netzbest®

IT-Guide Homeoffice

Desktop as a Service etabliert sich als der Königsweg

Die vielen positiven Erfahrungen haben dazu geführt, dass sich das Arbeiten aus dem Homeoffice als eine vielversprechende Option etabliert hat. Doch dazu muss die IT-Umgebung eines Unternehmens umgekrempelt werden – eine Aufgabe, die ein erfahrender IT-Dienstleister mit viel Kompetenz ideal umsetzen kann. Denn er versteht die verschiedenen Aspekte, die es anzugehen gilt: Organisatorische wie auch technische Faktoren spielen eine Rolle. Und zudem ist Vorsorge gegen die typischen Katastrophen erforderlich. Hier zeigen sich die Vorteile, die ein Desktop as a Service (DaaS) bringt. Der IT-Dienstleister netzbest hat mehr als 100 „Homeoffice-Projekte“ durchgeführt und aus diesem reichen Erfahrungsschatz alle nützlichen Aspekte in diesem IT-Guide zusammengefasst.

Im Zuge des zweiten Lockdowns ist die Diskussion um das Thema Homeoffice neu entbrannt. Die Gewerkschaften fordern sogar einen Rechtsanspruch auf das Arbeiten vom Homeoffice aus – und die Grünen bringen einen noch schärferen Vorschlag: Uneinsichtige Unternehmen sollen Bußgelder bezahlen, wenn sie es ihren Mitarbeitern nicht freistellen, von zuhause aus zu arbeiten, so zumindest der Stand Mitte Januar 2021.

Aus dem ersten Lockdown stammen einige interessante Ergebnisse: So hat die Hans-Böckler-Stiftung in einer Umfrage ermittelt, dass Ende Juni 2020 rund 16 Prozent der Befragten überwiegend oder ausschließlich zu Hause aktiv gewesen sind. Weitere 17 Prozent haben angegeben, abwechselnd im Betrieb oder zu Hause zu arbeiten. Daraus lässt sich ablesen, dass uns das Thema Homeoffice nicht so schnell verlassen wird.

Daher sollten Unternehmen, die sich dieser Herausforderung noch gar nicht gewidmet haben oder die zunächst in einem „quick and dirty“-Ansatz diese Umstellung angingen, nochmals mit den vielschichtigen Aspekten auseinandersetzen. Dabei gilt es, sich die Erfahrungen zunutze zu machen, die in bisherigen Homeoffice-Projekten gemacht wurden.

Sicherheit und Datenschutz im Homeoffice

Die Vorgaben für Unternehmen in Bezug auf den Umgang mit sensiblen Daten gelten auch dann im vollen Umfang, wenn sie ihre grundlegende IT-Konzeption ändern und ihre Mitarbeiter von zuhause aus arbeiten lassen. Dazu gehören Themen wie der Arbeitsschutz, die Regelungen durch die DSGVO (Datenschutz-Grundverordnung) aber auch branchenrelevante Vorgaben der zuständigen Aufsichtsbehörden.

Homeoffice bedeutet allerdings nicht, dass Firmenrechner im heimischen Wohn- oder gar Schlafzimmer zum Einsatz kommen. Die Situation erweist sich bei genauerem Hinsehen als weitaus komplexer: Da die Systeme sich nicht innerhalb der geschützten Büroinfrastruktur befinden, müssen Unternehmen besondere Sicherheitsmaßnahmen ergreifen.

Deswegen sind Rechner im Homeoffice stärker gefährdet als im vergleichsweise gut geschützten Unternehmensnetzwerk – das haben Cyber-Kriminelle bereits erkannt und schon in den ersten Tagen der Pandemie ihre Angriffsbemühungen intensiviert. IT-Verantwortliche stehen dem aber nicht machtlos gegenüber, sondern können einige grundlegende Maßnahmen umsetzen, um Systeme außerhalb der eigenen IT-Infrastruktur besser abzusichern.

Sicherheitsvorkehrungen im Homeoffice

Das Thema Sicherheit umfasst auch die Kontrolle von USB-Geräten: Um das Risiko einer Malware-Infektion zu reduzieren und zu verhindern, dass Firmendaten auf privaten USB-Speichern landen, können Unternehmen die USB-Ports der Heimarbeitsrechner zumindest für externe Speichermedien, wie USB-Sticks und Festplatten, sperren.

