer eines ACS spielen viele Faktoren eine Rolle.

- **Ist die Lösung nicht proprietär und baut auf einer offenen Architektur auf?**
  Ein nicht proprietäres ACS mit offener Architektur ist später leichter erweiterbar und anpassbar.
- **Hat der Lösungsanbieter ein Partnernetzwerk aufgebaut?**
  Ein Lösungsanbieter mit Technologiepartnern in Bereichen wie der Verwaltung von Vermögenswerten, Human Resources oder der Besucherverwaltung verspricht mehr Flexibilität und mehr Optionen sowohl während der Umrüstung als auch bei zukünftigen Anpassungen.
- **Verfügt der Lösungsanbieter über ein standardisiertes Software Development Kit (SDK)?**
  Ein standardisiertes SDK erlaubt individuelle Anpassungen, Scripting und die zukünftige Entwicklung von Plug-Ins für das IP-basierte ACS.

2.2 Weiterverwendung bestehender Ausstattung

Eine Umrüstung auf ein offenes, flexibles und IP-basiertes ACS kann Langzeitinvestitionen von Unternehmen in ihre bestehende Sicherheits-Infrastruktur gewinnbringender machen und zugleich absichern, indem die Lebensdauer bestehender Komponenten verlängert wird und neue Systemfunktionen und Anwendungen zum Einsatz kommen.

Eine Umrüstung auf ein IP-basiertes ACS kann Langzeitinvestitionen von Unternehmen in ihre bestehende Sicherheits-Infrastruktur gewinnbringender machen und zugleich absichern, indem die Lebensdauer bestehender Komponenten verlängert wird und neue Systemfunktionen und Anwendungen zum Einsatz kommen.

2.3 Parallele Arbeitsbereiche

Um eine nahtlose ACS-Migration zu realisieren, sollten parallel und offline Pre-Staging-Vorbereitungen getroffen werden, um die Software-Konfigurierung des neuen IP-basierten ACS zu erstellen, darunter:

- System-Mapping
- Import der Inputs und Outputs (IO) der Systemkomponenten
- Integration der Steuerungslogik für die Komponenten

2.4 Ausfallzeiten so gering wie möglich halten

Bei der Migration eines existierenden Systems müssen die Auswirkungen von Ausfallzeiten auf die Systemnutzer bedacht werden. Daher gilt es, während der Auswahlphase folgende Fragen zu beantworten:

- zu welchen Zeiten das ACS vollständig funktionieren muss
- ob das neue IP-basierte ACS Pre-Staging ermöglicht
- ob das neue IP-basierte ACS parallel mit mehreren Türen verbunden werden kann

Zusätzlich zur Analyse von Funktionen sollten Unternehmen auch ihren aktuellen Zutrittskontrollworkflow prüfen und sicherstellen, dass der neue Lösungsanbieter im neuen System diesen Workflow mindestens aufrechterhält und vielleicht sogar verbessert.

2.5. Sicherstellen, dass alle essentiellen Funktionen verfügbar bleiben

Es ist wichtig, dass Unternehmen prüfen, welche Hardware- und Software-Funktionen ihres aktuellen ACS verwendet werden, damit sie sich vergewissern können, dass diese Funktionen auch mit dem neuen System zur Verfügung stehen werden. Unter anderem sollten folgende Funktionen überprüft werden:

- die maximale Anzahl an Türen, die unterstützt wird
- Karteninhaber-Management
- Zugriffsrechte-Management
- Ausweisdesign
- Anforderungen an den Web Client
- Anforderungen an die Mobil-App
- Besucherverwaltung
- Geräteregistrierung

Zusätzlich zur Analyse von Funktionen sollten Unternehmen auch ihren aktuellen Zutrittskontrollworkflow prüfen und sicherstellen, dass der neue Lösungsanbieter im neuen System diesen Workflow mindestens aufrechterhält und vielleicht sogar verbessert.

3

Überblick: Was zu bedenken ist

Die folgenden Punkte sollen Unternehmen dabei helfen, ihr aktuelles ACS zu prüfen.

