LastPass •••|
by LogMeIn

DER LEITFADEN FÜR MODERNE IDENTITÄTS-VERWALTUNG

Schließt die Lücke zwischen Passwort und Identität

EINFÜHRUNG

Als IT- und Sicherheitsexperte sind Sie wahrscheinlich für mehr Aufgaben als je zuvor verantwortlich. Sie jonglieren eventuell mit vielen verschiedenen Prioritäten, von Helpdesk zu Netzwerkverwaltung bis hin zum Verwalten des Benutzerzugriffs und Sichern von Mitarbeiteridentitäten. Was genau ist Identität aber, und wie können Sie Sicherheit und Produktivität mit Lösungen für die Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM) maximieren? Vor allem, wenn Ihre Organisation vielleicht nicht über die erforderlichen Ressourcen verfügt.

LastPass hat das Marktforschungsunternehmen Vanson Bourne beauftragt, Einblicke in den Status der Identitätsverwaltung zu bieten. Wir haben 700 IT- und Sicherheitsexperten in Unternehmen mit 250–2.999 Mitarbeitern aus einer Vielzahl von Branchen in Nordamerika, Europa und Asien-Pazifik befragt. Die Befragten stammten dabei aus zahlreichen IT-Sicherheitsrollen, mit 37 % auf Führungsebene (C-Level), 40 % auf Managementebene und 23 % auf Administratorebene.

In diesem Bericht haben wir die Erkenntnisse von Vanson Bourne mit dem, was wir aus den Erfahrungen unserer Kunden gelernt haben, vereint. Auf den folgenden Seiten finden Sie eine Definition von Identität, einen Überblick über verschiedene Identitätstechnologien, einen Einblick in die Identitätsverwaltung bei Unternehmen sowie eine Erläuterung der individuellen Herausforderungen.

Wir möchten Sie über IAM aufklären und Ihnen Schritte für die Umsetzung dieses Wissens zur Verbesserung des IAM-Programms Ihres Unternehmens aufzeigen.

INHALTSVERZEICHNIS

1. WAS IST IDENTITÄT?

Identität beschreibt **Sie**. Sie besteht aus Ihrem Verhalten, Ihren Geräten, Ihrem Zugriff und Ihren einzigartigen Eigenschaften als individuelle Person. Anhand Ihrer Identität können Sie nachweisen, dass Sie wirklich die Person sind, die Sie vorgeben zu sein. Am Arbeitsplatz verbindet Ihre Identität Sie mit den richtigen Ressourcen auf den richtigen Geräten zur richtigen Zeit, damit Sie sicher und effizient arbeiten können.

Aber Identität ist komplex. Mitarbeiter nutzen rund um die Uhr viele Anwendungen (sowohl genehmigte als auch nicht genehmigte) über eine Vielzahl von Geräten, Netzwerken und Standorten. Bedrohungen gibt es überall und sie entwickeln sich immer weiter. Jeder Mitarbeiter hat seine eigene Identität, also muss jede Identität richtig verwaltet werden. Andernfalls können die falschen Benutzer auf die falschen Anwendungen und Ressourcen zugreifen, was zu Sicherheitslücken sowie Ineffizienz innerhalb des Unternehmens führt.

Technologie kann zur Komplexität der Identitätsverwaltung beitragen, ist aber auch unerlässlich für deren effiziente Verwaltung. In den nächsten Abschnitten stellen wir verschiedene Lösungen vor, die Ihnen einen besseren Einblick in den Benutzerzugriff im Unternehmen sowie größere Kontrolle über diesen Zugriff bieten.

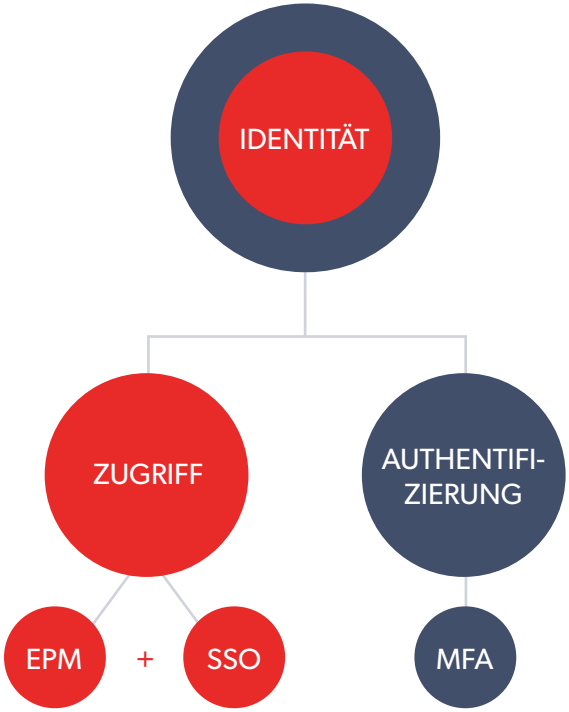
2. DIE MODERNE IDENTITÄTS-TECHNOLOGIE-LÖSUNGSPALETTE

Identitätstechnologien dienen zur sicheren Verwaltung von Benutzeridentitäten, damit Mitarbeiter mit der Technologie verbunden werden, die sie für ihre Tätigkeit benötigen.

