SIEMENS

Fachartikel

Infrastructure & Cities Sector
Building Technologies Division

Zug (Schweiz), 7. September 2012

Zutrittskontrolle: Integration, nicht Isolation

Im aktuellen wirtschaftlichen Klima nimmt das Preis-Leistungsverhältnis einen höheren Stellenwert ein denn je. Unternehmen überprüfen ihre Prozesse und Systeme gründlich und versuchen, die Wertschöpfungskette zu optimieren. Dies betrifft auch Sicherheitsthemen, beispielsweise Systeme für die Zutrittskontrolle und Arbeitszeiterfassung, beide ein wesentlicher Bestandteil eines integrierten Ansatzes. Die Vorteile eines solchen Ansatzes sind etwa ein besserer Schutz vor Eindringlingen und das Verhindern von Industriespionage. Auf diese Weise werden Sachwerte, geistiges Eigentum und nicht zuletzt Menschen besser geschützt. Wenn dazu Daten aus den unterschiedlichsten Quellen und Systemen, unter anderem Gebäudemanagementsystemen, genutzt werden, lassen sich die Anforderungen an ein Gebäude besser verstehen, und es kann einfacher gemanagt und optimiert werden.

Von Philippe Huysman, Global Portfolio Manager Access Control, Siemens Building Technologies

Die wichtigsten Kunden für größere Systemhersteller und -integratoren sind in der Regel große Unternehmen. Da bei ihnen ein Start auf der grünen Wiese meist nicht möglich ist, besteht das Geschäft im Zutrittskontrollmarkt also üblicherweise in der Modernisierung oder Migration bestehender Systeme, wobei häufig noch laufende Serviceverträge berücksichtigt werden müssen. Obwohl zahlreiche multinationale Unternehmen Zutritts- und Anwesenheitskontrollsysteme in ihre Prozesse einbinden, zeigt sich der Markt dennoch regional sehr unterschiedlich aufgestellt. Dies liegt hauptsächlich an unterschiedlichen Rechtsvorschriften, besonders bezüglich Datenschutz und Arbeitszeitregelungen, die von Land zu Land variieren.
Daher ist es empfehlenswert, Systemhersteller und -integratoren beizuziehen, die nicht nur globale Lösungen für Multi-Site- und Multi-Tenant-Applikationen bieten, sondern die auch über solide lokale Kompetenz und Erfahrung verfügen. Die Systeme wiederum müssen flexibel sein und gleichermaßen lokal für eine einzelne Filiale geeignet sein wie für vernetzte Standorte weltweit, die sich in unterschiedlichen Zeitzonen befinden.

Siemens Schweiz AG
Infrastructure & Cities Sector – Building Technologies Division
Gubelstraße 22, 6301 Zug, Schweiz

Public and Press Relations: Catharina Bujnoch
Telefon: +41 41 724-5677
E-Mail: catharina.bujnoch@siemens.com

Referenznummer: TA ICBT201209e Access control.doc

Die Kosten im Griff

Einer der wichtigsten Aspekte für Unternehmen, die ihre Zutrittskontrollsysteme neu überdenken und nach alternativen Anbietern suchen, sind die Kosten, nicht zuletzt aufgrund der aktuellen wirtschaftlich schwierigen Lage. Unternehmen sind bestrebt, den Wert ihrer Systeme und Prozesse zu optimieren, und Schutz und Sicherheit bilden hier keine Ausnahme.

Zur Mitarbeiterauthentifizierung werden nach wie vor am häufigsten ID-Karten eingesetzt. Die Hauptkosten für die Karten liegen nicht in ihrer Anfertigung, die mit drei bis fünf Euro pro Karte kaum ins Gewicht fällt, sondern in ihrer Verwaltung über den gesamten Lebenszyklus hinweg. Wenn eine Karte verloren geht, ist es nicht teuer, sie zu ersetzen, aber der administrative Aufwand steht dazu in keinem Verhältnis: Konfigurieren, Erneuern der zur Authentifizierung erforderlichen Zertifikate, Betreiben einer Local Registration Authority (LRA) – all dies schlägt sich in Zusatzkosten nieder. Sie lassen sich reduzieren, wenn anstelle von mehreren Karten eine einzige Karte für mehrere Anwendungen genutzt wird. Besonders in dynamischen Multi-Site-Applikationen mit potenziell Tausenden von ID-Karten, die häufige Aktualisierungen und Neudefinitionen von Zutrittsberechtigungen erfordern, ist die komplexe Verwaltung die Regel.

