mimecast®

Verbesserung der Cyber-Sicherheit im Home Office

13 Empfehlungen

April 2020

Viele Unternehmen befinden sich mitten in der praktischen Umsetzung des Home Offices.

Die Zahl der täglichen Zoom-Nutzer hat sich von Dezember 2019 bis März 2020 um das 20-fache auf 200 Millionen erhöht...
sprechen Sie über Netzkapazität!

Was sind die Auswirkungen der Corona-Krise auf die Cyber-Sicherheit? Und welche bewährten Praktiken im Bereich der Cyber-Sicherheit sind am wichtigsten, um diesen abrupten Wandel sowohl nahtlos, als auch sicher zu gestalten?

Die Verlagerung der Arbeit ins Home Office wird für immer Teil der Cyber-Resilienz-Strategie der meisten Organisationen sein - Teil der neuen Normalität im Bereich IT und Sicherheit. Wenn Ihre Mitarbeiter effektiv von zu Hause aus arbeiten können, sollten sich Ihr Unternehmen sehr glücklich schätzen, denn viele Branchen können das größtenteils nicht - wie Fluggesellschaften, Hotels, Kreuzfahrtgesellschaften und Fertigungsunternehmen, um nur einige zu nennen.

Eine notwendige Schlussfolgerung ist, dass Ihre IT- und Sicherheitssysteme das Arbeiten aus dem Home Office ermöglichen und nicht behindern sollten. Um das Arbeiten von zu Hause aus nahtloser und sicherer zu gestalten, bietet dieses eBook 13 wichtige Empfehlungen, von denen einige in kurzer Zeit ausgeführt werden können, während andere für die Umsetzung eine Weiterentwicklung der IT- und Sicherheitsstrategien und neue Investitionen erfordern. Diese Empfehlungen wurden aus Mimecasts eigenen Erfahrungen als globales Cyber-Sicherheitsunternehmen, den Erkenntnissen von Branchenanalysten und den Perspektiven von Mitgliedern **des Cyber Resilience Think Tank abgeleitet.**

Einige der Empfehlungen werden sich darauf beziehen, die Cloud für alles zu nutzen, sowohl für die IT als auch für die Sicherheit. Ein klarer Hinweis ist, dass kein Weg an der Cloud und ihre inhärente Skalierbarkeit, Zugänglichkeit, geografische Vielfalt und Belastbarkeit vorbeiführt. Stellen Sie sich vor, Home Office in dieser Qualität wäre bereits vor 10 Jahren möglich gewesen.

Mark O'Hare, der CISO von Mimecast, fasste Mimecasts eigene Erfahrungen als "In Cloud We Trust" zusammen, da Mimecast seit Jahren unsere eigene Cloud-first-Strategie für IT und Sicherheit umsetzt, sowohl in Vorbereitung auf einen Notfall als auch für die tägliche Unterstützung unserer hochmobilen, globalen und fest angestellten Mitarbeiter, die von zu Hause aus arbeiten. Die Umstellung auf eine 100%ige Remote-Arbeitsstrategie verlief relativ nahtlos und ermöglichte es dem Mimecast-Team, sich auf die "weicheren" Bedürfnisse der unter Quarantäne stehenden Mimecaster zu konzentrieren. Aber mehr zu diesen Bedürfnissen am Ende dieses eBooks.

Empfehlungen

Mike Rothman, Securosis-Analyst und Präsident

"Wir gehen davon aus, dass COVID-19 die bereits in Bewegung befindlichen Trends beschleunigen wird, wie z.B. die Umstellung auf SaaS und den Einsatz der meisten Anwendungen in der Public Cloud. Sicherheitsteams müssen ihre Tools und Betriebsprozesse anpassen, um für die Realität bewappnet zu sein."

ERSTENS.

Überprüfen Sie die wichtigsten Anwendungen und Geschäftsprozesse und bewerten Sie diese hinsichtlich ihrer Verfügbarkeit und Sicherheit.

Die Ausarbeitung einer Strategie und unterstützender Systeme nach Bedarf für jede Geschäftsfunktion ist wichtig. Die Aussage "es ist nicht möglich, von zu Hause aus zu arbeiten" ist jedoch keine akzeptable Antwort. Denn in einem Notfall ist "nicht möglich" keine Lösung.