In diesem Bericht werden die folgenden Identitätstechnologien behandelt:

- **Multifaktor-Authentifizierung (MFA):** Kombiniert zwei oder mehr Faktoren: etwas, das Sie sind (Eigenschaft), etwas, das Sie wissen (Wissen), und etwas, das Sie haben (Eigentum). Anhand dieser Faktoren wird ein Benutzer verifiziert, bevor Zugriff auf ein Konto gewährt oder eine Aktion autorisiert wird.
- **Single Sign-On (SSO):** Verbindet Mitarbeiter über einen Satz aus Zugangsdaten mit Anwendungen, sodass keine Passwörter für wichtige Dienste eingegeben werden müssen.
- **Passwortverwaltung der Enterprise-Klasse (Enterprise Password Management, EPM):** Erfasst und speichert Passwörter bei allen formularbasierten Webanmeldungen und füllt diese aus. Damit wird zudem das sichere Freigeben von Passwörtern erleichtert.
- **Privileged Access Management (PAM):** Sichert, kontrolliert, verwaltet und überwacht den Zugriff auf kritische Konten und Systeme.
- **Lifecycle Management:** Automatisiert die Bereitstellung, das Entfernen und die Verwaltung von Benutzeridentitäten.

Einzeln eingesetzt verhelfen diese Technologien einem Unternehmen zu beträchtlichen Vorteilen in puncto Sicherheit und Produktivität. Kombiniert man sie miteinander, erlangen Unternehmen absolute Sicherheit und volle Kontrolle über alle Benutzer und Zugangspunkte.



Da Ressourcen immer knapper werden, brauchen Sie eine Komplettlösung, in denen die Hauptkomponenten kombiniert und Investitionen in Identitätstechnologie maximiert werden.

3. UPGRADE DER IDENTITÄTSFUNKTIONEN HAT IM KOMMENDEN JAHR OBERSTE PRIORITÄT

In Bezug auf Sicherheit hört die Arbeit eines IT-Experten nie auf. Ob Upgrades alter Technologien, Kenntnisse der neuesten Bedrohungen oder effektivere Arten, Mitarbeiter zu schulen – IT-Teams stehen großen Herausforderungen gegenüber.

Fast alle der befragten IT-Experten **(98 %)** sind der Meinung, dass das allgemeine Sicherheitsverhalten ihrer Mitarbeiter (Erstellung starker Passwörter, sichere Freigabe und Zusammenarbeit) verbessert werden könnte. Für mehr als die Hälfte von ihnen **(53 %)** sind erhebliche Verbesserungen im Sicherheitsverhalten erforderlich. Sehr wenige IT-Experten **(<5 %)** sind der Meinung, dass alle Benutzer im Unternehmen sich komplett sicher verhalten. Offensichtlich sehen sich nur sehr wenige Unternehmen in der optimalen Sicherheitsposition. Das ist keine Überraschung, wenn man bedenkt, wie schnell sich Bedrohungen und Cybersicherheitslösungen weiterentwickeln.

98 %

der Befragten sehen einen Verbesserungsbedarf beim Sicherheitsverhalten ihrer Mitarbeiter

53 %

geben an, dass erhebliche Verbesserungen im Sicherheitsverhalten ihrer Mitarbeitern erforderlich seien

<5 %

sind der Meinung, dass alle Mitarbeiter sich komplett sicher verhalten

Aufgrund der unterschiedlichen Prioritäten fällt es IT-Teams schwer, ihre Sicherheitsanforderungen zu erfüllen. Das durchschnittliche Unternehmen hat sich für das kommende Jahr mindestens vier Ziele im Bereich IT-Sicherheit gesteckt, darunter das Sichern von Daten **(75 %)**, das Sichern neuer Technologien bei deren Einführung **(68 %),** und die Minderung von Risiken **(66 %)**. **65 %** stimmen zu, dass ein Upgrade ihrer IAM-Funktionen ebenfalls ein Hauptziel ist, das dazu beitragen kann, dass IT-Teams die ersten drei Ziele erreicht. Das Aufrechterhalten des Betriebs stand dabei an letzter Stelle **(26 %)**. Das zeigt also, dass in Bezug auf Sicherheit Bequemlichkeit keine Option ist.

DIE 4 WICHTIGSTEN IT-SICHERHEITSZIELE

75 % **Daten zu sichern**

68 % **Neue Technologien bei deren Einführung zu sichern**

68 % **Risiken zu mindern**

65 % **Upgrade von IAM-Funktionen**

4. DIE MEISTEN UNTERNEHMEN MÜSSEN BEI DER IMPLEMENTIERUNG EINER IDENTITÄTSLÖSUNG SOWOHL FÜR BENUTZERFREUNDLICHKEIT ALS AUCH FÜR SICHERHEIT SORGEN

Aufgrund des hohen Stellenwerts der Sicherheit für die meisten Unternehmen investieren viele von ihnen in Identitätslösungen. **Weniger als 1 % (0,29 %)** der IT-Experten sind der Meinung, die Verwaltung des Benutzerzugriffs sei für die allgemeine Sicherheit des Unternehmens nicht von Bedeutung.

Leider geben auch **92 %** der Unternehmen an, mindestens einer Herausforderung in Bezug auf die Identitätsverwaltung gegenüberzustehen. Das durchschnittliche Unternehmen hat mit diesen drei Herausforderungen in Bezug auf die Identitätsverwaltung zu kämpfen: **47 %** der Befragten gaben an, dass es schwierig sei, einen Ausgleich zwischen Benutzerfreundlichkeit und erhöhter Sicherheit zu schaffen, **40 %** nennen die allgemeine Sicherheit ihrer Lösungen und bei **37 %** fordern die Mitarbeiter eine benutzerfreundliche Lösung an.

