LastPass •••|
by LogMeIn

Identitäts- und
Zugriffsverwaltung
für Unternehmen

SICHERES ARBEITEN AN JEDEM ORT

EINLEITUNG

Viele Unternehmen haben innerhalb kürzester Zeit auf Homeoffice umgestellt, und die Vorteile lassen sich nicht leugnen. Die Risiken allerdings auch nicht.

Homeoffice und Teleworking sind kein neuer Trend, sondern eher unsere neue Normalität. Das Zeitalter, in dem wir von überall aus arbeiten, hat begonnen. Nahtloser und sicherer Zugriff für die Mitarbeiter und Sicherheit für das Unternehmen sind dabei ein Muss. Die Realität für IT-Teams sieht nun so aus, dass sie Mitarbeitern an vielen verschiedenen Standorten, die viele verschiedene Geräte nutzen, Zugriff auf viele verschiedene Apps gewähren müssen. Wie kann das IT-Team am besten überprüfen, ob jeder Benutzer der ist, für den er sich ausgibt?

Im Zeitalter des ortsunabhängigen Arbeitens benötigen Unternehmen eine Strategie für die Identitäts- und Zugriffsverwaltung (engl. Identity and Access Management, IAM), die jeden Mitarbeiter authentifiziert und autorisiert und ihm Zugriff auf die benötigten Firmenressourcen gibt.

Mit einer IAM-Strategie, die das Unternehmen unabhängig vom Arbeitsort seiner Beschäftigten schützt, erhalten die richtigen Benutzer zur richtigen Zeit Zugriff auf die richtigen Ressourcen. Gleichzeitig hat das IT-Team alle Logins im Blick und im Griff – und das ebenfalls von jedem Ort aus.

INHALT

SICHERES ORTSUNABHÄNGIGES ARBEITEN – DIE HERAUSFORDERUNGEN

Teleworking im Allgemeinen und Homeoffice im Speziellen bringen definitiv große Vorteile mit sich, aber auch einige Risiken.

Cyberkriminalität und Phishing-Angriffe sind auf dem Vormarsch; in manchen Unternehmen hat die Anzahl der Phishing-Angriffe auf Mitarbeiter im Homeoffice um bis zu 40 % zugenommen. Und die Unternehmen sind nicht darauf vorbereitet. Cyberkriminelle wissen das und nutzen jede Schwachstelle schamlos aus.

Wenn das Firmennetzwerk remote zugänglich ist, vergrößert das natürlich die Angriffsfläche für Cyberkriminelle. Gleichzeitig wird die IT-Umgebung komplexer und somit schwerer abzusichern, was nicht nur eine Herausforderung für die IT darstellt, sondern auch für die Mitarbeiter.

Beschäftigte arbeiten an mehr Orten denn je

IT-Teams müssen jeden Login absichern – wo auch immer die Mitarbeiter sind

Cyberkriminelle nutzen gefundene Schwachstellen aus

bis zu 40 %

mehr Phishing-Angriffe, die auf Mitarbeiter im Homeoffice abzielen

Aus Sicht des IT-Teams ...

IT-Teams waren es gewohnt, die Kontrolle zu haben. Diese entgleitet ihnen nun, wenn der Fernzugriff auf immer mehr Beschäftigte ausgeweitet wird. Ihre größte Herausforderung? Zu verwalten, **wo** und **wie** externe Benutzer auf Firmenressourcen zugreifen.

Damit sind unter anderem folgende Risiken verbunden:

- **Falsche Zugriffsrechte:** Je mehr Mitarbeiter im Homeoffice arbeiten, desto größer das Risiko, dass sie Zugriff auf Daten haben, die sie in ihrer Funktion nicht benötigen.
- **Datenschutzverletzungen:** Wenn die IT-Systeme eines Unternehmens nicht mehr auf das Bürogebäude begrenzt sind und Mitarbeiter von überall aus arbeiten, dann erhöht dies die Gefahr eines Datenlecks.

