



BYO- STRATEGIE? UNNÖTIG!

Entwickeln Sie eine Strategie
für digitale Arbeitsplätze – in
nur 5 Schritten

Ihre BYO-Strategie hat ausgedient

Bring Your Own Device(BYO)-Strategien spielen seit Jahren eine wichtige Rolle in IT-Organisationen. Durch die rasant wachsende Anzahl an vernetzten Geräten und Anwendungen verschwimmen die Grenzen zwischen geschäftlicher und privater Nutzung immer mehr.

Was in der Vergangenheit eindeutig war, ist es heute nicht mehr. Eigentumsverhältnisse verändern sich: zum einen werden Geräte vom Unternehmen ausgegeben zum anderen bringen Mitarbeiter ihre eigenen Geräte mit. Mitarbeiter wünschen sich heute auch mehr Agilität und weniger Einschränkungen. Ob im Homeoffice, im Außendienst oder am Schreibtisch: Angestellte und freie Mitarbeiter müssen auf dem aktuell genutzten Gerät zuverlässig und sicher auf Anwendungen und Informationen zugreifen können. Und diesem Umstand wird eine BYO-Strategie nicht immer gerecht.

Stattdessen benötigen IT-Organisationen eine Strategie für digitale Arbeitsplätze, die das Management von Anwendern, Geräten, Anwendungen und vielem mehr erleichtert. Und zwar auf derselben Managementplattform und unabhängig vom Geräteeigentumsmodell.



Anforderungen an den digitalen Arbeitsplatz

Der digitale Arbeitsplatz bietet eine einheitliche Anwendererfahrung, die Mitarbeitern einfachen, sicheren Zugriff auf Anwendungen, Services, Daten und Umgebungen verschiedener Geräte, Netzwerke, Standorte und Betriebssysteme ermöglicht.

Als ganzheitliches Konzept ermöglicht eine Strategie für digitale Arbeitsplätze die Abkehr von Standardisierung und Ressourcenmanagement. In den Fokus rücken stattdessen folgende Aspekte:

- Mehr Freiheiten für Mitarbeiter durch die Nutzung von Self-Service-Funktionen
- Anwenderfreundliche und robuste Geräteerfahrungen
- Verbesselter Zugriff auf moderne cloud-basierte Anwendungen

Von diesem mitarbeiterorientierten Ansatz profitieren alle Beteiligten. Ein höheres Maß an Kontrolle für die IT, gesteigerte Produktivität und mehr Sicherheit sind nur einige der Vorteile für das Unternehmen.



Gründe für einen digitalen Arbeitsplatz

Von digitalen Arbeitsplätzen profitiert nicht nur die IT, sondern das gesamte Unternehmen. Laut einer aktuellen Studie werden Unternehmen, die ihren Mitarbeitern bequemen Zugriff auf die benötigten Anwendungen bieten, dreimal häufiger als Vorreiter im Bereich digitale Transformation bewertet.¹ Und das ist nur der Anfang.



Ihre IT-Organisation profitiert folgendermaßen von digitalen Arbeitsplätzen:

- Anwendungen können mit intelligenten Zugriffskontrollen auf Gerätebasis verwaltet werden. Dadurch wird es einfacher, den Zugriff auf sensiblere Daten von nicht vertrauenswürdigen Geräten aus zu beschränken.
- Unternehmenseigene Geräte können bereits im Vorfeld so bereitgestellt werden, dass sich diese selbst ohne physischen Eingriff beim Unternehmen registrieren.



Ihre Mitarbeiter profitieren wie folgt:

- Die Geräte sind bereits im Auslieferungszustand einsatzbereit, wodurch das Onboarding beschleunigt wird und ein früherer Produktivitätsbeginn erzielt werden kann. Alle Mitarbeiter können nach der Anmeldung sofort mit der Arbeit beginnen.
- Mitarbeiter können problemlos zwischen Geräten wechseln, ohne sich Gedanken darüber machen zu müssen, welche Geräte „genehmigt“ wurden und welche nicht. Durch die Installation eines Profils, das Unternehmensdaten schützt und persönliche Anwendungen und Daten unberührt lässt, kann selbst nicht genehmigten Geräten „vertraut“ werden.

1. *The Impact of the Digital Workforce*, VMware-Report, 2017

Mitarbeiter an einem digitalen Arbeitsplatz profitieren von folgenden Vorteilen:²

63%

höhere
Produktivität

55%

höhere
Jobzufriedenheit

77%

schnellere Entschei-
dungsfindung

2. The Impact of the Digital Workforce, VMware-Report, 2017

Verabschieden Sie sich von BYO

Sind Sie bereit, Ihre BYO-Strategie gegen eine umfassendere, mitarbeiterorientierte Lösung zu tauschen?