92 %

der Unternehmen stehen mindestens einer Herausforderung in Bezug auf die Identitätsverwaltung gegenüber

47 %

Ausgleich zwischen Benutzerfreundlichkeit und Sicherheit

40 %

Allgemeine Sicherheit ihrer Lösungen

37 %

Wunsch der Mitarbeiter nach mehr Benutzerfreundlichkeit

Die Herausforderungen sehen auch in jedem Land anders aus. Der Ausgleich zwischen Benutzerfreundlichkeit und erhöhter Sicherheit steht in Frankreich **(56 %)**, in Großbritannien **(49 %)** und in den USA **(47 %) an oberster Stelle,** während die Sicherheit von IAM-Lösung in Deutschland **(50 %)** und Australien **(49 %)** ganz oben steht.

BENUTZERFREUNDLICHKEIT OHNE EINBUSSEN BEI DER SICHERHEIT IST DIE GRÖSSTE HERAUSFORDERUNG.

56 % FRANKREICH **49 %** VEREINIGTES KÖNIGREICH **47 %** USA

SICHERHEIT VON IAM-LÖSUNGEN IST DIE GRÖßTE HERAUSFORDERUNG.

50 % DEUTSCHLAND **49 %** AUSTRALIEN

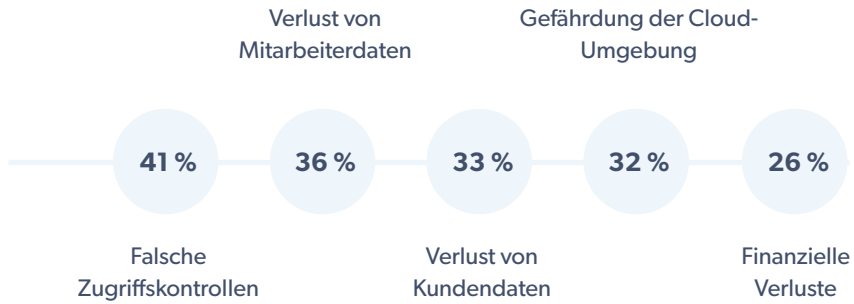
IT-Teams sind sich bewusst, dass Identitätstechnologie die Sicherheit im Unternehmen erheblich verbessern kann. Sie finden aber nur schwer Lösungen, die Mitarbeiter auch bereit sind einzusetzen. Jede Technologie, die mühselig ist oder den Benutzer aufhält, wird nur widerwillig angenommen. Die Wahl einer Identitätslösungen, die für Mitarbeiter einfach einzusetzen ist und dabei gleichzeitig die allgemeine Sicherheit im Unternehmen erhöht, ist für Unternehmen also ausschlaggebend.

5. IT-EXPERTEN SIND SICH EINIG, DASS IHRE UNTERNEHMEN AUFGRUND SCHLECHTER IDENTITÄTSPRAKTIKEN RISIKEN AUSGESETZT SIND

IT-Teams haben gute Beweggründe, Sicherheit zu priorisieren und in Identitätstechnologie zu investieren, weil sie die Folgen mangelnder Sicherheit kennen. **82 %** geben an, dass ihr Unternehmen aufgrund mangelhafter IAM-Praktiken einem Risiko ausgesetzt war, darunter falsche Zugriffskontrollen **(41 %)**, Verlust von Mitarbeiterdaten **(36 %)**, Verlust von Kundendaten **(33 %)**, finanzielle Verluste **(26 %)** und Gefährdung ihrer Cloud-Umgebung **(32 %)**. Das Risiko falscher Zugriffskontrollen stand in jedem Land an oberster Stelle, außer in Australien, wo die Gefährdung der Cloud-Umgebung als größtes Risiko genannt wurde **(40 %)**.

82 %

geben an, ihr Unternehmen sei aufgrund schlechter Identitäts- und Zugriffsverwaltung einem Risiko ausgesetzt gewesen.



Es ist kein Wunder, dass Unternehmen, bei denen das allgemeine Sicherheitsverhalten der Mitarbeiter sehr zu wünschen übrig lässt, am ehesten dem Großteil dieser Risiken ausgesetzt waren, in erster Linie falschen Zugriffskontrollen **(46 %)** und dem Verlust von Kundendaten **(46 %)**.

MANGELHAFTES SICHERHEITSVERHALTEN SORGT FÜR HÖHERES RISIKO.

Durchschnittliche Unternehmen*:

– Falsche Zugriffskontrollen **41 %**

– Verlust von Kundendaten **36 %**

Unternehmen mit mangelhafter Sicherheit*:

– Falsche Zugriffskontrollen **46 %**

– Verlust von Kundendaten **46 %**

Angesichts der Risiken und potenziellen Bedrohungen, denen sie ausgesetzt waren, stimmen **81 %** der IT-Experten zu, ihr Unternehmen müsse eine bessere Identitätsverwaltung implementieren, um sich vor einer Vielzahl von Sicherheitsrisiken zu schützen. Es ist daher nicht überraschend, dass **94 %** ebenfalls zustimmen, dass IAM eine höhere Priorität für das Unternehmen einnehmen sollte, als das derzeit der Fall ist. IT-Experten sind sich einig, dass die Vermeidung von riskantem Mitarbeiterverhalten anhand von Identitätstechnologien sich gut dazu eignet, Bedrohungen für das Unternehmen zu reduzieren.

