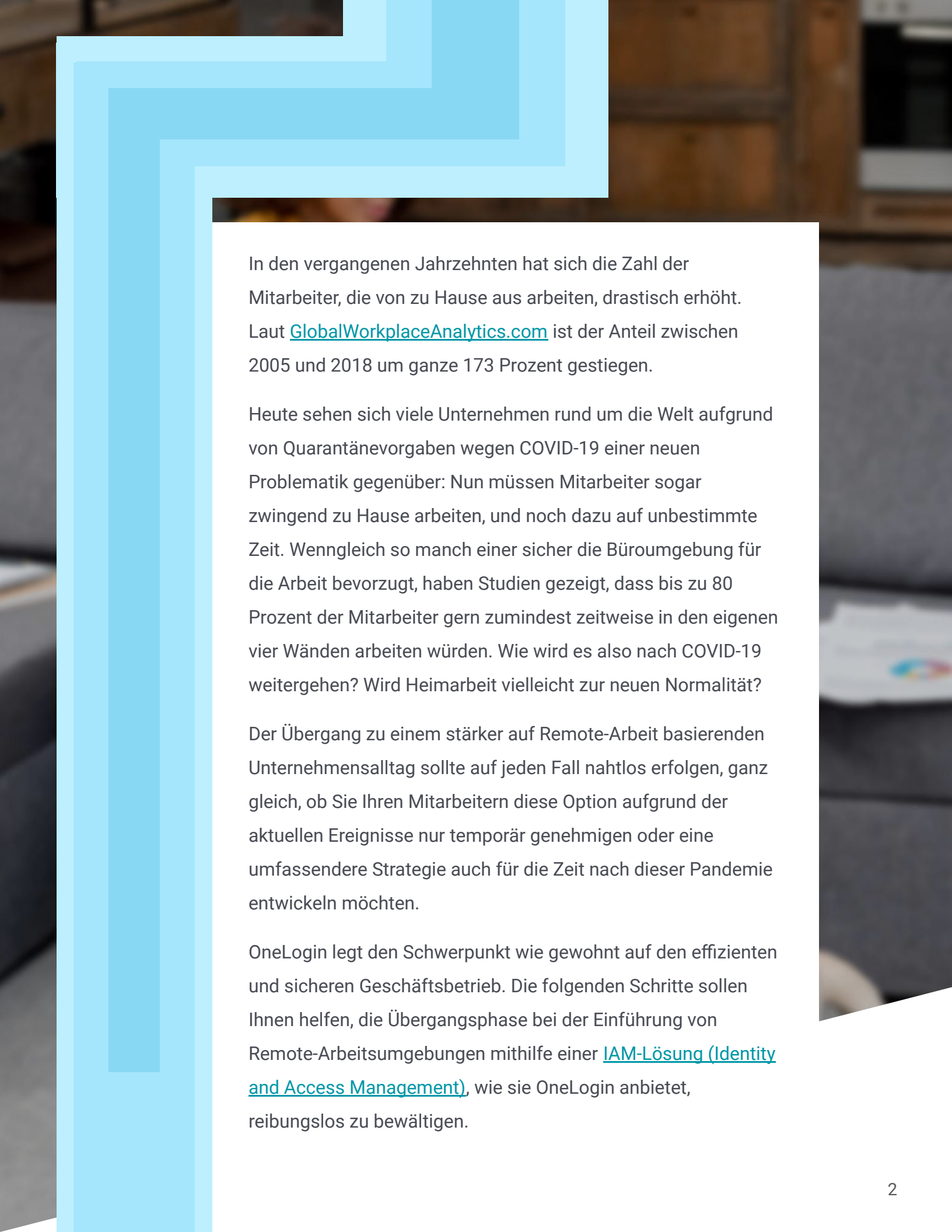
onelogin

CHECKLISTE

IN 5 SCHRITTEN

Zu einer sicheren Remote-Arbeitsumgebung, dank Identity Access Management (IAM)



In den vergangenen Jahrzehnten hat sich die Zahl der Mitarbeiter, die von zu Hause aus arbeiten, drastisch erhöht. Laut GlobalWorkplaceAnalytics.com ist der Anteil zwischen 2005 und 2018 um ganze 173 Prozent gestiegen.

Heute sehen sich viele Unternehmen rund um die Welt aufgrund von Quarantänevorgaben wegen COVID-19 einer neuen Problematik gegenüber: Nun müssen Mitarbeiter sogar zwingend zu Hause arbeiten, und noch dazu auf unbestimmte Zeit. Wenngleich so manch einer sicher die Büroumgebung für die Arbeit bevorzugt, haben Studien gezeigt, dass bis zu 80 Prozent der Mitarbeiter gern zumindest zeitweise in den eigenen vier Wänden arbeiten würden. Wie wird es also nach COVID-19 weitergehen? Wird Heimarbeit vielleicht zur neuen Normalität?

Der Übergang zu einem stärker auf Remote-Arbeit basierenden Unternehmensalltag sollte auf jeden Fall nahtlos erfolgen, ganz gleich, ob Sie Ihren Mitarbeitern diese Option aufgrund der aktuellen Ereignisse nur temporär genehmigen oder eine umfassendere Strategie auch für die Zeit nach dieser Pandemie entwickeln möchten.

