Ins Home Office – dank Cloud-only Strategie

Know-how Wenn die ganze Belegschaft auf einen Schlag ins Home Office muss, kann das für eine IT-Umgebung unter Umständen zur Feuerwehrübung werden. Die Experten erklären, wie man mit Microsoft-Bordmitteln einen flexiblen Arbeitsplatz für dezentrales Arbeiten bereitstellt.

Von Adrian Keller und Roman Jungi

Seine Arbeitnehmer ins Home Office schicken zu können, ist nicht selbstverständlich. Es stellen sich viele Fragen bezüglich der Produktivität der Mitarbeitenden, ihrer Zufriedenheit oder der Zusammenarbeit im Team. Und aus IT-Sicht kommen zu den genannten Fragen nochmal gefühlte 1000 Fragen dazu: Wie gewährleisten wir einen sicheren Zugriff auf unsere Unternehmensdaten aus der Ferne? Wie gehen wir vor, wenn ein Mitarbeiter sein Gerät verliert? Und wie stellen wir eine mobile Umgebung bereit, die sowohl Benutzerfreundlichkeit als auch einfaches Client Management garantiert?

Diese Fragen sind im Kontext grosser, lokaler Unternehmensdomänen seit vielen Jahren mehrheitlich geklärt, Best Practices wurden etabliert. Der Use Case einer mobilen, skalierbaren und gänzlich Cloud-basierten IT-Umgebung aber hat sich erst in den letzten Jahren zu einem wichtigen Bedürfnis von Unternehmen respektive deren Mitarbeitern entwickelt. Und wie die Coronakrise in der ersten Jahreshälfte 2020 gezeigt hat, kann ein solcher Anspruch auch durch äussere Faktoren entstehen.

Windows als Betriebssystem und die Office Suite als primäre Büro-Software haben sich hierzulande mehrheitlich durchgesetzt. Ausserdem hat Microsoft in den letzten Jahren mit einer Barrage an kompatiblen Cloud-Diensten und einem ganzheitlichen Angebot ein Cloud-only-Ökosystem lanciert, in dem kleine und mittlere IT-Umgebungen mit überschaubarem Aufwand eine mobile und trotzdem vollwertige Unternehmens-IT aufbauen können. Es ist damit heute verhältnismässig einfach, einen Arbeitsplatz auf Cloud-Basis bereitzustellen, der diesen Ansprüchen genügt – gerüstet für den Einsatz auf Geschäftsreisen, auf Montage und natürlich im Home Office.

Aufs Maximum reduzieren

Die der Schweiz auferlegte Home-Office-Pflicht in der ersten Jahreshälfte 2020 hat einen wichtigen Grundsatz zu Tage gefördert, der uns noch lange begleiten und vielleicht gar zum Standard der Unternehmens-IT wird: Es muss im Prinzip egal sein, wo sich ein Mitarbeiter aufhält, um seiner Arbeit vor dem Bildschirm nachzugehen.

Für kleinere Unternehmen durchaus eine Herausforderung. Nur schon für eine gemeinsame, immer erreichbare Dateiablage mussten früher ein lokaler Share und die entsprechenden sicheren Verbindungen oder ein Cloud-Produkt eines Drittherstellers integriert werden. Mehr Lizenzen, mehr Angriffsoberfläche, mehr Engineering, mehr Probleme.

Die erklärten Ziele sind damit eine Reduzierung auf möglichst wenige Anbieter, garantierte Kompatibilität, eine Reduktion der lokalen Infrastruktur und eine überschaubare Know-how-Pflege im Unternehmen. Hier kommt der Cloud-only-Ansatz ins Spiel, den Microsoft seit einigen Jahren massiv forciert.

Im Wesentlichen basiert dieser auf Microsoft 365 (ehemals Office 365) und den damit verbundenen Services. Mit Word, Excel und Powerpoint wird ein Grossteil der Büroarbeit ausgeführt, die Kommunikation findet über Teams und Outlook (Exchange Online) statt, die Client Security übernimmt unter anderem der Windows Defender und Sharepoint dient im Zusammenspiel mit Onedrive als Intranet respektive File Share im Unternehmen. Die Services sind eng verzahnt und arbeiten auf einer zentralen Cloud-Plattform (Azure) miteinander. Gleichzeitig gibt es unzählige Schnittstellen, die im Falle spezifischer Anforderungen die Integration von Dritt-Software ermöglichen. Seit 2019 gibt es auf Wunsch die Microsoft Cloud übrigens auch aus Schweizer Datenzentren.

