advisio
CORPORATE CONSULTING

Zutrittsmanagement in Rechenzentren

Das Identity- und Access Management (IAM) im Umfeld der physischen Sicherheit

Ein Bericht von Andreas Budich, Senior Consultant für Sicherheitsmanagement, Informationssicherheit, Datenschutz und Risikomanagement bei der advisio GmbH.

Zutrittsberechtigungen zu Gebäuden und Räumen mit Identity & Access Management (IAM)

Das Identity- und Access Management (IAM) im Umfeld der physischen Sicherheit ist ein unverzichtbarer Teil der IT-Organisation. Durch Authentifizierung und Autorisierung wird klar hinterlegt, wer wo zugangsberechtigt ist. Auch die Prozesse für das Management physischer Zutritte gehört zu einem IAM, sind doch Zutritte zu Gebäuden und Räumen ebenso kritisch, wie Zugriffe auf Daten und Applikationen, das Zutrittsmanagement sollte also ebenfalls im Fokus stehen.

Das IT-bezogene Zutrittsmanagement und das physikalische Zutrittsmanagement folgen dabei den gleichen Spielregeln, für den RZ-Betreiber ist dieser Ansatz der Schlüssel für überprüfbare Zutrittsprozesse.

In allen Einrichtungen der Kritischen Infrastruktur ist Zutrittsmanagement ein zentraler Aspekt der physischen Sicherheit. Am Beispiel Rechenzentren (RZ), die als Housing-Anbieter agieren, ist dies besonders gut erkennbar. Der Zutritt für die (IT-)Techniker der jeweiligen Kundenunternehmen ist einerseits exklusiv auf die jeweiligen Kundenbereiche zu begrenzen (Mandantenfähigkeit), andererseits benötigen die Techniker des RZ-Unternehmens Zugriff auf Infrastrukturbereiche, in die der Zutritt für Kunden nicht möglich sein soll.

Inhaltsübersicht

1.	Die rollenbasierte Rechteverwaltung als elementarer Erfolgsfaktor	3
2.	Funktionsbezogene Aufgabenbeschreibungen	3
3.	Funktionsbezogene Sicherheitsbereiche	4
4.	Steuerung der Zutrittsrechte	5
5.	Elemente des Zutrittsmanagements	6
6.	Anmerkungen	8

1. Die rollenbasierte Rechteverwaltung als elementarer Erfolgsfaktor

Bei Zugriff, wie auch bei Zutritt gilt der Grundsatz der Betriebsnotwendigkeit. Auf der einen Seite ist zu gewährleisten, dass jeder Mitarbeiter alle zur Aufgabenerfüllung notwendigen Werkzeuge erhält, auf der anderen Seite sind die Privilegien so zu beschränken, dass wissentliche oder unwissentliche Manipulationen in kunden- und fachfremden Arbeitsgebieten ausgeschlossen sind. Aus dem Unternehmenszweck und den sich daraus ergebenden Betriebsprozessen sollten sich die erforderlichen Rechte ableiten lassen.

2. Funktionsbezogene Aufgabenbeschreibungen

Fast zwangsläufig wird über den funktionsbezogenen Ansatz klar, auf welche Anwendungen, Services und Dateien mit welchen Rechten zugegriffen

werden darf. Genauso ergibt es sich aus dieser Betrachtung, welche Räumen betreten werden dürfen.
Die Administrierbarkeit wird hierbei durch Zuweisung von Rollen zu sinnvoll zusammengefassten Zugriffsprofilen vereinfacht. Bevorzugt wird ein bereits vorhandenes IAM-Tool genutzt, so dass die Zugriffsrechte- und Zutrittsrechteverwaltung einheitlich gesteuert werden

3. Funktionsbezogene Sicherheitsbereiche

Auf Basis eines Sicherheitszonenkonzepts werden funktionsbezogene Sicherheitsbereiche definiert, die wiederum Rollen zugeordnet werden. Für den einzelnen Mitarbeiter ergibt sich daraus ein Zutrittsrechteprofil. Der modulare Aufbau verschiedener Zutrittsrollen ermöglicht eine überschneidungsfreie Zuordnung der Rollen zu einer Funktion, z.B. die Zutrittsrolle „allgemeine Verwaltung“, die jeder Mitarbeiter erhält und „IT-Räume“, die sich aus der Funktion z.B. eines Netzwerkadministrators ableiten. Jede Zutrittsmöglichkeit sollte idealerweise nur einer Zutrittsrolle zugeordnet werden.

Die so entstandene Matrix erlaubt eine einfache und nachvollziehbare Zuordnung eines Mitarbeiters zu einer oder mehreren Rollen. Aus dieser „bedient“ sich die Zugriffsverwaltung, genauso wie die Zutrittskontrollanlage. Das mühselige und oft nicht mehr nachvollziehbare Zuweisen von Einzelrechten entfällt. Jede Veränderung von Zutrittsbereichen, beispielsweise durch Hinzufügen einer zutrittskontrollierten Tür oder den Zugang zu einer neuen Anwendung, wird automatisch an alle Nutzer der entsprechenden Rolle verteilt.