Die Ergebnisse haben direkten Einfluss auf die Fragen, (1) ob eine Umrüstung mit dem Austausch aller oder nur mancher Komponenten durchgeführt werden soll, (2) wie teuer die Umrüstung wird und (3) wie lange sie dauern wird.

3.1 Hardware

Jeder Wechsel von einem alten ACS auf ein offenes, flexibles und IP-basiertes ACS hat mit der Evaluierung des aktuellen Systems zu beginnen.

Eine Umrüstung auf ein IP-basiertes ACS ist einfacher, wenn das bestehende System nicht proprietäre Karten und Lesegeräte verwendet. Wenn hingegen die aktuellen Lesegeräte proprietäre Kommunikation unterstützen, ist sehr wahrscheinlich ein kompletter Austausch der alten Lesegeräte notwendig.

Es ist auch wichtig zu prüfen, ob die bestehenden intelligenten Controller und Panels der Downstream-Schnittstellen weiterhin verwendet werden können. Wenn die bestehenden Controller auf einer offenen Architektur basieren, können sie vielleicht in das neue ACS integriert werden.

3.2 Software

Es ist wichtig zu prüfen, was für das neue System portiert werden muss. Dabei müssen die native Datenstruktur der alten Datensätze, die möglichen Export-Tools beim Extrahieren der Daten aus der aktuellen Datenbank und Komponenten von Drittanbietern bedacht werden, die über das SDK in die derzeitige Konfiguration integriert worden sind.

Eine ACS-Umrüstung bedarf der Expertise von Presales Engineers, technischen Spezialisten, Field Services Engineers und Support Engineers.

3.3 Netzwerk

Auch die Netzwerkanforderungen des neuen IP-basierten Systems müssen evaluiert werden, wenn auf ein PoE-Zutrittskontrollsystem umgerüstet wird.

Zusätzlich müssen Unternehmen mögliche Latenz- und Bandbreitenprobleme bei der Kommunikation zwischen Standorten bedenken, wenn ein verteiltes System mit Komponenten vor Ort und an anderen Standorten umgerüstet wird.

3.4 Verkabelung

Da es eventuell möglich ist, einen Teil der bestehenden Verkabelung eines alten ACS im neuen IP-basierten ACS weiterhin zu nutzen, ist auch dieser Punkt zu beachten. Daher sollte vor der Umrüstung die bestehende Verkabelung mit den Anforderungen der neuen IP-basierten ACS-Geräte verglichen werden. Auch muss die zusätzliche Verkabelung bedacht werden, wenn Unternehmen ihr ACS parallel zur Umrüstung zusätzlich auch erweitern wollen.

3.5 Strombedarf

Vor der Umrüstung sollte auch das Stromnetz des aktuellen ACS evaluiert werden. Besonders wichtig ist es zu klären, ob es mit 12 V oder 24 V bzw. mit Gleich- oder Wechselstrom arbeitet und ob genug Stromleistung für den Betrieb der neuen Hardware-Komponenten verfügbar ist.

3.6 Schulungen

Für jede erfolgreiche Umrüstung auf ein offenes, flexibles und IP-basiertes System sind umfassende Schulungen zur Nutzung der neuen Software von essentieller Bedeutung. Entsprechend sollte auf Basis der verschiedenen Arbeitsbereiche und Anwendungsfälle bedacht werden, welche Schulungsarten für die unterschiedlichen Nutzer des ACS nötig sein werden.

3.7 Support während und nach der Umrüstung

Für eine erfolgreiche Umrüstung ist es wichtig zu bedenken, wie viel Support durch den Integrator, die Gerätehersteller und die Lösungsanbieter – aus deren Komponenten das neue System bestehen wird – bei der Installation des neuen ACS nötig sein wird. Eine ACS-Umrüstung bedarf der Expertise von Presales Engineers, technischen Spezialisten, Field Services Engineers und Support Engineers.

4

Schritte des Migrationsprozesses

Ein erfolgreicher Wechsel besteht aus mehreren Schritten. Zunächst spricht der Kunde mit einem Systemintegrator sowie möglichen Geräteherstellern und Lösungsanbietern, um Angebote einzuholen und einen Migrationsplan zu erstellen. Die Implementierung des Plans übernehmen der technische Support und Field Engineers, die das neue IP-basierte System aufbauen und konfigurieren.