Diese Vorgänge können optimiert werden, indem bestimmte Aufgaben von lokalen Administratoren übernommen werden, wobei Verwaltung und Auditing nach wie vor zentral erfolgen, damit die Einhaltung globaler Unternehmensrichtlinien gewährleistet ist. Es ist es wichtig, dass Systeme einfach zu verwalten und intuitiv zu bedienen sind, um den für die Zugangskontrolle verantwortlichen Personen die Bearbeitung von Mitarbeiterdaten, Zugriffsprofilen oder Gültigkeitsperioden zu erleichtern. Standardisierte Arbeitsabläufe können die Kosten weiter senken und die allgemeine Sicherheit erhöhen. Systeme zur Zutrittskontrolle müssen in der Lage sein, organisatorische Änderungen oder Umzüge ganzer Abteilungen effizient abzubilden. Mehr Effizienz in der Verwaltung bedeutet geringere Kosten.

Ein weiterer Bereich für potenzielle Kosteneinsparungen ist die Energieeffizienz. Sicherheit, und hier vor allem Zutrittskontrolle, spielt da eine wichtige Rolle, denn es sind die Sicherheitssysteme, die Daten zur Gebäudebelegung liefern. Warum wird ein Gebäude automatisiert? Warum sorgen wir für Komfort im Gebäude? Warum versorgen wir das Gebäude mit Energie? All dies geschieht für die Personen, die sich im Gebäude aufhalten. Letzten Endes dreht sich also alles um die Gebäudebelegung. Dank der zunehmenden Integration von Sicherheits-, Brandschutz- und Gebäudemanagementsystemen besteht das Potenzial, beträchtliche Energie- und damit Kosteneinsparungen zu erzielen. Wenn das Zutrittskontrollsystem erkennt, dass sich in einem bestimmten Raum niemand aufhält, können Heizung, Lüftung und Klimaanlage automatisch zurückgefahren werden. Ein solcher bedarfsorientierter Ansatz lässt sich über die reine Präsenzerkennung noch gezielter nutzen. So ist es beispielsweise möglich, in einem Labor die Bedingungen an die Anforderungen der Person anzupassen, die den Raum betritt. Ein

Siemens Schweiz AG
Infrastructure & Cities Sector – Building Technologies Division
Gubelstraße 22, 6301 Zug, Schweiz

Public and Press Relations: Catharina Bujnoch
Telefon: +41 41 724-5677
E-Mail: catharina.bujnoch@siemens.com

Zutrittskontrollleser identifiziert zum Beispiel das Reinigungspersonal und „weiß“ damit, dass es sich um einen Aufenthalt von kurzer Dauer handeln wird. Der Temperatursollwert kann daher niedriger, die konstante Raumluftwechselrate hingegen höher sein als bei einem Labortechniker, der am Morgen das Labor betritt.

Ein ganzheitlicher Ansatz für Sicherheit

Bei größeren Systemen, die vorhandene IT-Netzwerkinfrastrukturen nutzen, ist Integration ein wichtiger Faktor. Unternehmen, vor allem größere Betriebe, sind inzwischen von Strategie abgerückt, einzelne Systeme zu kaufen. Zunehmend ist die Sicht auf Sicherheit ganzheitlich, sowohl hinsichtlich der Integration unterschiedlicher Sicherheitsfunktionen als hinsichtlich der Integration von Schutz und Sicherheit in allgemeine Geschäftsprozesse. Auch beim Thema Konnektivität hat sich der Markt stark weiterentwickelt, besonders offene Architekturen werden populär. Bis vor Kurzem gab es bei der Verbindung von Videoüberwachung und Zutrittskontrolle eigentlich nur zwei Optionen: eine eher simple mit fest verdrahteten Signalen oder eine komplexe mit teurer, vom Systemintegrator individuell entwickelter Software. Aber weil offene Schnittstellen heute Trend sind, erwarten Kunden Integration als Standardfunktion.
Die Sicherheitsbranche, die ursprünglich von Netzwerkvideolösungen getrieben wurde, richtet ihr Augenmerk heute auf die Entwicklung neuer Standards für die Zutrittskontrolle und auf die Herstellung kompatibler Geräte. Zahlreiche führende Hersteller haben angekündigt, dass sie solche Geräte auf den Markt bringen wollen, einige wurden bereits eingeführt. Das BACnet-Protokoll dient als Impulsgeber für die Entwicklung offener Architekturen. Dieser Trend wird durch Standardprotokolle von Branchenverbänden wie ONVIF (Open Network Video Interface Forum) und PSIA (Physical Security Interoperability Alliance) bestärkt. Der Trend zur Integration ist nicht mehr aufzuhalten. Daher wird es immer wichtiger, Kunden zu unterstützen, sich von proprietären Kommunikationsprotokollen zu lösen und domänenübergreifende Management- und Leitstellenlösungen bereitzustellen, die diesen Schritt softwaretechnisch ermöglich.