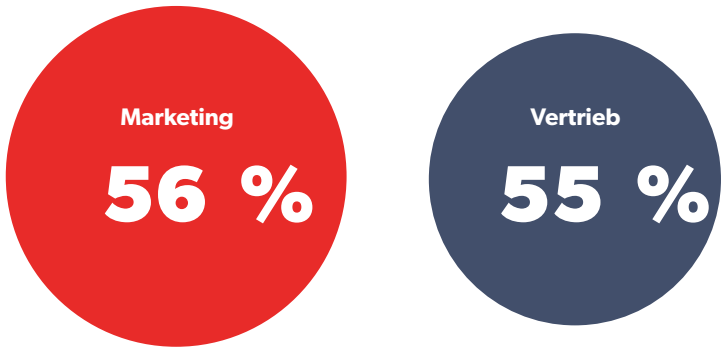
* *Die durchschnittliche Antwort unter allen 700 Befragten.*

* *Die durchschnittliche Antwort von Befragten, die einen großen Verbesserungsbedarf im allgemeinen Sicherheitsverhalten der Mitarbeiter angaben.*

6. MARKETING- UND VERTRIEBS-TEAMS GELTEN IM ALLGEMEINEN ALS DIE ABTEILUNGEN, DIE DAS GRÖSSTE RISIKO FÜR EIN UNTER-NEHMEN BERGEN

Wer setzt das Unternehmen Risiken aus? **56 %** der IT-Sicherheitsexperten geben Marketing als eine der zwei Abteilungen an, die am ehesten mit mangelnder Sicherheit arbeiten. Das Vertriebsteam steht direkt dahinter mit **55 %**. Warum? Diese Teams (insbesondere Marketing) arbeiten am ehesten mit externen Auftragnehmern oder Agenturen, wobei sie sich vermutlich nicht immer an die vorgeschriebenen Verfahren halten. Bei ihnen ist außerdem die Wahrscheinlichkeit am größten, neue Clouddienste im Hinblick auf deren Datenfunktionen und Produktivitätsvorteile zu testen – ohne Genehmigung der IT.

ABTEILUNGEN MIT DEN MEISTEN RISKANTEN HANDLUNGEN



ABTEILUNG MIT DEN WENIGSTEN RISKANTEN HANDLUNGEN

Finanzabteilung

31 %

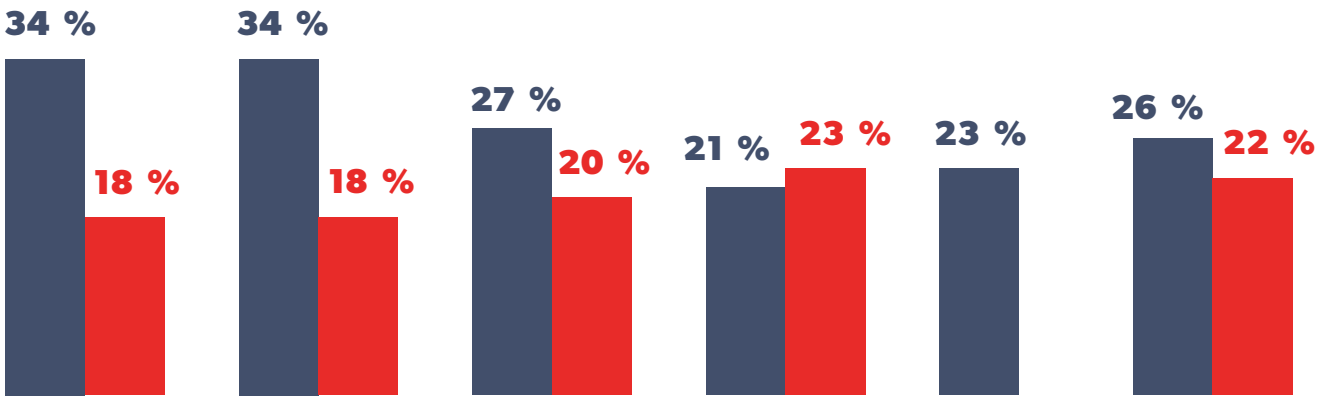
Die Finanzabteilung wurde am wenigsten **(31 %)** als eine der riskanten Abteilungen eingestuft. Der Grund dafür ist wahrscheinlich, dass aufgrund der dort verarbeiteten sensiblen Daten mehr Regeln zur Verhaltenssteuerung gelten.

Da Mitarbeiter auf allen Ebenen und in allen Abteilungen ein Risiko für das Unternehmen darstellen können, müssen IT-Teams unbedingt benutzerfreundliche Identitätstechnologien für alle Mitarbeiter bereitstellen. Identitätslösungen können riskantes Verhalten, wie schwache Passwörter oder das Freigeben des Kontozugriffs ohne administrative Kontrolle, minimieren oder ganz beseitigen.

7. PASSWÖRTER FÜHREN WEITERHIN ZU FRUSTRATION – UND RISIKEN

Leider wenden IT-Teams noch immer wertvolle Zeit und Ressourcen für Tickets im Zusammenhang mit Passwortproblemen und Sicherheitsbedenken auf.

DIE MEISTEN IT-TEAMS ERHALTEN TICKETS FÜR FOLGENDES:



Verlorene oder gestohlene Zugangsdaten einmal oder mehrmals im Monat (18 %)

Kompromittierte Zugangsdaten monatlich, obwohl 18 % zugaben, dass sie nicht wissen, wie oft kompromittierte Zugangsdaten gemeldet werden

Versehentliches Weitergeben von Zugangsdaten an die falsche Person einmal oder mehrmals im Monat (20 %)

Vergessene Passwörter täglich oder mehrmals pro Woche (23 %)

Unaufgeforderte Passwortaktualisierungen monatlich

Probleme mit angeforderten Passwortaktualisierungen monatlich oder sogar wöchentlich (22 %)

IT-Sicherheitsteams verbringen durchschnittlich **4 Stunden pro Woche** mit passwortbezogenen Problemen und erhalten **96 passwortbezogene Anforderungen pro Monat**. Einige IT-Teams erhalten über 25 Anforderungen am Tag wegen vergessenen Passwörtern. Ein Unternehmen gab sogar an, dass sein IT-Team bis zu 30 Stunden pro Woche mit der Passwortverwaltung verbringt!

