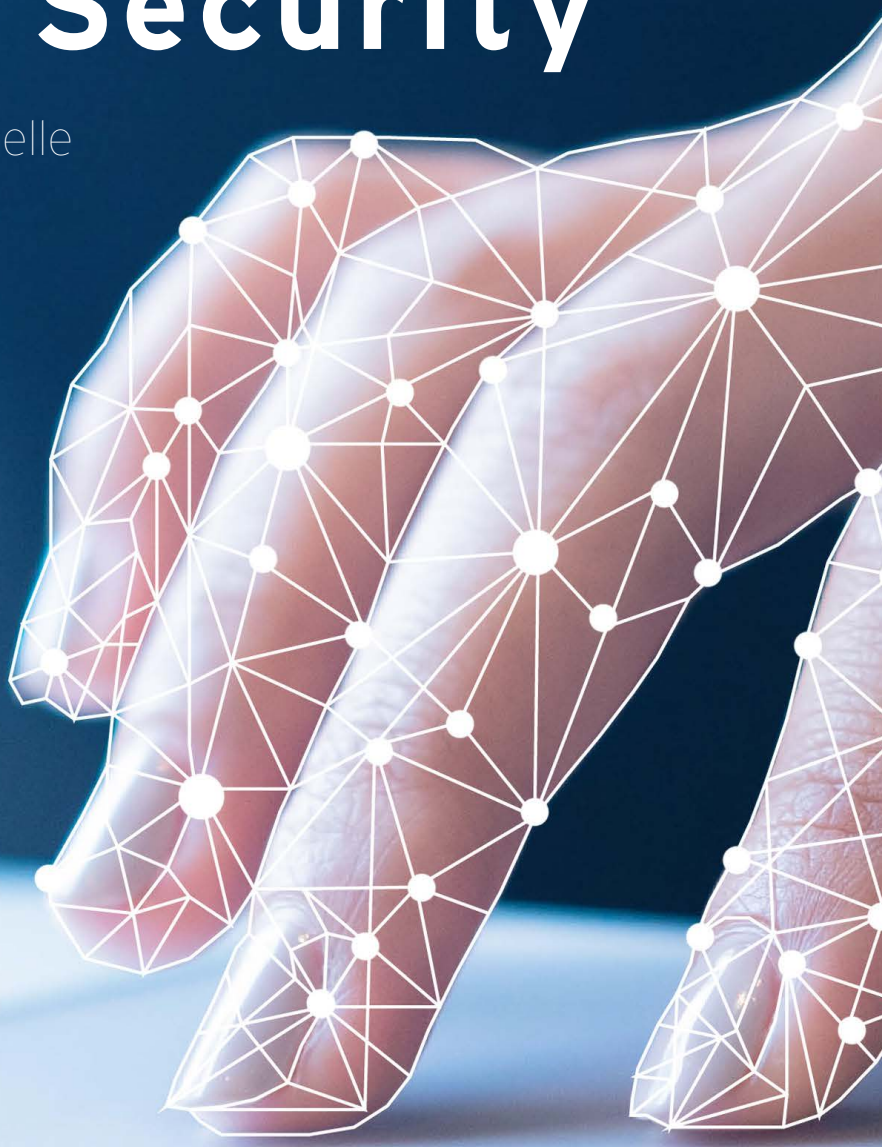
techconsult
The IT Market Analysts

Herausforderungen und Chancen beim Einsatz von **Identity Security**

Der Leaver als Gefahrenquelle



Unterstützt durch

SailPoint

Inhalt

Vorwort

Cloud, Home Office und mobiles Arbeiten – die neuen und veränderten Arbeitsweisen bedeuten auch ein Umdenken bei IT-Sicherheit. Während sich traditionelle Sicherheitsgedanken um die Absicherung von Endgeräten und Netzwerken beschäftigen, werden vorausgehende Aktivitäten meist unterschätzt. Denn mit jedem neuen Gerät und jedem neuen Cloud-Dienst steigt das Risiko, den Überblick über die Nutzer und deren Zugänge zu Unternehmensdaten zu verlieren. Besonders gefährlich wird es dann, wenn vergessen wird, einem Mitarbeiter, der das Unternehmen verlässt, auch wirklich alle Zugänge zu sperren.

Es muss sich die Frage gestellt werden, in welchem Ausmaß Unternehmen ihre Zugänge zu Unternehmensressourcen schützen. Werden automatisierte Identity Security Lösungen eingesetzt oder wird noch alles von der IT manuell freigegeben und entzogen? Wo stehen Unternehmen in Sachen Cloud-Adoption? Welche Probleme verhindern eine Einführung von Identity Security?

