



# Datacenter schützen

**Sicherheit** – Virtualisierte Datacenter sind in ihrer Rolle, Geschäftsprozesse zu unterstützen, nicht per se effizient und effektiv. Erst wenn sich die IT-Sicherheit um das Datacenter legt, profitiert das Unternehmen von den Geschäftsprozessen. Identity- und Access-Management setzt dazu den Hebel an den Applikationen an.

**D**ie meisten Anbieter und Anwender setzen Datacenter vor allem mit Servern, Speichern, flankierenden Geräten für Power & Cooling, Virtualisierung und Green-IT gleich. Für die Anbieter mit Interesse am Verkauf dieser Technologien mag diese Sichtweise aufgehen. Für die Anwender greift sie bei Weitem zu kurz. So bleiben über ein optimiertes Datacenter erwartete Leistungsschübe und Kosteneinsparungen schnell auf der Strecke, wenn die Sicherheit für die Anwendungen, Daten, Betriebs- und Geschäftsprozesse zu kurz greift. Dann drohen Geschäftsausfälle, unerwartete Zusatzaufwendungen, Datenklau, -zerstörung und -manipulation bis hin zu geschäftsschädigenden Imageverlusten. Return-on-Investment-(ROI-)Rechnungen werden dadurch buchstäblich auf den Kopf gestellt. Identity- und Access-Management (IAM) als Sicherheitsklammer um das Datacenter schützt vor solchen unliebsamen Überraschungen.

## Top-down die Unsicherheiten ausräumen

Das Datacenter erfüllt keinen Selbstzweck. Sinn und Zweck einer optimalen Datacenter-

Ausrichtung ist, die Geschäftsprozesse effizient und effektiv zu stützen. Die Verlässlichkeit und Qualität dieser Prozesse ist letztlich dafür entscheidend, wie gut oder schlecht das Unternehmen ins Geschäft kommt und im Geschäft bleibt. Das heißt im Umkehrschluss zweierlei: Erstens sollten die Anforderungen der einzelnen Geschäftsprozesse Top-down auf die IT-Infrastruktur des Datacenter abgebildet werden. Dabei sollten die Säulen »Speicher« und »Server«, genauer gesagt die dafür zuständigen Applikationen, besonders im Fokus der Top-down-Vorgehensweise stehen. Zweitens sollte direkt unterhalb der Geschäftsprozesse, bei den Applikationen, mit IAM der Sicherheitshebel angesetzt werden. Bevor Top-down weitere Sicherheitsmechanismen – so auf Netzebene, Betriebssystemebene und Virtualisierungsschicht – anvisiert werden sollten. Diese Sicht von Oben bewahrt den Datacenter-Betreiber davor, Sicherheitsvorkehrungen und -mechanismen durch unnötige Redundanzen kostspielig überzudimensionieren und zu verkomplizieren. Mit dieser Strategie wird außerdem der Sicherheitshebel vorrangig dort angesetzt, wo Angrif-

fe von Innen und Außen unmittelbar auf die Geschäftsabläufe durchschlagen.

## Alles gegenüber den Applikationen unter Kontrolle

Ein professionelles IAM-Modulset passt ideal zu dieser Absicherungsstrategie auf Applikationsebene. Über eine zentrale Benutzeradministration sind alle an den Geschäftsprozessen, genauer gesagt mit den Applikationen arbeitende Mitarbeiter, jederzeit eindeutig identifizierbar. Neuzugänge, Funktions- oder räumliche Veränderungen bei den Mitarbeitern können ad hoc im zentralen Benutzerverzeichnis »nachgezogen« werden. Über das Modul »Access Control« können sämtlichen Mitarbeitern jederzeit über das zentrale Verzeichnis die Zugriffsrechte und -rollen auf Applikationen zugewiesen werden, die sie zur Erfüllung ihrer Aufgaben brauchen. Gleich zielgenau und schnell können ihnen diese Rechte und Rollen, beispielsweise bei Ausscheiden eines Mitarbeiters, entzogen werden. Über diese für den Administrator hoch transparente Rechte- und Rollenvergabe werden nicht berechtigte Zugriffsversuche von Innen

und Außen verlässlich abgeblockt. Die unmittelbaren Träger der Geschäftsprozesse, die verarbeitenden und datenliefernden Applikationen, sind dadurch vor unberechtigter Benutzung gefeit. Sie können ungestört weiter Dienst tun.

### Administration absichern und transparent gestalten

Auch oder gerade von den Administratoren mit ihren erweiterten Befugnissen können Gefahren für die Applikationen und damit intakte Geschäftsprozesse ausgehen. Deshalb sind auch sie in die Zugriffskontrolle von IAM eingebunden. Durch eine feine Unterscheidung in Super- und normale Administratoren können zu vergebene Rechte und Rollen und damit Befugnisse gestaffelt werden. Werden Rechte und Rollen intelligent vergeben, kann so etwas wie ein Vier-Augen-Prinzip herausgebildet werden. Dadurch können selbst die Aktionen des Superadministrators kontrolliert werden. Umgekehrt kann er der Korrektheit seiner Rechtever-

Hintergrund freigeschaltet. Diese Hintergrundmethodik erspart den Mitarbeitern im Tagesverlauf viel Zeit. Nicht nur das: Der SSO kommt ohne für die Benutzer offensichtliche Autorisierungsprivilegien aus. Dadurch können die einzelnen Privilegien weder von ihnen vergessen werden noch geraten durch Abschaufen oder Zettelvermerke Applikationen durch unberechtigte Zugreifer in Gefahr. In beiden Fällen, ohne SSO, muss der Helpdesk immer wieder in Aktion treten. Er muss vergessene Privilegien wieder aktivieren oder (vermeintlich) gebrochene Privilegien durch neue ersetzen und sie sicher dem Mitarbeiter zuweisen. In jedem Fall wird zwischenzeitlich die Arbeit des Betroffenen unterbrochen, was komplette Geschäftsabläufe ins Stocken bringen kann.