Ein weiteres Sicherheitselement für ein Homeoffice ist der Einsatz von verschlüsselten WLANs: Viele Mitarbeiter nutzen zu Hause ein drahtloses Netzwerk. Damit Firmendaten geschützt sind, sollten sie eine sichere WLAN-Verschlüsselung mit WPA2 oder WPA3 aktivieren – die älteren Verschlüsselungsstandards WEP und WPA bieten schon lange keinen ausreichenden Schutz mehr. Eine WLAN-Verschlüsselung stellt sicher, dass Angreifer die übertragenen Daten nicht abfangen können, was gerade dann wichtig ist, wenn Mitarbeiter ohne eine Verschlüsselung der Übertragung via VPN (Virtual Private Network) nutzen oder nur bestimmte Verbindungen durch den VPN-Tunnel geleitet werden.

Auch den Router im Homeoffice gilt es vor unbefugten Zugriffen zu schützen, damit Cyber-Kriminelle ihn nicht kapern und alle Datenübertragungen mitlesen können. Ein sicheres Passwort für den Zugang zur Router-Konfiguration ist daher Pflicht – insbesondere, weil die einfachen Default-Passwörter vieler Router-Modelle öffentlich bekannt sind. Die komplexeren Standard-Passwörter, die manche Hersteller jedem Gerät individuell zuweisen, sind zwar sicherer, aber auch nicht ideal, da sie in der Regel auf dem Gerät aufgedruckt sind. Gäste, Handwerker oder andere Besucher könnten sie sich in einem unbeobachteten Moment notieren.

In Bezug auf den Datenschutz ist es generell wichtig, alle relevanten Bestimmungen zu verstehen und einzuhalten. Bei der Nutzung von IT und Computernetzwerken kommt ein ganzes Bündel von Fragen und Risiken hinzu. Viele Sicherheitslücken drohen, von denen Laien in der Regel nichts ahnen. Meist fällt einem Netzwerkadministrator die Aufgabe zu, Konfigurationen, Updates und das Verhalten der Anwender im Blick zu behalten. Wenn Beschäftigte private Geräte für die Arbeit nutzen, wird es schnell unmöglich, alle denkbaren Datenschutzlücken zu schließen – zu unterschiedlich sind die Software- und Hardware-Konfigurationen.

IT-Arbeitsplätze auf Basis einer Cloud-Infrastruktur von netzbest bieten eine elegante Lösung für ein kompliziertes Problem. Die Mitarbeiter greifen über verschlüsselte Verbindungen auf Software und Daten des Unternehmens zu. Ganz egal, welches Endgerät sie dafür verwenden - die IT bleibt im Rechenzentrum, das Datenschutz und -sicherheit auf höchstem Niveau gewährleistet.

VPN-Verbindung ins Firmennetz

Für die meisten Aufgaben benötigen Mitarbeiter einen Zugriff auf Daten oder Anwendungen im Firmennetzwerk. Nur wenn sie darauf einen einfachen Zugriff vorfinden, wird das Arbeiten aus dem Homeoffice auch effizient. Ein derartiger sicherer Zugriff wird in der Regel über ein VPN ermöglicht. Dabei handelt es sich um einen verschlüsselten Kommunikationstunnel zwischen dem Arbeitsgerät und der IT-Infrastruktur in der Firma. Allerdings gilt der Einsatz eines VPN in vielen Fällen als recht komplex.

Auf diese Weise verhindern Unternehmen, dass Außenstehende die Daten auf dem Übertragungsweg abgreifen oder manipulieren. Überdies tun sie sich auch leichter, Sicherheitsrichtlinien anzupassen sowie Updates zu installieren als bei Systemen, die keine Verbindung zum Firmennetz haben.

Für vielen Geschäftsreisende gehört es beispielsweise zum Alltag, über das öffentliche WLAN im Hotel zu arbeiten – das war schon vor der aktuellen Pandemie so. Das Abrufen von E-Mails oder die Teilnahme an einer Videokonferenz – das sind heutzutage typische Aufgaben, die zum Beispiel auch im Urlaub von Berufstätigen erwünscht sind.

