

Datenklau schwer gemacht: Zugriffsrechte verwalten

Die Angst vor Datenklau geht um: Viele Unternehmen fürchten, dass unzufriedene oder gekündigte Mitarbeiter Firmendaten entwenden könnten. Nicht zu unrecht, wie eine Studie des Ponemon Instituts zeigt: 24 Prozent der Befragten haben nach dem Ausscheiden aus dem Unternehmen noch Zugriff auf ihren ehemaligen Arbeitsplatzrechner. Das darf und muss nicht sein. econet, der Experte für serviceorientiertes Identitätsmanagement rät: Wer sein Unternehmen umfassend gegen Datenklau absichern möchte, darf den richtigen Umgang mit Benutzerkonten und Zugriffsrechten nicht vernachlässigen.

Beim Thema Datenklau sollten Unternehmen den Schwarzen Peter nicht ihren Mitarbeitern zuschieben. Die Verantwortung für den Verlust

sensibler Daten tragen Firmen zum großen Teil selbst. Oft ist noch nicht einmal auf organisatorischer Ebene geklärt, wer worauf autorisiert ist, oder welche Unternehmensdaten als besonders kritisch einzustufen sind. Das findet entsprechend Abbildung in chaotischen Berechtigungs- und Dateisystemstrukturen und wird so zur Angriffsfläche für Datendiebstahl. Die kontrollierte Vergabe und zentrale Verwaltung von Zugriffsrechten mithilfe einer Identity Management-Lösung, wie cMatrix von econet, kann die Entwendung sensibler Daten zwar nicht hundertprozentig verhindern, beugt ihr aber zu einem großen Teil vor.

Ein solches System bietet die richtliniengesteuerte Rechtevergabe, einen umfassenden Überblick auf alle Berechtigungen von zentraler Stelle aus

sowie sicheren Rechteentzug. Scheidet ein Mitarbeiter aus, lässt sich ein De-Provisioning-Prozess aktivieren, wobei sein Benutzerkonto und sämtliche Zugriffsberechtigungen automatisch gesperrt und nach einem vorab definierten Zeitraum endgültig gelöscht werden. So können Unternehmen von vornherein sensible Daten schützen.

Der Bonus: Das System dokumentiert die Verwaltung der digitalen Identitäten revisionssicher, macht Vergabe und Entzug von Zugriffsberechtigungen nachvollziehbar und garantiert so die Einhaltung von Compliance-Vorgaben.

Gegen die Anhäufung von Rechten, wie dies beispielsweise bei Abteilungswechsel, Unternehmensfusion oder Umorganisation geschehen kann, hilft ebenfalls ein zentral gere-

geltes De-Provisioning. Berechtigungs-Audits geben jederzeit und auf Knopfdruck Aufschluss darüber, welcher User auf welche Daten Zugriffsrechte besitzt, oder welche Mitarbeiter für eine bestimmte Dateiablage berechtigt sind.

„Auf der CeBIT waren wir doch sehr überrascht, wie viele Unternehmen ganz konkret von Data Leakage – also Datenverlust und Diebstahl – betroffen sind. Doch haben wir auch die Bereitschaft der Unternehmen gesehen, die Verantwortung dafür zu übernehmen und mit der geordneten Verwaltung von Dateisystemen und Berechtigungen dagegen vorzugehen,“ erklärt Thomas Reeb, Vorstand der econet AG. „Im Ernstfall kann dann bei Kündigungen sofort reagiert werden und alle Daten sind auf Knopfdruck geschützt.“