4.1 Alle Fakten auf den Tisch

Zuallererst hat der Systemintegrator die Konfiguration des aktuellen ACS abzubilden, darunter Details wie die Standorte von Elektronik- und Telekommunikationskammern, die Verkabelung und die derzeit verwendete Stromversorgung. Außerdem ist es wichtig, eine vollständige Liste der im aktuellen System verwendeten Hardwarekomponenten, Server und der Netzwerkausstattung zu erstellen sowie notwendige Informationen über aktuelle Softwarefunktionen einzuholen.

4.2 Die Anforderungen des neuen Systems verstehen

Folgende Anforderungen des neuen offenen, flexiblen und IP-basierten ACS müssen für eine erfolgreiche Umrüstung berücksichtigt und in ihrer Umsetzung bedacht werden:

- Hardwarekomponenten
- Softwarekomponenten
- Netzwerkkonfiguration
- Verkabelung
- Stromversorgung

Damit ein erfolgreiches Architekturdesign für das neue System gelingt, müssen die mit diesen Punkten zusammenhängenden Anforderungen klar sein.

Um zu ermitteln, welche Hardware, Software, Stromquellen, Verkabelung und Netzwerkkomponenten weiterhin genutzt werden können, ist ein vollständiges Bild des aktuellen ACS eines Unternehmens und der Anforderungen an das neue System erforderlich.

4.3 Standortsichtung

Der nächste Schritt ist ein Rundgang durch die Räumlichkeiten mit dem Kunden, dem Systemintegrator und, falls möglich, mit den Geräteherstellern. So wird sichergestellt, dass kein Aspekt des alten Systems unberücksichtigt bleibt. Eine Standortbesichtigung kann auch der allererste Schritt des Prozesses sein. Eine Standortsichtung dient dazu:

- eine klares Bild von der Architektur und vom Layout des aktuellen Systems zu erhalten
- zu bestimmen, an welchen Orten besonders viel Ausstattung vorhanden ist
- den Abstand zwischen Zutrittskontrollpunkten, Stromquellen und Lesegeräten zu messen

4.4 Weiter verwendbare Komponenten ermitteln

Um zu ermitteln, welche Hardware, Software, Stromquellen, Verkabelung und Netzwerkkomponenten weiterhin genutzt werden können, ist ein vollständiges Bild des aktuellen ACS eines Unternehmens und der Anforderungen an das neue System erforderlich.

4.5 Bestehende Komponenten testen

Nachdem ermittelt wurde, welche Komponenten des bestehenden Systems weiterhin genutzt werden können, sollten diese Komponenten auf ihre Kompatibilität hin getestet werden.

4.6 Benötigte neue Ausstattung ermitteln

Sobald klar ist, was aus dem aktuellen System weiterhin genutzt werden kann und was für das neue System benötigt wird, muss der Systemintegrator als Nächstes die neuen Anforderungen an das Netzwerk und die Zutrittskontrolle bestimmen.

4.7 Bestehende Datenbanken und ihre Datensätze verstehen

Der nächste Schritt des Umrüstungsprozesses ist die Beantwortung der Frage, wie bestehende Daten von Karteninhabern und Anmeldedaten in das neue IP-basierte ACS importiert werden sollen. Die Daten von Karteninhabern und Anmeldedaten müssen von technischen Spezialisten oder Field Engineers aus dem bestehenden System in einem kompatiblen Dateiformat exportiert werden, damit Drittanbieter-Daten weiterhin genutzt werden können.

4.8 Die Umrüstung planen

Um die Ausfallzeiten während der Migration möglichst gering zu halten, muss die Hardware-Umrüstung besonders genau geplant werden. So wird sichergestellt, dass Software- und Hardwareinstallationen so weit wie möglich parallel vorgenommen werden.