Doch wer zum ersten Mal per VPN auf das Unternehmensnetzwerk zugreifen will, erlebt oft eine unangenehme Überraschung: In vielen Fällen lässt das Hotel-WLAN keine VPN-Verbindungen zu. Doch auch dazu findet sich eine Lösung: Das VPN muss so konfiguriert werden, dass es über die Protokolle HTTP oder HTTPS funktioniert.

Noch einfacher ist es, einen kompetenten IT-Dienstleister einzubinden. Dann mit deren Lösung kommen verschlüsselte Verbindungen sogar ohne VPN aus und funktionieren auch in Hotels. Dabei übernimmt der Dienstleister die Einrichtung und steht für Fragen und Support zur Verfügung – auf Wunsch rund um die Uhr.

Passende Hardware für VPN-Verbindungen

IT-Umgebungen haben oftmals ein gewisses Problem: Eine Konfiguration funktioniert in einem Testfall mit geringer Belastung recht ordentlich – doch das muss nicht bedeuten, dass sie auch unter hoher Belastung ihren Aufgaben problemlos erfüllt. Jeder Homeoffice-Mitarbeiter mit aktiver VPN-Verbindung nimmt einen Teil der Server-Ressourcen im Unternehmen in Anspruch. Daher ist es für ein reibungsloses Arbeiten entscheidend, dass die Hardware diesen Anforderungen gewachsen ist. Der Einsatz einer richtig dimensionierten Server-Hardware wird umso mehr zur Herausforderung, als die Zahl der Angestellten stark schwanken kann, die sich über VPN mit dem Server verbinden.

Wer sich für eine virtuelle Arbeitsumgebung von einem erfahrenen IT-Dienstleister entscheidet, der hat auch dieses Problem gelöst: Ein VPN ist nicht nötig und für das Rechenzentrum des IT-Dienstleisters sind Belastungsspitzen kein Problem. Ein Unternehmen muss lediglich so viele Einzelplatz-Lizenzen erwerben, wie es benötigt. Dann profitiert jeder Mitarbeiter von einer erstklassigen IT-Infrastruktur, ohne dass eine Anschaffung von Hardware im eigenen Haus nötig wäre.

Vom Prinzip her kann man jede VPN-Verbindung wie ein Netzwerkkabel vom Homeoffice ins Büro auffassen. Dies bedeutet aber auch, dass jeder, der dieses Netzwerkkabel hat, auf alle Inhalte des Firmennetzwerks zugreifen kann. Hier braucht es ein granulares Sicherheitskonzept, das auf Benutzerrollen basiert. Als erfahrene Anbieter von Desktop-as-a-Service-Lösungen wissen die Experten eines IT-Outsourcers, worauf es dabei ankommt, und findet für jedes Anforderungsprofile eines Unternehmens die bestmögliche Lösung.

Die Frage nach der Bandbreite

In kleinen und mittleren Unternehmen mit vielen Homeoffice-Arbeitsplätzen entstehen oft Engpässe beim Upload, da große Datenmengen vom Firmenserver aus an die Rechner der Mitarbeiter übertragen werden müssen. Die Flaschenhälse sind zum einen im Internet-Anschluss des Mitarbeiters im Homeoffice zu suchen, aber auch bei der Auslastung der Internet-Zugangs des Unternehmens zu suchen.

Denn in einer IT-Architektur „ohne Homeoffice“ läuft der Informationsfluss der Mitarbeiter in erster Linie im Unternehmensnetzwerk, lediglich beim Zugriff auf externe Informationsquellen – sprich dem Internet – kommt es zur Belastung dieses Knotens. Dies kann frustrierend sein und die Produktivität beeinträchtigen. Ein Upgrade der Kapazität ist mit Kosten verbunden, die auch dann anfallen, wenn man die Bandbreite nur zu Stoßzeiten benötigt. Unter Umständen muss man sogar auf eine andere Netzwerk-Technologie wie SD-WAN umstellen.