Es ist jedoch sinnvoll, den Betrieb in einem abgeschwächten Modus zu planen, wenn die volle Funktionalität des Geschäftsprozesses zu teuer oder kompliziert ist, um aus der Ferne ausgeführt zu werden. Ein wesentliches Ziel ist es, vom eigenen Konzept nicht überwältigt zu werden, sollte es zu einer Störung kommen. Die einzige andere Möglichkeit besteht darin, die Durchführung dieser Geschäftsfunktion einzustellen oder zu versuchen, diesen Teil Ihres Unternehmens von Ihren lokalen politischen Führern als "kritisch" deklarieren zu lassen.

ZWEITENS.

Nutzen Sie jede Anwendung über die Cloud.

Cloud First, Second und Third sollte die Norm sein. Die Zahl der Anwendungen, die nicht in der Cloud gehostet und von dort aus betrieben werden können, geht zur Neige. Wenn wir eines aus dieser schnellen Umstellung auf Home Office gelernt haben, dann, dass die Cloud einsatzsbereit war. Sowohl SaaS als auch IaaS. Das Internet ist belastbar, die Heimnetzwerke für viele Mitarbeiter sind hervorragend und die Anbieter von Cloud-Diensten waren auf die erhöhte Last vorbereitet.

Wenn eine vorhandene, kritische Anwendung nicht in die Cloud migriert werden kann, fangen Sie an, eine neue, Cloud-basierte Anwendung an ihre Stelle zu setzen. In der Zwischenzeit sollten die verbleibenden Benutzer der standortbasierten Anwendungen für den fortgesetzten **VPN-Zugang** weiterhin Priorität haben. Aber mit der Zeit dürfte die Nutzung von VPNs deutlich zu-rückgehen.

Hinweis: Denken Sie daran, dass einige Länder den Zugang zu bestimmten Cloud-Anwendungen blockieren und nicht jeder, überall kostengünstigen Zugang zu schnellem und zuverlässigem Internet hat, also planen Sie entsprechend.

Jon Oltsik, Leitender Hauptanalyst, ESG

"Um mit der zunehmenden Zahl der aus dem Home Office arbeitender Mit-arbeiter fertig zu werden, konzentrieren sich die CISOs auf sichere DNS-Dienste als eine schnelle Möglichkeit, bei der Risikominderung zu helfen."

DRITTENS.

Verwenden Sie cloudbasierte oder zumindest cloud-zentrierter Sicherheitslösungen für jede Cyber-Sicherheitskontrolle.

Stellen Sie sicher, dass Ihre Cyber-Sicherheitskontrollen - Netzwerk, Web, E-Mail, Endpunkt, Identitätsmanagement, Authentifizierung, Zugriffsmanagement, SIEM/SOAR - ohne Rücksicht auf den Standort der Benutzer voll funktionsfähig sind (d.h. stellen Sie sicher, dass diese Cloud-basiert sind). Wenn Sie die Umstellung von On-Premise IT-Anwendungen und -Daten abgeschlossen haben, können Sie gleichzeitig On-Premise Sicherheitskontrollen abschaffen. Sie werden ohnehin zunehmend weniger wertschöpfend.

Cloud-basierte Sicherheitskontrollen reduzieren die Notwendigkeit des Backhauling von Datenverkehr aus entfernten Büros oder die Verwendung von VPNs zur Durchsetzung und Überwachung der Sicherheit und machen sie dann letztendlich überflüssig. Beginnen Sie mit den Sicherheitskontrollen, die von Ihren alltäglichen Benutzern verwendet werden - wie Authentifizie-rung und SSO - und gehen Sie im Laufe der Zeit zu spezialisierteren Teams wie IT und Sicherheit über.

Stellen Sie sicher, dass alle Ihre Software-Updates, Sicherheits- und Helpdesk-Funktionen ohne direkte Verbindung zum Unternehmensnetzwerk durchgeführt werden können.

VIERTENS.

Stellen Sie Firmen-Laptops / mobilen Geräte zur Verfügung und sorgen Sie für den Einsatz von Mobile Device Management (MDM) für BYOD-Geräten.

