INFOGRAFIK

IDENTITÄTSABSICHERUNG IM TAKT DES UNTERNEHMENS

Unternehmensbenutzer nutzen zunehmend Cloudtechnologien, um kritische Funktionslücken zu schließen. Das Ergebnis ist eine Dezentralisierung von Identitätskontrollen – zu einem Zeitpunkt, zu dem sich Identität zu einem wichtigen Angriffsvektor entwickelt. Sehen Sie sich die Statistiken an und finden Sie heraus, wie Sie auf den wachsenden, geschäftsorientierten IT-Trend setzen können, ohne Einbußen bei der Sicherheit in Kauf zu nehmen oder auf Benutzerkomfort oder unbedingt erforderliche Anwendungen zu verzichten.

CLOUDNUTZUNG

90 %

der Unternehmen verwenden die Cloud in irgendeiner Form.[1]

13 ANWENDUNGEN

Anzahl der Cloudanwendungen, die heute in Unternehmen durchschnittlich verwendet werden.[2]

40 %

Prozentsatz der Anwendungen und Plattformen, die sich bis 2018 in einer typischen IT-Abteilung in den lokalen Systemen befinden (d. h. es befinden sich mehr Anwendungen in der Cloud).[3]

RISIKEN DER CLOUD

63 %

der bestätigten Datenschutzverletzungen sind auf schwache, standardmäßige oder gestohlene Passwörter zurückzuführen.[4]

41 %

der Organisationen sind über die Sicherheit von Cloud-Computing besorgt (unbefugter Zugriff und Datenintegrität und -sicherheit).[3]

95 %

der Fehler bei der Cloudsicherheit werden 2020 durch Verschulden des Kunden, nicht des Cloudanbieters entstehen.[5]

VERSTREUTE CLOUDS

56 %

der IT-Führungskräfte sagen, dass Unternehmensbenutzer Anwendungen von Drittanbietern erwerben.[6]

75 %

der IT-Führungskräfte befürchten, dass die Fähigkeit der IT, das Unternehmen vor Cyberangriffen zu schützen, durch die dezentralen IT-Aktivitäten geschwächt wird.[6]

13 %

Prognostizierte Wachstumsrate der IT-Aktivitäten in den Geschäftsbereichen in den nächsten zwei Jahren; die Prognosen für Unternehmensfunktionen umfassen Vertrieb (12 %), Marketing (11 %) und Finanzen (10 %).[6]

SICHERHEIT FÜR IDENTITÄTSINSELN

Es ist tatsächlich möglich, Ihr Unternehmen **voranzubringen** und dabei die **Identitätsrisiken zu vermindern**.

HINZUFÜGEN

von Zwei-Faktor- oder Multifaktor-Authentifizierung, um sich zu vergewissern, dass die Cloudbenutzer die sind, für die sie sich ausgeben.

STEUERN

des Cloudzugriffs durch Zuweisen von Berechtigungen für Systeme oder Anwendungen nach den geschäftlichen Anforderungen der Benutzer.

BEREITSTELLEN

von angemessenem Cloudbenutzerzugriff mithilfe von kontextbezogenen und Risk-Based-Authentication-Strategien.

[1]Datapipe: *Overcoming Cloud Security Challenges*, David Lucky, 6. Mai 2016
[2]Web Host Industry Review: *Slack May Be Sexier but Office 365 Most Used Cloud-Based Business App*, Chris Burt, 29. März 2016
[3]Forbes: *Analytics, Data Storage Will Lead Cloud Adoption in 2017*, Louis Columbus, 20. November 2016
[4]Verizon: *2016 Verizon Data Breach Investigation Report*
[5]eWeek: *IT Modernization Presents Opportunities, Risks for Industry Pros*, Don Reisinger, 30. Januar 2017
[6]The Economist Intelligence Unit: *The IT archipelago: The decentralization of enterprise technology*, 2016.

Mit einer innovativen Authentifizierungs- und Identitätsabsicherungslösung wie RSA SecurID® Access können Sie **den richtigen Personen den angemessenen Zugriff** auf Ihre Systeme und Ressourcen erteilen und dabei einen **ausgewogenen Kompromiss zwischen Sicherheit und Benutzerfreundlichkeit** eingehen:

MELDEN SIE SICH UNTER RSA.COM/TRYSECURID AN, UM EINE KOSTENLOSE TESTVERSION ZU ERHALTEN.

RSA