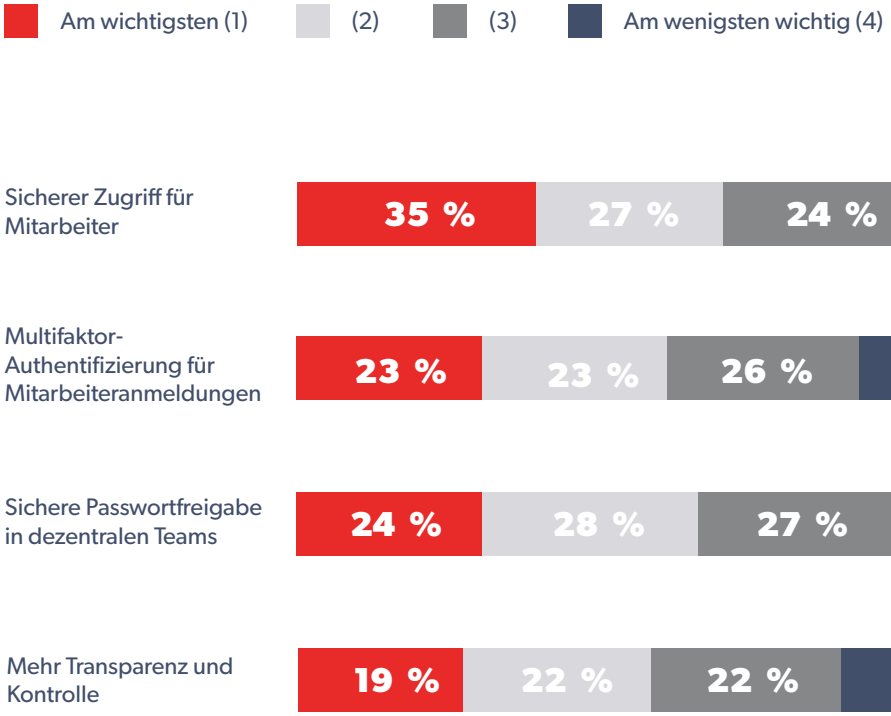
Aus Sicht der Mitarbeiter ...

Wenn IT-Teams Mitarbeitern im Homeoffice nicht auf sichere Weise Zugriff auf die Firmenressourcen gewähren können, dann wählen diese entweder unsichere Wege, die das Unternehmen Gefahren aussetzen, oder sie können gar nicht auf ihre Apps und Daten zugreifen und somit nicht produktiv arbeiten.

Laut einer Studie, die wir kürzlich gemeinsam mit IDG durchgeführt haben, bezeichnen Unternehmen den sicheren Zugriff der Mitarbeiter als ihre oberste IAM-Priorität in Sachen Teleworking. Entscheidungsträger sollten daher eine Single-Sign-On-Lösung (SSO) in Betracht ziehen, die Benutzer mit nur einem Login sicher auf die benötigten Ressourcen zugreifen lässt.

PRIORITÄTEN BEIM TELEWORKING

Von 1 bis 4 gereiht, wobei 1 der wichtigste Aspekt ist.



IAM IST ENTSCHEIDEND FÜR EINEN SICHEREN FERNZUGRIFF

Teleworking im Allgemeinen und Homeoffice im Speziellen sind zu unserer neuen Normalität geworden. Unternehmen benötigen eine robuste IAM-Strategie, die auf lange Sicht ausgelegt ist und auch Mitarbeiter außerhalb des Büros abdeckt – angesichts der mit dem Fernzugriff verbundenen Risiken und Herausforderungen eine zentrale Priorität.