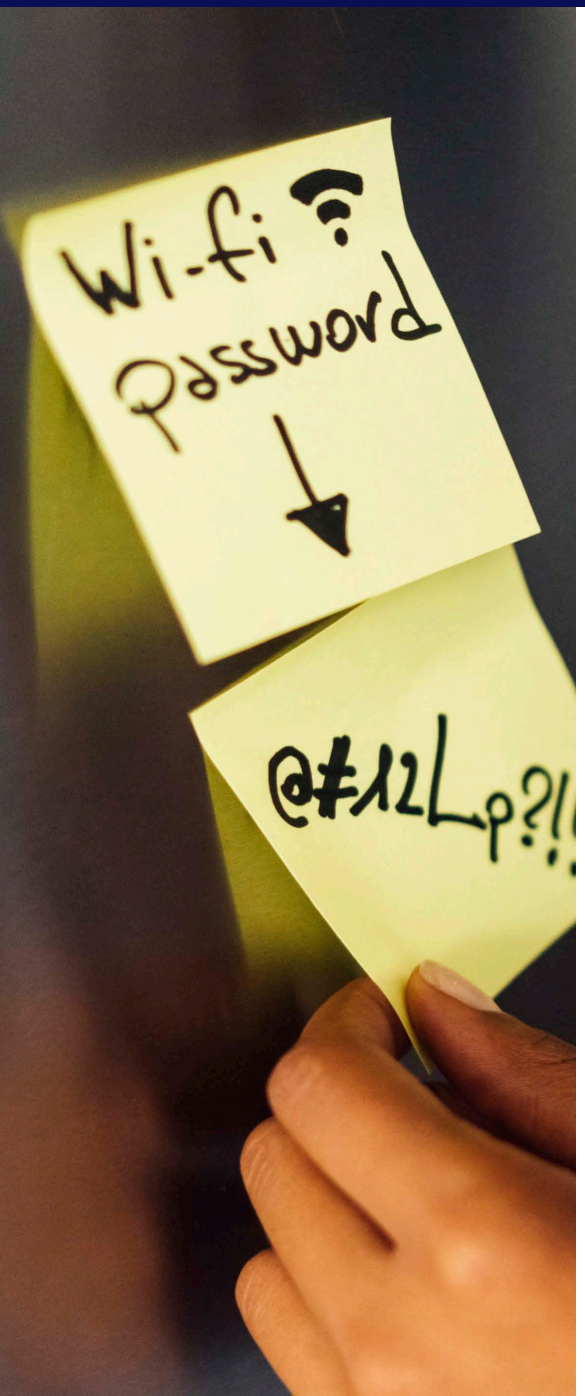
Die einzige Möglichkeit, den Endpoint effektiv abzusichern, besteht entweder darin, ihn selbst zu betreiben oder den Teil der Geschäftsanwendung über Mobile Device Management (MDM) zu sichern. Der Versuch, die PCs Ihrer Mitarbeiter vollständig zu sichern, kann auf eine Komplexität und Datenschutzprobleme stoßen, die nur schwer zu überwinden sind. Die Lösung: Einfach in den sauren Apfel beißen, Laptops bereit-stellen und MDM nach Bedarf für mobile Geräte einset-zen.

Vergewissern Sie sich außerdem, dass alle Ihre Software-Updates, Sicherheits- und Helpdesk-Funktionen ohne direkte Verbindung zum Unternehmensnetzwerk durchgeführt werden können. Sie sollten über einen Prozess verfügen, um neue Hardware auszustellen und Fehlerbehebungen mit Fedex, UPS oder USPS durchzuführen, ohne dass dazu Besuche im Büro erforderlich sind. Diese Prozesse helfen natürlich auch während normaler Zeiten bei der Unterstützung dauerhaft aus dem Home Office arbeitender Mitarbeiter.

FÜNFTENS.

Führen Sie die Multi-Faktor-Authentifizierung ein.