OneLogin legt den Schwerpunkt wie gewohnt auf den effizienten und sicheren Geschäftsbetrieb. Die folgenden Schritte sollen Ihnen helfen, die Übergangsphase bei der Einführung von Remote-Arbeitsumgebungen mithilfe einer IAM-Lösung (Identity and Access Management), wie sie OneLogin anbietet, reibungslos zu bewältigen.

Schritt

1

Gewähren Sie Zugang zu nötigen Anwendungen

Damit Ihre Mitarbeiter produktiv zu Hause arbeiten können, benötigen sie natürlich Zugang zu sämtlichen geschäftskritischen Anwendungen. Glücklicherweise läuft ein Großteil moderner Anwendungen heute über die Cloud. Allerdings könnte es problematisch werden, den Überblick über die Zugangsdaten für zahlreiche Websites zu behalten. Durch die Implementierung einer IAM-Lösung können Sie Benutzern den Zugriff auf die gewünschten Anwendungen über eine zentrale Konsole ermöglichen.

SSO

Bei IAM-Plattformen wie der von OneLogin genügt die einmalige Authentifizierung, also Single Sign-On (SSO). Benutzer melden sich an einer einfachen Konsole an und klicken dann auf die jeweils benötigte Anwendung – die Eingabe weiterer Zugangsdaten ist nicht mehr erforderlich. **OneLogin erledigt den Rest.**

Schritt

2

Bieten Sie Mitarbeitern mehrere Optionen zur schnellen und effizienten Kommunikation

Wenn Ihre Mitarbeiter den persönlichen Austausch im Büro gewohnt sind, brauchen sie unbedingt geeignete Kommunikationsalternativen als Ersatz. Implementieren oder formalisieren Sie entsprechende Richtlinien für Audio-/Videokonferenzen mit Tools wie Zoom oder für Sofortnachrichtendienste wie Slack. Mithilfe Ihrer IAM-Lösung können Sie Ihren Teams derartige Anwendungen schnell bereitstellen.

IAM

Über die integrierte Bereitstellungsfunktionalität kann OneLogin die nötigen Benutzerkonten für Ihre Mitarbeiter in Anwendungen wie Zoom sofort remote anlegen. Onboarding-Prozesse, die ehemals Stunden oder gar Tage dauerten, sind nun in wenigen Minuten abgeschlossen. Zudem können Sie auf diese Weise auch neu eingestellten Mitarbeitern den Zugriff auf Ihre Anwendungen ermöglichen – ein klarer Vorteil in Zeiten wie diesen, wenn Büroräume geschlossen bleiben müssen.

Schritt

3

SECURITY

Schärfen Sie das Bewusstsein Ihrer Mitarbeiter für die Sicherheit

Wenn aufgrund einer Krisensituation Daten auch außerhalb Ihres geschützten Unternehmensgeländes genutzt werden müssen, wird die Sicherheit zur besonderen Herausforderung. Zum Zugriff auf die Daten nutzen Ihre Mitarbeiter nun Systeme, die sich Ihrer Kontrolle entziehen, und WLAN-Verbindungen, die Sie nicht selbst gesichert haben. Obendrein gibt es in Ihrem Unternehmen möglicherweise Anwendungen, auf die normalerweise nur über Ihr Intranet zugegriffen wird und die nun einen Plan für den sicheren Fernzugriff erfordern.

Um Ihren Mitarbeitern zu verdeutlichen, wie wichtig die Sicherheit ist, können Sie verschiedene Ansätze verfolgen.

I

Ein möglicher Ansatz ist die Verwendung eines Virtual Private Network (VPN). Ein VPN bietet Mitarbeitern einen sicheren und verschlüsselten Tunnel, über den sie sich mit Ihrem Intranet und internen Unternehmensressourcen verbinden können. Im Idealfall melden sich die Benutzer am VPN mit denselben Zugangsdaten an, die sie auch zum Zugriff auf alle anderen Ressourcen verwenden.

Plattformen wie OneLogin stellen einen RADIUS-Endpunkt bereit, mit dem sich Ihr VPN verbinden kann, um die Authentifizierung Ihrer Benutzer zu ermöglichen. Folglich können sich Ihre Benutzer mit denselben Zugangsdaten am VPN und an ihren anderen Anwendungen anmelden. Bei Bedarf können Sie sogar festlegen, dass Benutzer am RADIUS-Endpoint eine zusätzliche Authentifizierungsmethode verwenden müssen, zum Beispiel ein Einmalpasswort.