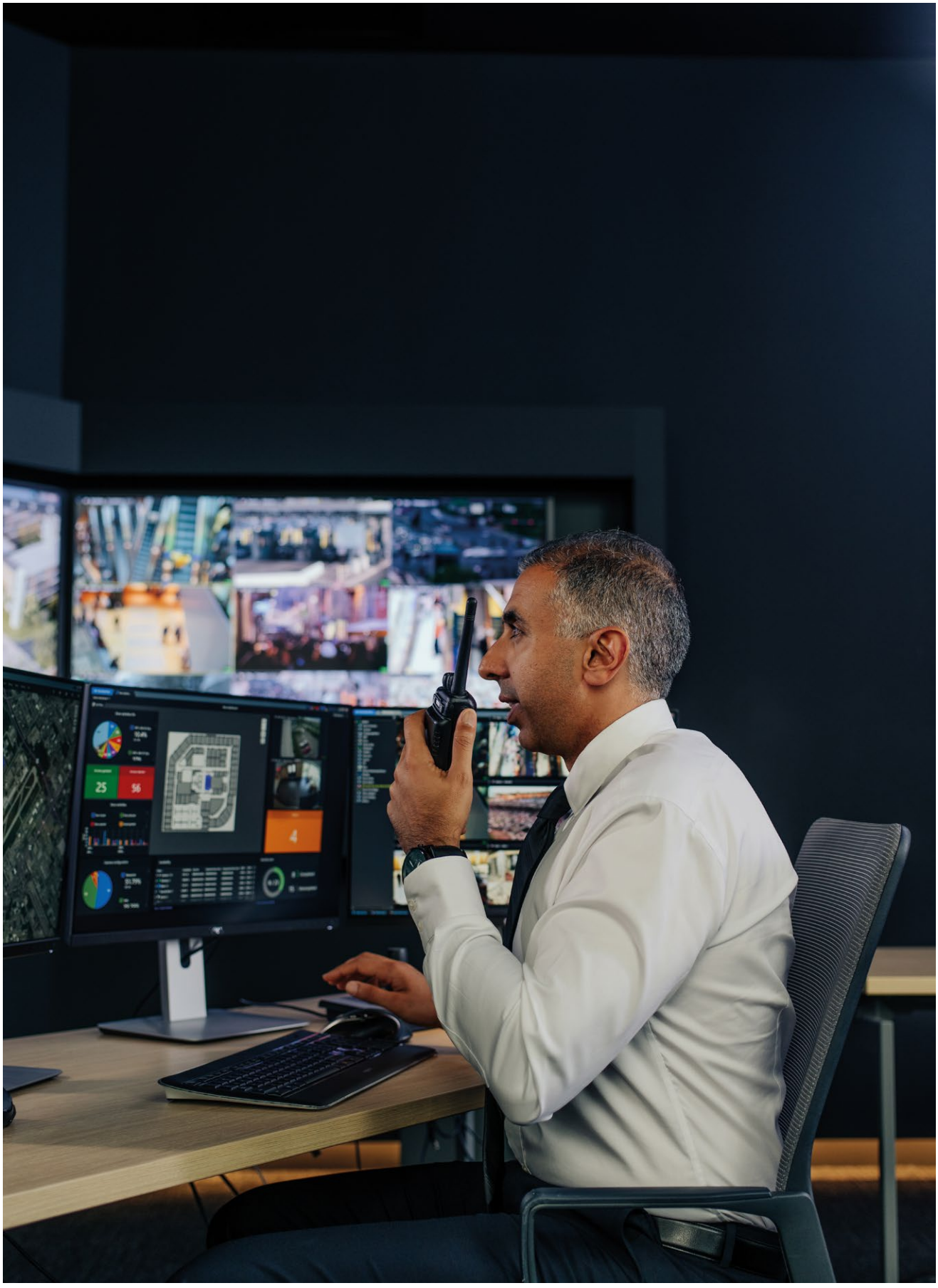
4.9 Das neue IP-System testen

Vor der Durchführung der Umrüstung sollte der Integrator im Sinne eines möglichst reibungslosen Ablaufs noch einen kompletten Testdurchlauf des neuen IP-Systems vornehmen.

