Prozessorientiertes Berechtigungsmanagement

Regelbasiert und automatisiert

Peter Kiess

Aktuell bietet der Markt eine nie dagewesene Vielfalt an technischen Geräten und Technologien, um definierte Schutzziele eines Unternehmens im Bereich der physikalischen Sicherheit auf unterschiedliche Arten zu erreichen. Ob Online- oder Offline-Systeme, mechanische Schließanlagen oder elektronische Depotsysteme – ein reichhaltiges Angebot der verschiedenen Hersteller bietet Lösungen für nahezu jede physikalische Schutzanforderung.

Aus dieser Vielfalt an spezifischen Lösungsoptionen ergeben sich jedoch neue Herausforderungen und organisatorische Aufgabenstellungen. Einzelne Hersteller liefern eigene Softwarelösungen, die ausschließlich zur Administration und Steuerung der eigenen Komponenten geeignet sind. Somit entstehen proprietäre Systemlandschaften, die nur schwer in die betriebliche IT-Umgebung eines Unternehmens integriert werden können, da deren Fokus im Betrieb der eigenen Systeme liegt und keine ausgeprägten Integrationsmechanismen vorhanden sind. Die Folgen sind eine Vielzahl von spezifischen Softwaresystemen, die hauptsächlich durch spezialisierte Administratoren bedient werden.

So stellt sich die Frage, ob sich auf diese Art der sehr spezifischen und herstellerfokussierten Prozess- und Systemgestaltung die täglichen Anforderungen der dynamischen Prozess- und IT-Umgebungen in Unternehmen tatsächlich beherrschen lassen und ob diese Vorgehensweisen den permanenten Veränderungen, wie sie in Organisationen täglich Programm sind, tatsächlich Stand hält. Die Frage ist nun: Kann so wirklich sichergestellt werden, dass die Vorgaben der betrieblichen- beziehungsweise gesetzlichen Sicherheits- oder Compliance-Verantwortlichen in allen Belangen eingehalten und auch operativ umgesetzt werden oder bedarf es nicht eher einer komplett anderen Herangehensweise – die eines speziellen Management-Werkzeugs, das die organisatorischen und prozessualen Seiten in den Fokus stellt.

Prozesssicherheit als neues Ziel

Im Kern betrachtet geht es bei der Steuerung von Berechtigungen für Zutritte oder Zugriffe lediglich darum, dass die richtigen Personen zur richtigen Zeit Zugang zu den richtigen Bereichen, Räumen oder Ressourcen erhalten und außerhalb dieser Regeln oder Vorgaben dies wirksam verhindert wird. Diese Steuerung muss auf jede Person und jeden Raum gleichermaßen und jederzeit nachvollziehbar angewendet werden. Das bedeutet konkret: Alle Veränderungen auf Mitarbeiterebene, dazu gehören beispielsweise Eintritts- und Austrittsvorgänge, Funktions-, Aufgaben- und Arbeitsplatzwechsel sowie alle Veränderungen auf Gebäudeebene, wie Umzug, Neubezug oder Umbau, die in allen betroffenen Sicherheitssystemen täglich berücksichtigt werden müssen — unmittelbar, nachvollziehbar und transparent. Weitere Herausforderungen auf unternehmerischer Ebene sind etwa „Mergers & Acquisitions“ (M&A) oder Mietverhältnisse, bei denen neue Zutrittssysteme rasch mit in die betriebliche Steuerung integriert werden müssen.

Self-Service-Prozesse und elektronische Workflows

Employee Self Services haben sich in vielen Unternehmensprozessen durchgesetzt. In den Bereichen Bestellwesen, Zeitwirtschaft und Reisemanagement werden Prozesse von Mitarbeitern direkt initiiert, durchlaufen (Genehmigungs-) Prozesse und werden ohne Medienbrüche direkt in die Zielsysteme transportiert. Hierbei wird durch schnelle Prozesslaufzeiten, geringen Bearbeitungsaufwand sowie eine transparente und fehlerfreie Durchführung Zeit und Geld gespart. Daher wird diese Art der Prozessgestaltung zunehmend auch im Bereich der Unternehmenssicherheit eingesetzt: Bestellungen von Mitarbeiterausweisen, Beantragung von Zutrittsmedien oder Berechtigungen, Voranmelde- und Anmeldeprozesse für Externe (etwa für Besucher, Warenverkehr, Handwerker oder externe Mitarbeiter) bis hin zur elektronischen Schulung und Unterweisung von Personen – immer mehr Unternehmensprozesse werden elektronisch abgebildet. Somit ist die Gewährleistung von physikalischer Sicherheit mittlerweile ein zentrales IT- und Prozessthema und nicht mehr in erster Linie eine Disziplin des klassischen Zutrittsadministrators oder Schlüsselverantwortlichen.

