Herausforderungen in Zeiten nomadischen Arbeitens

Durch eine freie Gerätewahl, die zunehmende Verlagerung ins Home Office und allgemein das Arbeiten von unterwegs sehen sich Unternehmen mit komplexen Anforderungen an den Gerätesupport und das Lifecycle-Mangement konfrontiert.

Text: Patrick Trevisan

Der Trend zu Remote-Arbeit bleibt ungebrochen. Zwar gewähren längst nicht alle Unternehmen ihren Mitarbeitenden in gleichem Masse das Home Office als Arbeitsoption wie während der Covid-19-Pandemie. Dass aber ein Grossteil der Mitarbeitenden heute mehr Freiheiten bezüglich Arbeitsplatz- und Arbeitszeitgestaltung von ihren Arbeitgebern erwarten, ist eine Tatsache. Hinzu kommt, dass mittels mobilem Computing und der Verlagerung in die Cloud die Digitalisierung von Arbeitsabläufen unumgänglich wird, um die Wettbewerbsfähigkeit der Unternehmen aufrechtzuerhalten. Alles in allem hat dies für die IT-Dienstleister, seien dies nun interne IT-Abteilungen oder externe Partner, eine Steigerung der Komplexität auf diversen Ebenen zur Folge. Die Anforderungen an die Sicherheit der Unternehmensdaten und an den Support werden durch die unterschiedlichen Arbeitsumgebungen, den Infrastruktur- und Gerätemix umfassender. Unternehmen lassen Mitarbeitende von unterwegs oder im Home Office arbeiten und geben dadurch die Kontrolle über die Cybersecurity ihres Unternehmensnetzwerks aus den Händen, im Speziellen, wenn Unternehmen ihr Datacenter in der Cloud betreiben. Vor allem aber setzen Unternehmen, die traditionell früher eine reine Windows-Strategie fuhren, mittlerweile in gewissen Abteilungen und im Sinne von CYOD (Choose Your Own Device) oder BYOD (Bring Your Own Device) auf zusätzliche Plattformen wie MacOS bei Laptops sowie Android und iOS bei Smartphones und Tablets.

Gesamtkosten so gut wie unbekannt

Allerdings herrscht nach wie vor in vielen Unternehmen eine falsche Vorstellung über die tatsächlichen Kosten, die die Bereitstellung von Services für die Mitarbeitenden auf mobilen Endgeräten verursacht. Viele Verantwortlichen schauen nur auf die teilweise für gewisse Geräte verhältnismässig geringen Kosten für Beschaffung und für die Mobilfunk- und Daten-Abos. Vielen IT- Entscheidungsträgern ist nämlich nicht bewusst, dass mobile Geräte neben der Beschaffung von Hardware und SIM-Karten der Telekommunikationsanbieter für die Abonnemente sehr viel versteckte Aufwände generieren. Verpflichten sich Unternehmen aber dazu, ihren Mitarbeitenden mobilen Support zu bieten und sie bei Unwägbarkeiten mit den Geräten und Apps zu unterstützen, müssen über die harten Kosten für Hardware, Software und Wartungsverträge auch Supportkosten für Lifecycle-Supportdienste, Ersatzteilpools oder den Helpdesk mitgerechnet werden. Ebenso gehören zur Wahrung der Kostentransparenz Produktivitätsverluste oder übermässiger Zeitaufwand für das IT-Management mitberechnet.

Mobilgeräte verursachen Arbeit

Damit zu den nackten Tatsachen: Einem 2021 von VDC Research veröffentlichten Bericht zufolge beträgt der Anteil der Kosten für Hardware und Software-Lizenzen bei mobilen Geräten lediglich die Hälfte der TCO (Total Cost of Ownership). Allein die Supportkosten betragen bis zu 43 Prozent – 17 Prozent durch Reparaturen und 26 Prozent gehen zu Lasten von IT-Services wie Bereitstellung, Konfiguration, technischem Support und Lifecycle Management. Zusätzlich führen die Marktforscher an, dass Arbeitsunterbrechungen mindestens 8 Prozent der Gesamtbetriebskosten ausmachen. Um die tatsächlichen Kosten zu kennen, müssen allerdings sämtliche Aspekte hinsichtlich Beschaffung, Wartung, Betrieb und Infrastruktur in die Rechnung einfliessen. Mobilgeräte verursachen über ihren Le-

benszyklus hinweg in den verschiedenen Abteilungen mehr Kosten, als sich meisten Verantwortlichen in den Unternehmen bewusst sind. Es herrscht vorwiegend keine Kostentransparenz. Für Beschaffung, Nutzerauthentifizierung, Geräteregistration, Inventarisierung, Konfiguration, Distribution von Kontroll- und Sicherheitseinstellungen, Management der Apps über Support, Monitoring, Reporting und Compliance, das Reparatur-Handling bis hin zu Ausserbetriebsetzung, Recycling oder Vernichtung der Geräte fallen gemäss dem Report in Unternehmen jährlich mindestens 4 bis 5 Stunden pro Mobilgerät an. Bei einer Firma mit 50 Mitarbeitenden, welche ein Smartphone und einen Laptop benutzen, bedeutet das jährliche Kosten in der Höhe von mindestens 50 Arbeitstagen.