Mit den folgenden fünf Schritten gelangen Sie von einer BYO-Strategie zu einer Strategie für digitale Arbeitsplätze:

1 Management von Anwendungen
anstelle von Geräten 

2 Moderne Managementmöglichkeiten
von PCs und Macs 

3 SaaS-Anwendungen 

4 Verschlüsseln und Löschen sensibler
Informationen wie E-Mails 

5 Hosten von Windows-Anwendungen
auf sicheren Servern, um Daten von
Endpunkten fernzuhalten 

1 Management von Anwendungen anstelle von Geräten



Während es bei einer BYO-Strategie um Gerätemanagement geht, bietet ein digitaler Arbeitsplatz eine konsistente Anwendererfahrung, unabhängig davon, wem das Gerät gehört. Bei diesem Ansatz werden die üblichen Managementprinzipien auf Anwendungen, nicht auf Geräte angewendet.

Worin liegen die Vorteile von anwendungsbasiertem Management?

- Mitarbeiter erhalten die Flexibilität, ohne Sicherheitseinbußen von ihrem bevorzugten Smartphone, Tablet oder Laptop aus zu arbeiten.
- Sowohl für die IT als auch für Mitarbeiter ist nicht länger entscheidend, wer das Gerät besitzt, sondern welche Anwendung genutzt wird.
- Es handelt sich um ein effizienteres, effektiveres und sichereres Verfahren für den Schutz von Daten und das Management von Zugriffsrechten.
- Die IT kann Richtlinien und Berechtigungen bei Bedarf weiterhin flexibel ändern, während Mitarbeiter effektiver und bequemer arbeiten können.

Fazit: Ein Gewinn für alle Beteiligten

Mitarbeiter mit hochverfügbarem Zugriff auf Anwendungen und Daten verbringen fast 20% weniger Zeit mit manuellen Prozessen und verbessern die eigene Produktivität um 15%.³



3. The Impact of the Digital Workforce, VMware-Report, 2017

2

Moderne Managementmöglichkeiten von PCs und Macs



Mit einer Plattform für digitale Arbeitsplätze werden nicht nur Smartphones und Tablets als BYO-Geräte unterstützt. Sowohl Windows 10 als auch Apple Mac OS unterstützen die Möglichkeit, einem persönlichen Gerät mit einem Profil zu vertrauen, das die Installation von Anwendungen und die Verwendung eines Zertifikats für sicheren Zugriff auf Unternehmensdaten erlaubt. Mitarbeiter können die benötigten Ressourcen an jedem beliebigen Standort und mit Geräten aller Art abrufen.

Gründe für einen modernen Ansatz

- Mitarbeiter können eigene Geräte, wie beispielsweise Laptops, über den Enterprise-Katalog mit der Arbeitssystemumgebung verbinden.
- Das Entstehen einer Schatten-IT wird vermieden, da Mitarbeiter nicht auf ungenehmigte Ressourcen auszuweichen brauchen, um ihre Anforderungen zu erfüllen.
- Ihre IT-Organisation behält die Kontrolle über Informationen, ohne dabei die Arbeitsweise der Mitarbeiter einzuschränken.
- Mitarbeiter genießen mehr Freiheit und Mobilität, während Sie sich auf sicheren Datenzugriff verlassen können.

„Mitarbeiter der Stadtverwaltung benötigen Zugang zu den neuesten Tools für den digitalen Arbeitsplatz ... Dank der VMware Workspace ONE-Plattform können wir Mobil- und Cloud-Desktop-Technologien von VMware nutzen. Unsere Mitarbeiter verfügen damit über sicheren Zugriff auf die erforderlichen Softwaretools und Informationen, um einen besseren und effizienteren Kundenservice zu bieten.“

COLLIN BOYCE
CIO
STADT LANSING

Erfahren Sie, warum die Stadt Lansing eine Strategie für digitale Arbeitsplätze eingeführt hat >

3 SaaS-Anwendungen



Das „Software as a Service“ (SaaS)-Modell revolutioniert das Anwendungszugriffsmanagement. Die IT kann damit zentral gehostete Software auf Abonnementbasis lizenzieren. SaaS-Anwendungen sind nativ oder webbasiert. Die Umgebung wird jedoch vom Anbieter verwaltet, sodass die Version der Client-Anwendung nicht von der IT verwaltet werden muss.

Gründe für das Management von SaaS-Anwendungen mithilfe einer Strategie für digitale Arbeitsplätze

- Anwendungen werden geräte- und gerätetypübergreifend zur Verfügung gestellt.
- IT-Mitarbeiter erhalten mehr Zeit und das Risiko für Anwender oder Daten wird verringert.
- Sie müssen sich keine Gedanken über Eigentumsverhältnisse machen, solange Geräte sorgfältig mit geeigneten Zugriffskontrollen verwaltet werden.



