



# Hybrid Work ist nicht das Ziel

Es ist erst der Anfang

Hybrides Arbeiten  
läuft vielerorts  
so gut, dass  
Führungskräfte  
es inzwischen für  
die Patentlösung  
halten – dabei ist  
der Ansatz noch  
viel zu simpel.

Ein ortsunabhängiges Büro bringt unrealistische Erwartungen mit sich: Von den Arbeitnehmenden wird verlangt, dass sie weiterhin – egal wo, egal wann – mit der gleichen Geschwindigkeit, Effizienz und Sicherheit arbeiten, als säßen sie an ihren Büroschreibtischen. Damit diese Wunschvorstellung tatsächlich real werden kann, ist die IT gefragt.

Moderne Zusammenarbeit ist ein guter Ansatzpunkt. Die IT muss dafür sorgen, dass alle Mitarbeitenden das Gefühl haben, dabei zu sein – selbst wenn Teams Hunderte von Kilometern voneinander entfernt arbeiten. Das gilt auch für die individuelle Produktivität: Der Fokus muss darauf liegen, dass Mitarbeitende ihre persönliche Topleistung abrufen können, egal wo sie sind.

Gleichzeitig müssen wir uns auf die Zukunft vorbereiten. Wenn wir innerhalb der letzten zwei Jahre etwas gelernt haben, dann wohl, dass Ungewissheit die einzige Gewissheit ist.

Aber wie plant man mit Ungewissheit? Es klingt wie ein Widerspruch in sich, doch viele Führungskräfte stellen diese Prämisse bereits in den Mittelpunkt ihrer Unternehmensstrategien. Die Zeiten des Fünfjahresplans, dem Mitarbeitende kompromisslos folgen, sind vorbei. An seine Stelle ist das gerückt, was der Ökonom und Autor Dr. Bill Conerly als „die flexible Haltung“ beschreibt.

Scott Kirby, CEO der United Airlines, hat sich diese Strategie zu eigen gemacht, indem er alle Budgets für 2021 gestrichen hat. Stattdessen stellte Kirby „Bounceback-Teams“ zusammen, die herausfinden sollten, welche Ressourcen United benötigen würde und welche nicht, außerdem sollten sie Blocker wie den Mangel an flugbereiten Piloten prognostizieren, sobald die Nachfrage wieder stieg.

Kirbys Gedanken enthalten eine einfache Botschaft, die für alle Führungskräfte gilt: Entweder man bereitet sich auf Unsicherheiten vor, oder man ist bereit zu scheitern.



# Wie man sich auf Ungewissheit vorbereitet

Jedes Unternehmen ist anders. Daher wird es nie eine Goldene Regel geben, die für alle gilt. Allerdings gibt es vier Prinzipien, die auf jedes Unternehmen anwendbar sind:

## MITEINANDER VERNETZEN

---

Es spielt keine Rolle, wo die Menschen arbeiten. Sei es ihr Zuhause, ein zentrales Büro oder unterwegs im Zug – sie sind auf kollaborative Tools angewiesen, die sie zu einem vollwertigen Teil des Teams machen.

## SICHERHEIT ERLEICHTERN

---

Die Pandemie hat gezeigt, dass Cyberkriminelle und ihre Angriffe unter dem Zustand von Ungewissheit geradezu florieren. Chief Information Security Officers (CISOs) müssen sich darauf vorbereiten, indem sie sich jetzt auf Grundprinzipien konzentrieren.