Keine Ausreden. Bei Daten und Anwendungen in der Cloud (oder auf dem Weg dorthin) ist der Verlust eines einzigen, SSO-fähigen Berechtigungsnachweises das Todesurteil für die Sicherheit. Mit diesem einzigen Berechtigungsnachweis hätte ein böswilliger Akteur Zugang zu einer Vielzahl von Daten. Darüber hinaus kann das Risiko einer Account-Übernahme weitgehend durch **Multi-Faktor-Authentifizierung** angegangen werden. Der damit verbundene SSO-Service macht den Anwendungszugriff für Ihre Mitarbeiter unglaublich einfach, egal wo sie sich befinden!



SECHSTENS.

Integrieren Sie Ihre Aktivitäten zur Cloud-Sicherheitskontrolle, Bedrohungsaufklärung und sicherheitsrelevante Fernmesstechnik in ein zentralisiertes System zur Erkennung und Reaktion auf Bedrohungen (SIEM/SOAR), die ebenfalls Cloud-basiert sind.

Verwenden Sie keine Sicherheitskontrollen, die nicht genügend APIs und Standardintegrationen bieten, um dies zu erreichen. Die Cloud sollte nicht das Silo-Problem replizieren, das in der Welt der Sicherheitskontrollen vor Ort so weit verbreitet ist. Nur weil Ihre Sicherheitskontrollen in der Cloud betrieben werden, bedeutet das nicht, dass Sie die Sichtbarkeit und den investigativen Nutzen dieser Kontrollen verlieren sollten.

SIEBTENS.

Helfen Sie Mitarbeitern bei der ordnungsgemäßen Sicherung ihrer Heimnetzwerke.

Die Heimnetzwerke der Mitarbeiter sind Teil Ihres Business-Continuity-Programms, also betrachten Sie diese auch als solche. Vermeiden Sie die Verwendung von Standard-Administrator-Passwörtern auf ihren Routern und die Verwendung von schwachen oder leicht zu erratenden WiFi-Zugangspasswörtern. Verlangen Sie von Ihren Mitarbeitern, dass diese ein leistungsfähiges Heimnetzwerk zur Verfügung haben - egal ob kabel- oder satellitengestützt. Ihre Mitarbeiter sollten außerdem über ihre mobilen Geräte einen Backup-Zugang zum Internet haben. Mit der bevorstehenden Einführung von 5G-Mobilfunknetzen wird dieser Teil der Gleichung zunehmend kosteneffizienter werden.

James Lugabihl, Leitender Direktor, Globale Sicherheit, ADP

"Während eines Sicherheitsvorfalls ist eine klare und präzise Kommunikation mit Ihren Benutzern von ausschlagebender Bedeutung."

ACHTENS.

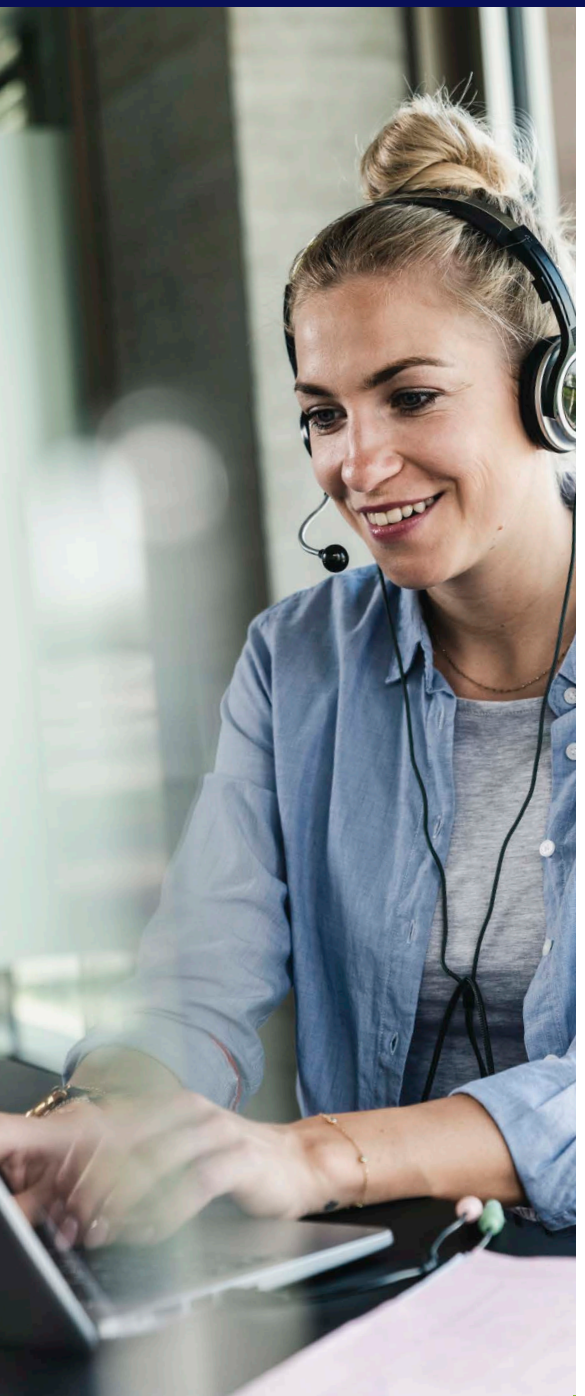
Seien Sie darauf vorbereitet, die Automatisierung Ihres Schulungsprogramms zum Sicherheitsbewusstsein zu intensivieren, zu personalisieren und zu fördern.