### Compliance inbegriffen

Für den Schutz von Oben im Datacenter gewinnt außerdem das vierte IAM-Modul, Auditing & Reporting, für die Unternehmen an Be-

nen« lückenlos nachvollziehen und dokumentieren zu können.

Hier genau setzt das im IAM-System integrierte Auditing & Reporting an. Es schneidet alle Zugriffe, Folgeaktionen und Zugriffsversuche mit, um das Erfassungsmaterial anschließend über Reporting gezielt auszuwerten. Die Befolgung externer Vorschriften und interner Vorgaben kann dadurch ohne hohen Aufwand lückenlos und nachweislich dokumentiert werden. Gestärkt wird Compliance durch stets eindeutige Identitäten und ihnen zu jeder Zeit verbindlich zuzuordnende Rechten und Rollen. Zulässige können dadurch mittels Auditing & Reporting immer klar von unzulässigen Handlungen unterschieden werden. Das gilt auch für die Administratoren. Auch ihre Zugriffe und Handlungen werden darüber nachweislich transparent.

Eine zweite, stringente Methode für mehr Compliance ist, statt sich jeweils die Log-Dateien anschauen zu müssen, über Attribute den Hebel bei den Rollen anzusetzen. Eine applikationsunabhängige Rollenvergabe ist die Voraussetzung dafür. Dann kann im Revisionsfall schnell Soll und Ist jeder Rolle inklusive aller vergebenen Rechte gegenübergestellt werden. Durch diesen Compliance-Check wird unter anderem auch transparent, welche Rechte wirklich gewollt sind oder nicht. Gleich sicher können mit diesem Check nicht mehr aktuelle Rechte eliminiert werden. Diese Methode schafft für Compliance gerade bei automatisierten Prozessen wie Provisioning mehr Transparenz. Allerdings muss dazu der Hersteller des IAM-Systems diese zweite Methode einräumen.

### Intelligenz absichern

Ohne die unmittelbaren Träger der Geschäftsprozesse, die verarbeitenden und datenliefernden Applikationen, verlässlich vor Angriffen von Innen und Außen zu schützen, wird kein noch so gut optimiertes Datacenter das Unternehmensgeschäft hinreichend stützen. Hardwarezentrische Optimierungsmaßnahmen allein helfen dem Datacenter-Betreiber nicht weiter, solange die für ein profitables Geschäft gefährlichsten Flanken, die Applikationen, nicht vollständig gedeckt sind. Schon das erklärt, wie wichtig IAM mit seinen Modulen für ein insgesamt effizient und effektiv funktionierendes Datacenter ist. Dort, wo Hard- und Software sich ballen und nahtlos ineinander wirken, kann sich das Unternehmen Attacken auf die Programmier- und Geschäftsintelligenz am Wenigsten leisten. Und diese Intelligenz steckt nicht in der Hardware und in den Betriebssystemen, sondern in den geschäftsprozessstragenden Applikationen.

**Norbert Drecker,**  
Geschäftsführer von Twinsec



gabe gemäß dem Vier-Augen-Prinzip absichern lassen. Beides trägt auch auf der Administrationsseite zu mehr Zugriffssicherheit und Transparenz bei.

### SSO als Arbeitsvereinfacher und Prozessabsicherer

Über das dritte IAM-Modul, Single-Sign-On (SSO), werden die beiden Schritte Authentisierung (generelle Netzeinwahl) und Autorisierung (Berechtigungsprüfung gegenüber den Applikationen) in der Form kombiniert, dass die Mitarbeiter nur noch ihr Authentisierungsprivileg eingeben müssen. Die für sie autorisierten Applikationen werden danach automatisch im

deutung. Dafür sprechen viele Gründe. Mit der Virtualisierung wichtiger IT-Säulen wie Server und Speicher entsteht bereits innerhalb der IT-Infrastruktur ein komplexes Beziehungsgeflecht mit einer kaum nachvollziehbaren dynamischen Zuweisung dieser Kapazitäten. Aus diesem Geflecht heraus, wiederum, werden den Applikationen Daten und Verarbeitungskapazitäten automatisch zugeordnet. Das komplette Datacenter einschließlich der darin ablaufenden Applikationen wird dadurch förmlich zu einer Dunkelkammer mit undurchsichtigen Wechselbeziehungen. Dennoch ist es für Compliance, also für die Befolgung von rechtlichen Vorschriften und internen Revisionsauflagen, wichtig, Licht in dieses Dunkel zu bringen, zumindest die Zugriffe, Folgeaktionen und Zugriffsversuche mit Zielrichtung »Applikatio-