Plug and Play

Für ein KMU mit überschaubaren Anforderungen bietet die Cloud-Lösung von Microsoft heute ein Rundum-Sorglos-Paket, das in kürzester Zeit die grundlegenden Bedürfnisse eines Unternehmens abdeckt. Ein Beispiel: Für ein Kleinunternehmen, beispielsweise in der Baubranche, kann in ungefähr einem halben Tag eine vollumfängliche IT-Umgebung bereitgestellt werden. Dies beinhaltet alle notwendigen Grundstrukturen für eine funktionale Unternehmens-IT, inklusive Security-Massnahmen, File Share, Office Suite, Mail Accounts, Single-sign-on-Zugang und Kollaborations-Features.

Das eröffnet gerade kleinen Unternehmen neue Möglichkeiten, beispielsweise bei der Gründung, Expansion oder wenn eben schnell ins Home Office gewechselt werden muss. Der Cloud-basierte Arbeitsplatz ist mit dem entsprechenden Know-how heute wahrlich «Plug and Play» und in enorm kurzer Zeit betriebsbereit. Auch entfallen mit der Eliminierung lokaler Server-Infrastrukturen die Anschaffungskosten und die Lifecycle-Pflege ebendieser. Das bedeutet für die IT-Abteilung weniger Troubleshooting, weniger Security Engineering und damit auch oft sinkende Kosten und Risiken.

Der User in der Mitte

Der vielleicht wichtigste Punkt, um diesen Lösungsansatz aus Engineering-Sicht zu verstehen, ist, dass das Endgerät im Kontext der Cloud beinahe irrelevant geworden ist. Es steht damit nicht mehr das Gerät, sondern der Benutzer im Mittelpunkt. Dies ist etwa am Beispiel von Firmen-Policies gut ersichtlich: Diese werden nicht mehr zwingend explizit auf den lokalen Client angewendet, sondern beziehen sich auf die Verbindung zwischen dem Benutzer und der Cloud-Instanz.

In der Folge spielt es eine untergeordnete Rolle, mit welchem Gerät die Mitarbeiter auf die Umgebung zugreifen. Bring your own Device (BYOD) ist heute nicht mehr das Buzzword, das es einmal war, sondern schlicht Realität: Nur schon indem Mitarbeiter mit dem privaten Smartphone auf ihre Geschäfts-Mails zugreifen, steigen firmenfremde Geräte verhältnismässig tief in die Business-IT ein.

Ein Beispiel aus aktuellem Anlass: Durch die unlängst bekannt gewordenen massiven Sicherheitslücken in der iOS Mail App musste in kurzer Zeit zahlreichen Mitarbeitern die Nutzung der App untersagt werden. Mit der erwähnten Policy-Struktur kein Problem – denn die Cloud-Instanz registriert, woher der (im Zentrum stehende) User sich einloggt. Und wenn das aus der iOS Mail App passiert, erhält er keinen Zugang – so einfach kann Security sein.

Das Beispiel ist auch aus dem vorhergegangenen Punkt interessant. Es war im Kontext der Sicherheitslücke nicht notwendig, die iPhones der Mitarbeiter vollumfänglich zu managen, um die Security-Richtlinie umzusetzen. Denn die Policy sitzt auf dem User und regelt dessen Zugriff auf die Cloud, das Gerät (und in diesem Fall sogar das Betriebssystem) ist irrelevant.

Trotzdem lassen sich Geräte natürlich auch vollständig fernverwalten, wenn sie entsprechend integriert werden. Unter registrierten Geräten versteht man eine weiche Kontrolle mit Policies, wie beim oben genannten Beispiel. Wenn ein Gerät als fully managed integriert wird, lässt es sich komplett aus der Ferne verwalten, etwa zur Wiederherstellung (Wipe & Reset), zum Löschen aller Firmendaten (Remote Business Data Wipe) oder für das Security Monitoring in Echtzeit.