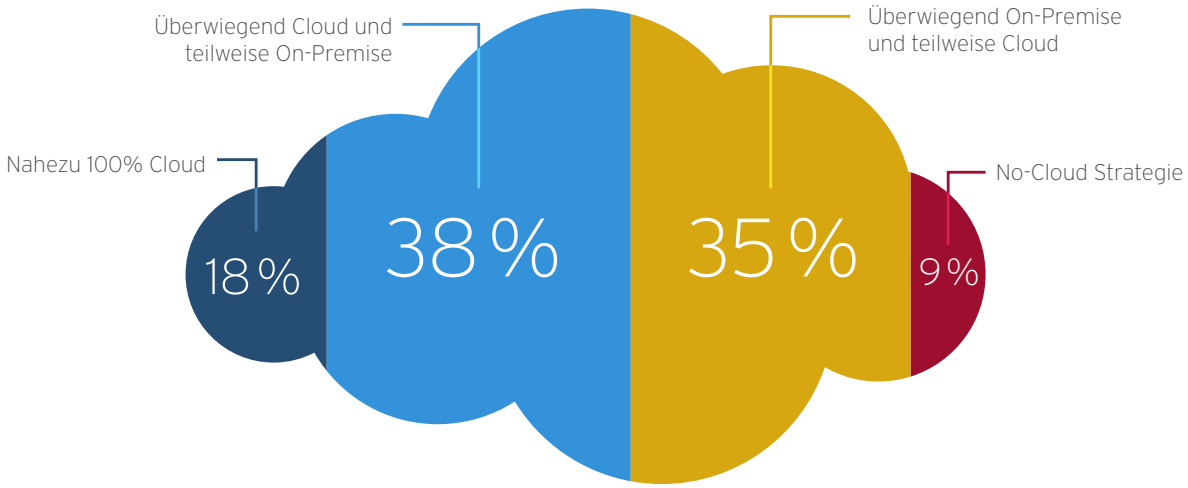
Um diesen Fragen auf den Grund zu gehen, wurden im Rahmen dieser Studie 100 Entscheider oder stark am Entscheidungsprozess beteiligte Personen zu ihren Eindrücken bezüglich Identity Security im Unternehmen, Herausforderungen beim Einsatz von Identity Security Lösungen, sowie den für sie größten Gefahren im Bereich IT-Security befragt. Dafür wurden Unternehmen ab 1000 Mitarbeitern über verschiedene Branchen hinweg im März 2021 befragt.

Cloud Boom in deutschen Unternehmen

Cloud-Technologien sind schon lange kein Neuland mehr. Nicht nur im privaten Bereich erfreuen sich Menschen der Nutzung der Cloud, auch in Unternehmen jeglicher Couleur spielt die Cloud eine immer größere Rolle. Die vielen Vorteile der Cloud sind unlängst fast jedem bekannt. Verringerte Anschaffungskosten und eine generelle Veränderung der Kostenstruktur, erhöhte Sicherheit durch die Expertise seitens der Anbieter oder auch die Möglichkeit flexibel Ressourcen bereitzustellen, sind nur einige der wichtigsten Pluspunkte im Einsatz von Cloud-Technologien.

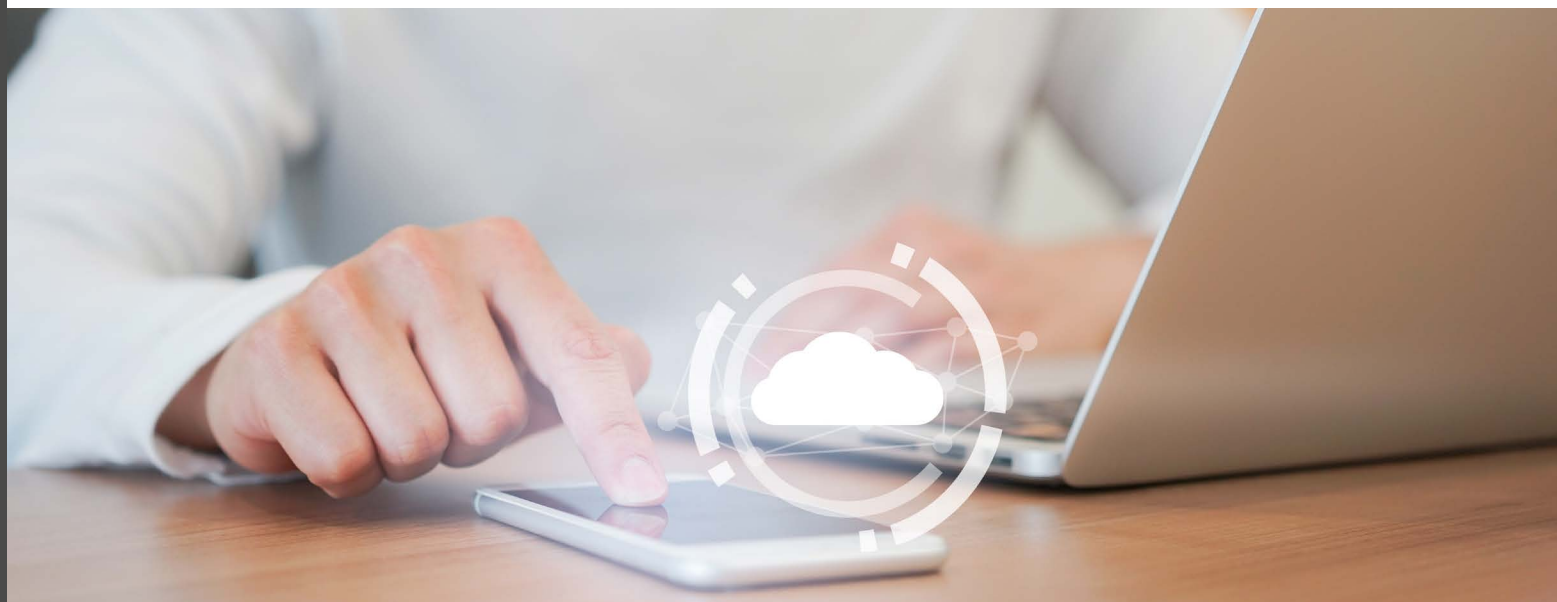
Durch den kurzfristigen Wechsel zur mobilen Arbeit haben Unternehmen viele oder alle Daten in die Cloud verlagert. Bereits heute überwiegt der Anteil an Unternehmen, die überwiegend auf die Cloud setzen jenen, die noch in klassischen On-Premise-Umgebungen unterwegs sind. Fast ein Fünftel der Unternehmen ab 1000 Mitarbeitern hat der On-Premise-Infrastruktur den Rücken gekehrt und setzt nahezu vollständig auf die Cloud.