Angesichts der umfangreichen Ressourcen, die Unternehmen für die Passwortverwaltung aufbringen müssen, ist es kein Wunder, dass fast alle **(95 %)** der IT-Sicherheitsexperten der Ansicht sind, ihr Unternehmen sollte größeren Stellenwert auf hohe Passwortqualität legen. Diese Einstellung ist vor allem in Deutschland mit **98 %**weit verbreitet.

Viele der Befragten aus Unternehmen, die in eine EPM-Lösung investiert haben oder planen, in eine EPM-Lösung zu investieren, stimmen zu, dass diese Lösung für größere Unternehmenssicherheit **(54 %)**, vereinfachte Verwaltung von Benutzerprofilen und Zugangsdaten **(47 %)** und höhere Produktivität der Mitarbeiter **(43 %)** sorgen würde.

Diese Daten verdeutlichen, dass viele Unternehmen noch nicht alle passwortbezogenen Hindernisse und Sicherheitsrisiken in ihrem Unternehmen beseitigt haben. Interessanterweise geben **90 %** der Befragten, die einen großen Verbesserungsbedarf im allgemeinen Sicherheitsverhalten der Mitarbeiter ihrer Unternehmen sehen, an, dass sie bereits eine Unternehmenslösung nutzen. Das deutet darauf hin, dass EPM lediglich den Anfangspunkt in der Identitätsverwaltung darstellt.

4 Stunden

pro Woche für Probleme bei der Passwortverwaltung

95 %

der IT-Sicherheitsexperten sind der Meinung, dass ihr Unternehmen mehr Wert auf hohe Passwortqualität legen sollte

93 %

der IT-Experten geben an, dass sie sich gut oder hervorragend mit EPM-Lösungen auskennen

8. SINGLE SIGN-ON IST ENTSCHEIDEND, STELLT ABER IN ISOLATION EINE KRITISCHE SICHERHEITSLÜCKE DAR

Die meisten IT-Experten stimmen zu, dass die Verwaltung des Benutzerzugriffs entscheidend ist. Tatsächlich sagen **90 %**, dass die Verwaltung des Benutzerzugriffs entweder entscheidend oder sehr wichtig für die allgemeine Sicherheit des Unternehmens ist. Diese Einstellung wird vor allem von Befragten aus dem Vereinigten Königreich vertreten **(93 %)**. Angesichts der Risiken und des Ressourcenaufwands im Zusammenhang mit Passwörtern können Single Sign-On-Lösungen (SSO) Passwörter für von der IT unterstützte Anwendungen beseitigen und die Anmeldung für Mitarbeiter vereinfachen, die auf wichtige Anwendungen in der Cloud und hinter der Firewall zugreifen.

Die meisten Unternehmen haben in eine Form von SSO investiert. Immerhin nutzen **74 %** der Befragten bereits eine SSO-Lösung. Es ist daher nicht überraschend, dass viele IT-Experten umfassende Kenntnisse von SSO-Lösungen haben (**54 %** gaben ein hervorragendes Verständnis und **40 %** ein gutes Verständnis an). Der Kenntnisstand ist am höchsten in den USA, wo **63 %** ein hervorragendes Verständnis angaben, und am niedrigsten in Australien mit nur **39 %**.

Etwa die Hälfte der IT-Sicherheitsexperten **(49 %)** aus Unternehmen, die in eine SSO-Lösung investiert haben oder planen, in eine solche zu investieren, stimmen zu, dass diese Lösung die Verwaltung von Benutzerprofilen und Zugangsdaten vereinfachen **(49 %)**, die Unternehmenssicherheit erhöhen **(48 %)** und die Produktivität der Mitarbeiter steigern würde.

SSO verringert die Risiken aufgrund des Passwortverhaltens der Mitarbeiter, da der Passwortbedarf wegfällt. Viele IT-Experten sind sich aber gleichzeitig bewusst, dass SSO die Anmeldung vereinfacht, da Mitarbeiter sich nur ein Passwort merken müssen. Beachten Sie zudem, dass Transparenz keiner der erwarteten Vorteile ist (**nur 31 %**). Das bedeutet, dass viele IT-Experten zustimmen, dass eine SSO-Lösung alleine keine umfassenden Einblicke in den Benutzerzugriff im Unternehmen bietet.

SSO ist leider kein Allheilmittel. **38 %** der befragten IT-Experten geben an, dass SSO von allen in diesem Bericht behandelten Technologien bei alleiniger Verwendung der mangelhafteste Ansatz für die Identitätsverwaltung ist. Viele Apps sind nicht in eine SSO-Lösung integriert – weil sie SSO nicht unterstützen, nicht wichtig genug für die IT sind, um SSO dafür zu konfigurieren, oder das IT-Team noch nicht einmal weiß, dass sie genutzt werden. Deshalb stimmen **80 %** der IT-Experten zu, dass bei SSO als einzige Lösung viele Cloud-Anwendungen und Konten mit hohen Berechtigungen ungesichert bleiben. Eine Kombination aus SSO-Technologien und einer EPM-Lösung sorgt dafür, dass jeder Zugriffspunkt gesichert ist, während gleichzeitig die meisten, wenn nicht sogar alle, Zugriffshindernisse für Mitarbeiter beseitigt werden.