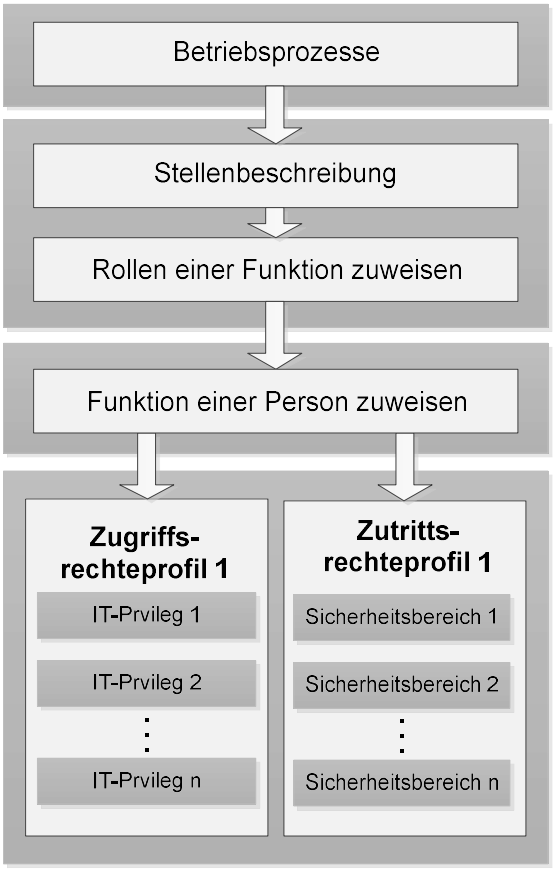

Abb. 1 Zusammenhang Zutritts- und Zugriffsmanagement beim RZ-Betreiber

4. Steuerung der Zutrittsrechte

„Zutritt managen“ ist mehr als nur der Betrieb einer Zutrittskontrollanlage (ZKA). Vom Ablauf her betrachtet ist die ZKA nur ein Erfüllungsgehilfe, denn auch eine Schließanlage oder ein Pförtner können Teil der Prozesskette sein. Wichtig ist das Zutrittsrecht, welches sich in unterschiedlichen Ausprägungen zeigt:

- Digital hinterlegtes Recht, welches z.B. durch eine Zutrittsausweis oder durch ein biometrisches Merkmal wahrgenommen werden kann.
- Organisatorisch hinterlegtes Recht, z.B. durch Namenslisten an der Pforte

- Mechanisch hinterlegtes Recht, wie es typischerweise mit einem Schlüssel verbunden ist

Die Zutrittsrechtesteuerung sollte so funktionieren, dass alle Ausprägungen des Zutrittsrechts („Träger des Zutrittsrechts“) transparent gemanagt werden. Eine Parallelwelt, z.B. durch eine getrennte Schlüsselverwaltung, führt unweigerlich zu Inkonsistenzen im Zutrittsmanagement.

5. Elemente des Zutrittsmanagements

Ein administrierbares und prüffähiges Zutrittsmanagement setzt sich aus mehreren Teilaspekten zusammen:

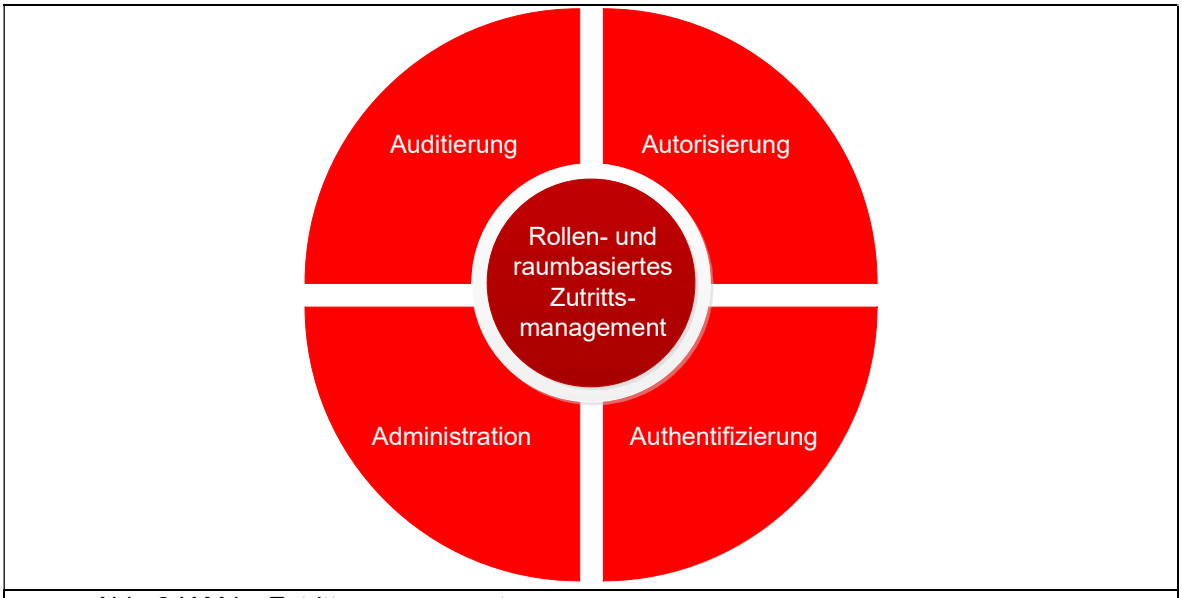

Abb. 2 IAM im Zutrittsmanagement

5.1 Autorisierung

Die Autorisierung definiert die Zuweisung von Rechten; eine Person wird in die Lage versetzt, etwas tun zu dürfen. Dieser Bereich gliedert sich in die Teilbereiche