II

Die Konfiguration des VPN-Clients kann etwas Zeit in Anspruch nehmen, ebenso wie die Einweisung Ihrer Benutzer in die nötigen Schritte zum Herstellen der Verbindung. Als Alternative bietet sich ein Softwareagent an, der Ihren Benutzern den Zugriff auf Anwendungen im Unternehmensrechenzentrum über Ihre IAM-Lösung gewährt. Durch das Zwischenschalten der IAM-Plattform bleiben Ihre Anwendungen sicher hinter Ihrer Firewall geschützt und der Softwareagent fungiert quasi als Vermittler. Diese Art von Funktionalität kann als Fundament für eine robuste und sichere Hybridumgebung dienen, in der einige Anwendungen im Rechenzentrum vor Ort und andere Anwendungen in der Cloud ausgeführt werden.
Die entsprechende Funktion bei OneLogin heißt OneLogin Access und kann die Rolle des Softwareagenten übernehmen, der von Ihren Anwendungen im Rechenzentrum aus mit der Cloud und umgekehrt kommuniziert – ohne Beeinträchtigungen für die Benutzer.

III

Für viele Unternehmen ist es wichtig, dass ihre Mitarbeiter von zu Hause aus auf dieselben Rechner zugreifen können, an denen sie auch im Büro sitzen. Systeme wie Remote Desktop Gateway von Microsoft ermöglichen genau das. Damit dies funktioniert, müssen Ihre Mitarbeiter auf sichere Weise auf Remote Desktop Gateway zugreifen.

OneLogin sorgt für die nötige Sicherheit. Über das RDG-Plug-in von OneLogin konfigurieren Sie Benutzer, die sich mit ihren Zugangsdaten für OneLogin am RDG-Server anmelden können. Hierfür lässt sich bei Bedarf auch die Multi-Faktor-Authentifizierung einrichten, sodass sich wirklich nur diese berechtigten Benutzer mit Ihrem RDG-Server und Ihren VMs verbinden können.

Schritt

4

Schützen Sie Ihre Systeme durch sichere Passwörter und Zugriffsprotokolle

Viele Unternehmen nutzen in ihren Rechenzentren Verzeichnisdienste wie Active Directory von Microsoft, um den Zugriff auf Ressourcen zu kontrollieren. Sobald ein neuer Mitarbeiter freigeschaltet wurde, kann er mit seinen individuellen Zugangsdaten auf Netzwerkressourcen zugreifen. Ihr Administrator sorgt dabei mithilfe von Sicherheitsrichtlinien und -verfahren dafür, dass Passwörter komplex genug sind und oft genug geändert werden. Wenn Benutzer jedoch zum Beispiel in einer Krisensituation von zu Hause aus arbeiten, kann das Anlegen neuer Benutzerkonten und die Konfiguration von Active Directory eine gewisse Zeit in Anspruch nehmen.

DESKTOP

Wie können Sie also den Zugriff auf Ihre Systeme auch ohne Active Directory zuverlässig steuern? Software wie Desktop Pro von OneLogin bietet eine Lösung für dieses Problem. Wurde OneLogin Desktop Pro auf einem Arbeitsrechner installiert, kann sich ein berechtigter Benutzer automatisch mit seinen Zugangsdaten für OneLogin an Ihren Systemen anmelden. So wird sichergestellt, dass Benutzer ihre Passwörter in den empfohlenen Abständen ändern und Ihre Vorgaben in Sachen Passwortkomplexität beachten. Bei Bedarf können Sie zudem eine zusätzliche Authentifizierungsmethode fordern, zum Beispiel ein Einmalpasswort.

Schritt

5

Implementieren Sie die Multi-Faktor-Authentifizierung

Wenn Ihre Mitarbeiter außerhalb Ihrer Büroräume arbeiten, fehlen die üblichen physischen Schutzvorkehrungen und es besteht die Gefahr, dass unbefugte Benutzer auf ihre Arbeitsrechner zugreifen. Betrüger und Kriminelle könnten Benutzernamen und Passwörter ausspähen, um sich den Zugang zu Ihren Systemen zu verschaffen. Die Multi-Faktor-Authentifizierung (MFA) bietet hier besseren Schutz. Benutzer müssen ihre Identität über eine zusätzliche Authentifizierungsmethode nachweisen, zum Beispiel über ein Einmalpasswort, einen YubiKey oder gar ihren Fingerabdruck. So wird es böswilligen Akteuren deutlich erschwert, sich für einen Ihrer Mitarbeiter auszugeben.

VIGILANCE AI

Moderne IAM-Lösungen sollten heutzutage die MFA standardmäßig unterstützen. OneLogin geht mit SmartFactor Authentication™ noch einen Schritt weiter. Diese Funktion kann mithilfe von maschinellem Lernen potenziell verdächtige und gefährliche Verhaltensmuster von Benutzern erkennen. Zu diesem Zweck erstellt die Vigilance AI™ Engine von OneLogin Profile mit dem typischen Benutzerverhalten, beispielsweise basierend auf Standort, Gerät, normalerweise genutzten Anwendungen, regulären Arbeitszeiten usw. Je nach erkanntem Risiko werden dann unterschiedlich starke Authentifizierungsmethoden gefordert. Obendrein kann SmartFactor die Zugangsdaten eines Benutzers mit einer Datenbank abgleichen, in der bekannte kompromittierte Benutzerkonten und Passwörter erfasst sind. Falls ein Benutzer versucht, solche kompromittierten Zugangsdaten zu verwenden, wird der Anmeldeversuch automatisch abgewiesen.