IT-Deployment und -Management
im Zeichen von New Work.

Modern Workplace – IT-Arbeitsplätze, schnell, effizient und sicher bereitstellen und verwalten.

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE

Die Herausforderungen steigen.

Verteiltes Arbeiten, Cloud Computing und Mobilität haben die Komplexität und den Aufwand für die Einrichtung, Bereitstellung und Verwaltung von IT-Arbeitsplätzen drastisch erhöht. Mit der richtigen Strategie und den passenden Werkzeugen lässt sich die IT-Abteilung allerdings deutlich von Routineaufgaben entlasten.

Die Art und Weise, wie und wo Menschen ihren Beruf ausüben, hat sich in den vergangenen Jahren stark verändert. Arbeiteten laut Statistischem Bundesamt 2017 gerade einmal elf Prozent der deutschen Erwerbstätigen teilweise oder ganz im Homeoffice[1], waren es im Frühjahr 2021 über 30 Prozent[2]. Der Trend zur ortsunabhängigen mobilen Erwerbstätigkeit wird sich aller Voraussicht nach noch verstärken. Zahlreiche Unternehmen haben angekündigt, nicht mehr zur Fünf-Tage-Woche im Büro zurückzukehren[3]. Angestellte, die Erfahrung mit dem Homeoffice gemacht haben, wollen nur in einem von zehn Fällen zurück zur ausschließlichen Präsenzarbeit[4].

Aber nicht nur die Firmenkultur und die Erwartungshaltung der Beschäftigten haben sich geändert, auch die Arbeitsmittel und Werkzeuge sind heute ganz andere als noch vor zehn Jahren. Laptop, Smartphone und Tablet gehören heute laut dem Digital Index 2020/2021 der Initiative D21[5] bei der Mehrheit der Arbeitnehmer mit Bürojob zum Alltag. Hinzu kommt die vermehrte Verwendung von Konferenzdiensten, Kollaborationstools und Fernzugängen. Auch die Nutzung von Cloud-Diensten wie Software-as-a-Service ist zur Selbstverständlichkeit geworden[6].

Für die IT-Mitarbeiter in den Unternehmen stellt diese Entwicklung eine enorme Herausforderung dar. Sie müssen immer komplexere und diversere Arbeitsumgebungen zur Verfügung stellen und verwalten sowie Support leisten, ohne direkten Zugriff auf die Geräte zu haben. Zudem ist es nötig, IT-Sicherheit zu gewährleisten, egal von wo und mit welchem Gerät ein Mitarbeiter auf das Firmennetz zugreift.

[1] https://www.destatis.de/DE/Themen/Arbeit/Arbeitsmarkt/Erwerbstaetigkeit/Publikationen/Downloads-Erwerbstaetigkeit/broeschuere-arbeitsmark-blick-0010022189004.html

[2] https://initiatived21.de/app/uploads/2021/02/d21-digital-index-2020_2021.pdf#page=45

[3] https://www.nextmedia-hamburg.de/umfrage-so-gestalten-unternehmen-die-arbeitswelt-nach-corona/

[4] https://initiatived21.de/app/uploads/2021/02/d21-digital-index-2020_2021.pdf#page=45

[5] https://initiatived21.de/

[6] https://www.bitkom-research.de/de/PK-Cloud-Monitor-2021

Onboarding

– Wie neue Mitarbeiter schnell zur passenden IT-Ausstattung kommen.