Denken Sie daran, dass es bei der Arbeit aus dem Home Office für Ihre Mitarbeiter viel schwieriger ist, ihren Bürokollegen um Sicherheitsratschläge zu bitten. Lenken Sie die Aufmerksamkeit Ihrer Teams auf die Sicherheit. Regelmäßige und aktuelle Videos zur Schulung des Sicherheitsbewusstseins sind eine gute Möglichkeit, dies zu erreichen. **Regelmäßige Kommunikation ist entscheidend!**

NEUNTENS.

Ein klarer Prozess für Mitarbeiter und gegebenenfalls Kunden/Partner ist wichtig, um potenzielle Sicherheitsprobleme, auf die sie stoßen, zu melden.

Als Ihre letzte Verteidigungslinie können Menschen ein sehr wirksames Sicherheitsfrühwarnsystem sein. Außerdem steht Ihrem Helpdesk- und Sicherheitsteam im Backend natürlich ein Prozess zur Verfügung, mit dem es die Meldungen der Helpdesks und Sicherheitsteams sammeln, verwalten, einordnen, untersuchen und bearbeiten kann.



ZEHNTENS.

Nutzen Sie die Vorteile von Cloud-basierten Collaboration Tools.

Stellen Sie in diesem Zusammenhang sicher, dass deren eingebaute Sicherheitseinstellungen verwendet werden (z.B. um unbefugten Zugriff zu vermeiden). Auf diese Weise nutzen Ihre Mitarbeiter bereits die Werkzeuge, auf die sie sich verlassen werden, wenn sie von zu Hause aus arbeiten. Wenn Sie keine Kollaborationswerkzeuge als Teil Ihres Standard-IT-Pakets bereitstellen, werden Ihre Mitarbeiter alles einsetzen, was es kostenlos oder billig gibt, um ihre Arbeit weiterhin zu erledigen; das bedeutet, dass Sie die Sicherheitstransparenz und -kontrolle verlieren.

ELFTENS.

Vergessen Sie Ihre IT- und Sicherheitsteams nicht. Sie müssen in der Lage sein, genauso sicher und effizient zu arbeiten, wie alle anderen in der Organisation.

Haben Sie eine Sicherheitszentrale im Büro mit einer Infrastruktur gebaut, der voraussetzt, dass sich alle im selben Raum befinden? Benötigen Ihre IT- und Sicherheitsmitarbeiter direkten oder lokalen Zugang zu den Administrationssystemen? Siehe Empfehlung #1 - #3, aber in der Zwischenzeit ist ein fortgesetzter VPN-Zugang für diese Mitarbeiter vertretbar, wenn es sein muss. Vermeiden Sie außerdem die Überlastung Ihres Teams.

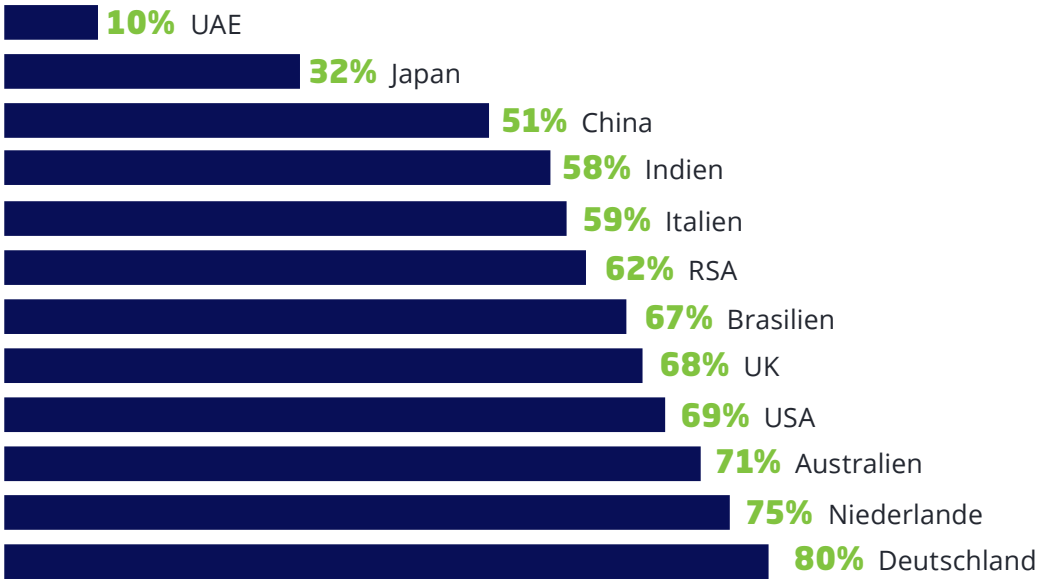
Betonen Sie erneut, dass die Arbeit von zu Hause aus nicht bedeutet, rund um die Uhr zu arbeiten.

Und vergessen Sie nicht, neues Sicherheitspersonal einzustellen (das gilt eigentlich für alle Positionen). Der natürliche Prozess des Lernens “wer und was” nach Osmose kann nicht stattfinden, wenn jeder aus dem Home Office arbeitet, also planen Sie ein dezentrale Onboarding von neuem Personal ein. Selbst wenn Sie während einer Sondersituation keine neuen Mitarbeiter einstellen, ist es sehr gut möglich, dass eine verstärkte Arbeitsteilung und Schichtarbeit während der Krise Mitarbeiter Verantwortungen übernehmen, die normalerweise nicht Teil Ihrer Arbeit sind.