Zusätzliche Herausforderungen

Jedes Zutrittskontrollsystem muss berücksichtigen, dass es zwar Funktionen gibt, die immer gebraucht werden, die individuellen Anforderungen jedoch je nach Unternehmen und Gebäude stark variieren können. Sehen wir uns als Beispiel die Pharmaindustrie an: Daten aus dem Zutrittskontrollsystem sind ungemein wertvoll, um im Nachhinein festzustellen, welcher Mitarbeiter an der Produktion eines bestimmten Arzneimittels beteiligt war, falls Probleme auftauchen. Auch die Vereinheitlichung von unternehmensweiten Sicherheitsrichtlinien kann wichtig sein, besonders wenn eine Konsolidierung heterogener Zutrittskontrollsysteme ansteht, wie das zum Beispiel nach einer Firmenübernahme der Fall ist, wobei länderspezifische Aspekte berücksichtigt werden müssen.

Siemens Schweiz AG
Infrastructure & Cities Sector – Building Technologies Division
Gubelstraße 22, 6301 Zug, Schweiz

Public and Press Relations: Catharina Bujnoch
Telefon: +41 41 724-5677
E-Mail: catharina.bujnoch@siemens.com

Ein weiterer Aspekt der Zutrittskontrolle ist die eigentliche Migration. Um getätigte Investition zu schützen, sollte die Hardware möglichst übernommen werden, einschließlich der Verkabelung. Die nötigen Updates sollten primär per Software vorgenommen werden können. Feldgeräte wie Kartenleser, Schlösser und Karten sind in der Regel wieder verwendbar, während Module auf Automationsebene wie Türcontroller ausgetauscht werden müssen. Auch Daten spielen in einem Zutrittskontrollsystem eine wichtige Rolle. Wenn das neue System die Daten aus der bestehenden Datenbank nicht übernehmen kann, fallen beträchtliche Zusatzkosten an. Ein umfassender Migrationsplan ist empfehlenswert. Dieser kann zum Beispiel definieren, dass die vorhandene Infrastruktur nicht komplett eliminiert werden muss, sondern dass mit Hilfe von Software der nahtlose Betrieb älterer Feldgeräte und Hardware gewährleistet und neue Geräte als Ergänzung installiert werden können.

Integration mit Unternehmenssoftware

Auch bei der Zutrittskontrolle sind einige wegweisende Trends zu verzeichnen. Einer ist die Forderung nach erweiterter Funktionalität. Die Entwicklung geht ganz klar in Richtung Smartcards. Die Karten, mit denen man früher nur Zutritt zum Gebäude erlangte, werden heute für zahlreiche weitere Applikationen verwendet. Dies reicht vom Parken im Parkhaus über bargeldloses Bezahlen in der Kantine bis hin zu zusätzlichen Sicherheitsfunktionen, beispielsweise die Authentifizierung für den Zugriff auf IT-Netzwerke und -Anwendungen, digitale Unterschriften und E-Mail-Verschlüsselung, biometrische Daten oder Druckermanagement.
Zunehmend werden standardisierte und zertifizierte Schnittstellen zu ERP-Systemen wie SAP, zu Personalverwaltungssystemen sowie zum Facility-Management entwickelt. Durch Anbindung an das Personalwesen oder ähnliche identitätsbezogene Datenquellen wird das Identity-Provisioning und -Deprovisioning automatisiert, so dass zum Beispiel Zugriffsrechte aufgrund des Rollenprofils einer Person automatisch zugewiesen werden. Die betriebswirtschaftlichen Einsparungen, die sich damit erzielen lassen, sowie die erhöhte Datenkonsistenz und -sicherheit sind offensichtlich. Trotzdem wird dieses Potenzial häufig nicht ausgeschöpft.