Die Herausforderungen beginnen schon damit, dass mit dem Einrichten neuer Arbeitsplätze ein hoher Abstimmungs- und Arbeitsaufwand einhergeht. Oft müssen die IT-Mitarbeiter mühsam recherchieren, welche Rolle und Aufgaben der neue Kollege wahrnimmt, welche Hard- und Software er benötigt und welche Zugänge und Berechtigungen einzurichten sind. Auch das nachfolgende individuelle Konfigurieren der Geräte, Applikationen und Berechtigungen ist aufwendig und zeitraubend. In der Regel erstellt die IT zuerst ein nutzerspezifisches Image, testet es und installiert es über ein Client Management Tool auf den neuen Rechner des Mitarbeiters. Dann muss ein geeigneter Termin für die Übergabe gefunden werden. Das gestaltet sich vor allem dann schwierig, wenn sich diese Person im Homeoffice oder im Außendienst befindet. Aufwendige Abstimmungsschleifen sind die Folge – von Zeitverlust und Frust auf beiden Seiten ganz zu schweigen.

Moderne Werkzeuge erleichtern diesen Vorgang erheblich. Mit der Tool-Sammlung Windows Autopilot[7] kann der IT-Mitarbeiter beispielsweise einen Windows-Rechner für die Nutzung vorbereiten, ohne ihn jemals in der Hand gehabt zu haben. Er legt dazu ein Profil an, das die sogenannten OOBE-Einstellungen (Out of the Box Experience) enthält. Der IT-Mitarbeiter kann auch definieren, ob der Anwender seinen Rechner selbst verwalten darf oder nicht. Über das Microsoft-Partner-Portal können die Geräte dann für den Autopilot Deployment-Service registriert und anschließend einem Autopilot-Profil zugewiesen werden. Optional lässt sich ein Gerät fest einem bestimmten Nutzer zuordnen. Der Anwender erhält seinen Rechner direkt an den Arbeitsplatz oder nach Hause geliefert und wird dort beim ersten Starten mit den persönlichen Konfigurationen, Zugangsdaten und Berechtigungen versorgt. Aufwendige Terminabsprachen, zusätzliche Postlaufzeiten und Übergaben entfallen.

Ähnlich einfach ist es, ein Android-Smartphone oder einen Mac-Arbeitsplatz zur Verfügung zu stellen. Google beispielsweise bietet die Zero-Touch-Registrierung für IT-Administratoren[8] an. Android-Geräte, die Zero Touch unterstützen, prüfen beim ersten Start, ob ihnen eine Unternehmenskonfiguration zugewiesen wurde. Ist dies der Fall, lädt das Smartphone die Device Policy Controller App herunter. Diese ruft die vom Administrator vorgegebenen Einstellungen ab und richtet das Gerät automatisch ein.

Mit dem „Programm zur automatischen Registrierung“ (vormals „Device Enrollment Program“, DEP) von Apple lassen sich auch Geräte auf iOS- und MacOS-Basis einfach bereitstellen[9]. Ähnlich wie beim Autopilot benötigt der IT-Administrator keinen direkten physischen Zugriff auf die Geräte, sondern kann sie aus der Ferne einrichten und verwalten. Er muss sie dazu nur vorab in seinem Gerätemanagementsystem registrieren. Aktiviert ein Anwender ein neues Gerät, gleicht DEP die Seriennummer mit den bekannten Registrierungen ab. Ist das Gerät in der Liste enthalten, wird es automatisch an das Gerätemanagement angebunden und erhält die darin definierten Einstellungen und Applikationen. DEP versetzt iOS-Geräte zudem in einen „Supervised Mode“, der zusätzliche Schnittstellen für die Verwaltung freischaltet. Administratoren können dann beispielsweise installierte Apps ausblenden oder neue installieren.

[7] https://www.bechtle.com/marken/microsoft/microsoft-windows-autopilot

[8] https://support.google.com/work/android/answer/7514005?hl=de

[9] https://www.bechtle.com/ueber-bechtle/news/bechtle-blog/it-loesungen/mobile-solutions/dep-vpp-intelligente-nutzung-der-apple-bereitstellungsprogramme#uc-corner-modal-show

Warum automatisiertes Gerätemanagement zu weniger Verwaltung, mehr Produktivität und höherer Nutzerzufriedenheit führt.