Die Management-Ebene

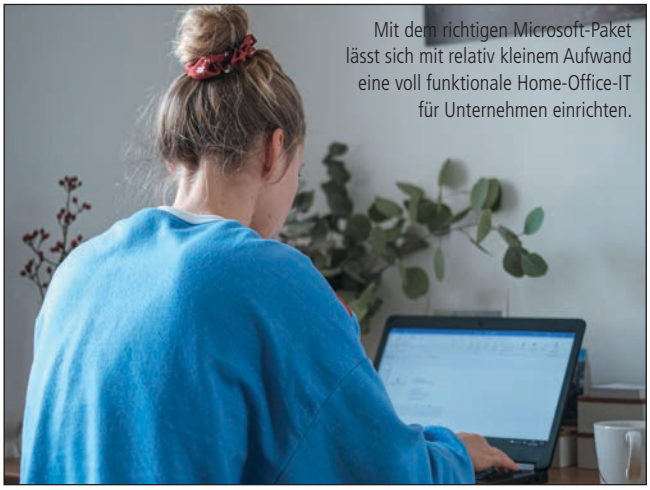
Aus Engineering-Sicht ist das Herzstück einer solchen Cloud-Infrastruktur die Management-Plattform Intune. In Kürze ist Intune der kleine, Cloud-basierte Bruder des Management-Molochs Microsoft Endpoint Configuration Manager (früher System Center Configuration Manager) von Microsoft, der in grossen Unternehmen mehrheitlich als Client Management Tool eingesetzt wird. Das Tool dient unter anderem zur Verteilung von Software und Patches und übernimmt die Inventarisierung von Soft- und Hardware. Weiter können damit die oben erwähnten Richtlinien definiert und Sicherheitsvorgaben und -Massnahmen umgesetzt werden, was Intune zum Cloud-Pendant von Group Policy Management macht. Hierzu gehören unter anderem die Konfiguration von Windows Defender (Antivirus) sowie Richtlinien zur WiFi-Nutzung, Geräteverschlüsselung und Windows Hello (z.B. Fingerprint-Login). Neben Intune hilft Autopilot bei der Bereitstellung von bestehenden und neuen Clients.

Ein weiterer wichtiger Bestandteil ist Azure AD, das Pendant zu Active Directory (AD), wie man es aus lokalen Domänen kennt. Azure AD dient als Identity Provider aus der Cloud, ist also für die Benutzer-, Geräte- und Gruppenverwaltung sowie die Kontrolle über Zugriffe und Berechtigungen für Clients und User verantwortlich. Weitere Aufgaben von Azure AD sind etwa das Passwort-Management und die Mehrfaktorauthentifizierung (MFA). Azure AD lässt sich im Fall einer Hybrid-Architektur übrigens auch mit dem On-Prem AD synchronisieren.

Zusammenarbeit im Team

Unified Communications (UC) ist ebenfalls ein enorm wichtiges Thema, wenn es um Arbeit in dezentralen Firmenstrukturen geht. Die Microsoft-Lösung hierfür besteht aus der Interaktion der bereits genannten Produkte wie Outlook für den E-Mail-Austausch, Teams für Instant Messaging, Voice- und Video-Konferenzen sowie Sharepoint für Kollaboration an Dokumenten. Gerade in Zeiten der Isolation sind Videochats und der schnelle Austausch mit Kollegen – etwa mit Microsoft Teams – ein notwendiges Element für Mitarbeiterzufriedenheit und Produktivität. Aber wie steht es um das Engineering und die Integrationstiefe in die restliche Umgebung?

Mit sehr überschaubarem Aufwand kann eine Teams-Instanz initiiert werden und ist in kurzer Zeit einsatzbereit. Falls nötig, erlaubt die Management-Konsole dann granulare Einstellungen, etwa für das Setzen von Berechtigungen. Ausserdem ist Teams tief in die restliche Microsoft-365-Welt integriert: Sharepoint und Onedrive sind als Account-übergreifende Datenablage in Teams verbaut, weiter hat das UC Tool Zugriff auf den Outlook-Kalender, die Meeting-Planung, das ERP Dynamics und Schnittstellen zu einer Vielzahl 3rd-Party-Produkten wie Code Repositories oder CRM Tools. Mit etwas Mehraufwand und zusätzlichen Lizenzen kann auch die gesamte VoIP-Telefonie des Unternehmens in Teams integriert werden.