Doch mit dem Einsatz einer Cloud-Desktop-Lösung (sprich einem Desktop-as-a-Service) hat sich dieses Problem erledigt. Die Mitarbeiter greifen über den Browser auf den Firmenrechner zu, als würden sie das Internet nutzen. Nur die Bildschirmausgabe wird an sie übertragen. Ein Upload großer Datenvolumen ist daher nicht nötig. Eine komplette Auslagerung der IT an einen IT-Dienstleister ist ebenso möglich, wie eine Erweiterung einer bestehenden Infrastruktur durch Cloud-Ressourcen auf Enterprise-Niveau. In jedem Fall bekommt man ein leistungsstarkes System, das mit Belastungsspitzen leicht fertig wird.

Organisatorische Aspekte

Weil in Folge des ersten Lockdowns viele Mitarbeiter sehr kurzfristig ins Homeoffice umziehen mussten, fehlte es vielfach an mobilen Computern. Daher nutzten die meisten Beschäftigen zu Hause einfach ihren privaten PC – und tun das teilweise immer noch. Doch auf diesen Geräten können Unternehmen in der Regel keine Sicherheitsrichtlinien durchsetzen und müssen sich auf die vom Mitarbeiter eingerichteten Schutzmaßnahmen verlassen. Daher sind solche „pragmatischen" Lösungen ein Risiko und sollten dringend abgelöst werden – vielfach mit der Devise: „Keine privaten Geräte".

Des Weiteren sollten die IT-Zuständigen im Unternehmen darauf achten, dass mit dem Einführen des Homeoffice auch neue Cloud-Services und Online-Dienste für den Datenaustausch und die Kommunikation zum Zug kommen. Hier sollten sie unbedingt evaluieren, ob diese tatsächlich den eigenen Sicherheits- und Datenschutzanforderungen genügen – etwa ob sie eine sichere Verschlüsselung nutzen, ob und wo sie Daten speichern oder wie sie sich in die bestehende Sicherheitsinfrastruktur des Unternehmens integrieren lassen. Das lässt sich beim Einsatz eines externen IT-Dienstleisters recht einfach umsetzen.

Klare und verbindliche Vorgaben zum Umgang mit Daten, Anwendungen und Geräten im Homeoffice stellen sicher, dass Mitarbeiter aus Unwissenheit die IT-Sicherheit gefährden oder gegen den Datenschutz verstoßen. Daher sollten Unternehmen auch Kommunikationswege und Ansprechpartner definieren, damit alle Abläufe klar geregelt sind, und Mitarbeiter nicht auf Betrugsversuche wie „Scam-Anrufe" (mit einer missbräuchlichen Nutzung einer Telefonnummer) vermeintlicher Support-Mitarbeiter hereinfallen. Spezielle Awareness-Schulungen im Umfeld der IT-Sicherheit können überdies helfen, das Bewusstsein für Cyber-Gefahren weiter zu schärfen.

Eine weitere Frage lautet, ob die Software sichere VPN-Verbindungen unterstützt. Wenn eine wichtige Software dies nicht erlaubt, kann dies eine erhebliche Hürde für den effizienten Homeoffice-Betrieb darstellen. Es sei denn, ein Unternehmen setzt auf einen IT-Dienstleister, der eine virtuelle Arbeitsumgebung bereitstellen kann. In diesem Fall greifen die Homeoffice-Mitarbeiter einfach per HTTPS auf einen zentralen Server zu, der Software und Daten für die Arbeit bereitstellt.

Die Frage der Lizenzierung

Beim Einsatz eines VPN sollte man auch sicherstellen, dass genügend Lizenzen vorrätig sind. Denn die VPN-Lizenzen bedürfen ebenso wie andere Software-Lizenzen einer aufmerksamen Planung und Verwaltung. Es gilt stets den Überblick zu behalten, wer welche Lizenz nutzt. Neue Mitarbeiter benötigen neue Lizenzen, und verlässt dagegen ein Mitarbeiter das Unternehmen, wird eine Lizenz frei. Dabei ist auch zu beachten, ob Lizenzen an Endgeräte oder Nutzer gekoppelt sind. In ungünstigen Fällen müssen neue Lizenzen angeschafft werden, während andere ungenutzt bleiben.