Die vorgenannten Tools erleichtern das Onboarding erheblich. Ihre volle Wirkung entfalten sie aber erst, wenn sie mit einem modernen, regelgesteuerten Gerätemanagement verbunden sind. Darüber lassen sich Endgeräte nicht nur bei der Einrichtung konfigurieren, sondern über den gesamten Lebenszyklus hinweg weitgehend automatisiert verwalten. Solche zentralen Administrationsplattformen wurden zunächst als Mobile Device Management (MDM) für die Verwaltung mobiler Endgeräte eingeführt. Inzwischen können jedoch sämtliche Endpunkte über eine einheitliche, Unified Endpoint Management (UEM) genannte Oberfläche administriert werden. Zu den bekanntesten UEM-Lösungen gehören MobileIron[10], Microsoft Endpoint Manager/Intune[11] und VMware Workspace ONE[12]. Darüber hinaus kann das Gerätemanagement auch als Managed Service bezogen werden, beispielsweise als Bestandteil des Bechtle SMART Workplace Angebots[13].

UEM-Lösungen und -Services konsolidieren Gerätesilos und bieten damit eine einheitliche Sicht auf alle Endgeräte über eine einzige Managementkonsole – und zwar unabhängig von Formfaktor, Betriebssystem oder Standort. Betriebssystem-Updates, Security-Patches und Software-Aktualisierungen werden automatisch installiert, sobald sie von der IT-Abteilung für das Deployment freigegeben sind und der Anwender sich mit dem Firmennetz verbindet. Alle Endpunkte sind damit immer auf dem neuesten Stand, was nicht nur Sicherheit und Stabilität erhöht, sondern auch den Pflegeaufwand minimiert. Moderne Gerätemanagementlösungen können darüber hinaus potenzielle Probleme auf dem Endgerät erkennen und proaktiv beheben, bevor es zu einer Störung kommt. Das entlastet den Helpdesk deutlich.

[10] https://www.mobileiron.com/de

[11] https://docs.microsoft.com/de-de/mem/endpoint-manager-overview

[12] https://www.vmware.com/de/products/workspace-one.html

[13] https://www.bechtle.com/aktion/modern-digital-workplace/smart-workplace

Eine weitere wichtige Aufgabe ist die Überwachung und Einhaltung von Sicherheitsrichtlinien und Datenschutzvorgaben. Über die Managementkonsole definieren Administratoren, auf welche Daten von einem Endgerät zugegriffen und ob diese geteilt werden dürfen. Während sich Firmendaten in einem eigenen verschlüsselten Sektor des Geräts speichern lassen, kann die Nutzung privater Applikationen und Daten unterbunden oder auf einen separaten Bereich begrenzt werden. Auf diese Weise sind auch Bereitstellungsmodelle wie COPE (Company Owned Personally Enabled) oder BYOD (Bring Your Own Device) realisierbar, bei denen eine Mischnutzung von Firmen- beziehungsweise Privatgeräten vorgesehen ist. Bei Verlust oder Diebstahl sind die Daten vor fremden Blicken geschützt, da die Geräte proaktiv verschlüsselt werden. Der Administrator ist darüber hinaus in der Lage, verlorene oder gestohlene Endgeräte aus der Ferne zu sperren oder zu löschen.

Moderne Managementkonsolen machen es außerdem möglich, neben Endgeräten auch Applikationen zentral zu verwalten. Mitarbeiter erhalten bereits beim Onboarding automatisiert alle für ihre Arbeit notwendigen Anwendungen. Über einen Firmen-App-Store fordern sie selbständig weitere Applikationen an und installieren diese. Alle Aktualisierungen erfolgen daraufhin direkt automatisch aus der Verwaltungsplattform.

Von der Rundumsicht auf Geräte und Anwendungen profitiert nicht nur die IT. Auch Finanzabteilung und Controlling erhalten dadurch einen wesentlich besseren Einblick in den Ressourcenbestand und dessen Nutzung. Das erlaubt eine realistischere Bewertung von Assets und Risiken und erleichtert die Budgetplanung.