Einsatz von Cloud-Lösungen



Basis: 100 Unternehmen

Dazu kommen noch knapp 40 Prozent, die überwiegend auf Cloud-Lösungen bauen, jedoch einige wichtige kritische Funktionen weiterhin vor Ort betreiben. Ein knappes Drittel der Unternehmen setzt primär auf lokale Lösungen, setzt aber punktuell auf die Cloud. Und weniger als 10 Prozent der Unternehmen setzen überhaupt keine Cloud ein. Hauptsächlich handelt es sich bei den „Cloud-Verweigerern" um Institutionen aus der Öffentlichen Verwaltung. Das kann vielfältige Gründe haben. Als Beispiele wären veraltete und starre Legacy-IT-Infrastrukturen oder ein allgemeines Hinterherhinken in Sachen Digitalisierung sein. Die Privatwirtschaft ist an diesen Punkten schon deutlich weiter und für die lässt sich definitiv sagen: Infrastrukturen auf Basis der Cloud sind nicht nur die Zukunft, sie sind bereits die Gegenwart.



Richtlinien erfordern Identitätssicherheit

Der Siegeszug der Cloud und die – auch durch die Pandemie – beschleunigte Digitalisierung sorgen auch für veränderte Arbeitsweisen. Überwiegend oder dauerhaft aus dem Home Office arbeiten, mit verschiedenen Endgeräten – dienstlich oder privat – auf Firmenressourcen zugreifen und die Nutzung verschiedenster Cloud-Dienste können für Arbeitnehmer und Arbeitgeber äußerst positiv sein.

Doch die schöne neue Welt sollte in IT-Abteilungen die Alarmglocken schrillen lassen. Denn die Kehrseite der Medaille sind nie da gewesene Risiken für die IT-Sicherheit. Immer mehr Applikationen, Cloud-Dienste und neue, strengere Datenschutz- und Compliancebestimmungen machen es IT-Abteilungen ungemein schwer den Überblick zu behalten und die entsprechenden Schnittstellen zum eigenen Unternehmen abzusichern. Während Maßnahmen zum Schutz von Endpunkten oder E-Mail-Servern in den meisten Unternehmen zum Standard gehören oder sollten, werden Themen wie Zugriffsberechtigungen gerne vernachlässigt. Welcher Nutzer hat mit welchen Geräten und welchen Applikationen Zugriff auf welche Unternehmensressourcen und Daten? Das sind alles Fragen, die sich Unternehmen im Zuge der fortschreitenden Digitalisierung stellen müssen und beispielsweise mithilfe einer geeigneten Identity Governance Strategie beantworten.

Identity Governance beschreibt eine Richtlinien-basierte und zentralisierte Steuerung von Identitätsverwaltung und Zugangskontrollen und ist dabei mehr als eine Identity und Access Management (IAM) Lösung. Neben den klassischen IAM-Funktionen werden mit Identity Governance Lösungen diese auch mit den Compliance-Vorgaben verbunden. So könne man beispielsweise die Zugriffe einzelner Nutzer überwachen, wie es bei einigen Richtlinien und Regelungen der Fall ist.

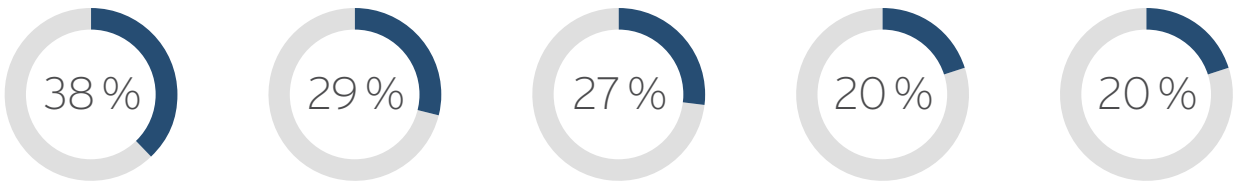
An welche Regelwerke und Standards sich Unternehmen halten müssen, hängt von der Art der Leistungserbringung der Unternehmen ab.