Es zeichnet sich ab, dass die oben beschriebenen Anforderungen hinsichtlich

Bild: Fotolia/ pressmaster

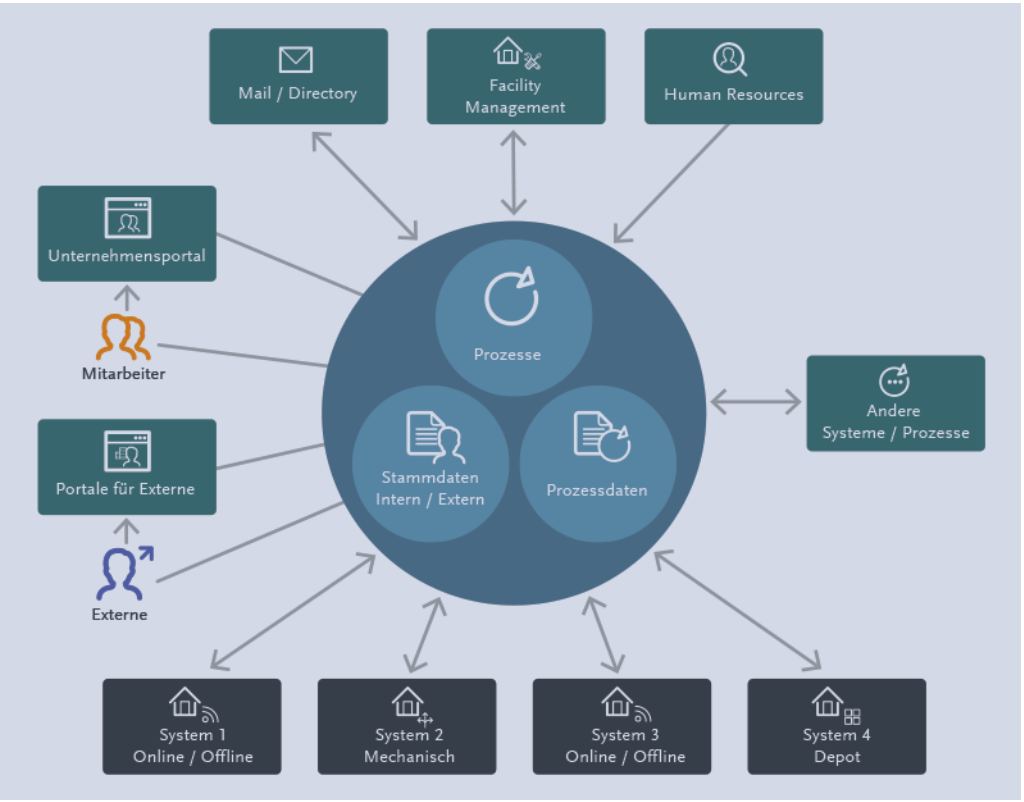
Dynamik, Mitarbeiterfokussierung und operativer Umsetzung mit herkömmlichen Vorgehensweisen gar nicht oder nur mit sehr hohen personellen und finanziellen Aufwendungen durchgeführt werden können. Welche Eigenschaften müssen Standardsysteme daher aufweisen, um die Anforderungen im betrieblichen Umfeld zu gewährleisten?

Zentrale Plattform für unterschiedliche Zutrittssysteme

Eine zentrale Management Plattform sollte daher über folgende Kernfunktionen verfügen, um die oben genannten Anforderungen zu erfüllen:

- zentraler Informationspool für alle relevanten Stamm- und Prozessdaten aus führenden Unternehmensanwendungen
- zentrale und eigenständige Datenhaltung für weitere Steuerungsparameter
- Sammel-, Verteil- & Steuerungscontainer für spezifische und proprietäre Zutrittssysteme – hersteller- und technologieunabhängig
- zentrale Reporting- und Steuerungsstelle
- Möglichkeit (Genehmigungs-) Prozesse, Self Services und eigenständige, operative Anwendungen anzubieten oder zu verarbeiten
- einfacher, rollenbasierter Zugriff für alle Berechtigten
- jederzeit revisionssichere und transparente Vorgangsbearbeitung, mit Fokus auf Datenschutz- und Datensicherheit.

