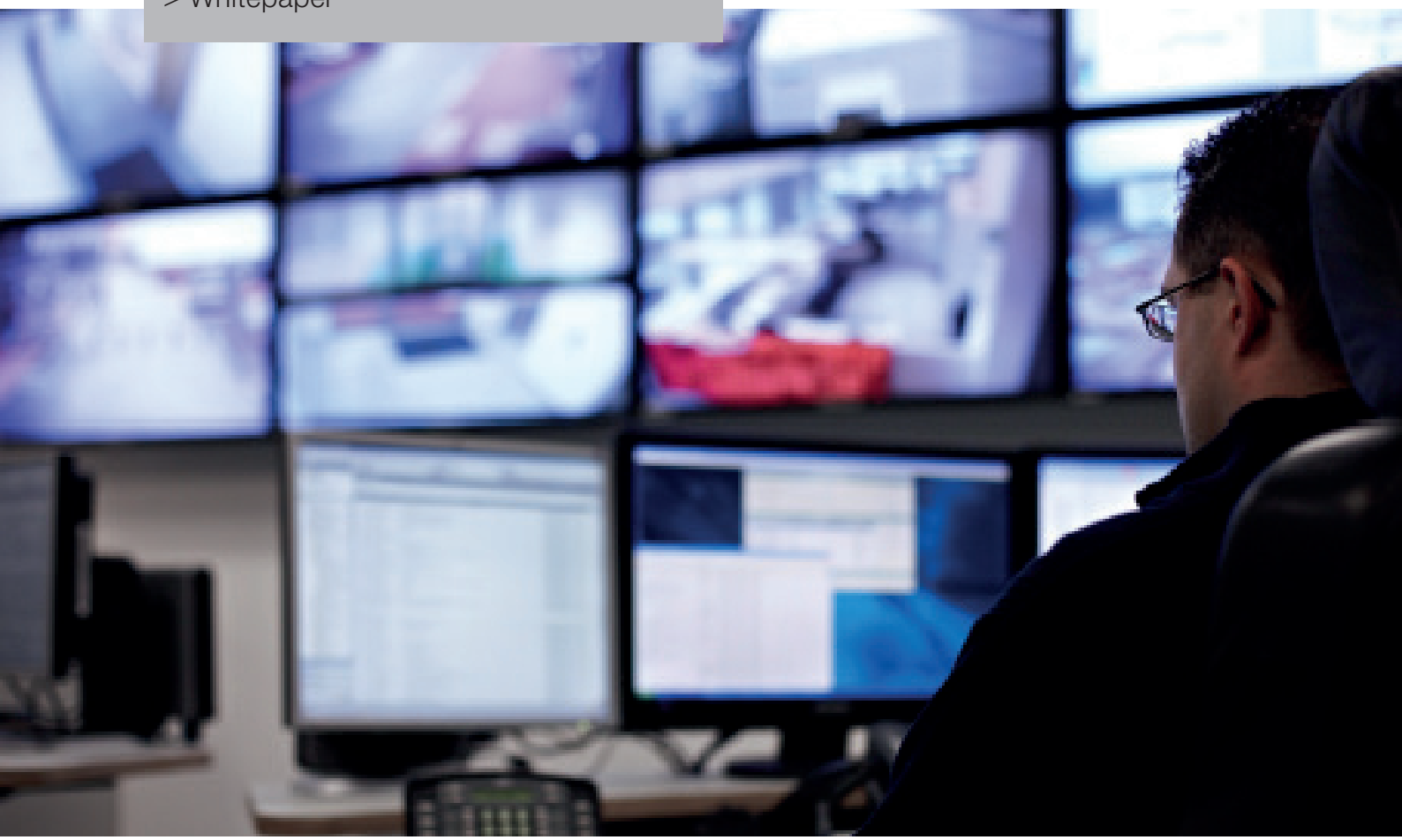
e-shelter

Zutrittsmanagement in Rechenzentren

Identity- und Access Management (IDM) im Umfeld der physikalischen Sicherheit

> Whitepaper



Zutrittsmanagement in Rechenzentren

IDM wird in der IT derzeit viel diskutiert. Weniger im Fokus ist das Zutrittsmanagement, welches in mehrfacher Hinsicht zu diesem Thema gehört.

In Rechenzentren, die als Housing-Anbieter agieren, ist Zutrittsmanagement ein zentraler Aspekt der Serviceleistung. 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. Der Betreiber des RZ, wie auch deren Nutzer sollten sich bei der Gestaltung des Zutrittsmanagements verdeutlichen, dass das IT-bezogene Zugriffsmanagement und das physikalische Zutrittsmanagement den gleichen Spielregeln folgen. Für den RZ-Betreiber ist dieser Ansatz Voraussetzung für überprüfbare Zutrittsprozesse.

Nachvollziehbare Herleitung von Rechten

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 unterbunden werden. Die erfolgreiche Rechte sollten sich aus dem Unternehmenszweck und den sich daraus ergebenden Betriebsprozessen ableiten lassen. Ein elementarer Erfolgsfaktor ist dabei die rollenbasierte Rechteverwaltung.

Dies erfolgt beim RZ-Betreiber durch 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, zutrittsseitig werden funktionsbezogene Sicherheitsbereiche auf Basis eines Sicherheitszonenkonzepts definiert, die wiederum Rollen zugeordnet werden. Für den einzelnen Mitarbeiter ergibt sich daraus ein Zutrittsrechteprofil. Jede Zutrittsmöglichkeit sollte idealerweise nur einer Zutrittsrolle zugeordnet werden. Der modulare Aufbau verschiedener Zutrittsrollen ermöglicht dann 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.