Beispiele für solche Regelwerke wären unter anderem die Mindestanforderungen an das Risikomanagement, kurz MaRisk, das für Banken und Finanzdienstleister vorgesehen ist oder auch Standards für die Sicherung von Kritischen Infrastrukturen (KRITIS), die aufgrund ihres hohen Stellenwerts besonders geschützt werden müssen.

Der höchste Anteil entfällt mit 38 Prozent auf KRITIS. Das ist wenig verwunderlich, denn KRITIS umfassen deutlich mehr Branchen, als das für zum Beispiel MaRisk der Fall ist. Unternehmen, die dem BSI-KritisV unterliegen, können aus dem Energiesektor, der Wasserversorgung, Telekommunikation, Finanzwesen, Logistik oder auch aus der öffentlichen Verwaltung kommen. Betreiber kritischer Anlagen müssen ein Mindestniveau an IT-Sicherheit einhalten und dafür Sorge tragen, dass diese vor erheblichen Schäden bewahrt werden. Dazu zählen Naturereignisse, technisches und menschliches Versagen sowie vorsätzliche Handlungen mit kriminellem Hintergrund. Während Ersteres nicht durch Identity Security Maßnahmen gestoppt werden kann, ist dies bei technischem und menschlichem Versagen sowie kriminellen Handlungen möglich.

Da scheint es unumgänglich zu sein, eine starke Identity Governance Lösung einzusetzen. Denn für Cyberkriminelle stehen unternehmenskritische Daten, beispielsweise Mitarbeiter-, Kunden- oder auch Finanzdaten ganz oben auf der Liste. Auch Cyberkriminelle wissen, dass das schwächste Glied der Sicherheitskette immer noch der Mensch ist. So nutzen Cyberkriminelle diese Schwachstelle gezielt, um in Systeme einzudringen, die über fast unüberwindbare technische Absicherung verfügen. Mit einer Identity Governance Lösung könnte ein solcher Vorgang abgewehrt werden. Beispielsweise durch die Tatsache, dass der Angreifer von einem nicht autorisierten System versucht in das Unternehmensnetzwerk einzudringen. Allein die Vorstellung, was ein Angreifer im schlimmsten Fall im IT-System eines Stromnetzbetreibers anrichten könnte, sollte Grund genug sein, die eigene IT-Sicherheit unter die Lupe zu nehmen und geeignete Identity Governance Lösungen einzuführen.

Regularien, Standards und Regelwerke im Unternehmen



Basis: 100 Unternehmen | Mehrfachnennungen

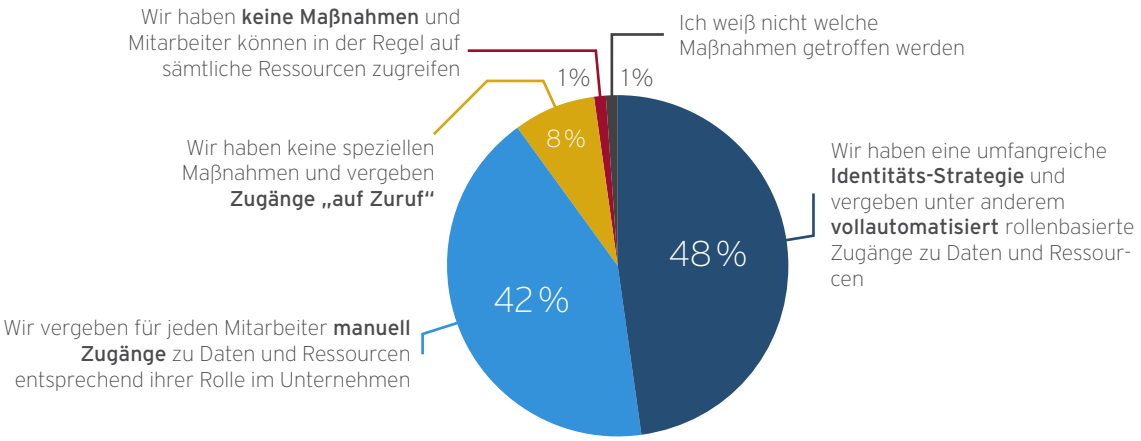
Identitätsmanagement vielerorts noch manuell

Doch wie genau sieht die Umsetzung von Identity Governance in den Unternehmen aus? Wird eher automatisiert oder noch manuell gearbeitet? Die Ergebnisse sind teilweise ernüchternd.

Weniger als die Hälfte der Unternehmen gab an, über eine umfangreiche Identitätsstrategie zu verfügen, mit der beispielsweise vollautomatisiert rollenbasierten Zugänge zu Daten und Ressourcen vergeben werden. 42 Prozent der Unternehmen vergeben Zugänge für jeden Mitarbeiter individuell und entsprechend ihrer Rolle im Unternehmen. Der Rest verfügt über keine vorab definierten Maßnahmen zur Steuerung von Zugängen und Zugriffsberechtigungen im Unternehmen.