Anspruchsvolles Besuchermanagement

Im Sicherheitssystem muss stets genau hinterlegt sein, welche Besucher oder Lieferanten sich in einem Gebäude aufhalten. Der Ein- und Auscheckprozess und der Durchruf an die Person, die den Besucher erwartet, soll professionell und effizient in der Gebäudelobby erfolgen. Dieser Vorgang lässt sich durch webbasierte Vorabregistrierung und Autorisierung des Besuchers vor seiner Ankunft beschleunigen. Eine enge Integration mit dem Zutrittskontrollsystem erhöht die Sicherheit noch weiter, da der Besucher nur Zutritt erhält, wenn er von seinem Gastgeber begleitet wird.

Siemens Schweiz AG
Infrastructure & Cities Sector – Building Technologies Division
Gubelstraße 22, 6301 Zug, Schweiz

Public and Press Relations: Catharina Bujnoch
Telefon: +41 41 724-5677
E-Mail: catharina.bujnoch@siemens.com

Immer häufiger werden elektronische Türzylinder und -komponenten verwendet, hauptsächlich weil damit die Installationskosten reduziert werden. Smartcards, die alle Berechtigungen und gültigen Zutritte einer Person speichern, machen solche Lösungen höchst attraktiv für Türen, bei denen grundlegende Zugangskontrollen erforderlich sind, nicht aber für Türen, die rund um die Uhr online überwacht werden müssen. Ein Beispiel hierfür ist der Zugang zu geschlossenen Meetings, der auf autorisierte Teilnehmer beschränkt werden kann, indem herkömmliche Türgriffe durch Kartenlesegeräte ersetzt werden. Sogar eine Integration mit Microsoft Office ist denkbar, so dass bei der Planung einer Besprechung und Buchung eines Konferenzraums nur den Personen Zutritt gewährt wird, die eine Einladung erhalten haben. Durch Kombination von elektronischen Türsteuerung und Onlineüberwachung lässt sich eine optimale Balance zwischen Kosteneffizienz und Sicherheit erzielen. Um die Vorteile jedoch voll und ganz auszuschöpfen, müssen die Verwaltung und das Reporting in einer einzigen Managementanwendung erfolgen.

Starke Smartcard-Verschlüsselung

Je mehr Anwendungen gesteuert werden können, desto stärker wächst das Potenzial von Smartcards und desto wichtiger wird es, dass ihre Sicherheit durch starke Verschlüsselung der darauf gespeicherten Daten gewährleistet ist. In Branchen, die eine hohe Zutrittskontrollsicherheit erfordern, wie die Pharma- und Chemieproduktion, ist dies ganz besonders wichtig. Auch mit NFC (Near Field Communication) ausgerüstete Smartphones dürften in absehbarer Zeit ihren Weg in die Zutrittskontrolle finden. Smartphones, die immer mit dem Internet verbunden sind und über Funktionen zur Standortbestimmung verfügen, bieten völlig neue Möglichkeiten, die Smartcards verschlossen sind. Obwohl die Forschung in diesem Bereich auf Hochtouren läuft und sich einige Pilotprojekte in Entwicklung befinden, ist diese Technologie noch nicht weitverbreitet und eine weitere Ausgestaltung des kompletten NFC-Ökosystems ist erforderlich.

Zusammenführen von Informationen

Für Unternehmen wird es immer wichtiger, das Potenzial ihrer Systeme und Prozesse umfassender auszuschöpfen. Daher sollen alle Systemmodule, so auch der Zutrittskontrolle, ihren Beitrag zur Wertschöpfung leisten. Der Schwerpunkt liegt eindeutig auf der Integration, und die Rolle der IT ist im Sicherheitsbereich fundamental. Auch die Wertverschiebung von physischen zu informationsbasierten Werten und die damit einhergehende Verschiebung in Richtung Onlinedatenspeicherung unterstreicht die Rolle der Informationstechnologie und führt zu Forderungen nach besserer Datensicherheit. Doch aus Sicht der Sicherheit ist IT nicht alles. Informationen gehören zu den wertvollsten Gütern eines Unternehmens und stellen damit einen der größten Risikobereiche dar.