Beim Einsatz eines kompetenten IT-Dienstleisters entfallen diese Aufwände und Verluste. Den Mitarbeitern steht über eine verschlüsselte Verbindung ein voll ausgestatteter IT-Arbeitsplatz zur Verfügung. Dafür ist lediglich eine monatliche Gebühr pro Nutzer zu bezahlen und die Unternehmen können nach Bedarf flexibel Arbeitsplätze hinzubuchen oder sie auch wieder kündigen.

Zentrale Verwaltung der genutzten Geräte

Das Management der Systeme ist eine wichtige Aufgabe. Dabei kommen Fragen ins Spiel wie: Welche Geräte nutzen die Mitarbeiter im Homeoffice? Wird die Hardware vom Unternehmen gestellt oder wird auf Benutzer-eigenen PCs, Macs, Tablets und anderen Geräten gearbeitet? In beiden Fällen kann eine zentrale Verwaltung der Geräte nötig sein, um sicherzustellen, dass alles funktioniert. Doch dies wird schnell aufwendig und unübersichtlich. Wer installiert die Software? Wer hilft bei technischen Problemen? Wer kümmert sich um Updates? Wer behält den Überblick über die verschiedenen Konfigurationen?

Mit Cloud-basierten Arbeitsplätzen haben sich diese Fragen für ein Unternehmen erledigt. Die einzelnen Teams eines Unternehmens arbeiten auf virtuellen Desktops, die in einem passend dimensionierten Rechenzentrum eines IT-Diensleisters bereitgestellt und durch eine verschlüsselte Verbindung an die Geräte der Anwender übertragen werden. Dies gewährleistet maximale Flexibilität bei der Gerätenutzung und eine sichere, stabile IT-Umgebung.

Dabei ist das komplette System schnell eingerichtet und erfordert vom Unternehmen praktisch keinen Verwaltungsaufwand, da die gesamte IT ausgelagert ist und von den Experten des Dienstleisters rund um die Uhr gepflegt und gewartet wird.

Tipps aus der Praxis

Nur wer verschiedene Projekte im Bereich der Umstellung auf Homeoffice oder zum Themenbereich „New Work“ durchgeführt hat, kann auch nützliche Tipps geben. In diesem IT-Guide sind die Erfahrungen zusammengefasst, die die Experten von netzbest in mehr als 100 Projekten gemacht haben. Sie sollen Unternehmen helfen, die vor entsprechenden Aufgaben stehen – denn man sollte keine Fehler machen, die andere schon vermieden haben. Zudem können Interessenten jederzeit Kontakt zu netzbest aufnehmen: Tel. +49 30 80 20 81 30 oder via E-Mail beratung@netzbest.de

Typische Katastrophen vermeiden

Die typischen Fehler und Katastrophen, die in den meisten IT-Infrastrukturen auftreten, lassen sich mit Hilfe von vorbeugenden Maßnahmen beheben bzw. deren Auswirkungen deutlich einschränken. Hier wirkt sich die Expertise eines externen IT-Dienstleisters sehr positiv aus, der bestehende Notfallpläne vorhält und die meisten Katastrophen schon „durchexerziert“ hat.

- **Laptop gestohlen und alle Projektdaten weg**
  Der größte Vorteil von Laptops ist gleichzeitig ein Nachteil. Sie lassen sich bequem mitnehmen – leider auch von Langfingern. Aber es muss nicht immer Diebstahl sein: Immer wieder werden Laptops und Tablets in Zügen oder an anderen öffentlichen Orten vergessen. Das kann neben den Kosten vor allem zwei ernste Probleme bedeuten: Erstens sind die auf dem Gerät gespeicherten Daten futsch, zweitens fallen diese nun Unbefugten in die Hände. Bei der Kooperation mit einem IT-Dienstleister ist ein Hardware-Verlust kein Datenverlust, denn die Daten liegen bei ihm im Rechenzentrum und nicht auf dem Laptop. Von einem Ersatzgerät aus lassen sich nahtlos und sofort die Daten weiter bearbeiten. Ohne das Passwort kann der Dieb oder Finder des abhanden gekommenen Laptops nicht auf dessen Daten zugreifen. Im Extremfall kann man so weit gehen, das Gerät komplett zu verschlüsseln, so dass es sich überhaupt nicht von Unbefugten nutzen lässt.

netzbest®

Know-how des IT-Dienstleisters ebnet den Weg ins Homeoffice.