Wie aus der Aufstellung hervorgeht, ist neben einer hohen Flexibilität und erheblichen Funktionsumfang vor allem die Ausprägung leistungsfähiger Schnittstellen und -technologien von entscheidender Bedeutung. Die permanenten Veränderungen müssen erkannt, bewertet und automatisch zu den entsprechenden Zielsystemen transportiert werden. Hierfür sind flexible und belastbare Schnittstellen erforderlich, die mit betrieblichen IT-Monitorsystemen überwacht werden können.



Grafik: Gis

Mit der Plattform für Sicherheitsmanagement und Zutrittskontrolle „.secure“ der Gesellschaft für integrierte Informationssysteme (Gis) können Daten unterschiedlicher Systeme aus verschiedenen Branchen systematisiert und verwaltet werden.

Zentraler Informationspool

Relevante Stamm- und Prozessdaten werden automatisch aus vorhandenen Unternehmensanwendungen in den zentralen Informationspool übertragen und synchronisiert. Dabei können mehrere parallele Datenquellen entsprechend vollständige Stammsätze liefern. Typische Datensourcen für interne Mitarbeiter sind beispielsweise HCM-Anwendungen (zum Beispiel SAP HR für Mitarbeiterdaten und prozessrelevante Organisationshierarchien) und Unternehmens-Directories (etwa Microsoft Active Directory) um Stammsatzdaten, Anmeldeinformationen, E-Mail- und Arbeitsplatzinformationen zu halten. Somit kann jeder Mitarbeiter grundsätzlich per „Single Sign On“ (SSO) Zugriff erlangen. Gleichzeitig können alle prozessrelevanten Änderungen identifiziert und entsprechende Veränderungsprozesse automatisch generiert werden.

Zentrale und eigenständige Datenhaltung

Weitere Stamm- und Prozessdaten sollten in der zentralen Management Plattform verfügbar sein. Dabei handelt es sich typischerweise um Daten von externen Personen, Gebäudestrukturen, Sicherheitszonen, Zutrittssystemen und deren Komponenten. Eine Management Plattform für Zutrittsmanagement muss in der Lage sein, die angeschlossenen Zutrittssysteme, idealerweise sogar direkt deren Einzelkomponenten, möglichst automatisch und vollständig zu steuern. Somit ergibt sich die Möglichkeit, Berechtigungssteuerung unabhängig von Herstellersystemen oder Technologien zu modellieren und umzusetzen. Je nach Möglichkeiten der proprietären Systeme sind dies:

- vollständiges Lifecycle Management der Personenstammsätze (erstellen, ändern, sperren, löschen und deaktivieren)
- vollständige Berechtigungen berechnen und automatisch aktivieren: das Management System steuert bis auf Endgeräteebene den Zutritt (zum Beispiel Leser, Schlüssel, Offline-Berechtigung, Berechtigung auf ein Depotfach und Kombinationen daraus)
- „Einsammeln“ von definierten Buchungsereignissen aus den Subsystemen für bedarfsorientiertes Reporting.

Zentrale Reporting- und Steuerungsstelle

In einer zentralen Plattform müssen alle Regeln und Vorgänge über die angeschlossenen Prozesse und Systeme hinweg zusammenfließen. Sicherheitsvorgaben werden hier definiert und an alle Systembestandteile automatisch verteilt. Ein zentrales Reporting gibt jederzeit und auf einen Klick Auskunft darüber, welche Berechtigungen ein Mitarbeiter im Unternehmen hat. Dies ist unabhängig von den betroffenen Zutrittssystemen, der Tatsache, ob eine Person einen mechanischen Schlüssel oder einen Mitarbeiterausweis verwendet oder ob der Zutritt über biometrische Merkmale erfolgt. Es muss einfach abrufbar sein, welche Berechtigungen und somit welchen Zugang zu welchen Räumen eine Person hat und welche die zugrundeliegenden Anträge sowie deren Genehmiger sind oder waren. Diese Informationen müssen sowohl für historische als auch für zukünftige Zeiträume gleichermaßen verfügbar sein.