Mitarbeiter mit einem digitalen Arbeitsplatz erfahren 5-mal häufiger eine Steigerung ihrer eigenen Produktivität und 4-mal häufiger Zufriedenheit am Arbeitsplatz.⁴



4. *The Impact of the Digital Workforce*, VMware-Report, 2017

4 Verschlüsseln und Löschen sensibler Informationen wie E-Mails



Das Management von Daten auf einer wachsenden Anzahl von Endpunkten spielt eine wichtige Rolle bei der Aufrechterhaltung der Sicherheit. Was passiert, wenn Daten auf dem persönlichen Gerät eines Mitarbeiters verloren gehen oder kompromittiert werden? Wie können Mitarbeiter verhindern, dass wichtige Informationen per E-Mail gesendet werden? Mit einer Strategie für digitale Arbeitsplätze beugen Sie diesen Risiken vor.

So verbessert eine Strategie für digitale Arbeitsplätze die Sicherheit

- Größere Kontrolle über eine höhere Anzahl von Datentypen – sowohl auf Smartphones und Laptops, die vom Unternehmen bereitgestellt werden, als auch auf mitarbeitereigenen Geräten
- Möglichkeit, E-Mail-Filterrichtlinien anzuwenden, sensible Daten zu verschlüsseln und E-Mail-Anhänge in Containern zu halten, damit diese nicht über persönliche E-Mail-Accounts nach außen gelangen
- Einfacheres Löschen von Anwendungen etwa bei Verlust oder Diebstahl eines Geräts oder bei Ausscheiden eines Mitarbeiters

Die folgenden Personengruppen gelten in Unternehmen als häufigste Verursacher von Sicherheitsvorfällen:⁵

- 30% der derzeitigen Mitarbeiter
- 27% der ehemaligen Mitarbeiter
- 23% unbekannte Hacker

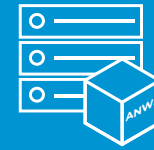
Zu den Folgen zählen hauptsächlich kompromittierte Kunden- und Mitarbeiterdatensätze sowie der Verlust oder die Beschädigung von internen Datensätzen.



5. IDC, 2018 Global State of Information Security Survey™

5

Hosten von Windows-Anwendungen auf sicheren Servern, um Daten von Endpunkten fernzuhalten



BYO-Ansätze kontrollieren Geräte – und lassen dabei Anwendungen außer Acht, was in einer Ansammlung ungesicherter Daten auf Endpunkten resultiert. Ohne zentralen Hosting-Standort verliert die IT schnell den Überblick.

Durch das Hosten von Anwendungen auf einem Server statt auf einem Endpunkt ergeben sich folgende Vorteile:

- Die Einhaltung von Compliance-Richtlinien und Sicherheitsauflagen kann leichter überprüft werden.
- Performance und Sicherheit vieler bestehender Windows-Anwendungen werden verbessert, wenn einzelne Anwendungen (RDSH) oder ganze Desktops (VDI) in sicheren Rechenzentren gehostet werden.
- Autorisierten Mitarbeitern wird der Zugriff auf moderne und Legacy-Windows-Anwendungen, webbasierte Anwendungen sowie SaaS-Anwendungen gewährt. Auf diese Weise bleiben Anwendungen sicher und können ohne Einschränkung geräteübergreifend genutzt werden.

Einfaches Installieren von Windows-Patches und -Updates

Es ist riskant, sich darauf zu verlassen, dass Mitarbeiter ihre Software beim Erscheinen eines Windows-Sicherheitspatch aktualisieren. Bei einem digitalen Arbeitsplatz können automatische Patches mithilfe von cloud-basierten Tools an Mitarbeiter gesendet werden. Unternehmen erreichen dadurch eine höhere Sicherheit mit weitaus weniger Aufwand.



Auf in die Zukunft mit einer Strategie für digitale Arbeitsplätze

Technologie hat einen umfassenden Wandel bei der Produkt- und Service-Bereitstellung in Unternehmen herbeigeführt – und dieser Prozess ist noch nicht abgeschlossen. Unternehmen kehren traditionellen Ansätzen den Rücken und wenden sich im Rahmen der digitalen Transformation flexiblen, optimierten Strategien zu.

Mit einem anwenderorientierten Ansatz steigern Sie Produktivität und Zufriedenheit Ihrer Mitarbeiter ohne Sicherheitseinbußen. Eine Strategie für digitale Arbeitsplätze bietet Ihnen die Möglichkeit, Lösungen proaktiv umzusetzen und damit den reaktiven Zyklus ständiger Problembehebung zu durchbrechen. Nutzen Sie die dadurch gewonnenen Zeit- und Kosteneinsparungen, um Ihr Business voranzutreiben.

JETZT STARTEN

Weitere Informationen zu
digitalen Arbeitsplätzen >

VMware online:



vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Freisinger Str. 3 85716 Unterschleißheim/Lohhof
Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de

Copyright © 2018 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch US-amerikanisches und internationales Copyright und Gesetze zum Schutz des geistigen Eigentums geschützt. Produkte von VMware sind durch ein oder mehrere Patente geschützt, die auf der folgenden Webseite aufgeführt sind: <http://www.vmware.com/go/patents>. VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt. Artikelnr.: vmware-think-you-need-a-byo-strategy-think-again-EDW-0800_DE

01/18