IDENTITÄTEN WIE SAND AM MEER

Benutzer- und Rechteverwaltung
im Digitalen Zeitalter

Im Zeitalter des Internets der Dinge werden Unternehmen von einer Vielzahl digitaler Identitäten bevölkert. Nicht nur Mitarbeiter, sondern auch Wearables, Computer, vernetzte Werkzeuge oder Applikationen haben eine digitale Identität. Um diese zunehmende Zahl von Identitäten spannt sich ein hochkomplexes Netz aus Informationen mit dazugehörigen Authentisierungs- und Autorisierungsverfahren.

ZUM SCHUTZ PERSÖNLICHER DATEN

Die Verwaltung all dieser Identitäten und Zugriffsrechte ist schwierig – und wird durch die neue EU-Datenschutzgrundverordnung (DSGVO), die ab Mai 2018 in Kraft tritt, nicht einfacher. Um persönliche Daten von Mitarbeitern, Kunden, Zulieferern etc. zu schützen, gibt es neue Richtlinien, welche Personen auf diese Informationen zugreifen dürfen. So sollten zu jedem Zeitpunkt nur diejenigen auf persönliche Daten Zugriff haben, die damit arbeiten müssen. Wechselt ein Mitarbeiter beispielsweise aus der Personalabteilung in einen anderen Unternehmensbereich, sollte ihm die Berechtigung, auf Bewerberdaten zugreifen zu können, entzogen werden.

WER IST ES – UND WAS DARF ER?

Damit das Management dieser zahlreichen digitalen Persönlichkeiten nicht im Chaos endet, brauchen Unternehmen eine regelkonforme, umfassende Lösung zum Identity und Access Management (IAM).

Eine effektive IAM-Lösung definiert zu jeder Zeit, welche digitale zu welcher natürlichen Identität gehört und welche Rollen und Rechte diese hat.

Dabei geht es nicht nur darum, jedem Mitarbeiter durch Nutzung automatisierter Prozesse und Workflows mit den erforderlichen Berechtigungen auszustatten. Es geht immer mehr darum, Unternehmen vor Cyber-Angriffen zu schützen. Laut einer Studie des Analystenhauses Pierre Audoin Consultants in Zusammenarbeit mit KuppingerCole, an der sich unter anderem Computacenter beteiligt hat, betrachten 65 Prozent der befragten Entscheider Schatten-IT als echte Herausforderung für eine sichere IAM-Lösung. Fast die Hälfte hält ein mangelndes Verständnis und unzureichende Schulungen der Mitarbeiter für die Hauptursache für IAM-bezogene Angriffe.

ALLE IDENTITÄTEN IM GRIFF

Computacenter bringt Ordnung in Ihr Identitäten-Chaos. Mit passgenauen Konzepten, die sich aus den folgenden Bausteinen zusammensetzen:

Access Management
- Zentrales Passwortmanagement für administrative Accounts
- Multifaktor-Authentifizierungslösungen
- Publik-Key-Infrastrukturen zur Ausstellung, Verteilung und Überprüfung digitaler Zertifikate

Provisionierung
- automatische Synchronisation von Personen- und Organisationsdaten
- Automatisierung von Administrationsvorgängen
- Self Services/IT Service-Portal
- Passwort-Reset-Verfahren

Identity Compliance
- Prüfung der Berechtigungen anhand eines Compliance-Regelwerks
- Auditing/Reporting der Prüfung

Rollenmanagement
- Effiziente Verwaltung der Berechtigungen mittels Rollenmodellierungen
- Role Mining und Definition der Rollen
- Definition von SOD-Regelungen

Computacenter

Computacenter AG & Co. oHG
Europaring 34–40, 50170 Kerpen

computacenter.de
+49 (0)2273 5970