Laut unserer jüngsten Umfrage, die wir gemeinsam mit IDG durchgeführt haben, hatte die Umstellung auf Homeoffice in 96 % der Unternehmen Auswirkungen auf die IAM-Strategie, und 98 % der Entscheidungsträger in der IT halten die Identitäts- und Zugriffsverwaltung für maßgeblich, damit Beschäftige von jedem Ort aus sicher arbeiten können. Um einen angemessenen Schutz zu bieten, muss die Identitäts- und Zugriffsverwaltung anders als bisher gehandhabt werden – Stichwort Zukunftsfähigkeit. Die wenigen Akteure, die das nicht tun, setzen ihre geschäftskritischen Funktionen großen Risiken aus.

96%

der Unternehmen passten ihre IAM-Strategie homeofficebedingt an.

98%

finden IAM entscheidend für einen sicheren Fernzugriff ihrer Mitarbeiter.

So kann IAM die Sicherheit an jedem Ort erhöhen:

- **Single Sign-On (SSO):** Mit SSO haben Sie die Kontrolle über den Mitarbeiterzugriff, von wo auch immer Ihre Teammitglieder sich anmelden. Ob im Büro, im Homeoffice oder anderswo, die Benutzer erhalten mit nur einem Passwort Zugang zu einer ganzen Reihe von Apps. Eine sichere Verbindung, gekoppelt mit der nahtlosen Authentifizierung, macht die benötigten Ressourcen problemlos verfügbar. Und während der einfachere Fernzugriff nicht nur das Nutzungserlebnis verbessert, sondern auch die Produktivität der Mitarbeiter, erhält das IT-Team mehr Kontrolle über die Logins. Wenn man bedenkt, dass der sichere Zugriff als die oberste IAM-Priorität für ortsunabhängiges Arbeiten gilt, ist anzunehmen, dass SSO für Unternehmen im Homeoffice-Zeitalter zu einem Muss werden wird.
- **Passwortverwaltung:** Mitarbeiter können nur dann von überall aus effizient arbeiten, wenn sie Daten und vertrauliche Informationen auf einfache und sichere Weise austauschen können. Wenn zwei Kollegen nicht im selben Büro sind, kann sogar etwas so Banales wie das Weitergeben eines Passworts ein Risiko darstellen. In den meisten Unternehmen gibt es Konten, die von mehreren Personen genutzt werden. Und ohne einen eigenen Passwort-Manager werden diese immer den schnellsten Weg einschlagen, um ein Passwort mit anderen zu teilen – und der ist häufig unsicher. Mit einem Passwort-Manager lassen sich Passwörter mit nur wenigen Klicks für andere freigeben, ohne die Sicherheit zu gefährden.

- **Multifaktor-Authentifizierung (MFA):** MFA ist eine weitere interessante Technologie beim Identitätsmanagement für Unternehmen. Die Multifaktor-Authentifizierung zählt zu den effektivsten Methoden, um einen sicheren Fernzugriff zu gewährleisten, da die Benutzer ihre Identität bei der Anmeldung mit zwei oder mehr Faktoren bestätigen müssen.

62%

der IT-Entscheidungsträger bezeichnen MFA als die wirksamste Methode für einen sicheren Fernzugriff.

Angesichts dessen, dass 80 % aller Sicherheitsverletzungen rein auf Passwörter zurückzuführen sind, ist die Multifaktor-Authentifizierung heutzutage wichtiger denn je. Phishing-Betrügereien werden immer mehr – MFA stellt eine zusätzliche Schutzschicht dar. Außerdem minimiert sie Gefahren wie Spear-Phishing, Keylogging, Credential-Stuffing, Brute-Force-Angriffe und mehr. Ein weiterer Vorteil der Multifaktor-Authentifizierung ist, dass sie absolut nahtlos ist: Mit seinen biometrischen Daten kann sich jeder Mitarbeiter im Handumdrehen anmelden – ein Win-Win für IT-Teams *und* Beschäftigte.