Die nun 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 nicht mehr nachvollziehbare Zuweisen von Einzelrechten entfällt. Jede Veränderung von Zutrittsbereichen, beispielsweise durch Hinzufügen einer zutrittskontrollierten Tür oder der Zugang zu einer neuen Anwendung, wird automatisch an alle Nutzer der entsprechenden Rolle verteilt.

Zusammenhang Zutritts- und Zugriffsmanagement beim RZ-Betreiber

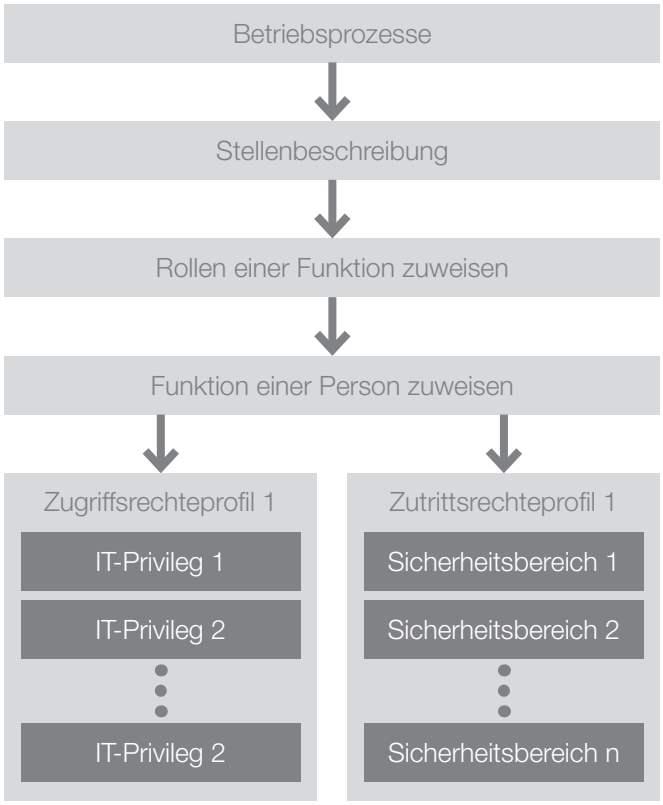


Abbildung 1

Elemente des Zutrittsmanagements im Rechenzentrum

„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.

Die **Autorisierung** definiert die Zuweisung von Rechten; eine Person wird in die Lage versetzt, etwas zu tun. Dieser Bereich gliedert sich in die Teilbereiche „Recht zur Veränderung in der Zutrittskon-

Zutrittsmanagement in Rechenzentren

trolle“ 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.

Die Authentifizierung existiert in zwei Ausprägungen. Einerseits wird die Identität des Privilegienbesitzers 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.

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.

IDM im Zutrittsmanagement

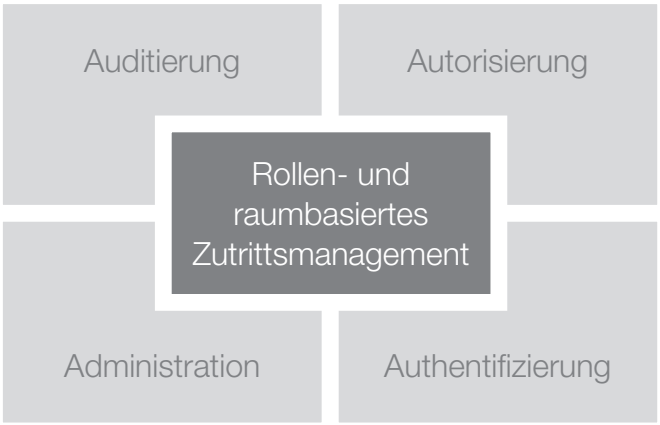


Abbildung 2

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.

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.

Das reibungslose Zusammenwirken der Elemente des IDM 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.

Autor: Andreas Budich, Director Compliance & Security Management,
e-shelter services GmbH

Informationen über e-shelter

Hochverfügbare Rechenzentren bilden das Rückgrat für die digitale Ökonomie und das Internet. Seit 2000 plant, baut und betreibt e-shelter hochverfügbare Rechenzentren, deren Infrastruktur den höchsten Standard physischer Sicherheit und betrieblicher Ausfallsicherheit gewährleistet. Das Unternehmen betreibt insgesamt rund 90.000 m² Rechenzentrumsfläche an acht Standorten. Davon allein 60.000 m² Fläche an seinem Hauptstandort Frankfurt am Main, der damit Europas größter einzelner Rechenzentrumsstandort ist. Weitere Standorte befinden sich in Berlin, Frankfurt, Hamburg, München, Wien und Zürich. Zu den e-shelter Kunden zählen Finanzdienstleistungsund Teleko-mmunikationsunternehmen sowie IT- und Cloud-Service-Anbieter. Als Teil von NTT Communications Corporation bietet e-shelter Zugang zu 140 Rechenzentren weltweit.

Unser eigenes Sicherheitspersonal der e-shelter security gewährleistet den Schutz unserer Rechenzentren und entwickelt Sicherheitskonzepte nach individuellen Anforderungen.

Mit unserer weitreichenden Erfahrung im Betrieb von Rechenzentren sind wir schon heute ein gefragter Ansprechpartner, besonders wenn individuelle Lösungen für komplexe Projekte und hohe Leistungsdichten gefragt sind. Aufgrund der Größe unserer Datacenter bieten wir insbesondere für hybride IT Lösungen die erforderliche Flexibilität und direkten Zugang zu Cloud-Anbietern.

www.e-shelter.de