Elektronische Workflow- und Genehmigungsprozesse sowie Self Services sind in vielen Unternehmen im Einsatz. Prozesse im Bereich der physikalischen Sicherheit benötigen für die Steuerung oftmals sehr spezifische Informationen (zum Beispiel die Art der Sicherheitszone, die Kritikalität der Schutzziele), welche den herkömmlichen Workflow-Systemen nicht zur Verfügung stehen. Aus diesen Gründen sollten solche zentralen Systeme auch in der Lage sein. Standardprozesse anzubieten, die betrieblich angepasst werden können.

Darüber hinaus ist es erforderlich, dass solche Managementsysteme weitere Funktionen – in der Regel als Module – direkt anbieten oder Schnittstellen zu anderen Spezialanwendungen besitzen, etwa Besuchermanagement beziehungsweise Verwaltung von Externen, Identitäten- und Medienverwaltung wie RFID-Ausweise, biometrische Merkmale und Schließmedien sowie Unterweisungsmanagement und Gebäude- beziehungsweise Raumplanung und deren Verwaltung.

Einfacher, rollenbasierter Zugriff für alle Berechtigten

Die Benutzer solcher Systeme, insbesondere bei Self-Service-Anwendungen, sollten sehr einfach auf die Anwendungen und Prozesse zugreifen können. Die Zugriffssteuerung und deren Berechtigung erfolgt idealerweise automatisiert und die Bedienung der Systeme über den vorhandenen Browser, das ist heutzutage obligatorisch, ohne jegliche Installation von lokalen Softwarebestandteilen. Die Authentifizierung sollte automatisch über Single Sign On erfolgen,

damit der persönliche Zugriff schnell und sicher möglich ist.

Jede relevante Änderung im Managementsystem, ob sie nun durch Schnittstellen oder durch direkte Prozessvorgänge innerhalb des Systems initiiert wurde, muss nachvollziehbar, transparent und revisionssicher mit einer zentralen Funktion für die beteiligten spezifischen Personengruppen abrufbar sein. Im gleichen Maße sind diese Daten entsprechend den gesetzlichen und betrieblichen Datenschutz- und Datensicherheitsvorgaben zu behandeln. Dazu gehört auch das Sicherstellen von Datenlöschungen und die Datenvermeidung.

Systeme integrieren, Lebenszyklen beherrschen, regelbasiert automatisieren

Die entscheidende Herausforderung aus Sicht der Verantwortlichen für die physikalische Sicherheit ist: Wie können die Sicherheitsvorgaben trotz permanenter Veränderungen in der täglichen Unternehmenswelt tatsächlich operativ umgesetzt und die Ergebnisse validiert werden? Konkret: Wie kann sichergestellt werden, dass alle Änderungen an die beteiligten Systeme weitergegeben und die Vorgaben exakt und nachprüfbar eingehalten werden? Aus IT- und Prozesssicht müssen alle relevanten Veränderungen automatisiert an die entsprechend relevanten Systeme übertragen werden, um permanent über tagesaktuelle (Zutritts-) Berechtigungen zu verfügen. Diese Veränderungen gelten insbesondere für

- Personen (intern, extern)
- Organisationen und deren Organisationseinheiten
- Gebäude und deren Nutzung
- Zutrittssysteme und deren Komponenten
- Berechtigungsvorgaben selbst.

All diese Veränderungen – egal ob sie aus den führenden Systemen oder aus Prozessvorgängen generiert werden – müssen erkannt, bewertet und dann automatisch an die entsprechenden Systeme weitergeben werden, um die gewünschten Schutzziele sicherzustellen.

Der Einsatz derartiger zentraler Management Systeme gewährleistet diese Mechanismen und ermöglicht den Verantwortlichen mehr strategische Optionen hinsichtlich des Betriebs unterschiedlicher Herstellersysteme beziehungsweise Technologien. Darüber hinaus werden durch die konsequente Anbindung von Systemen, durch leistungsfähige Schnittstellen und die Bereitstellung von Prozessen und Self Services, Medienbrüche eliminiert und der manuelle Bearbeitungsaufwand minimiert.

Peter Kiess, Geschäftsführer Gis GmbH
www.gis-consulting.de

Artikel als PDF
www.sicherheit.info
Webcode: 1140539