4.10 Umrüstung durchführen und Akzeptanz prüfen

Nun können der Systemintegrator und der Kunde – gemäß dem als Teil des Umrüstungsplans erstellten Zeitplan – mit dem Übergang vom alten zum neuen ACS beginnen. Gerätehersteller sollten in dieser Phase für Support bereitstehen, falls Probleme mit neuen ACS-Komponenten auftreten.

Vor der Durchführung der Umrüstung sollte der Integrator im Sinne eines möglichst reibungslosen Ablaufs noch einen kompletten Testdurchlauf des neuen IP-Systems vornehmen.



5

Unsere Herangehensweise an eine Umrüstung

Um eine reibungslose Migration zu ermöglichen, ist Genetec während des gesamten Prozesses ansprechbar – vom ersten Prüfungsvorgang über die Planung der Umrüstung bis hin zum Systemtest und anschließenden Support. Als Lösungsanbieter vermittelt Genetec Presales Engineers, Field Engineers und Technical Support Engineers an Systemintegratoren.

Security Center Synergis™, das IP-basierte Zutrittskontrollsystem von Genetec, bietet Kunden alle Vorteile einer Plattform mit offener Architektur. Synergis erlaubt es Unternehmen, jederzeit Upgrades auf die neuesten unterstützten Technologien vorzunehmen oder auch ihre operativen Abläufe sowie ihre Sicherheitsarchitektur mit einer einzigen Plattform zu vereinheitlichen. Diese Plattform mit offener Architektur bietet Kunden darüber hinaus mehr Flexibilität in Sachen Drittanbieter-Systemintegration. Dank der Anpassungsfähigkeit von Synergis können Unternehmen ihr System an neue Anforderungen anpassen und so dessen Sicherheit mit einem höheren Return of Investement ständig optimieren.

Genetec wurde 1997 gegründet und ist der weltweit führende Anbieter von einheitlichen Sicherheitsplattformen mit einem umfassenden, vielfältigen Angebot an Sicherheitskomponenten.

Videoüberwachung: Verbessern Sie die Situationseinschätzung und die Sicherheit in Ihrer Stadt dank der Möglichkeit, Kameras für verschiedene Behörden und Organisationen freizugeben. So erhalten Sie ein gemeinsames Bild der Situation und verkürzen die Reaktionszeit bei Vorfällen.

Zutrittskontrolle: Mit einer integrierten IP-fähigen Plattform können Sie die Sicherheit Ihrer Organisation erhöhen, effektiv auf Bedrohungen reagieren sowie schneller klare Entscheidungen treffen – ganz gleich, ob Sie ein neues Zutrittskontrollsystem installieren oder eine bestehende Installation aktualisieren.

Automatische Nummernschilderkennung: Automatisieren Sie die Erkennung gesuchter Fahrzeuge, setzen Sie Parkvorschriften effizienter durch und beschleunigen Sie Untersuchungen zum Schutz der Öffentlichkeit, indem Sie Nummernschilddaten an ausgewählte Behörden und Partnerorganisationen weitergeben, ohne Abstriche beim Eigentums- und Datenschutz.

Operationelle Entscheidungsunterstützung: Gestalten Sie den Umgang mit Vorfällen sowie die Entscheidungsfindung effizienter – mit fortschrittlichen Workflows, **die Sicherheitsverantwortliche durch das System führen** - von der Warnmeldung über richtlinienbasierte Vorgehensweisen bis hin zum Export detaillierter Fallzusammenstellungen.

Investigative Fallverwaltung: Mit einer Plattform, auf der Sie digitale Beweise zentral ablegen und sicher mit Ermittlern, externen Stellen und der Öffentlichkeit zusammenarbeiten können, lässt sich die Fallverwaltungvereinfachen und Untersuchungen beschleunigen.

Cloud-Services: Erweitern Sie die Funktionen Ihres lokalen Sicherheitssystems und senken Sie die IT-Kosten – dank äußerst skalierbarer On-Demand-Cloud-Services, mit denen Ihre Stadt die sich rasch verändernden Sicherheitsanforderungen problemlos bewältigen und effizienter arbeiten kann.

Genetec Inc.
genetec.com/standorte
info@genetec.com
@genetec

AKTUALISIERT: 12. JUL 21