49 %

der Unternehmen mit SSO stimmen zu, dass die Lösung die Verwaltung von Benutzern und Zugangsdaten vereinfacht

80 %

stimmen zu, dass bei SSO als einziger Lösung viele Cloud-Anwendungen und Konten mit hohen Berechtigungen ungesichert bleiben

38 %

der IT-Experten geben an, dass SSO bei alleiniger Verwendung der mangelhafteste Ansatz für die Identitätsverwaltung ist

9. STÄRKEN DER BENUTZERAUTHENTIFIZIERUNG MIT MFA HAT HOHE PRIORITÄT

Die Multifaktor-Authentifizierung (MFA) ist in den letzten paar Jahren immer beliebter geworden, da Unternehmen feststellen, dass Passwörter alleine nicht genug Schutz bieten. Die meisten Unternehmen haben in MFA-Lösungen investiert. Dabei geben **73 %** an, dass sie bereits MFA-Technologie nutzen, während **19 %** eine Investition in MFA im kommenden Jahr erwarten. Bei MFA sind zusätzliche Faktoren zum Nachweis der Identität eines Benutzers erforderlich, bevor der Zugriff erteilt wird. So sind Unternehmen vor den Risiken schwacher und kompromittierter Passwörter geschützt.

73 %

der Unternehmen geben an, dass sie bereits MFA-Technologie nutzen

19 %

erwarten eine Investition in MFA im kommenden Jahr

59 % der IT-Experten stimmen zu, dass die Benutzerauthentifizierung gestärkt werden muss, und geben dies als eine ihrer wichtigen Prioritäten zum Verbessern ihrer Identitätsverwaltung an. MFA ist vor allem in Deutschland eine Priorität, wo **63 %** der IT-Experten zustimmen, dass sie eine ihrer wichtigen IAM-Ziele ist. Es wird Sie daher nicht überraschen, dass ein Drittel aller Befragten **(35 %)** MFA als besten Ansatz für den Einstieg in die Identitätsverwaltung angeben.

Die meisten IT-Experten geben ein gutes **(45 %)** oder hervorragendes **(48 %)** Verständnis von MFA an. Allerdings haben nur **35 %** der Fachkräfte in Frankreich und Australien laut ihren Angaben ein hervorragendes Verständnis von MFA. Daher ist wahrscheinlich weitere Fortbildung notwendig, um das notwendige Vertrauen zur Verwendung und Bereitstellung von MFA-Lösungen aufzubauen.

Die für MFA spezifische Implementierung von Biometrie ist für **36 %** der Unternehmen eine Priorität. In Deutschland ist die Priorisierung der Biometrie mit **39 %** am höchsten. Wir erwarten, dass die Nutzung von Biometrie in den nächsten Jahren weiter zunimmt, während die zugehörigen Funktionen immer mehr auf Smartphones verfügbar werden und Mitarbeiter Hemmungen in Bezug auf Authentifizierungsoptionen wie Fingerabdruck, Sprach- und Gesichtserkennung abbauen. Unternehmen, die MFA-Lösungen mit biometrischen Funktionen einsetzen möchten, sollten wissen, wie die Daten verwendet und gespeichert werden, und Kompatibilität mit allen Anwendungsfällen im Unternehmen sicherstellen.

59 %

der IT-Experten stimmen zu, dass die Stärkung der Benutzerauthentifizierung entscheidend ist

93 %

der IT-Experten geben an, dass sie sich gut oder hervorragend mit MFA auskennen

36 %

der befragten Unternehmen betrachten die Implementierung von Biometrie als Priorität

IT-Sicherheitsexperten aus Unternehmen, die in MFA investiert haben oder planen, in MFA zu investieren, erwarten eine bessere Unternehmenssicherheit **(60 %)**, weniger falschen Zugriff auf vertrauliche Informationen **(48 %)** und ein verringertes Risiko von Zugangsdaten-/Passwortdiebstahl **(47 %)** als wahrscheinliche Vorteile. Auch hier ist die Transparenz kein erwarteter Vorteil von MFA (nur **33 %**). Eine Lösung, die bessere Einblicke in die Authentifizierung im Unternehmen bietet, wäre also in Kombination mit MFA von enormem Nutzen.

Die meisten IT- und Sicherheitsexperten sind sich einig, dass MFA eine wertvolle und notwendige Technologie ist. Tatsächlich erwarten nur **1 %** keine Vorteile von MFA. Sie führt zu einer erheblichen Verbesserung der Sicherheit eines Unternehmens, da Benutzer zusätzliche Faktoren bereitstellen müssen, bevor sie auf Systeme zugreifen können. Dank Schlüsselfunktionen wie biometrischen Daten und adaptiver Authentifizierung erhalten IT-Teams mehr Flexibilität und Sicherheit. Unternehmen sollten aber nach Lösungen suchen, die angemessene Betriebskosten und minimalen Verwaltungsaufwand mit sich bringen.

60 %

erwarten größere Unternehmenssicherheit als einen der wahrscheinlichsten Vorteile von MFA-Lösungen

1 %

der Befragten sehen keinen Vorteil in MFA

10. IDENTITÄTSVERWALTUNG WIRD ZUNEHMEND AUTOMATISIERT

Durch die Automatisierung der Aufgaben in der Identitätsverwaltung können Unternehmen Zeit und Ressourcen sparen. Im Durchschnitt priorisieren **40 %** aller Befragten die Automatisierung von Identitätsprozessen als wichtiges Ziel; fast die Hälfte sind es dabei in Deutschland **(47 %)** und Australien **(46 %)**.

Wir erwarten, dass die Automatisierung in Zukunft eine noch wichtigere Rolle spielt, während immer mehr Unternehmen Identitätsprogramme bereitstellen. Lifecycle-Management-Lösungen können das Bereitstellen und Entfernen von Identitäten automatisieren. So erhalten Benutzer automatisch den für ihre Funktion erforderlichen Zugriff, während das Konto einfach entfernt wird, sobald der Benutzer das Unternehmen verlässt oder eine neue Funktion übernimmt.