MFA, SSO und Zero Trust

– Wie ein sicherer Zugang in einer verteilten Arbeitswelt gelingt.

Wenn Mitarbeiter auf Endgeräte, Firmendaten, Software oder Cloud-Services zugreifen, sind diese Zugänge traditionell nur mit einer Kombination aus Nutzername und Passwort gesichert. Diese seit mehr als 50 Jahren übliche Form der Authentifizierung und Autorisierung ist jedoch hochgradig unsicher. Die Website „Have I Been Pnwed[14]?" verzeichnet mehr als elf Milliarden kompromittierte Accounts, bei denen Nutzernamen und Passwort gestohlen wurden. Das ist nicht nur für die betroffenen Konten und Zugänge problematisch. So versuchen Cyberkriminelle durch sogenanntes Credential Stuffing mit denselben Daten auch andere Accounts zu übernehmen. Dabei haben sie allzu häufig Erfolg, da rund zwei Drittel der Anwender ein und dasselbe Passwort für mehrere Accounts[15] nutzen.

Traditionell sind IT-Sicherheitsverantwortliche bestrebt, dieses Risiko durch unternehmensweit geltende Passwortrichtlinien zu verringern. Sie schreiben lange, komplexe Passwörter vor, die auch noch in regelmäßigen Abständen geändert werden müssen. Viele Anwender sind von diesen Vorgaben allerdings überfordert und können sich die Vielzahl komplizierter Passwörter nicht mehr merken. In der Folge werden Kennwörter auf Post-Its notiert oder in Word-Dokumenten gesammelt.

Ein modernes IT-Management sollte deshalb folgende drei Maßnahmen ergreifen, um Risiken zu minimieren und die Produktivität zu erhöhen:

- **Multi-Faktor-Authentifizierung (MFA) einführen:** MFA basiert darauf, die Identität eines Anwenders auf zwei Kanälen zu überprüfen. Zusätzlich zum Passwort können beispielsweise biometrische Daten wie Fingerabdruck, Iris-Scan oder Gesichtserkennung als Identitätsmerkmal eingesetzt werden. Alternativ oder je nach Sicherheitsstufe auch zusätzlich ist der Nutzer in der Lage, sich über einen Hardware-Dongle oder eine Authentifizierungs-App, die Einmalpasswörter (One-Time Password, OTP) generiert, auszuweisen.

Noch vor wenigen Jahren war MFA teuer in der Einführung und komplex in der Verwaltung. Heute ist es kein Problem mehr, MFA-Funktionen als Service in nahezu jede Infrastruktur zu integrieren. Hardware-Dongle sind weitgehend überflüssig geworden, weil fast jeder Anwender ein Smartphone besitzt, das sich als Basis für den zweiten Faktor eignet. Wie die Microsoft-Sicherheitsexperten Lee Makler und Alexander Weinert auf der RSA Konferenz 2020 zeigten[16], schützt MFA nahezu vollständig vor Account-Übernahmen. Von