Schätzungen zufolge fallen rund eine Million Menschen pro Tag Internetkriminalität zum Opfer. Die Angriffsmethoden sind vielfältig, sowohl extern als auch intern, und rund 80 Prozent aller

Siemens Schweiz AG
Infrastructure & Cities Sector – Building Technologies Division
Gubelstraße 22, 6301 Zug, Schweiz

Public and Press Relations: Catharina Bujnoch
Telefon: +41 41 724-5677
E-Mail: catharina.bujnoch@siemens.com

Sicherheitsverletzungen gehen auf das Konto von Insidern, meist Mitarbeitern. Firewalls helfen beim Verhindern von Angriffen, bieten aber keinen umfassenden Schutz, vor allem nicht vor Insiderattacken, sie sollten also keinesfalls isoliert eingesetzt werden. Unternehmenssicherheit muss auf einem Outside-In- und Inside-Out-Ansatz basieren, der IT-gestützte Maßnahmen mit physischen Sicherheitsmethoden verbindet, um Informationen zuverlässig zu schützen. Zutrittskontrollsysteme verhindern den Zugang unbefugter Personen zu Bereichen, in denen sensible Daten gespeichert sind, und bieten Identitätsmanagement durch Zutrittskontrolltechnologien.
In der Zutrittskontrolle spielt die IT schon immer eine wichtigere Rolle als in anderen Sicherheitsbereichen, denn sie stützt sich auf Datenbanken, Transaktionsprotokolle und IP-Infrastrukturen. Die IT-basierten Anforderungen des Marktes dürften weiter wachsen, denn durch eine integrierte Methode zum Überwachen und Verwalten von Gebäuden erhöht sich deren Nachhaltigkeit und Energieeffizienz, was sie letztendlich sicherer und komfortabler macht.
Es wird darauf ankommen, neue Methoden zu entwickeln, die alle diese Informationen zusammenführen. Heute ist die Sicherheit fest mit der IT verzahnt, und nahezu alle Protokolle sind offen. Es wird deshalb immer einfacher, die entsprechenden Daten aktiv in den Sicherheitsprozess einzubinden. Häufig sind die Daten zwar vorhanden, werden aber nicht in ausreichendem Maße zur Verbesserung der Sicherheit genutzt. Um dies zu erreichen, müssen die Ressourcen aktiver genutzt werden. Erst dann lässt sich erkennen, welche Informationen zur Erhöhung der Sicherheit beitragen und damit den gesamten Geschäftsprozess aufwerten.

Der **Siemens-Sektor Infrastructure & Cities** (München) mit rund 87.000 Mitarbeitern bietet nachhaltige Technologien für urbane Ballungsräume und deren Infrastrukturen. Dazu gehören integrierte Mobilitätslösungen, Gebäude- und Sicherheitstechnik, Stromverteilung, Smart-Grid-Applikationen sowie Nieder- und Mittelspannungsprodukte. Der Sektor setzt sich aus den Divisionen Rail Systems, Mobility and Logistics, Low and Medium Voltage, Smart Grid und Building Technologies zusammen. Weitere Informationen finden Sie im Internet unter www.siemens.com/infrastructure-cities

Die **Siemens-Division Building Technologies** (Zug, Schweiz) ist weltweit führend auf dem Markt für sichere und energieeffiziente Gebäude („Green Buildings“) und Infrastrukturen. Als Dienstleister, Systemintegrator und Produktlieferant verfügt Building Technologies über Angebote für Gebäudeautomation, Heizungs-, Lüftungs- und Klimatechnik (HLK) sowie Brandschutz und Sicherheit. Weitere Informationen finden Sie im Internet unter www.siemens.com/buildingtechnologies

Siemens Schweiz AG
Infrastructure & Cities Sector – Building Technologies Division
Gubelstraße 22, 6301 Zug, Schweiz

Public and Press Relations: Catharina Bujnoch
Telefon: +41 41 724-5677
E-Mail: catharina.bujnoch@siemens.com