40 %

aller Befragten priorisieren die Automatisierung von Identitätsprozessen als wichtiges Ziel

Schwerpunkt auf Verbesserung der Automatisierung

Deutschland **47 %** Australien **46 %**

11. IT-EXPERTEN KENNEN DIE SICHERHEITSVORTEILE VON PRIVILEGED ACCESS MANAGEMENT

Mehr als die Hälfte **(60 %)** der Befragten haben in Privileged Access Management (PAM) investiert. **51 %** der Befragten geben ein hervorragendes Verständnis von PAM an. Dabei sind die Befragten aus Deutschland am wenigsten mit der Technologie vertraut (**40 %** mit einem hervorragenden Verständnis). Weitere **38 %** der Fachkräfte geben ein gutes Verständnis an. Insgesamt wäre weitere Fortbildung zu PAM für IT-Experten auf der ganzen Welt nützlich.

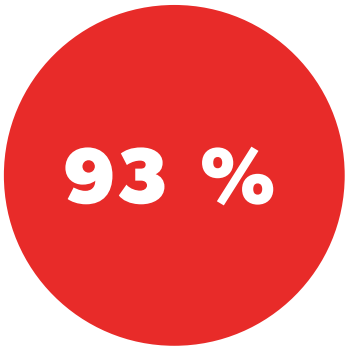
51 % **der IT-Experten mit Erfahrungen in PAM-Technologie stimmen zu, dass diese größere Unternehmenssicherheit bietet**

IT-Experten aus Unternehmen, die in PAM investiert haben oder planen, in PAM zu investieren, erwarten als Hauptvorteile von PAM-Lösungen eine bessere Unternehmenssicherheit **(51 %)**, weniger falschen Zugriff auf vertrauliche Informationen **(45 %)** und gesteigerte Mitarbeiterproduktivität **(42 %)**. Darüber hinaus planen **26 %**, im kommenden Jahr in eine PAM-Lösung zu investieren.

12. UNTERNEHMEN BENÖTIGEN EINE GANZHEITLICHE LÖSUNG, DIE EINFACH ZU IMPLEMENTIEREN IST UND BEREITWILLIG VON BENUTZERN EINGESETZT WIRD

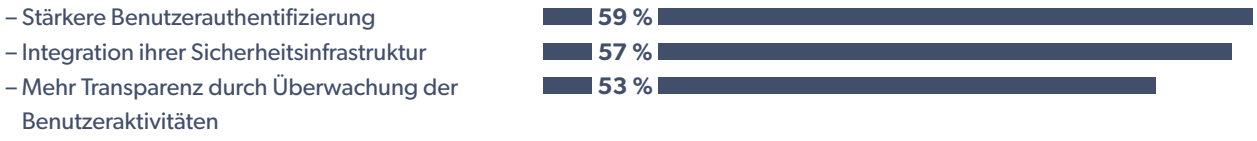
In Anbetracht der in diesem Bericht gesammelten Daten wird Eines ganz deutlich: IT-Fachkräfte wissen zwar, wie wichtig die Identitätsverwaltung ist, müssen aber immer noch eine umfassende Identitätslösung in ihrem Unternehmen einführen. **93 %** der IT-Experten stimmen zu, dass sie nicht in viele einzelne Lösungen investieren, sondern die verschiedenen Aspekte bei der Identitäts- und Zugriffsverwaltung in einer Lösung kombinieren sollten. Das würde erheblich zur allgemeinen Sicherheit im Unternehmen beitragen. Angesichts der begrenzten Ressourcen stimmen wir zu, dass Unternehmen eine Komplettlösung zur Identitätsverwaltung brauchen.

Die Minderheit der Teilnehmer **(23 %–38 %)** muss ihre Investition in alle Identitätsaspekte noch abschließen. Nur **24 %** der befragten IT-Experten gaben das Budget als IAM-Herausforderung an. Also ist das Hauptproblem womöglich nur, die richtige Lösung für Ihr Unternehmen zu finden.

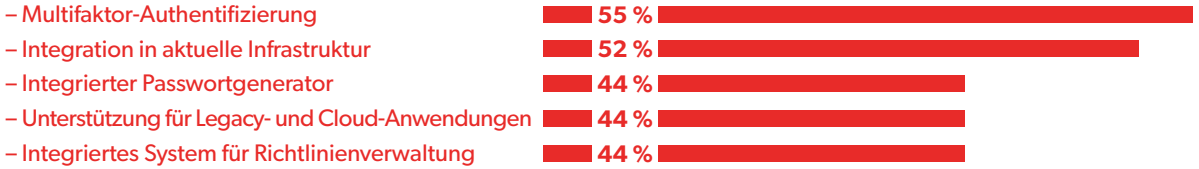


DER UNTERNEHMEN STIMMEN ZU, DASS IHR UNTERNEHMEN VON EINER EINHEITLICHEN IAM-LÖSUNG PROFITIEREN WÜRDE

Bei der Beurteilung ihrer aktuellen Identitätsfunktionen sehen IT-Experten in folgenden Bereichen Verbesserungsbedarf:



Die Befragten gaben auch mehrere Funktionen ihrer idealen Identitätslösung an:



Mit anderen Worten: Die ideale IAM-Lösung unterstützt zahlreiche Anwendungsfälle, integriert und unterstützt das vorhandene Technologie-Ökosystem im Unternehmen, sorgt für hohe Passwortqualität und ermöglicht Administratoren die flexible Anpassung der Lösung, um die einzigartigen Sicherheitsanforderungen des Unternehmens zu erfüllen.

In der Praxis geben IT-Experten im Durchschnitt vier Hauptprioritäten für ihr Unternehmen in Bezug auf verbesserte IAM-Funktionen an, zuoberst: Stärken der Benutzerauthentifizierung **(59 %)**, Integration der Sicherheitsinfrastruktur **(57 %)**, Überwachung der Benutzeraktivitäten **(53 %)** und Vereinfachen des Benutzerzugriffs **(44 %)**. Diese Prioritäten spiegeln im Allgemeinen die größten Herausforderungen dieser Unternehmen wider. Durch Stärken der Benutzerauthentifizierung und Integration der Sicherheitsinfrastruktur können beispielsweise Identitätslösungen gesichert werden, während das Vereinfachen des Benutzerzugriffs die Anforderung der Mitarbeiter nach einer benutzerfreundlichen Lösung erfüllt.

Wie der Bericht ganz deutlich macht, sollen Identitätstechnologien sowohl Sicherheits- als auch Produktivitätsvorteile mit sich bringen. Tatsächlich stimmen die meisten Befragten **(93 %)** zu, dass ein besserer IAM-Ansatz die Mitarbeitereffizienz steigern könnte. Um diese Vorteile zu erreichen, müssen Sie in eine ganzheitliche Lösung investieren, die sowohl Benutzerfreundlichkeit als auch Sicherheit bietet.

13. SO GEHT ES WEITER: WAS MÜSSEN SIE WISSEN, UM DIE IDENTITÄTSVERWALTUNG VORANZUTREIBEN?

Als IT-Experte müssen Sie unter Umständen schwierige Situationen in Bezug auf Ihr Identitätsprogramm bewältigen. Vielleicht haben Sie bereits in IAM-Technologie investiert und möchten weitere Lösungen hinzufügen. Vielleicht hat Ihr Unternehmen derartige Lösungen lange genutzt, ist aber nun der Ansicht, sie wären nicht mehr ideal für Ihr Business? Vielleicht gibt es auch überhaupt kein Identitätsprogramm in Ihrem Unternehmen und Sie wissen nicht, wo Sie anfangen sollten.

ALS ERSTES SOLLTEN SIE FOLGENDE PUNKTE BEDENKEN:

- **Die Probleme, die Sie lösen möchten:** Ist die Verwaltung des Benutzerzugriffs ein Hindernis? Gehen Mitarbeiter sicher mit ihren Passwörtern um? Wird die Produktivität der Mitarbeiter durch zu viele Sicherheitsmaßnahmen beeinträchtigt?
- **Ihre Anforderungen beim Lösen dieser Probleme:** Welcher Typ von Identitätslösung eignet sich für die jeweilige Herausforderung? Gibt es eine einheitliche Lösung, die all diese Anforderungen erfüllen kann?
- **Die Technologien, mit denen Sie diese Anforderungen derzeit erfüllen:** Verwenden Sie Passwortverwaltung? Single Sign-On? Multifaktor-Authentifizierung?
- **Aktuelle Lücken in den genutzten Technologien:** Verwenden Sie bestimmte IAM-Technologien in Isolation?
- **Weitere Technologien, die diese Lücken schließen können:** Wie können Sie Ihre vorhandenen IAM-Lösungen ergänzen, um Benutzeridentitäten sicher zu verwalten?

Indem Sie Ihre aktuelle Lage und Situation in Bezug auf die Identitätsverwaltung genau eingrenzen, können Sie in Frage kommende Technologien und Lösungen gezielt evaluieren und beurteilen. Sorgfältige Planung und Entscheidungsfindung ist der ideale Weg, um das Maximum an Produktivität und Sicherheit aus Ihrer Investition herauszuholen.

Eine ganzheitliche Lösung, die alle Vorteile jeder IAM-Technologie kombiniert, ist für jeden die beste Option. Eine intuitive und benutzerfreundliche Komplettlösung, mit der jeder Zugriffspunkt zentral verwaltet und kontrolliert werden kann, führt am ehesten zu einer erfolgreichen Implementierung. Dank einheitlicher Einblicke in Benutzerzugriff und Authentifizierung für das ganze Unternehmen können Sie nicht nur die Benutzerfreundlichkeit verbessern, sondern auch die Sicherheit erhöhen.

BENUTZERIDENTITÄTEN MIT EINER EINZIGEN LÖSUNG VERWALTEN

LastPass Identity bietet Ihnen einfache Kontrolle und einheitliche Transparenz, und zwar für jeden „Einstiegspunkt" zu den Daten Ihres Unternehmens. Der intuitive Zugriff und die Multifaktor-Authentifizierung funktionieren sowohl für Cloud- und mobile Apps als auch für ältere, vor Ort installierte Tools. Von Single Sign-On über die Passwortverwaltung bis hin zur adaptiven Authentifizierung gibt LastPass Identity Ihrem IT-Team die volle Kontrolle und ermöglicht Ihren Benutzern einen reibungslosen Zugriff.

- Zentrale Steuerung durch Administratoren
- Mehr als 1.200 Single Sign-On-Anwendungen
- Branchenführender Passwort-Manager für Unternehmen
- Mehr als 100 Zugriffssicherheitsrichtlinien
- Erweiterte Berichterstattung
- Sichere Freigabe von Passwörtern
- Integration von Benutzerverzeichnissen
- Adaptive Multifaktor-Authentifizierung
- Eine Lösung

LastPass •••|
by LogMeIn

Zugriff und Authentifizierung in einem:

www.lastpass.com/de/products/identity

© 2019 LogMeIn, Inc. Alle Rechte vorbehalten.

06.26.19/PDF/ LMI0638C