- „Recht zur Veränderung in der Zutrittskontrolle“ im Sinne eines abgestuften Zugriffskonzepts zur Administration der ZKA,
- dem „Recht zur Vergabe von Zutrittsrechten“ und
- dem „Zutrittsrecht“ selbst. Im Sinne einer revisionssicheren Dokumentation ist es unabdingbar, dass jeder dieser Bereiche schriftlich festgelegt und durch eine berechtigte Person freigegeben wird. Mit der Autorisierung sollte generell eine Einweisung in die Regeln des Zutrittsmanagements verbunden sein.

5.2 Authentifizierung

Die Authentifizierung existiert in zwei Ausprägungen. Einerseits wird die Identität des Privilegien-Besitzers bei der Zuordnung/ Aktivierung der Rechte überprüft, beispielsweise bei der Übergabe des Zutrittsmediums (z.B. Chip-Karte). Andererseits wird bei jeder Buchung am Ausweisleser kontrolliert, ob das Zutrittsrecht aktuell noch besteht und Zutritt gewährt werden kann.

5.3 Administration

Die Autorisierung schafft die Grundlagen der Berechtigungszuordnung, im täglichen Betrieb findet diese ihren Niederschlag in der Administration der Rechteverwaltung. Zunächst gibt es die vertrauten Rollen „Administration Zutrittskontrolle“, gegebenenfalls mit verschiedenen Stufen, und in der

operativen Umsetzung „Parametrierung Zutrittsrechte“ durch den Sicherheitsmitarbeiter. Administration kann aber auch die Verwaltung von Schlüsseln bedeuten.

5.4 Auditierung

Ein ungeliebter, aber bedeutender Aspekt für funktionierendes und transparentes Zutrittsmanagement ist die Auditierung der Rechtezuordnung, die den Nachweis einer einwandfrei funktionierenden Prozesskette durch interne Prüfungen und externe Revisionen erbringt. In regelmäßigen Abständen wird intern im Vier-Augen-Prinzip geprüft, ob die Struktur der Berechtigungserteilung noch mit der Organisation des Unternehmens übereinstimmt. ebenso sind alle Personen mit einem Zutrittsrecht darauf zu überprüfen, ob sie dieses Recht noch benötigen. Hier liegt der Prüfschwerpunkt auf dem Abgleich der Vorgabedokumentation und der Umsetzung in der Zutrittskontrollanlage. Externe Auditoren ergänzen diese Betrachtung durch Prüfung des vorgelagerten Autorisierungsprozesses.

6. Anmerkungen

Das reibungslose Zusammenwirken der Elemente des IAM im Zutrittsmanagement beim RZ-Betreiber selbst, wie auch im Zusammenwirken mit den RZ-Nutzern ist als Baustein für umfassende Informationssicherheit eine unabdingbare Voraussetzung für ein funktionierendes Zutritts- und Zugriffsmanagement in Rechenzentren.

Diese Ausführungen beziehen sich nur auf den Regelprozess für permanent Zutrittsberechtigte. Im Grundsatz lassen sich die Gedanken auch auf das

Besuchermanagement (für temporär Zutrittsberechtigte), notfall- und störungsbedingte Zutritte, eingeschränkt auch auf Sonderzutritte (durch Polizei oder Feuerwehr etc.) übertragen.

Über advisio

Das Team der advisio GmbH besteht aus kompetenten Mitarbeitern, die langjährige Erfahrung im Sicherheitsmanagement, in der Informationssicherheit, im Datenschutz, bei Digitalisierung und weiteren Betriebsprozessen haben.

Der Aufbau von Sicherheitsmanagementsystemen gehört zu unseren Kernkompetenzen. Business Impact Analysen, Risikoanalysen, Erstellung von Maßnahmenplänen, Schulungen und Notfallplanung werden auf Wunsch durch unsere Fach-Spezialisten durchgeführt. Dies nicht nur im Aufbau, sondern auch im Betrieb der Managementsysteme.

Über den Autor

Andreas Budich ist als erfolgreicher Senior Consultant und Auditor mit den Schwerpunkten Informationssicherheit, Datenschutz und Sicherheitsmanagement tätig.
Er verfügt über umfassende Expertise im Bereich des Anforderungs- und Risikomanagements.
Herr Budich verfügt über ein hohes Maß an ausgewiesener Methodenkompetenz.