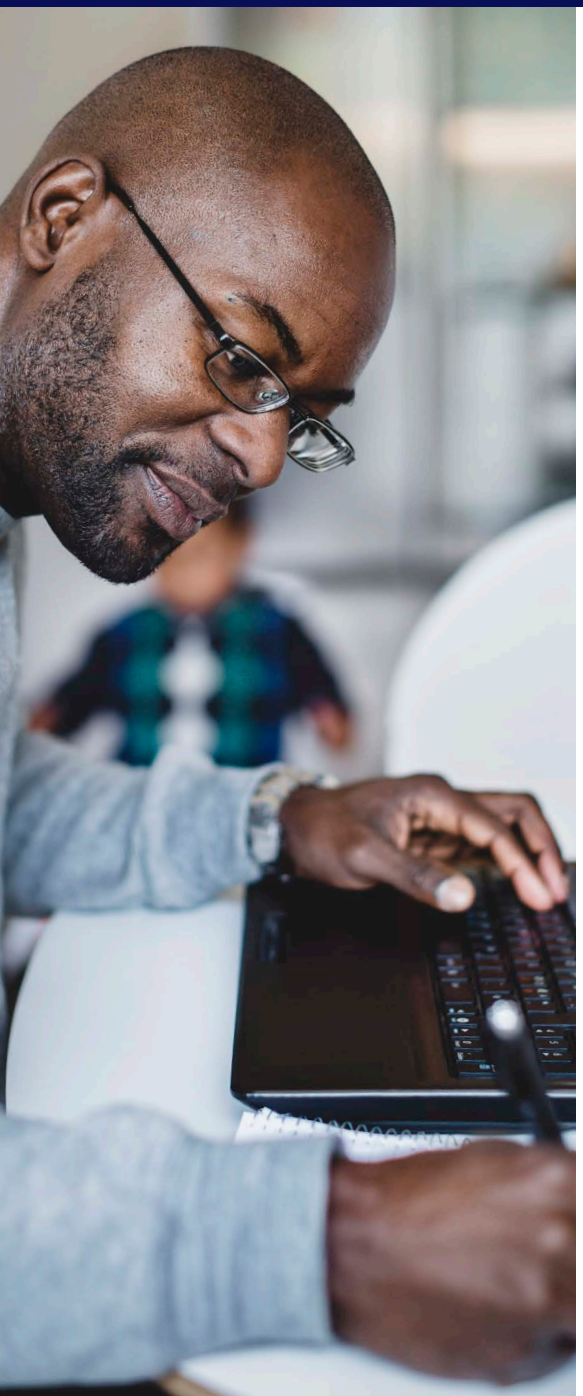
62%

INTERNATIONALER DURCHSCHNITT

PROZENTSATZ DER MITARBEITER DIE VOR DER CORONA-KRISE 1-2 TAGE/WOCHE AUS DEM HOME OFFICE GEARBEITET HABEN



Quelle: IWG Global Workplace Study 2019



ZWÖLFTENS.

Führen Sie regelmäßige Tests durch, auch wenn Ihre Mitarbeiter nicht während einer Ausnahmesituation von zu Hause aus arbeiten.

Führen Sie jedes Jahr eine Testwoche durch, in der alle Mitarbeiter Ihrer Organisation ausnahmslos zu Hause arbeiten. Suchen Sie sich eine Woche aus, die Sinn macht, klären Sie das mit dem Management und erklären Sie diese Woche jedes Jahr für die gesamte Organisation zur Home Office Woche. Testphasen sind der Schlüssel zur Verbesserung der Widerstandsfähigkeit.

Lockern Sie bei Bedarf auch Ihre Richtlinien für Tätigkeiten, die nicht unmittelbar im Rahmen eines Notfalls anfallen, so dass die für Home Office notwendigen Betriebssysteme das ganze Jahr über kontinuierlich getestet werden und sich Ihre Mitarbeiter daran gewöhnen, bevor der Ernstfall eintritt.

In vielen Regionen ist ein regelmäßiges Home Office bereits sehr verbreitet - mit einem weltweiten Durchschnitt von 62%, die vor der Pandemie 1-2 Tage pro Woche von zu Hause aus arbeiten, in einigen Regionen jedoch weniger. Vergleichen Sie Ihre Organisation mit den Statistiken der Grafik und erwägen Sie ernsthaft, Vorbereitungen zu treffen, um Ihre Organisation während normaler Zeiten weiter vorzubereiten. Es wird sich in Notfällen auszahlen.

DREIZEHNTENS.

Wenn sich die Dinge von der aktuellen Krise beruhigen (und das wird sie), sollten Sie eine umfassende Retrospektive durchführen....

... sodass das Gelernte in Ihr Programm zurückgeführt werden kann und als Richtschnur für zukünftige Investitionen dient. Bei längeren Unterbrechungen kann die Durchführung selektiver Zwischenberichte helfen, notwendige Korrekturen vorzunehmen. Gestalten Sie diese Beurteilungen, ob während oder nach der Krise, anhand von Personen, Prozessen und Technologien, um Ihre wichtigsten Stärken und Schwächen am besten herauszufinden.

Zusätzliche Empfehlung

Wenn Sie in den oben genannten Punkten gut abschneiden, werden Ihre IT- und Sicherheitssysteme und -prozesse nicht Ihre Hauptherausforderungen sein. Dafür zu sorgen, dass alle Ihre Mitarbeiter emotional und sozial versorgt sind, wird ganz oben auf Ihrer Prioritätenliste stehen. Lassen Sie der Kreativität freien Lauf, um dies zu erreichen!

Einige Ideen zur Bewältigung der sozialen Isolation:

- Zoom Happy Hour
- Aufnahmen vom plötzlichen Auftauchen der Kinder während eines Zoom Meetings
- Verrückte Hunde Fotos
- Bad Hair Day Wettbewerbe
- Lustige GIFs in Slack-Kanälen
- Bester Hintergrund in Video-Konferenzen
- Virtuelle Talentshows