[14] https://haveibeenpwned.com/

[15] https://www.lastpass.eu/de/psychology-of-passwords

[16] https://www.youtube.com/watch?v=B_mhJO2qHlQ

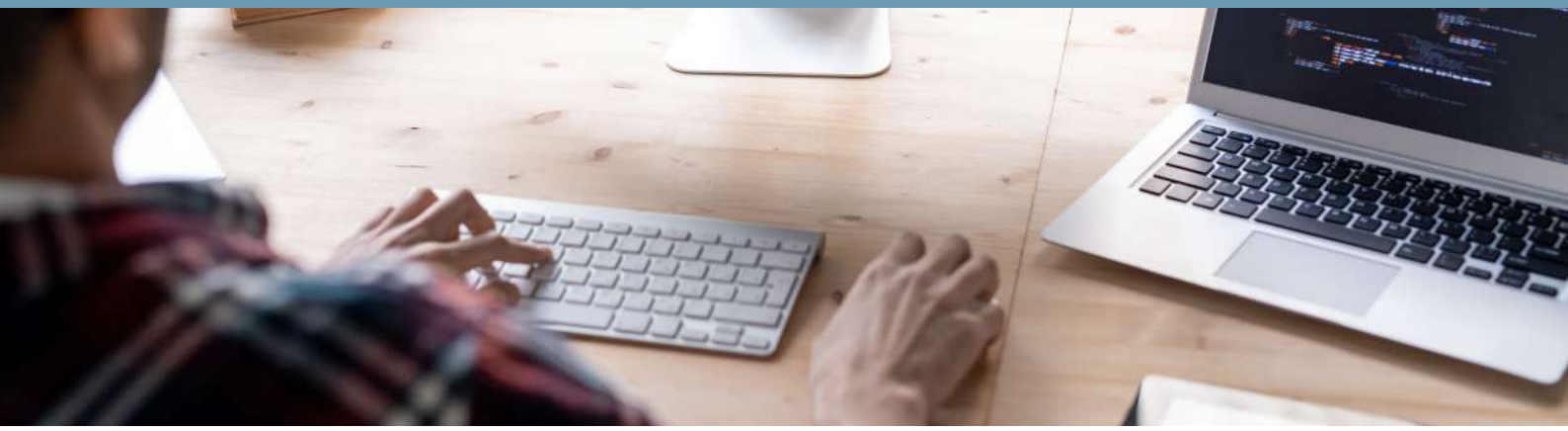
den im Januar 2020 kompromittierten Accounts waren fast alle nur durch eine Kombination aus Nutzername und Passwort geschützt, weniger als 0,01 Prozent wiesen eine MFA-Absicherung auf.

- **Single Sign-On (SSO) zur Verfügung stellen:** Je mehr Passwörter Nutzer zu verwalten haben, desto größer ist die Gefahr, dass diese mehrfach verwendet, auf Post-Its geschrieben oder in Excel-Listen verwaltet werden. Unternehmen sollten deshalb eine Infrastruktur schaffen, die es Mitarbeitern ermöglicht, über einen einzigen Zugangspunkt auf alle für sie freigegebenen Ressourcen, Lösungen und Services zuzugreifen.

- **Zero Trust und Conditional Access implementieren:** Traditionell gilt ein Anwender oder Endgerät als vertrauenswürdig, sobald er beziehungsweise es sich an der Firmeninfrastruktur identifiziert und autorisiert hat. Das ist in einer verteilten Arbeitswelt ein problematisches Verfahren, denn es macht die Kombination aus Nutzername und Passwort zur letzten Verteidigungslinie. Hat ein Angreifer die Daten erbeutet oder erraten, kann er sich ungehindert im internen Netz bewegen. Besonders gefährlich ist das, wenn es sich um einen privilegierten Account mit Administratorenrechten handelt. Dann lassen sich sogar Server übernehmen oder umkonfigurieren. Das gilt auch und insbesondere, wenn Anwender aus dem Homeoffice auf das Firmennetz zugreifen. Ist beispielsweise das Endgerät des Mitarbeiters mit Malware verseucht, hat diese über den scheinbar sicheren Tunnel Zugriff auf interne Ressourcen und kann sich leicht im Firmennetz ausbreiten.