SO BEZIEHEN SIE MITARBEITER IM HOMEOFFICE IN IHRE IAM-STRATEGIE EIN

IT-Teams müssen nicht nur möglichst viele Sicherheitsmechanismen implementieren, sondern auch das Leben der Mitarbeiter so einfach wie möglich machen. Das Credo lautet Benutzerfreundlichkeit, also sollten Unternehmen Lösungen wählen, die die Zusammenarbeit fördern und die benötigten Ressourcen rasch zugänglich machen. Die richtige IAM-Strategie, die Mitarbeitern in und außerhalb des Büros einen sicheren und nahtlosen Zugriff bietet, wird alle zufriedenstellen.

Aber wie genau können Sie Ihr Firmennetzwerk absichern und dabei den Nutzerkomfort maximieren? Am besten mit einer Kombination aus Single Sign-On (SSO), Passwort-Manager und Multifaktor-Authentifizierung (MFA). Unsere Daten besagen, dass 90 % der Unternehmen SSO für ihre allgemeine Sicherheit für wichtig halten, während 59 % im Bereich MFA am meisten Verbesserungspotenzial sehen. Darüber hinaus finden 95 % der Unternehmen, dass sie gute Passwortgewohnheiten in ihren Teams fördern sollten. Es liegt also auf der Hand, dass alle drei Technologien beim Thema IT-Sicherheit eine zentrale Rolle spielen.

Jede Technologie für sich allein trägt dazu bei, Datenschutzverletzungen vorzubeugen und den Nutzerkomfort zu erhöhen – aber gemeinsam können sie Unternehmen eine nahtlose und ganzheitliche Identitätslösung bieten.

Die Vorteile eines kombinierten IAM-Ansatzes:

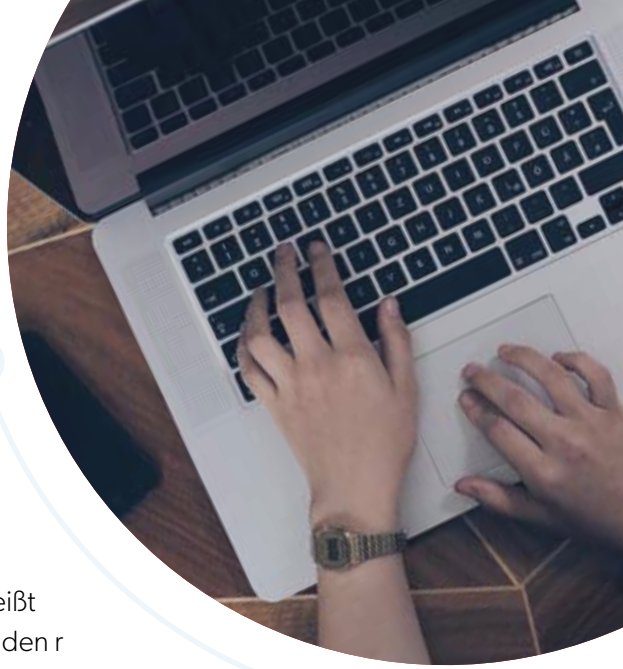
- **Komplette Zugriffsverwaltung:** Ihr IT-Team kann Benutzern in Echtzeit Zugriff gewähren bzw. den Zugriff aufheben. Bei SSO kommt ein starkes Authentifizierungsprotokoll zum Einsatz, das von den Mitarbeitern nur ein Passwort erfordert und der IT die volle Kontrolle gibt. Das bedeutet, dass Teammitglieder mit nur einem Login über ihr Mobilgerät, ihren Laptop oder ihr Tablet auf das Firmennetzwerk zugreifen können.
- **Einfacher Zugriff von jedem Ort:** Einfacher und sicherer Fernzugriff ist die ideale Grundlage für das ortsunabhängige Arbeiten und die digitale Transformation. Ihre Teams können an verschiedenen Standorten und in verschiedenen Zeitzonen effektiv zusammenarbeiten – und das mit einem Höchstmaß an Nutzerkomfort und Sicherheit.
- **Geringere IT-Kosten:** Unternehmen, die möglichst viele Aspekte des Identitätsmanagements automatisieren und standardisieren, holen mehr aus ihren IT-Ressourcen heraus. IAM lässt IT-Teams effizienter arbeiten, was langfristig zu bedeutenden Kosteneinsparungen führt.
- **Einfacheres Auditing und Reporting:** Wenn Sie Identitäten und Passwörter unter einem Dach vereinen (nämlich SSO), kann Ihre IT-Abteilung Benutzerzugangsdaten leichter überprüfen und problemlos detaillierte Berichte erstellen. Ihr IT-Team steht nicht vor einer langen Liste mit Geräten, sondern sieht anhand einer einzigen Identität und Anmeldung sofort, wer auf das Netzwerk zugreift.

