

Sicherheitsrisiko Mitarbeiter

Gefahr durch Schlummerkonten

Mitarbeiter des eigenen Unternehmens gehören zu den größten Sicherheitsrisiken: Dies hat jetzt eine aktuelle Studie von McAfee und ICM Research bestätigt. econet warnt in diesem Zusammenhang vor den Gefahren, die durch einen sorglosen Umgang mit Benutzerkonten und deren Zugriffsrechten entstehen können.

Viele Unternehmen unterschätzen die Gefahr von Datendiebstahl: Nicht nur die so genannten Schlummerkonten von ehemaligen Mitarbeitern, die noch nicht gelöscht wurden, sondern auch Accounts von Anwendern, die urlaubs- oder krankheitsbedingt fehlen, können dabei zur Einstiegsschleuse für Datendiebe werden. So glauben viele Unternehmen, dass eine regelmäßige Überprüfung von Benutzerkonten auf deren Aktivität vor Missbrauch bewahre.

Weit gefehlt: „Oft wird übersehen, dass ein aktives Benutzerkonto eine Gefahr darstellen kann, denn es ist nicht gewährleistet, dass der rechtmäßige User selbst auf die für ihn freigegebenen Daten zugreift. Im Gegenteil: Ist dieser eine Zeit lang abwesend oder bereits aus dem Unternehmen ausgeschieden, können seine Zugriffsberechtigungen von anderen genutzt und für unlautere Zwecke missbraucht werden“, erklärt Max Peter, econet AG. „Manuelle Kontrollen, die nur darauf ausgelegt sind, inaktive Konten aufzuspüren, werden die von Datendieben gekaperten Accounts nicht entdecken können. Der Dieb mit einer gestohlenen digitalen Identität kann also ungehemmt weiter in internen Daten stöbern.“



Um diesem Problem von vornherein entgegenzuwirken, sollten Unternehmen daher Benutzerkonten für alle Mitarbeiter zentral verwalten. Dies ist mit einem serviceorientierten

Identity und Access Management zu bewerkstelligen.

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 auch temporäre Fehlzeiten wie Urlaub, Krankheit oder Mutterschutz ohne großen administrativen Aufwand abgedeckt werden. 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. www.econet.de