Mit dem richtigen Microsoft-Paket lässt sich mit relativ kleinem Aufwand eine voll funktionale Home-Office-IT für Unternehmen einrichten.

Blech kostet keine Miete

Es liegt auf der Hand – wer zu Miete wohnt, macht auf lange Sicht einen schlechteren Deal als ein Hauseigentümer. Bei der Frage, ob man eigene Server betreiben (kaufen) oder die Cloud Services beziehen (mieten) will, wird es aber etwas komplizierter. Je nach Anforderungen, etwa wenn man strengen Regulatorien unterliegt, können Security-Bemühungen das Budget eines KMU überlasten. In der Cloud stellt der Provider eine Security-Basis sicher, im Falle der Azure Cloud also Microsoft. Auch

wächst kaum eine Wohngemeinschaft so schnell, wie das manche Firmen tun, daher ist schnelle und flexible Skalierung ohne grosse initiale Investition, etwa in Form weiterer Server-Ressourcen, ebenfalls ein entscheidender Faktor.

Für die genaue Errechnung, wie sich die Kostenlast bei der Umstellung auf das Cloud-Modell verschiebt und welches Modell für ein Unternehmen geeignet ist, empfiehlt es sich, einen Cloud-Experten, zum Beispiel einen Microsoft-Partner, zu Rate zu ziehen. Es existieren schlicht zu viele Variablen, um eine allgemeingültige, fundierte Aussage über den Kostenvergleich von On-Prem zu Cloud zu treffen. Beispiele solcher Faktoren sind neben den Security-Anforderungen unter anderem Sizing und Leistung der Server, Laufzeit und Verfügbarkeit, Lizenzen und Backups.

Das Klumpenrisiko

Das Microsoft-Modell aus der Cloud kommt als umfassende Lösung, mit der einfache Business Cases auf Windows-Basis mit äusserst wenig Aufwand umgesetzt und effizient gepflegt werden können. Dank den offenen Schnittstellen und Windows als etabliertem Betriebssystem ist sie ausserdem beliebig erweiterbar und skaliert schnell, falls nötig. Die Microsoft Cloud ist flexibler und resilienter als lokale Infrastruktur und eignet sich daher perfekt für den Einsatz im Home Office.

Ein zu bemerkender Minuspunkt ist aber ein wachsendes Klumpenrisiko (Provider Lock-in), denn die Abhängigkeit zu Microsoft wächst natürlich entsprechend. Problematisch können hier etwa unerwartete Änderungen am Lizenzmodell, den Features oder an den Preisstrukturen sein. Und letztlich belasten die Lizenzen auch die jährlichen Fixkosten, stehen aber einem reduzierten Budget für interne Infrastruktur gegenüber.

Wer als Kleinunternehmen bereits vor der Krise den Schritt ins Cloud-only-Ökosystem von Microsoft gewagt hat und notgedrungen ins Home Office wechseln musste, hat im Nachhinein eine unbezahlbare Entscheidung getroffen: Als Corona die Wirtschaft international auf den Kopf stellte, konnten diese Unternehmen ohne jegliche Einbussen von einem Tag auf den nächsten ins Home Office wechseln. Und das ohne, dass ein Engineer auch nur einen Finger krümmen musste. ■

DIE AUTOREN

Adrian Keller ist Senior System Engineer und Mitglied der Geschäftsleitung beim Workplace-Spezialisten Clearbyte. Er ist ein ausgewiesener und zertifizierter Microsoft-Client-Spezialist und hat mehr als 20 Jahre Engineering-Erfahrung durch diverse Projekte bei Gross - und Kleinkunden.

Roman Jungi ist System Engineer bei Clearbyte und ist zertifizierter Spezialist für virtualisierte IT-Umgebungen und Client Engineering mit Microsoft 365, Azure und Citrix.