59%

der Unternehmen halten es für sehr wichtig, die Sicherheit im Homeoffice in den nächsten zwölf Monaten zu erhöhen.

Nr. 1

Die Absicherung des Mitarbeiterzugriffs hat in Sachen IAM höchste Priorität, wenn es um ortsunabhängiges Arbeiten geht.



EINE NEUE NORMALITÄT – ABER SICHER

Das ortsunabhängige Arbeiten ist zu unserer neuen Normalität geworden, und Unternehmen, die diese neuen Arbeitsweisen nur zögerlich unterstützen, werden unweigerlich den Anschluss verlieren. Wenn Sie Ihr Unternehmen zukunftssicher machen wollen, dann führt an der digitalen Transformation kein Weg vorbei. Und warum auch? Sie kann Ihnen auf lange Sicht helfen, fähige Mitarbeiter an sich zu binden, neue zu gewinnen und Ihre Prozesse effizienter zu gestalten.

Mehr Homeoffice bedeutet auch mehr Sicherheitsrisiken, aber das heißt nicht, dass Ihr Unternehmen diesen Risiken ausgesetzt sein muss. Mit den r ichtigen IAM-Technologien und -Richtlinien kann Ihr IT-Team von jedem Ort für einen sicheren Fernzugriff auf das Firmennetzwerk sorgen. Während immer mehr Unternehmen auf Teleworking und Homeoffice umsteigen, ist eines klar: Sie müssen sich Gedanken über die Identitäts- und Zugriffsverwaltung machen.

In Folge der jüngsten Ereignisse gestatteten Unternehmen wie Twitter ihren Mitarbeitern, auf unbegrenzte Zeit von zu Hause aus zu arbeiten. Ob groß oder klein, Arbeitgeber möchten ihren Beschäftigten mehr Flexibilität bieten, und viele müssen veraltete Systeme ins 21. Jahrhundert holen. Nur so kann der Umstieg auf neue digitale Arbeitsweisen von Erfolg gekrönt sein.

Die Identitäts- und Zugriffsverwaltung wird in nächster Zukunft immer wichtiger werden. Der Grund dafür liegt auf der Hand: Ein Netzwerk lässt sich viel leichter absichern, wenn wir wissen, wer damit verbunden ist. Mit einer IAM-Lösung, die Identitäten und Logins unter einem Dach vereint, können IT-Teams mit Hilfe vordefinierter Protokolle wieder die Kontrolle über die Benutzer und ihre Zugriffsstufen erlangen.

Die richtige IAM-Strategie gibt Ihnen nicht nur die volle Kontrolle über den Mitarbeiterzugriff, sondern Sie können auch zusätzliche Sicherheitsmaßnahmen einführen, die im Hintergrund aktiv sind, und Ihren Teammitgliedern die Zusammenarbeit erleichtern. Von einer flexiblen Umgebung wie dieser profitieren alle – nicht zuletzt die Mitarbeiter, die eine bessere Work-Life-Balance haben. Eine ganzheitliche IAM-Strategie minimiert die Gefahr von Cyberangriffen auf Ihr Unternehmen und lässt Ihre Mitarbeiter auf sichere Weise von überall aus arbeiten.

08.06.20/PDF/ LMI1526