- **Ransomware – nur noch Zeichensalat**
  Immer wieder machen im Internet unsympathische Gesellen die Runde, die in der Unternehmens-IT zur wahren Katastrophe werden können: Trojaner/Ransomware, also kleine Schadprogramme, die sich auf das System schmuggeln und dort sämtliche Daten verschlüsseln. Der Besitzer sieht nur noch Zeichensalat – bis er für ein Lösegeld das Passwort für die Entschlüsselung von den Tätern erhält. Mit einer Cloud-Desktop-Lösung bereitet einem diese Gefahr keine schlaflosen Nächte mehr. Das System erstellt regelmäßig Snapshots, also genaue Abbilder der Daten auf dem Server. Wenn ein Verschlüsselungstrojaner zuschlägt, kann man anhand dieser Snapshots sozusagen die Zeit zurückdrehen und so die unverschlüsselten Daten im Zustand vor dem Angriff wiederherstellen.

- **Daten beschädigt, verloren oder gar gelöscht**
  Ein Mitarbeiter hat drei Tage an einer Präsentation gearbeitet und dann passiert ein Unfall und die Datei ist weg, oder defekt. Aber sie wird bald dringend benötigt. Soll er jetzt alles von vorne erarbeiten? Das ist nicht nur frustrierend, sondern wirft auch alle Zeitpläne und Deadlines über den Haufen. Solche Situationen versetzen IT-Nutzer immer wieder in Panik. Datenverluste sind kaum zu vermeiden, und wenn man nicht vorgesorgt hat, ist guter Rat teuer. Zum Glück ist in den Cloud-Desktop-Systemen eines erfahrenen IT-Dienstleisters ein hochwertiges Backup-Konzept immer enthalten. Anwender klicken einfach auf den betreffenden Ordner, dann auf „Vorgängerversion wiederherstellen“ – und schon ist die vermisste Datei wieder da. Das System erstellt regelmäßig Sicherungskopien aller Daten, auf die Sie im Notfall jederzeit zugreifen können. Als Cloud-Betreiber kann ein IT-Dienstleister ein leistungsstarkes Backup-System günstig bereitstellen, da die Kosten unter all seinen Nutzern geteilt werden. Die Sicherung ganz unterschiedlicher Systeme ist möglich, etwa im Rechenzentrum des IT-Outsourcers, lokal beim jeweiligen Unternehmen oder bei weiteren Cloud-Diensten.

- **Technische Störung**
  Wer kennt dieses Problem nicht – ein Kunde wartet auf die versprochene Präsentation, sei es am Telefon oder im Konferenzraum – und ausgerechnet jetzt tritt eine technische Störung auf. Die Telefonleitung bricht zusammen, das Internet ist tot oder ein wichtiger Dienst wie Exchange Online, Dropbox oder ERP Online ist nicht erreichbar. Was nun? Wer seine EDV an einen IT-Dienstleister ausgelagert hat, dem steht der Kundendienst jederzeit zur Verfügung – auf Wunsch rund um die Uhr. Da sich die Techniker bestens auskennen und mit den betreffenden Systemen vertraut sind, können sie in kürzester Zeit das Problem eingrenzen und im direkten Kontakt mit dem betreffenden Lieferanten lösen. Selbst bei einem Internetausfall hilft der IT-Support des Dienstleisters weiter und setzt sich mit dem Provider in Verbindung, um die Störung so schnell wie möglich zu beheben.