## REAKTIVE WORKFLOWS WÄHLEN

---

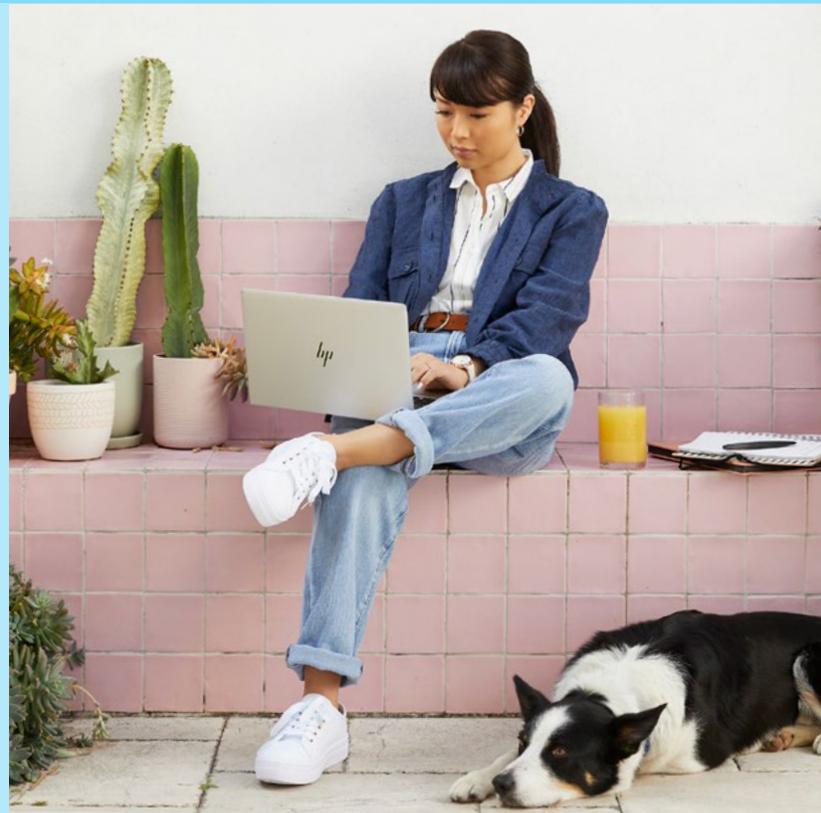
Die Zukunft wird mehr neue Tools, zusätzlichen Bedarf und eine höhere Nachfrage nach standortunabhängigem Arbeiten mit sich bringen. Diese Zukunft braucht Vorbereitung. Unterbrechungen sind der Feind.

## AUF FLEXIBLE PLANUNG SETZEN

---

Ein Paradox? Das muss flexible Planung nicht sein. Wir müssen Ungewissheit wahrnehmen, anstatt sie zu ignorieren.

In diesem E-Book können Sie sich auf die Erfahrungen von vorausschauenden Führungskräften, Sicherheitsexperten, und IT-Entscheidern verlassen, die bereits dabei sind, herausfordernde Entscheidungen zu treffen und neue Lösungen zu implementieren.



50 % der Informationsarbeiter:innen aus den Vereinigten Staaten und Europa glauben daran, dass die Pandemie die Welt für immer verändert hat und wir nicht mehr zur „Normalität“ zurückkehren werden. Forrester<sup>3</sup>

# Menschen verbinden

Früher haben sich Kolleg:innen ganz natürlich im Büro miteinander vernetzt. Doch diese Umgangsform muss neu gedacht werden. Unternehmen müssen moderne Tools integrieren, die den Menschen die Freiheit geben, von jedem Raum aus „da“ zu sein.



## FRÜHER →

Zentralisierte Büros waren die Norm – mobile Arbeitnehmer waren die Ausnahme

Die Erwartungen der Mitarbeitenden waren ähnlich und vorhersehbar

Zusammenarbeit fand hauptsächlich im Büro statt

## JETZT →

Hybrides Arbeiten ist die Norm – doch Menschen nutzen die Tools, die sie bereits haben

Mitarbeitende streben je nach Lebenssituation nach unterschiedlichen Dingen

Die Zusammenarbeit erfolgt ad hoc

## IN ZUKUNFT

Der Standort ist irrelevant – Arbeitnehmer wollen Tools mit denen Sie überall arbeiten können

Mitarbeitende fordern in Bezug auf Tools und Status Gleichheit zwischen der Arbeit unterwegs und der Arbeit im Büro

Die IT ermöglicht eine nahtlose Zusammenarbeit für die dezentralisierte Belegschaft

„Es wird sich noch zeigen, welche Unternehmen tatsächlich die gute Seite der Pandemie erkennen und ein für alle Mal verstehen, dass Mitarbeitende nicht in einem bestimmten Postleitzahlgebiet sitzen müssen, um ihren Job zu erledigen“, sagt Labrador.

Labradors Argumente spiegeln die von Forrester Research wider. Laut Forrester werden es die 60 % der Unternehmen, die auf ein hybrides Arbeitsmodell umstellen, nicht leicht haben: Gut ein Drittel der ersten Versuche, die Organisationen unternehmen, um „work anywhere“ zu ermöglichen, werden schlichtweg nicht funktionieren.

„Führungskräfte werden Unterstützung für ein Hybridmodell beanspruchen, aber dennoch Meetings, Jobs und Aufstiegsmöglichkeiten entwerfen, die nicht ohne den Face-to-Face-Kontakt auskommen“, heißt es im Forrester 2022-Leitfaden. „Sobald klar wird, dass die Produktivität leidet, werden dieselben Führungskräfte die hybride Arbeit beschuldigen, statt in den Spiegel zu schauen.“

Doch wie löst man dieses scheinbar unlösbare Problem? Durch den Einsatz von Technologie, welche die Mitarbeitenden in Verbindung hält. Dazu gehört das Neudenken von Konferenzräumen, um entfernte Mitarbeitende

in den Mittelpunkt zu stellen, genauso wie die Ausstattung von Mitarbeitenden mit der passenden Hardware, um einen professionellen Eindruck hinterlassen zu können.

„Führungskräfte entwerfen immer noch Meetings, Jobs und Aufstiegchancen, die nicht ohne Face-to-Face-Kontakt auskommen.“

Forrester Research<sup>4</sup>

Vor allem bedeutet es aber, Mitarbeitende miteinander zu vernetzen – egal ob sie von zu Hause aus, im Büro oder in einem Strandhaus arbeiten. Es ist völlig egal, wo sie sitzen: Ihre Stimmen müssen gehört werden.

Mitarbeiter sollen dabei sein, egal wo sie sind: HP Presence.

HP Presence



# Sicherheit erleichtern



HP WOLF SECURITY



Heute gelten die gleichen Sicherheitsprinzipien wie schon vor zehn Jahren, auch wenn das Volumen der Angriffe und die Anzahl der Endpunkte steigen. Es ist die Art und Weise Abwehrmaßnahmen zu implementieren, die sich ständig anpassen muss.

## FRÜHER →

Der Schwerpunkt lag auf dem Schutz der Mitarbeitenden im Büro

Die Daten wurden auf Servern zentralisiert, die durch die Cloud ergänzt wurden

Cyberkriminelle haben es auf Unternehmen mit einem bestimmten Profil abgesehen

## JETZT →

Der Fokus liegt auf dem Schutz von Endpunkten überall

Daten werden in die Cloud verlagert und mit lokalen Servern gekoppelt

Automatisierte Angriffe verbreiten Ziele während Cyberkriminelle die neuen Gelegenheiten nutzen

## IN ZUKUNFT

Der Schwerpunkt liegt auf Assets mit integriertem Schutz

Daten müssen ortsunabhängig werden aber brauchen dennoch Schutz vor Cyberangriffen

Angriffe werden ebenso zunehmen wie die Anzahl der Endpunkte - Hardware mit eingebautem Schutz ist notwendig

Dr. Rois Ni Thuama ist Leiterin der Cyber-Governance bei Red Sift, einem Unternehmen, das sich um Regierungen und einige der größten Firmen der Welt kümmert. Und sie hat einige beruhigende Ratschläge für besorgte CISOs: Keine Panik.

Seit den letzten zehn Jahren weist Ni Thuama jedes Jahr auf den Bericht über die Bedrohungslandschaft hin, den die Agentur der Europäischen Union für Cybersicherheit (ENISA) veröffentlicht. Die Namen der Top-Bedrohungen ändern sich zwar ständig, doch im Kern bleiben sie unverändert: Ransomware, Malware und E-Mail-bezogene Angriffe.

Wenn es also um die Verteilung von Ressourcen und Investitionen geht, sollte man sich laut Ni Thuama auf diese Bedrohungen konzentrieren: „Für Endpunkte muss die Endpunkt-Multifaktor-Authentifizierung eingesetzt werden. Wir brauchen starke Passwörter. Wir brauchen DMARC.“

Labrador fügt die Forderung nach einer starken Governance hinzu, denn diese kann sicherstellen, dass Updates für den Schutz gegen Zero-Day-Angriffe bereitgestellt werden. Sie sagt: „Niemand will wegen einer großen Datenpanne in den Nachrichten landen. Man braucht eine starke Führung. Man braucht eine zuverlässige Schwachstellenbehebung und die beginnt damit, wie gut getrackt wird, wo sich die IT-Assets befinden.“

Zudem kann man nicht davon ausgehen, dass die Personen, die Zugriff auf Hardware, Software und sensible Daten haben, sofort neue Patches installieren werden, sobald sie verfügbar sind. „Wenn ich ein Mitarbeitender im Callcenter bin, der nicht auf Software-Warnungen reagiert“, so Labrador, „dann muss sichergestellt sein, dass ich mich zwei Tage später nicht mehr einloggen kann.“

Um diesen Plan in die Tat umzusetzen, braucht es entsprechende Hard- und Software, die sowohl Mitarbeitende als auch das Unternehmen schützt, egal wo die Arbeit stattfindet. Eine Lösung sind PCs mit integrierten Sicherheitsfeatures zum Schutz, zur Früherkennung und Wiederherstellung nach Cyberangriffen, bevor sie die dezentrale Belegschaft stören können.



# Equipment, das Teams fördert

Unternehmen, die im New Normal erfolgreich sein wollen, müssen aktiv auf die veränderten Arbeitsweisen zugehen. Das bedeutet ein grundlegendes Umdenken hinsichtlich der Tools, die Teams nutzen.



## FRÜHER →

Im besten Fall hatten Mitarbeitende die Wahl zwischen Desktop-PC oder Notebook

IT-Teams stellten Infrastruktur und Geräte bereit - ohne Kompromisse

Es gab eine langsame, stetige Verschiebung in Richtung digitaler Transformation

## JETZT →

Mitarbeitende arbeiten mit der Hardware, die sie bekommen

Arbeitnehmer nutzen Tools von Drittanbietern

Digitale Transformation geschieht in halsbrecherischer Geschwindigkeit

## IN ZUKUNFT

Die IT stattet die Mitarbeitenden mit Hardware aus, die auf nahtlose Produktivität ausgelegt ist

Die IT nutzt Präsenz-basierte Technologien, um dezentrale Teams zu fördern

Quick Fixes müssen durch dauerhafte Lösungen ersetzt werden

„Als ich mit dem Computing anfang, gab es in Bezug auf Hardware, Betriebssysteme und Software fast einen eiszeitlichen Wandel“, sagt Mark Evans, Managing Partner bei Define:Athene, einem Beratungsunternehmen, das in Bezug auf Strategie, Governance, Risiko-Compliance und Cybersicherheit berät. „Diese Veränderung hat sich exponentiell beschleunigt,“ erklärt er weiter.

Doch diese Veränderung wurde nicht durch Tools vorangetrieben, die IT-Abteilungen bereitstellen, sondern von Tools, die Menschen eigenständig kaufen. „Wir haben Markteinsteiger gesehen, die niemand vorhersehen konnte“, sagt Evans. „Fraglich, ob wir den Geist jemals wieder zurück in die Flasche bekommen“, fügt er hinzu.

IT-Führungskräfte müssen in Bezug auf die Standorte von Einzelpersonen und die von ihnen gewählten Arbeitsmittel mit Ungewissheit fertig werden. „Einige Organisationen werden Veränderungen begrüßen“, sagt Evans, „und einige Organisationen werden sie lediglich akzeptieren und dann

versuchen sie einzuschränken. Wieder andere Organisationen werden einfach nein zur Veränderung sagen - und das bedeutet, dass sie sich nicht weiterentwickeln werden.“

Eine zukunftsorientierte Denkweise ist nur ein Teil des großen Ganzen. IT-Führungskräfte müssen ihre Mitarbeitenden mit Lösungen - Hardware, Software oder einer Mischung aus beidem - ausstatten, die es ihnen ermöglichen, überall produktiv zu sein. Ganz gleich, ob im Homeoffice, im Café oder in einem Pop-up-Arbeitsbereich, Remote-Mitarbeitende müssen den Teams im Büro gleichgestellt sein.

Doch was heißt das konkret für die Umsetzung? Im Homeoffice bedeutet es hochwertige Monitore plus einfache Erweiterbarkeit über Docking-Lösungen. Unterwegs bedeutet es leichte Notebooks mit langer Akkulaufzeit. Und für alle beliebigen Arbeitsorte gemeinsam, bedeutet es, dass sich die Mitarbeitenden nahtlos und ohne Unterbrechungen miteinander vernetzen können - als würden sie an einem Büroschreibtisch sitzen.

# Auf flexible Planung setzen



Budgets und langfristige Pläne waren in der jüngsten Vergangenheit falsche Freunde. Nun stellt sich die Frage, wie sehr man sich in Zukunft auf sie verlassen kann.

## FRÜHER →

Fünfjahrespläne machten Sinn

Die meisten Bestandteile eines Geschäfts waren vorhersehbar, vom Verkaufsvolumen bis hin zu erforderlichen Skills

Pläne kamen von oben und wurden (meistens) eingehalten

## JETZT →

Ein einjähriger Businessplan scheint optimistisch

Sogar nur ein Jahr im Voraus zu planen, ist schwierig

Arbeitnehmer bekommen mehr Möglichkeiten durch den Einsatz neuer Tools

## IN ZUKUNFT

Partner reagieren so schnell wie man selbst

Partner helfen dabei, die Zukunft greifbar zu machen

Partner können genau die Lösungen liefern, die benötigt werden

„Ein Fünfjahresplan ist gefährlich“, sagt Labrador. Es ist natürlich in Ordnung, solche Pläne zu machen, doch bei langfristiger Planung werden Feedback-Schleifen ausgelassen und auch die Flexibilität, die zum Erlernen neuer Dinge benötigt wird, leidet.

**Bis 2023 werden 80 % der Unternehmen KI-gestützte, Cloud-verknüpfte Governance-Dienste nutzen, um dezentrale Ressourcen/ Daten zu verwalten, zu optimieren und zu sichern.**

IDC<sup>5</sup>

Budgetierung ist das andere große Thema. Wenn IT-Abteilungen auf Jahresbasis budgetieren, woher nehmen Sie dann die Mittel, um auf einen unmittelbaren Bedarf zu reagieren und eine gerade entdeckte Schwachstelle zu schließen?

Labradors Team entdeckte bei einer Gelegenheit eine Schwachstelle in Geldautomaten, die in Mexiko eingeführt werden sollten. Da keine Mittel vorhanden waren, um eine Notfall-Fehlerbehebung abzudecken, wurde die Schwachstelle nicht behandelt. „Der fehlerhafte Code wurde an einem Samstag um zwei Uhr morgens eingeführt“, erklärt sie, „um 2:05 Uhr morgens war die Bank um 45 Millionen US-Dollar leichter.“

Dies spricht für ein bekanntes Problem: unflexible Pläne, die auf veralteten Prinzipien basieren. IT-Teams müssen Probleme weiterhin allein bekämpfen und sind so sehr damit beschäftigt, aktuelle Brände zu löschen, dass sie das herannahende Inferno gar nicht sehen.

Schon vor zwei Jahren war das schlimm genug. Angesichts der dezentralen Belegschaft von heute und der ständig steigenden Anzahl von schützenswerten Endpunkten benötigen IT-Teams Partner, der nicht nur Produkte verkaufen, sondern dabei helfen, Probleme zu lösen, bevor sie auftreten.



# Den Standpunkt ändern

Ein „Zurück zur Normalität“ gibt es nicht. Die Welt hat sich von vorhersagbar zu völlig ungewiss gewandelt. Dies gilt für alle Branchen, alle Länder und alle Aspekte unseres Arbeitslebens. Ob es die Überwindung der Pandemie, Schwierigkeiten in der Lieferkette oder ökologische Herausforderungen sind, niemand weiß genau, was das nächste Jahr bringt – geschweige denn die nächsten fünf.

Zukunftsorientierte Unternehmen müssen sich dieser neuen Ära stellen. Sie müssen sich mit einer flexiblen Haltung auf diese Ungewissheit vorbereiten. Mit der Unterstützung von zukunftsorientierten Technologieanbietern wie HP werden die Herausforderungen von heute zu den Chancen von morgen.

## Wie kann HP helfen?

Mit HP Presence von überall anwesend sein [↗](#)

Mit HP Wolf Security dafür sorgen, dass Endpunkte und Daten sicher bleiben [↗](#)

Mitarbeitende mit HP Elite PCs und Ökosystemen ausstatten, um sie zu fördern [↗](#)

Mit HP Services Probleme lösen, bevor sie auftreten [↗](#)

## Quellen

<sup>1</sup> Bill Conerly, PhD, "The Flexible Stance: Thriving in a Boom/Bust Economy," 2016.

<sup>2</sup> Wall Street Journal, "What Happened When United Stopped Trying to Predict the Pandemic," October 21, 2021, <https://www.wsj.com/articles/united-airlines-predicting-covid-travel-flying-11634751129>

<sup>3</sup> Forrester Q1 2021 European PandemicEX Survey and Forrester Q2 2021 US PandemicEX Survey.

<sup>4</sup> Forrester Research, "Predictions 2022: Disruptive Forces Necessitate Bold Decisions," 2021, <https://www.forrester.com/predictions/predictions-2022>

<sup>5</sup> IDC FutureScape: Worldwide IT Industry 2022 Predictions, October 2021, <https://www.idc.com/getdoc.jsp?containerId=US48312921>

Interviews with Mark Evans, Lynne Labrador, and Dr. Rois Ni Thuama, 2021.