Das Marktforschungsunternehmen Forrester hat deshalb vor rund zehn Jahren das Zero-Trust-Konzept entwickelt, das diese Sicherheitslücke schließen soll. Es basiert auf dem Prinzip des „Conditional Access“: Statt durch die Eingabe der Login-Daten ungehinderten Zugang zu erhalten, werden dem Mitarbeiter nur die Rechte zugewiesen, die er aktuell braucht und die zum Kontext passen. Auch das Sicherheitsniveau der Anmeldung kann kontextabhängig angepasst werden. Meldet sich ein Mitarbeiter beispielsweise aus dem Büro von einer bekannten IP-Adresse aus an, genügt für die Anmeldung ein Passwort. Greift er dagegen aus dem Homeoffice oder einem Café zu, ist eine Mulit-Faktor-Authentifizierung notwendig, besonders sensible Datenbereiche bleiben zudem gesperrt. Bei ungewöhnlichen Zugriffsversuchen, etwa aus dem Ausland oder mitten in der Nacht, wird der Zugang verweigert. Auch der Status des Endgeräts, mit dem der Anwender sich ins Firmennetz einloggen will, kann eine Rolle spielen. Fehlen beispielsweise Patches oder entdeckt der Virenscanner Malware auf dem Gerät, wird der Zugang gesperrt, bis das Gerät aktualisiert beziehungsweise desinfiziert ist.

Wie Cloud-Lösungen mobiles Arbeiten erleichtern.



Die Homeoffice-Welle der vergangenen Monate hat die Bedeutung von Cloud-Diensten für die Flexibilität und Krisenfestigkeit von Unternehmen deutlich gemacht. Wer beispielsweise Arbeitsplätze über eine Virtual Desktop Infrastructure (VDI) oder Workplace as a Service (WaaS) aus der Cloud genutzt hat, konnte relativ schnell und einfach neue mobile Arbeitsplätze zur Verfügung stellen. Dagegen mussten eher traditionell aufgestellte Unternehmen erst einmal Hardware beschaffen und Remote-Zugänge einrichten. Bürosoftware, Konferenzdienste und Team-Plattformen skalieren in der Cloud ebenfalls wesentlich besser als im eigenen Rechenzentrum. Idealerweise wird das Angebot an Standard-Cloud-Lösungen durch ein ebenfalls cloudbasiertes Company-Portal ergänzt. Über dieses Portal können Mitarbeiter selbständig die Applikationen buchen und verwenden, die sie für ihre Arbeit benötigen.

Der Einsatz von Cloud-Apps erleichtert auch die Einrichtung, Absicherung und Verwaltung von Fernzugängen erheblich. In traditionellen Rechenzentrumsumgebungen nutzen Mitarbeiter, die sich nicht direkt ins Firmennetz einloggen, in der Regel ein Virtual Private Network (VPN) für den sicheren Zugang. Dabei werden die Daten durch einen verschlüsselten Tunnel über das öffentliche Internet übertragen. Für die IT-Administration ist die Verwaltung solcher VPN-Infrastrukturen aufwendig und fehleranfällig. Sie müssen Schlüssel und Zertifikate erstellen, verteilen und gegebenenfalls auch wieder löschen oder widerrufen. Häufig führen Schwierigkeiten, die beim Einrichten und beim Verbindungsaufbau entstehen, zu einem erhöhten Supportaufkommen. Tunneling und Verschlüsselung benötigen zudem zusätzlich Bandbreite und Performance. Sie können sich daher negativ auf Übertragungsgeschwindigkeit und -qualität auswirken. Für Cloud-Apps, die beispielsweise über den Azure App Proxy veröffentlicht werden, ist dagegen keine VPN-Verbindung mehr erforderlich, die Absicherung des Zugangs kann per MFA erfolgen.

In fünf Schritten zu einer modernen IT-Verwaltung

Es ist von großer Bedeutung, die Transformation von traditionellen Deployment- und Managementstrategien hin zu einer modernen IT-Administration sorgfältig zu planen und strukturiert durchzuführen – am besten gemeinsam mit erfahrenen Modern-Workplace-Spezialisten wie den Bechtle IT-Architekten und IT-Consultants. Die Experten von Bechtle empfehlen folgendes Vorgehen und unterstützen Unternehmen im Rahmen eines Workshops bei der Umsetzung:

1. Analyse der Ist-Situation

Zu Beginn sollten sich die IT-Verantwortlichen einen Überblick darüber verschaffen, welche Geräte, Betriebssysteme und Applikationen im Unternehmen im Einsatz sind und wie diese verwaltet werden. Dabei ist es wichtig, auch die „Schatten-IT" zu betrachten – also möglichst alle IT-Ressourcen zu erfassen, die von Fachabteilungen oder einzelnen Mitarbeitern an der zentralen IT vorbei angeschafft und genutzt werden.