- **Veraltete Hardware - und die IT in der Sackgasse**
  Jede Computer-Hardware ist irgendwann überholt. Und obwohl das Altern ein allmählicher Prozess ist, kann es sich auch in plötzlich auftretenden Problemen bemerkbar machen: Ein Unternehmen schafft eine neue wichtige Software an oder möchte ein Update installieren und muss feststellen, dass die alte Hardware dafür nicht leistungsfähig genug ist. Was nun? Eine Runde neue Hardware anschaffen und alles neu installieren? Wer seine IT an einen innovativen IT-Dienstleister auslagert, kann aufatmen, denn diese Situation wird nicht auftreten. Die Systeme der Anwenderunternehmen laufen auf der leistungsstarken Hardware des IT-Dienstleisters, die immer auf neuestem Stand ist und von den Experten gewartet wird. Die Mitarbeiter im Unternehmen benötigen lediglich minimal ausgestattete Endgeräte für den Zugriff auf ihren Cloud-Desktop – somit kann man das Problem der IT-Sackgassen ad acta legen.

- **Expansion steht an, aber wächst die IT auch mit:**
  Viele kleine und mittlere Unternehmen betreiben eine IT, die mit der Zeit gewachsen ist und den Anforderungen mehr oder weniger genügt. Doch wenn ein neuer Standort oder viele neue Mitarbeiter hinzukommen, erweist sich die Technik nicht als flexibel genug oder es fehlt am Know-how, um das komplette System nahtlos zu skalieren. Es dauert „ewig", bis am neuen Standort alles läuft, die Mitarbeiter sind frustriert und für Wochen liegt die Produktivität im Argen. Ganz anders eine Cloud-Desktop-Lösung: Sie skaliert schnell und mühelos. Da die gesamte IT im Rechenzentrum des IT-Dienstleisters läuft, ist die Einrichtung eines neuen Firmenstandortes sehr einfach: Benutzer anlegen, Applikationen freigeben und Rechte vergeben – und fertig ist die Umgebung. Vor Ort muss nur ein einfaches Netz aufgebaut werden. Mit passenden Endgeräten (Thin Clients) und Monitoren sind die Mitarbeiter innerhalb von einem Tag startklar. Keine zusätzlichen Installationen, keine neue Serverhardware und keine besonderen Anforderungen an die Internet-Leitung. Perfekt.

Ausblick

Vor allem kleine und mittelständische Unternehmen stehen vor der Frage: „Lohnt sich für das Homeoffice-Projekt der Einsatz eines IT-Dienstleisters? Sprengt das nicht die Kosten und kann ich mir in der Corona-Zeit eine solche zusätzliche Belastung überhaupt leisten?

Aber auch wenn die Unterstützung durch einen externen Dienstleisters Kosten nach sich zieht, sollten Unternehmer die Risiken abwägen, wenn sie bei den Themen IT-Sicherheit und Datenschutz eher nach Bauch als nach konkretem Wissen vorgehen. Zudem lassen sich bei den Kosten in den meisten Fällen – Stichwort Lizenzen – Einsparungen erzielen, so dass sich die Wahl eines DaaS in der Praxis sogar als die günstigere Option erweist.

Wer alle Chancen der Digitalisierung optimal nutzen möchte, sollte einen IT-Dienstleister wie netzbest hinzuziehen. Er bietet Beratung beim Aufbau und Betrieb einer professionellen IT-Infrastruktur und sorgt mit seinen Cloud-Lösungen für stabile und sichere Anwendungen im gesamten Unternehmen.

Bei allen Produkten setzt netzbest auf das Konzept „IT as a Service", das heißt: Der IT-Dienstleister installiert und betreibt IT-Arbeitsplätze bei sich im Rechenzentrum. Der Vorteil für die Kunden: Sie brauchen keine Hardware bestellen, keine Software pflegen und keinen Support aufbauen. Und alle Anwendungen laufen auf sicheren Servern in Deutschland.

Mit dem „IT-as-a-Service Konzept" und dem damit verbunden Ansatz, die IT für Kunden zugänglich zu machen, wurde netzbest bereits 2014 in der Kategorie „IT-Service" beim Innovationspreis unter tausenden Bewerbern als Sieger ausgezeichnet. Somit blickt man bei netzbest auf eine jahrelange Erfahrung in diesem Bereich zurück.

Haben Sie noch Fragen?

Tel. +49 30 80 20 81 30
beratung@netzbest.de

Illustrations designed by slidesgo and stories / Freepik