Der hohe Anteil an manueller Freigabe kann als bedenklich angesehen werden. Denn wo immer der Mensch selbst Hand anlegen muss, steigt die Gefahr für etwaige Fehler und Versäumnisse. Beispielsweise könnte ein Mitarbeiter durch die IT-Abteilung eine falsche Rolle zugeteilt werden. Man stelle sich vor, ein Mitarbeiter erhält plötzlich Zugänge zu Ressourcen und Daten, die nur der Geschäftsführung vorbehalten sind. Die Informationen, die der Mitarbeiter erlangen könnte, wären für das Unternehmen fatal.

Zugänge und Zugriffsberechtigungen zu Daten und Ressourcen



Basis: 100 Unternehmen

Der Leaver: Hohe Gefahr für das Unternehmen

Nachdem für Mitarbeiter diverse Zugänge geschaffen worden sind, ob automatisch auf Basis von Rollen oder manuell, hört die Arbeit für die IT an dieser Stelle vorerst auf. Doch irgendwann kann der Tag kommen, an dem sich die Rolle des Mitarbeiters verändert, er in eine andere Abteilung wechselt oder das Unternehmen verlässt. Stellen Sie sich nun die Frage: Würden Sie nach vielen Jahren noch wissen, wer mit welchem Gerät Zugang zu welchen Ressourcen hat?

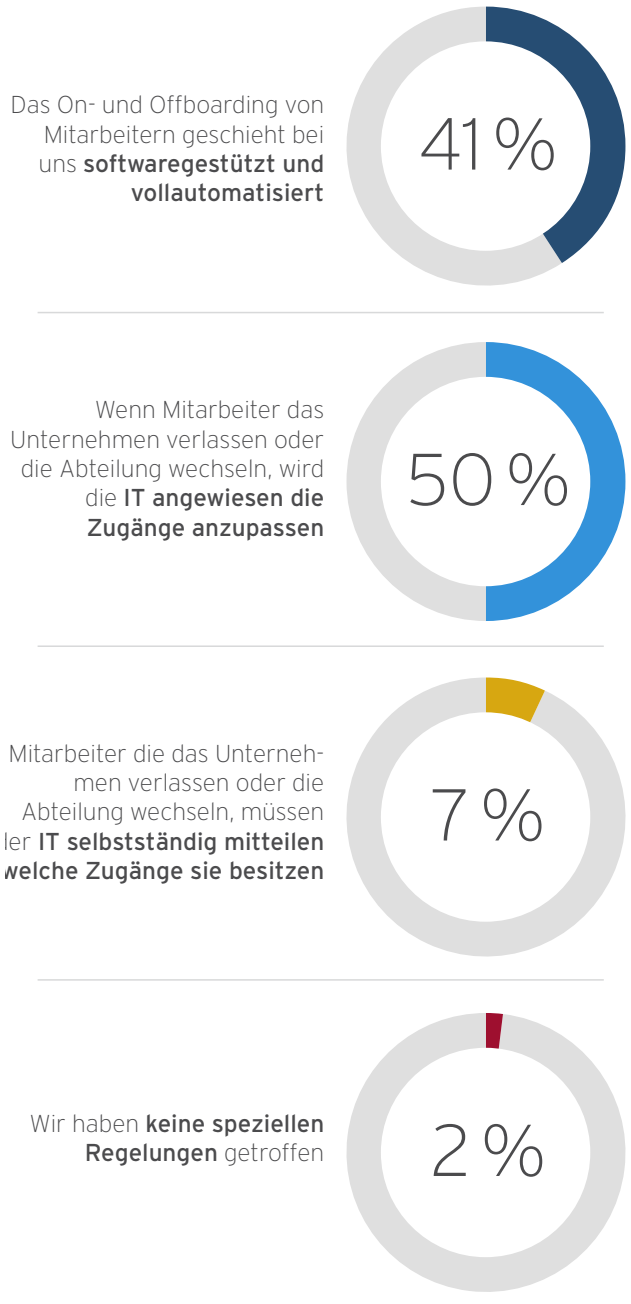
Dieses Problem lässt sich mit einer geeigneten Identity Governance Strategie relativ einfach beheben. Beispielsweise dann, wenn geeignete Maßnahmen für das On- und Offboarding von Mitarbeitern implementiert worden sind. Mit solchen Maßnahmen können neuen, wechselnden oder ausscheidenden Mitarbeitern softwaregestützt und vollautomatisiert Zugänge zugewiesen oder entzogen werden.

Wenn Mitarbeiter das Unternehmen verlassen oder die Abteilung wechseln, findet mehrheitlich noch ein manueller Prozess innerhalb der IT statt um die Rechtevergabe anzupassen. In der Hälfte der Unternehmen wird die IT von den Abteilungen oder dafür vorgesehenen Personen damit beauftragt die Zugänge entsprechend anzupassen und zu sperren. An dieser Stelle können eklatante Fehler entstehen. Vor allem dann, wenn beispielsweise nicht dokumentiert ist mit welchen Geräten betroffene Mitarbeiter Zugang zu Unternehmensressourcen haben. Stellen Sie sich vor, ein Mitarbeiter verlässt das Unternehmen und hat beispielsweise auf Zuruf einst einen Zugang zu bestimmten Cloud-Diensten mit seinem Privathandy erhalten. Wenn dies nicht dokumentiert ist, besteht die Gefahr, dass dieser Zugang einfach vergessen wird und der Mitarbeiter auch noch lange nach dem Ausscheiden aus dem Unternehmen Zugang zu sensiblen Unternehmensdaten hat.

Besser ist es vor allem im Hinblick auf die steigende Anzahl von mobilen und Home Office Arbeitsplätzen, BYOD-Strategien und der damit zusammenhängenden rapide ansteigenden Zahl von Geräten mit Netzwerkzugriff auf eine Strategie zu bauen, die vollautomatisiert agiert. Erfreulich, dass bereits 40 Prozent der Unternehmen auf automatisiertes On- und Offboarding von Mitarbeitern setzen.

Und das restliche Zehntel? Dieses hat keine Regelungen festgelegt oder verlässt sich darauf, dass Mitarbeiter, die das Unternehmen verlassen oder die Abteilung wechseln von sich aus bei der IT die Sperrung ihrer Zugänge beantragen. Ob das in ausreichendem Maß geschieht, kann an dieser Stelle bezweifelt werden. Vor allem bei Mitarbeitern, die nicht aus freiwilligen Stücken das Unternehmen verlassen.

Entfernen der Zugänge zu Daten und Ressourcen für Leaver/Mover



Basis: 100 Unternehmen

Finanzielle Probleme Hauptgrund für Versäumnisse

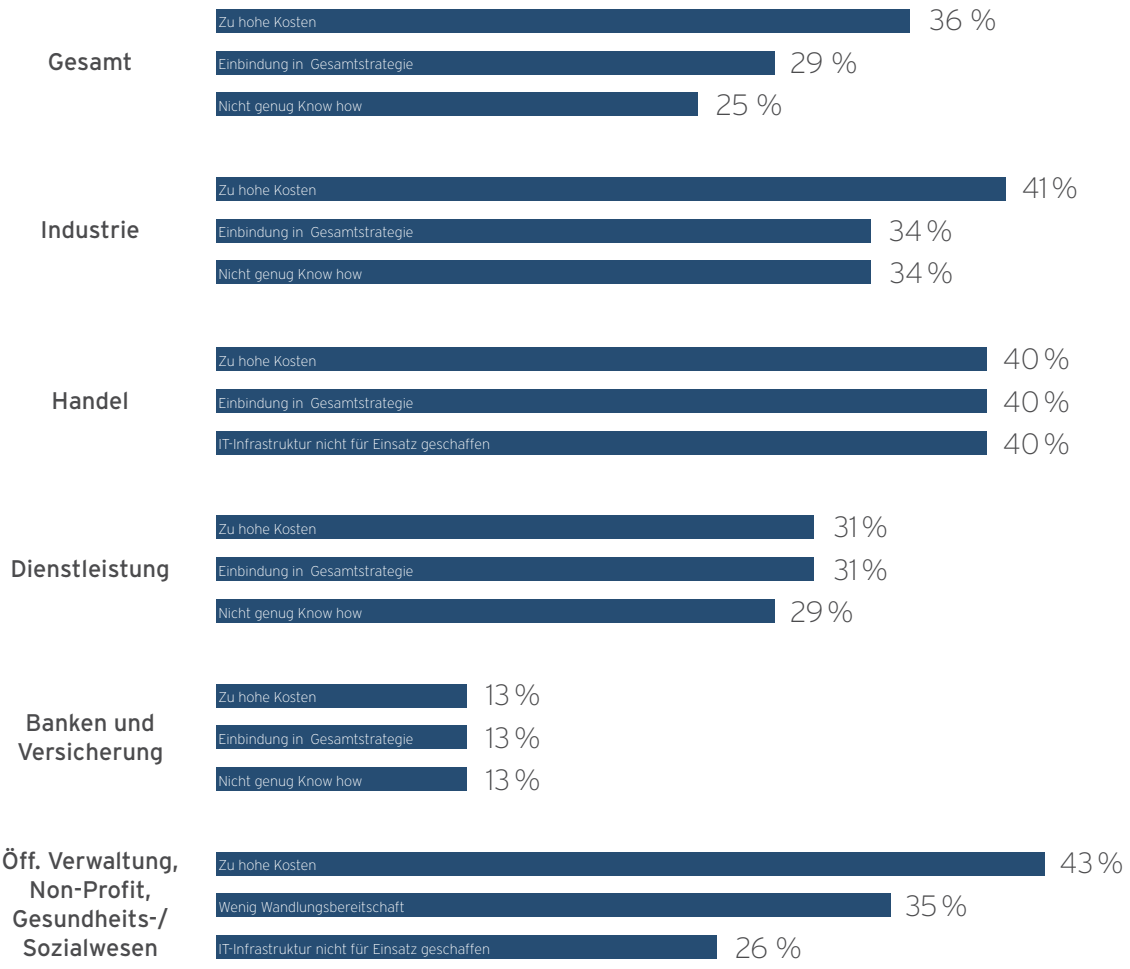
Obwohl Unternehmen von der Einführung einer Identity Governance Lösung profitieren würden, setzen immer noch zu viele Unternehmen auf manuelle Vorgänge. Doch warum genau gestaltet sich die Umsetzung einer Identity Governance Umsetzung so schwierig?

Einer der Hauptgründe ist unter anderem in den vemeintlich hohen Kosten für Identity Governance Lösungen zu finden. Während Unternehmen aus dem Finanzwesen mit der Kostenfrage nur wenige Probleme haben und für umfangreiche Identity Governance Lösungen tief in die Tasche greifen, sehen sich Öffentliche Verwaltungen, Industrieunternehmen oder der Handel hier stärker herausgefordert. In diesen Branchen sind es jeweils knapp 40 Prozent, die Kosten als Haupthinderungsgrund nennen. Das ist in Zeiten von Umsatzeinbußen in Folge der Pandemie nachvollziehbar. Dennoch sollten betroffene Unternehmen trotz allem ihre Identity Governance Strategie nicht vernachlässigen. Tatsächlich lässt sich Identity Governance ohne große Kosten im eigenen Unternehmen implementieren.

Das gelingt dann, wenn Identity als gemanagte, reine SaaS-Lösung bezogen wird. Hier werden klassische Kostenfaktoren herkömmlicher On-Premise-Lösungen vermieden und die Kostenstruktur bewegt sich einem OPEX- zu einem CAPEX-Ansatz.

Für 30 Prozent der Unternehmen gestaltet sich die Einbindung der Identity Governance Strategie in die Gesamtstrategie des Unternehmens. Auf Rang 3 folgt der Mangel an Know-how im Unternehmen, um umfangreiche Identity Governance Projekte umzusetzen. Ein Viertel sieht ein großes Kompetenzproblem im eigenen Unternehmen, welches sich jedoch recht pragmatisch lösen lässt. Fehlt die eigene Kompetenz, muss sie eben eingekauft werden. Zum Glück gibt es auf dem Markt Anbieter, die sich ganz speziell auf das Thema Identity Governance spezialisieren und Unternehmen bereitwillig unter die Arme greifen. So muss niemand im Blindflug versuchen Identity Governance selbst im Unternehmen zu implementieren, sondern kann sich vollkommen auf die Expertise der dedizierten Anbieter verlassen.

Die drei größten Probleme bei der Implementierung von Identity-Governance-Lösungen



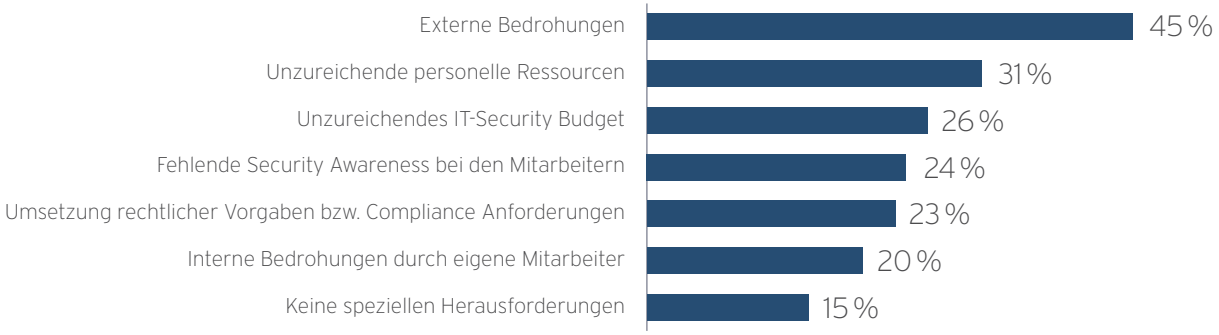
Basis: 100 Unternehmen | Mehrfachnennungen

Externe Bedrohungen und Budgetprobleme

Die bereits durchgeführten und noch bevorstehenden Veränderungen der Arbeitswelt hat auch Auswirkungen auf die IT-Sicherheit. Die Umsatzeinbußen, gekürzte Budgets und der oftmals sehr kurzfristige Umstieg auf mobile Arbeit stellen IT-Sicherheitsverantwortliche vor zahlreiche Herausforderungen. Die größten Sorgenfalten bereiten weiterhin externe Bedrohungen. 45 Prozent der Unternehmen nannten externe Gefahren als die Top-Herausforderung in diesem Jahr. Nahezu täglich entwickeln Cyberkriminelle neue Angriffsmethoden, um Schadsoftware in Unternehmensnetzwerke zu schleusen.

Und die Reaktionsgeschwindigkeit von Cyberkriminellen auf aktuelle Entwicklungen ist nicht zu unterschätzen. Beispielsweise wurde binnen kürzester Zeit das Coronavirus für Phishing-Kampagnen erfolgreich instrumentalisiert. Die Cyberkriminellen von den eigenen Unternehmensnetzwerken fernzuhalten sollte Kernaufgabe jeder IT-Abteilung sein. Dafür müssen die die internen Sicherheitsprozesse analysiert und bei Bedarf optimiert werden.

Herausforderungen im Rahmen von IT-Sicherheit



Basis: 100 Unternehmen | Mehrfachnennungen

Doch diese Analyse und Optimierung der eigenen Sicherheitsprozesse benötigt unter anderem Geld und Personal. Doch an diesen beiden Punkten hapert es in vielen Unternehmen. Immerhin landen unzureichende personelle Ressourcen und unzureichende IT-Security Budgets direkt hinter den externen Bedrohungen auf Rang 2 und 3 der Topherausforderungen in diesem Jahr. Die Krise hat einen klaren Effekt auf die Budgetsituation in den Unternehmen. Viele versuchen die sinkenden Umsätze durch strikte Kostenkontrolle aufzufangen.

Dazu gehören eben nicht nur reine Kostensenkungen, sondern auch Personalabbau. Unternehmen müssen trotz der Krise weiterhin versuchen, ein Gleichgewicht zwischen Kostensenkungen in der IT und der bestmöglichen IT-Exzellenz zu erreichen. Nur so gelingt es Unternehmen am Ende nicht als Verlierer der Krise da zu stehen. Unternehmen sollten weiterhin die notwendigen Investitionen tätigen, um die langfristige Wettbewerbsfähigkeit zu erhalten oder sogar steigern.

Fazit

Durch die Krise ändern sich die Arbeitsweisen von vielen Unternehmen sehr kurzfristig. Während immer mehr Menschen mobil arbeiten und der Einsatz von Cloud-Diensten immer weiter ansteigt, werden Sicherheitsaspekte oftmals erst nachgelagert beachtet. Einer dieser vernachlässigten Sicherheitsaspekte ist der Schutz digitaler Identitäten.

Dabei sollten Unternehmen mehr denn je darauf Wert legen, Überblick über die Zugänge ihrer Mitarbeiter von außerhalb des Unternehmensnetzwerks zu erlangen, um nicht beispielsweise im Zuge von ausgeklügelten Phishing-Kampagnen, Opfer von Cyberkriminellen zu werden. Denn Cyberkriminelle passen sich schnell an neue Situationen an und greifen gezielt die Schwächen des Menschen an, um sich Zugriff auf geschäftliche Konten zu verschaffen.

Leider haben nicht alle Unternehmen die Notwendigkeit der Sicherung von Identitäten erkannt und verwenden noch heute hauptsächlich manuelle Verfahren, um Zugriffe auf Daten und Unternehmensressourcen zu vergeben. Hier können viele Fehler entstehen. Es empfiehlt sich daher, auf eine moderne und vollautomatisierte Identity Governance Lösung zu setzen. Zwar fehlt vielerorts das Know-how für die Umsetzung von Identity Governance im Unternehmen, doch mit der Hilfe von auf Identity Governance spezialisierten Dienstleistern lässt sich die Identity Security auf ein neues Level heben. Und mit cloudbasiertem Identity as a Service müssen sich Unternehmen um nichts mehr kümmern und können die gesamte Identity Security in Hände von Experten legen. Denn das Vernachlässigen von Identity Security ist keine Option.

Weitere Informationen

Impressum

tech**consult** GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: **info@techconsult.de**
Tel.: +49-561-8109-0
Fax: +49-561-8109-101
Web: **www.techconsult.de**

Kontakt

Raphael Napieralski
Analyst
tech**consult** GmbH
Baunsbergstr. 37
D-34131 Kassel

E-Mail: **raphael.napieralski@techconsult.de**
Tel.: +49-561-8109-181

(Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.)

Über techconsult GmbH

Die tech**consult** GmbH, gegründet 1992, zählt zu den etablierten Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt tech**consult** über einen im deutschsprachigen Raum einzigartigen Informationsbestand, sowohl hinsichtlich der Kontinuität als auch der Informationstiefe, und ist somit ein wichtiger Beratungspartner der CXOs sowie der IT-Industrie, wenn es um Produktinnovation, Marketingstrategie und Absatzentwicklung geht.

Über SailPoint

SailPoint ist der führende Anbieter von Identity Security für Cloud-Unternehmen. Wir haben es uns zur Aufgabe gemacht, die Risiken auszuräumen, die mit der Bereitstellung von Benutzerzugriffen für eine vielfältige und verteilte Belegschaft einhergehen. Unsere Identitätslösungen schützen und unterstützen Tausende von Unternehmen weltweit. Sie vermitteln unseren Kunden hervorragende Übersicht über ihre gesamte digitale Belegschaft und sorgen dafür, dass alle Mitarbeiter genau die Zugriffe haben, die sie für ihre Arbeit benötigen – nicht mehr und nicht weniger. Mit SailPoint als Grundlage der Unternehmenssicherheit können unsere Kunden sicheren Zugriff gewährleisten, ihre Assets bedarfsgerecht schützen und die Compliance-Vorgaben erfüllen.