2. Aufnahme der Anforderungen

Ist die vorhandene Basis geklärt, geht es an die Definition der Soll-Situation: Welche Struktur-, Funktions- und Leistungsmerkmale sind aus Sicht der Organisation, der IT und der Endnutzer essentiell? Welche sind zusätzlich wünschenswert?

3. Definition der Lösung

Mit den Informationen aus Schritt 1 und 2 können Unternehmen nun gemeinsam mit den Bechtle-Experten die passende Modern-Management-Lösung designen, die Rahmenbedingungen für eine Migration festlegen und eine Roadmap für den Übergang erstellen. Ein wesentlicher Bestandteil dieser Phase ist außerdem eine Risikoanalyse. Alle relevanten Risiken sind dabei zu erfassen und in einer Matrix darzustellen.

4. Durchführung der Migration

In der nächsten Phase erfolgt der Übergang vom herkömmlichen Deployment und Management zur neuen weitgehend automatisierten Verwaltungsumgebung. Die IT-Business-Architekten von Bechtle stellen dabei sicher, dass der Übergang unterbrechungsfrei erfolgt.

5. Übernahme des Betriebs

Modern Deployment und Management entlastet die IT-Abteilung bereits deutlich von Routineaufgaben. Um noch mehr Effizienz zu gewinnen und IT-Ressourcen von Verwaltungstätigkeiten zu befreien, kann das Workplace-Management auch komplett als Managed Service an Bechtle ausgelagert werden.

Wie modernes Deployment und Management zum Treiber der digitalen Transformation wird.

Durch die digitale Transformation hat sich die Rolle der IT-Abteilung stark verändert. Musste sie früher vor allem für einen reibungslosen Betrieb der IT-Infrastruktur sorgen, so ist sie heute ein integraler Bestandteil der Wertschöpfung und Treiber neuer Geschäftsmodelle. Um für diese Anforderungen die notwendigen Freiräume zu schaffen, sollten IT-Mitarbeiter von Routineaufgaben entlastet werden. Vor allem die Einrichtung und Verwaltung von Endgeräten, Betriebssystemen und Applikationen bindet immer noch zu viele Ressourcen. Ein modernes Deployment und Gerätemanagement ist daher essentieller Bestandteil jeder nachhaltigen IT-Strategie. Es ermöglicht ein Onboarding per Knopfdruck und ohne persönliche Geräteübergabe sowie eine weitgehend automatisierte Verwaltung der Geräte inklusive aller notwendigen Patches, Updates und Applikationen. Moderne Managementumgebungen bieten mit Funktionen wie Geräteverschlüsselung, MFA und Conditional Access ein deutlich erhöhtes Sicherheitsniveau. In Kombination mit Cloud-Apps machen sie zudem die Einrichtung von VPN-Umgebungen überflüssig.

Wir unterstützen und betreuen mittelständische und internationale Unternehmen sowie öffentliche Einrichtungen. Wir sind Ihr Partner von der Beratung über die Strategie- und Konzeptentwicklung bis hin zu Roll-Out, Implementierung sowie Management in Betrieb und Services. Sie wollen mehr zum Thema Modern Workplace erfahren? Setzen Sie sich noch heute mit uns in Verbindung und vereinbaren Sie einen Beratungstermin mit unseren Experten.

Kontaktieren Sie uns unter
marketing.direct-ch@bechtle.com

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE