WHITE PAPER – **MÄRZ 2020**

Wichtige Überlegungen beim Unterstützen von Homeoffice-Richtlinien für Business Continuity

vmware®

Inhaltsverzeichnis

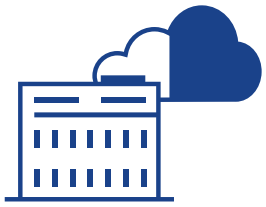
Außergewöhnliche Ereignisse können Unternehmenskulturen schneller verändern als jede andere Maßnahme. Naturkatastrophen und Pandemien beispielsweise zwingen Unternehmen dazu, Remote-Arbeitsprozesse und -Technologien umgehend zu überdenken oder einzuführen, um Produktivitätsverluste zu minimieren, wenn Mitarbeiter aufgrund von Vorgaben – seien sie selbst oder von Führungskräften bzw. Behörden auferlegt – isoliert werden müssen.

Es gibt keine Patentlösung, um optimale Mitarbeitererfahrungen im Fall von Geschäftsunterbrechungen zu gewährleisten. Dennoch können sich Unternehmen weiterentwickeln, um die Situation von Homeoffice-Angestellten entsprechend zu verbessern und unternehmensweite, remoteorientierte Ziele mit einer digitalen Arbeitsplatzstrategie schneller zu erreichen.

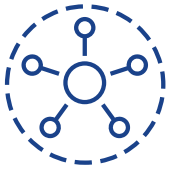
Fünf IT-Grundsätze für eine bessere Mitarbeitererfahrung

Durch eine Verbesserung der digitalen Mitarbeitererfahrung können Führungskräfte heute die Grundlage für den Erfolg des Digital Business oder einen Wettbewerbsvorsprung in der Zukunft schaffen. Dazu müssen sich IT-Abteilung und Führungsebene in Bezug auf einige – nicht unbedingt neue – Grundsätze einig sein:

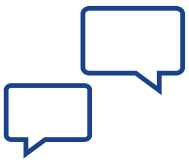
Welche Anwendungen benötigen Mitarbeiter?



Wo befinden sich wichtige Anwendungen und Daten?



Wie greifen Mitarbeiter heute (und voraussichtlich in Zukunft) auf Arbeitsressourcen zu?



Wie gestalten sich Kommunikation und Zusammenarbeit zwischen Unternehmensführung und Mitarbeitern heute (und voraussichtlich in Zukunft)?

Welche Hilfe steht Mitarbeitern bei Problemen zur Verfügung?

Kenntnis der von Mitarbeitern benötigten Anwendungen

Anwendungen zählen zu den Grundlagen des modernen Business – von der Kundenerfahrung bis zu Lieferkettenprozessen. Viele Wissensarbeiter – die ihrer Tätigkeit hauptsächlich zu regelmäßigen Arbeitszeiten in herkömmlichen Büros nachgehen – sind gut auf Remote-Arbeit vorbereitet, weil sie hauptsächlich mit gängigen Produktivitätsanwendungen arbeiten. Für andere Mitarbeiter gilt dies jedoch nicht.

Angestellte ohne klassische Bürotätigkeit, etwa in der Sozialarbeit, im Gastgewerbe, im Gesundheitswesen oder im technischen Bereich, besprechen ihre täglichen Aufgaben häufig vorab mit einem Vorgesetzten. Wenn die Arbeit im Homeoffice über einen längeren Zeitraum als etwa eine oder zwei Wochen erforderlich ist, sind wichtige Anwendungen (außer E-Mail) nicht unbedingt ohne Risiko für das Unternehmen von jedem Standort aus zugänglich. Daher ist es aus Sicht sowohl der Unternehmensführung als auch der IT-Abteilung unerlässlich, die Nutzung jeder Anwendung außerhalb des Unternehmensnetzwerks genau zu kennen.

Kenntnis des Speicherorts wichtiger Anwendungen und Daten

Mithilfe einer Liste der Anwendungen, die von den einzelnen Abteilungen oder Gruppen als unternehmenskritisch erachtet werden, können IT-Mitarbeiter die Speicherorte der jeweiligen Anwendungen und der zugehörigen Daten – On-Premises in einem unternehmenseigenen Rechenzentrum oder in einer Private oder Public Cloud – sowie alle Abhängigkeiten ermitteln. So sind beispielsweise herkömmliche Client-Server-, .NET- und Java-Anwendungen für den Zugriff auf Daten häufig an Unternehmensnetzwerke gebunden und hochgradig von Client-Konfigurationen abhängig. Dagegen sind interne, browserbasierte Anwendungen zwischen Client-Geräten portabel, können aber dennoch nur über die Anwendungsserver im Unternehmensnetzwerk bereitgestellt werden. Besonders flexible SaaS-Anwendungen lassen sich noch einfacher bereitstellen, weil sie nicht vom Unternehmensnetzwerk abhängig sind – solange die IT noch keine Zugriffskontrollen eingeführt hat, die den Gerätezugriff ausschließlich innerhalb des Unternehmensnetzwerks zulassen.

Kenntnis, welche Geräte verbunden werden (unternehmenseigene, private oder beide)

Nur mit dem Wissen, welche Anwendungen Mitarbeiter benötigen und wo sich die Daten befinden, können IT-Abteilung und Unternehmensführung eine effektive Strategie dafür entwickeln, welche Geräte auf welche Weise mit dem Unternehmensnetzwerk verbunden werden können und sollten. Auf unternehmenseigenen Laptops sind häufig VPN-Verbindungen vorkonfiguriert, die Mobilität und Portabilität von Anwendungen ermöglichen.

Wenn solche Geräte jedoch länger außerhalb des Unternehmensnetzwerks betrieben werden, stellt sich für die IT-Abteilung die Frage, wie Management-Aktualisierungen, Patching und Richtlinien unterstützt werden können, um Risiken für das Unternehmen zu reduzieren. Ebenso müssen Szenarien berücksichtigt werden, in denen keine Zeit mehr für das Provisioning neuer Laptops bleibt und Mitarbeiter ihre eigenen Geräte wie Smartphones, iPads, Workstations und PCs nutzen müssen, auf denen verschiedene Betriebssysteme und nicht unterstützte Software ausgeführt werden. Einer Situation, in der Geräte potenziell anfällig für schädliche Angriffe über das Internet sind und später wieder mit dem Unternehmensnetzwerk verbunden werden, können IT-Teams durch angemessene Vorbereitung vorbeugen.

Verstehen der unternehmensinternen Zusammenarbeit und Kommunikation

In Branchen wie der Informationstechnologie und zunehmend auch dem Finanzwesen sind viele Führungskräfte und Wissensarbeiter bereits daran gewöhnt, mit Mitarbeitern, Kollegen, Kunden und Partnern über Onlinekanäle wie Videokonferenzen, E-Mails und Instant Messaging zusammenzuarbeiten. Sie müssen sich daher kaum umstellen. Sobald jedoch ein Unternehmen und sämtliche Mitarbeiter (z.B. Vertriebsleute, Finanzfachkräfte, Wartungspersonal usw.) auf eine umfangreiche oder ausschließliche Zusammenarbeit und Kommunikation über Software angewiesen sind, können schnell Ausfallzeiten entstehen, da sich Führungskräfte, Abteilungsleiter und Einzelpersonen zunächst mit den neuen Arbeitsweisen vertraut machen müssen.

Um Unterbrechungen auf ein Mindestmaß zu begrenzen, müssen IT-Abteilung und Führungsebene bei einer plötzlich hochgradig verteilten Belegschaft gemeinsam und umgehend die zahlreichen Methoden der täglichen Kommunikation an Arbeitsplätzen, in Banken, in Kliniken und andernorts dokumentieren, bevor sie neue virtuelle Workflows und Prozesse zur Unterstützung der Remote-Arbeit einführen können.

Erkenntnis, dass Support ein Problem sein wird

Zu den größten Unbekannten bei der Arbeit im Homeoffice zählt die Frage, welches Maß an Support die Mitarbeiter für welche Anwendungen und Geräte an welchen Orten und zu welchen Zeiten benötigen werden. IT-Abteilung und Führungsebene oder Führungsteams können die aktuellen Prozesse skizzieren, um wesentliche Problembereiche vorab zu ermitteln und zu beseitigen. Dazu gehört unter anderem eine Überprüfung der Optionen für Remote-Support-Tickets, der Self-Service-Funktionen und der personellen Situation.

In Branchen mit Fachkräftemangel haben Mitarbeiter die Auswahl. Hier kann eine hervorragende Erfahrung bei der Arbeit im Homeoffice ein Alleinstellungsmerkmal sein. *Aktuellen Umfrageergebnissen* zufolge sind sich 73 Prozent der Mitarbeiter und Entscheidungsträger im Personalwesen darüber einig, dass die Flexibilität bei den für die Arbeit benötigten Tools (etwa Technologie, Anwendungen und Geräte) ihre Entscheidung für eine Bewerbung oder Zusage bei einem Unternehmen beeinflusst.[1]

Unterstützen der Mitarbeiter mit VMware-Lösungen bei der Arbeit im Homeoffice

In den heutigen anwendungsorientierten Unternehmen gestaltet sich die Lösungsfindung für jedes Gerät sowie für jede Anwendung, Compliance-Regel, Identität und Berechtigung schon unter Idealbedingungen schwierig – ganz abgesehen von einer Krisensituation. Kaum ein IT-Team verfügt über das nötige Personal, Budget oder über angemessene Anreize, um bei diversen Kombinationen aus Clients, Verbindungen, Compliance-Problemen, Anwendungstypen und Authentifizierungen einen reibungslosen Betrieb zu gewährleisten. Bisher waren die meisten Mitarbeiter, die sich innerhalb des Unternehmensnetzwerks auf vertrauenswürdigen Computern bei einer Unternehmensdomäne anmelden und sowohl intern als auch extern geschäftliche E-Mail-Konten nutzen, mit dieser Situation zufrieden. Sobald jedoch alle Mitarbeiter remote arbeiten müssen, kann sich das schnell ändern.

„Dies ist eine Chance für jeden Einzelnen und jedes Unternehmen, Positives und Negatives bei der Kommunikation und Produktivität genau zu analysieren.“[2]

TECHCRUNCH

Zwar sind sich die Mitarbeiter heute der Komplexität von IT-Umgebungen in Unternehmen bewusst. Sollten aber Unterbrechungen regelmäßiger auftreten, werden Fachkräfte die Mitarbeitererfahrung häufiger hinterfragen. Aus diesem Grund setzen Unternehmen, die Wert auf eine optimale Mitarbeitererfahrung legen und kein Risiko eingehen möchten, wenn die Arbeit im Homeoffice betrieblich angeordnet wird, auf den digitalen Arbeitsplatz von VMware.

Die End-to-End-Plattform auf der Grundlage von VMware Workspace ONE® vereint Zugriffskontrolle, Anwendungsmanagement und plattformübergreifendes Endpunktmanagement in einer konsistenten, einheitlichen Arbeitsumgebung.

Zugriff auf alle Anwendungen unabhängig von Gerät und Netzwerk

Unternehmensführung und IT-Abteilung können darauf vertrauen, dass die Workspace ONE-Plattform Zugriff auf alle Anwendungen unabhängig von Gerät und Netzwerk sicherstellt und dadurch drei zentrale Initiativen unterstützt:

- IT-Modernisierung
- Mitarbeiterinteraktion
- Zero-Trust-Sicherheit

Gerätemanagement

Über Workspace ONE können IT-Mitarbeiter alle Geräte wie Laptops, Tablets, Smartphones, Desktop-PCs oder Macs, die Zugriff auf Unternehmensressourcen benötigen, registrieren und kontinuierlich überwachen. Dabei stehen ihnen intelligente Informationen und Automatisierungsfunktionen zur Verfügung. Die Lösung stellt einen einwandfreien Systemzustand sicher, indem Geräte-, Anwendungs- und Anwenderdaten aggregiert und korreliert werden. Gleichzeitig können mithilfe der Lösung die IT-Kosten reduziert, die Sicherheit verbessert und Erfahrungen optimiert werden.

Wenn Mitarbeitern vom Unternehmen verwaltete Geräte für die Arbeit im Homeoffice zur Verfügung gestellt werden, kann die IT dank dieser Lösung wertvolle Administrationszeit einsparen, da der vollständige Zustand jedes Geräts schnell erfasst und das Gerät über die Cloud verwaltet werden kann, solange das Gerät mit dem Internet verbunden ist. Wenn Mitarbeiter zu Hause mit eigenen Geräten wie Smartphones und Tablets arbeiten, vereinfacht Workspace ONE das IT-Management, indem Unternehmensdaten von privaten Anwendungen isoliert und gleichzeitig Regeln für minimalen bedingungsbasierten Zugriff zum Schutz der Unternehmensressourcen angewendet werden.

1 Vanson Bourne, „The Digital Employee Experience“, Mai 2019

2 TechCrunch, *„How to work during a pandemic“,* Devin Coldeway, März 2020

Mithilfe des digitalen Arbeitsplatzes von VMware können Unternehmen konsistente Prozesse und Richtlinien unter iOS, Android, Windows 10, macOS, Chrome OS und allen anderen Betriebssystemen, die ihre Mitarbeiter nutzen, anwenden. Durch den Cloud-basierten Echtzeitansatz können die Kosten und das Lebenszyklusmanagement für Legacy-Produkte ergänzt oder ganz vermieden werden.

Die umfassende VMware-Plattform bietet mehrere Zero-Touch-Optionen für Mobilgeräte sowie für macOS- und Windows 10-PCs, um IT-Teams das Onboarding neuer Geräte und Anwender zu erleichtern. Konfiguration, Richtlinien, Patches und Aktualisierungen werden über automatisierte Richtlinien drahtlos unterstützt. IT-Teams profitieren von einfachen, geräteübergreifenden Berechtigungs-, Provisioning- und Bereitstellungsvorgängen für Anwendungen und können auf diese Weise Datenverlust verhindern. Anwendungen – einschließlich großer Win32-Anwendungen – lassen sich effizient drahtlos oder durch Peer-to-Peer-Distribution verteilen. Mit Workspace ONE® Assist können IT- und Helpdesk-Mitarbeiter zudem Probleme mit Android-, iOS-, macOS- und Windows-Geräten in Echtzeit über Funktionen für das Remote-Management und die Remote-Steuerung beheben.

Auch bei betrieblich angeordneter Arbeit im Homeoffice können weiterhin neue Mitarbeiter eingestellt werden. Als besonderes Leistungsmerkmal des digitalen Arbeitsplatzes von VMware können IT-Mitarbeiter Cloud-basierte Laptops direkt an remote arbeitende neue Mitarbeiter ausliefern und dabei die Compliance wahren.

Services zur Mitarbeiterinteraktion

Workspace ONE verbessert die Mitarbeitererfahrung für potenzielle Mitarbeiter ebenso wie für neue und langjährige Mitarbeiter, die auf betriebliche Anordnung im Homeoffice arbeiten. Workspace ONE® Intelligent Hub für Einzelziele bietet Mitarbeitern einheitliche und automatisierte Onboarding-Workflows, einen aktualisierten Anwendungskatalog sowie Zugriff auf Hub-Services. Über die Intelligent Hub-Anwendung lassen sich außerdem native Anwendungen installieren.

Die folgenden Hub-Services bieten eine durch und durch sichere, konsistente und plattformübergreifende Möglichkeit zur Kommunikation und Zusammenarbeit für Einzelanwender ebenso wie im gesamten Unternehmen:

- **VMware Workspace ONE® Notifications:** von der IT verwaltete Push- und In-App-Benachrichtigungen mit benutzerdefinierten Daten oder Verbindungen zu Geschäftssystemen von Drittanbietern mit VMware Workspace ONE® Mobile Flows™
- **VMware Workspace ONE® Catalog:** Anzeigen, Starten und Installieren aller Arten von Anwendungen (z.B. Web, SaaS, virtuell und cloudnativ) über Single Sign-On (SSO) unabhängig vom verwendeten Gerät
- **VMware Workspace ONE® People:** schnelle Suche nach Kollegen über ein Mitarbeiterverzeichnis, mit einem Organigramm mit Namen, E-Mail-Adressen, Telefonnummern und Suchfunktion
- **VMware Workspace ONE® Home:** Zugriff auf Unternehmensressourcen durch Integration eines Intranet- oder Unternehmensportals
- **VMware Workspace ONE® Assist:** Zugriff auf häufig gestellte Fragen (FAQs) und Artikel in einer Knowledgebase (KB), damit Mitarbeiter Probleme selbstständig beheben und weiterhin produktiv arbeiten können Ein in die Intelligent Hub-Anwendung integrierter virtueller digitaler Assistent oder Chatbot liefert ebenfalls umgehend Antworten und unterstützt IT-Teams damit beim Support, wenn Mitarbeiter bei der Arbeit im Homeoffice Fragen haben.

Bereitstellung virtueller Desktops und Anwendungen

Digitale Arbeitsplatzumgebungen, die als Grundlage remoteorientierter Strategien dienen, müssen Abhängigkeiten zwischen lokalen Windows-Anwendungen unterstützen. Diese werden noch in zahlreichen Unternehmenssystemen eingesetzt. Dank Workspace ONE mit VMware Horizon® Service lassen sich Konflikte lösen, die entstehen, wenn Anwendungen bestimmte Konfigurationen, Browser, Plug-ins oder ähnliches erfordern, besonders dann, wenn Probleme bei der Interaktionen zwischen Anwendungen bekannt sind.

Workspace ONE mit Horizon Service unterstützt zudem die unternehmenskritischen Networking-Anforderungen in streng regulierten Branchen wie dem Gesundheitswesen oder Behörden. Durch eine virtuelle Desktop-Infrastruktur (VDI) mit virtuellen Desktops als Proxys werden Client-Endpunkte vollständig isoliert, sodass Geräte und deren Anwendungen nicht mit dem Unternehmensnetzwerk in Kontakt kommen.

In Unternehmen, die ihren Mitarbeitern generell Laptops zur Verfügung stellen, erlaubt eine VDI den Remote-Zugriff von jedem Gerät aus („Bring Your Own Device“) über einen Browser. Die VDI erstreckt sich von On-Premises-Rechenzentren bis in Cloud-Umgebungen und bietet folgende Integrationen und unmittelbaren Vorteile:

- **On-Premises:** Bei Nutzung der VMware-Plattform für digitale Arbeitsplätze mit vorhandenen virtuellen Infrastrukturen und Kapazitäten können IT-Teams bestehende VDI-Ressourcen einfach über die Cloud-Orchestrierung und Hyperconverged Infrastructure von VMware wie VMware Cloud Foundation™ auf Basis von Dell EMC VxRail hinzufügen.
- **Hybrid und Multi-Cloud:** Bei Nutzung der VMware-Plattform für digitale Arbeitsplätze ohne Kapazität können IT-Teams neue virtuelle Desktops über VMware Horizon® Cloud on Azure oder VMware Horizon® 7 on VMware Cloud™ on AWS schnell bereitstellen und dabei auch die Funktionen im Rahmen einer kostenlosen Testversion evaluieren.
- **Remote-Zugriff auf physische PCs:** Mit der VMware-Plattform für digitale Arbeitsplätze können IT-Teams den Remote-Zugriff auf physische Windows 10-PCs einrichten, die im Unternehmensnetzwerk oder -perimeter verbleiben müssen, sodass die Remote-Arbeit an diesen Systemen von jedem Standort aus möglich ist.

Zugriffsservices

Sicherheitsbedrohungen sind für IT-Abteilungen und Führungskräfte ein gleichermaßen wichtiges Thema und ein potenzieller Unsicherheitsfaktor bei der Arbeit im Homeoffice. Selbst beim Einsatz zuverlässiger VPN-Technologie ist das IT-Team mit komplexen Zugriffs- und Authentifizierungsszenarien konfrontiert.

Workspace ONE vereinfacht die Einführung von Zero-Trust-Zugriffskontrollen. Cloud-basierte VMware-Zugriffsservices ermöglichen die SSO-Authentifizierung mit integrierter Mehrfach-Authentifizierung (MFA) oder Unterstützung für vorhandene MFA. Die Plattform lässt sich außerdem nahtlos in vorhandene Cloud-Identitätstechnologien wie Okta integrieren.

IT-Teams in Unternehmen können jederzeit darauf vertrauen, dass ihre Anwendungen und Daten geschützt sind. Eine einzige Appliance fungiert als Bridge zwischen On-Premises-Ressourcen und nutzt bedingungsbasierte Zugriffsrichtlinien für sämtliche Ressourcen – von Microsoft SharePoint und Dateifreigaben über Intranet-Sites und interne APIs bis hin zu virtuellen Desktops und Anwendungen (z.B. Horizon und Citrix).

Endpunktsicherheit

Eine für alle Mitarbeiter geltende betriebliche Anordnung zur Arbeit im Homeoffice ist für IT-Teams leichter umsetzbar, wenn Geräte mithilfe des digitalen Arbeitsplatzes von VMware verwaltet werden, da die Plattform den Gerätezustand, die Anwenderdetails und den Authentifizierungskontext kontinuierlich verfolgt, um das Risiko für Anwender und Gerät zu bewerten. Darüber hinaus wird der Zugriff automatisch zugelassen oder verweigert. Ebenso werden MFA oder Remediation für den Zugriff vorausgesetzt.

Außerdem kann das IT-Team einen gewünschten Zustand für alle vom Unternehmen zur Verfügung gestellten Geräte durchsetzen oder einen minimalen Compliance-Zustand für jede Anwendung oder Verbindung zu sensiblen Ressourcen festlegen. Im Rahmen des bedingungsbasierten Zugriffs kann Workspace ONE Richtlinien für Identitäts-, Geräte- und Anwendungsszenarien erstellen und verwalten. Erweiterte Risikoanalysefunktionen erkennen Anomalien, die auf schädliche Absichten hinweisen können.

Die Plattform ist auch optimal zur Reaktion auf Bedrohungen geeignet, beispielsweise für Remediation, falls Mitarbeiter bei der Arbeit im Homeoffice Opfer eines von VMware Carbon Black EDR erkannten Phishing-Angriffs werden sollten. Durch die automatisierte Reaktion auf Bedrohungen stellt die Plattform Anwender oder Geräte, die ein erhöhtes Risiko darstellen, in Quarantäne. Zum weiteren Schutz von Anwendungen und Daten sichert die VMware-Plattform den Datentransport über anwendungsspezifische VPNs, die den Kontakt zu bestimmten internen Ressourcen reduzieren.

Gezieltes Entwickeln einer Strategie für remoteorientiertes Arbeiten

Da sich die Natur nicht beeinflussen lässt und die meisten Unterbrechungen unerwartet eintreten, müssen Unternehmen jetzt mit der Vorbereitung auf die nächste Notfallsituation beginnen, indem sie gezielt eine Strategie für remoteorientiertes Arbeiten sowie eine Umgebung für digitale Arbeitsplätze entwickeln, mit der sie ihre Mitarbeiter, die IT-Abteilung und das Unternehmen als Ganzes unterstützen können.

Unabhängig von Zeit und Ort stellen Homeoffice-Vorgaben die Unternehmenskultur völlig auf den Kopf. In Unternehmen, die ihren Mitarbeitern bereits mehr Verantwortung übertragen und einen ergebnisorientierten Ansatz fördern, wird dieser Prozess reibungsloser funktionieren, da sich Teams entsprechend anpassen müssen.

Jedes Unternehmen, das noch nicht vollständig vorbereitet ist, muss jetzt die sich zunehmend verändernden Denkmuster und Budgetplanungen dazu nutzen, die Erwartungen an die Arbeit im Homeoffice heute und in Zukunft zu erfüllen. Dazu müssen die zuständigen Teams die Sicherheit von innen heraus stärken und gewährleisten, dass verteilte Mitarbeiter mühelos und bedarfsorientiert auf alle Anwendungen und Daten zugreifen können, die sie für eine bessere Zusammenarbeit und Produktivität benötigen – und zwar unabhängig davon, wann und wo sie arbeiten.

Weitere Informationen zur Unterstützung durch VMware bei betrieblich angeordnetem Arbeiten im Homeoffice mit Auswirkung auf die Business Continuity finden Sie *auf unserer Business-Continuity-Website*.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland
Willy-Brandt-Platz 2 81829 München Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de