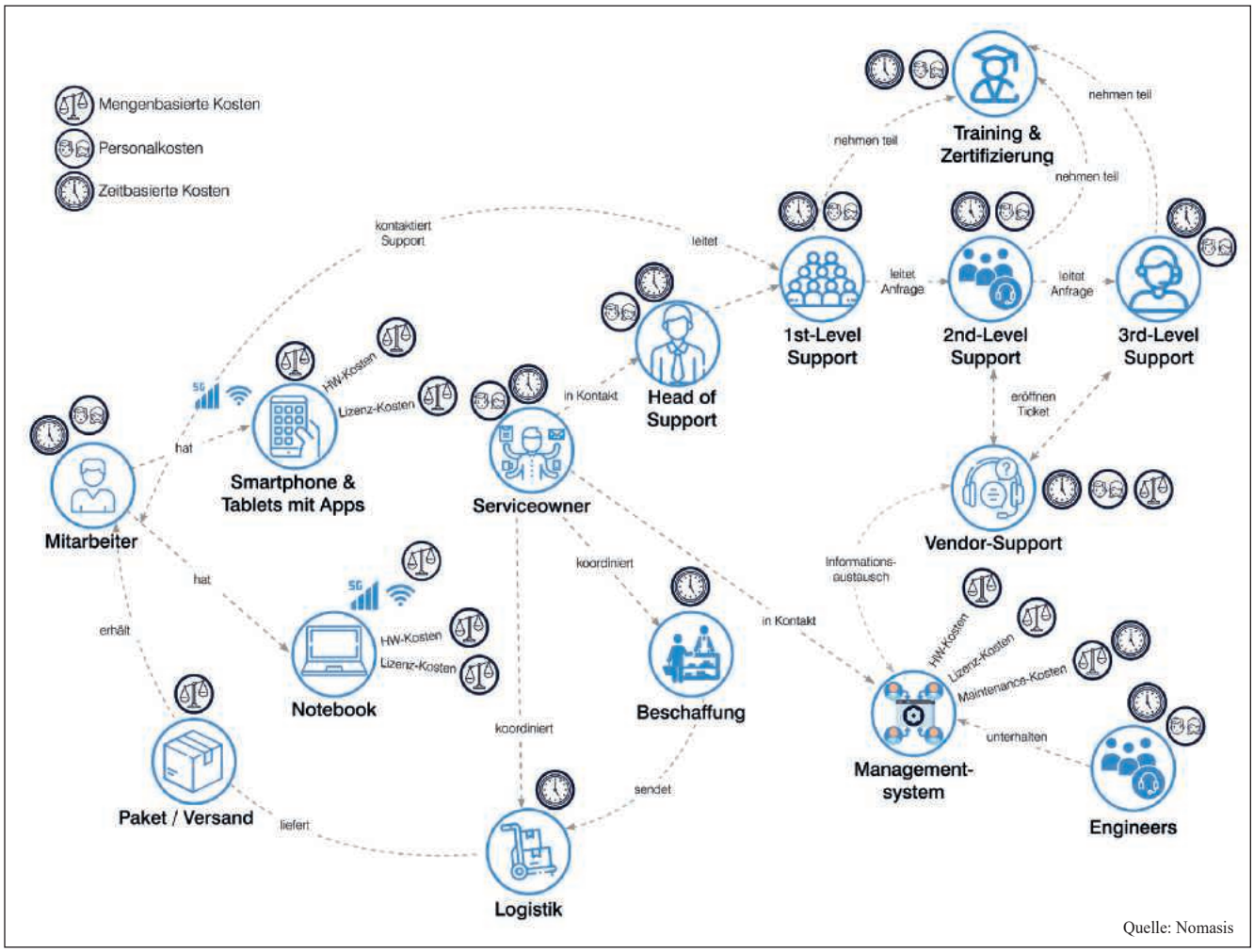
Auslagerung an Partner

Entsprechend müssten Support-Organisationen heute eigentlich Support für Macbooks, iPads, iPhones und Android-Smartphones und -Tablets anbieten. Während auf der einen Seite die Varietät an Gerätemodellen, Plattformen, Versionen von Betriebssystemen und Apps für Geschäftsprozesse ständig zugenommen hat, fehlt es aber meistens beim Support am notwendigen Wissen. Wenn man aber deshalb nur einen minimalen Support auf Geschäftsfunktionen für MacOS, iOS und Android anbietet, riskiert man wiederum mehr Support-Anfragen und unzufriedene Nutzer. Entscheiden sich Unternehmen hingegen dazu, ihren Mitarbeitenden ein ausgezeichnetes Nutzererlebnis zu bieten, geschieht dies idealerweise damit, intern beim Support eine Windows-Strategie zu verfolgen und Nutzer anderer Geräte über einen externen Supportpartner zu bedienen. Ein solcher ist auf seinem Gebiet spezialisiert und kann über den Support hinaus auch das Geräte-, Infrastruktur- und Lifeecycle-Management übernehmen.

Geräte professionell verwalten

Insbesondere Apple-Rechner, iPads und iPhones werden zu hohen Kosten beschafft, und mit grösserem Aufwand manuell aufbereitet. Nicht selten werden diese und auch andere Nicht-Windows-Geräte nur unvollständig oder gar nicht ins Unternehmensnetzwerk eingebunden. Auch das führt dazu, dass bezüglich Verwaltung und IT-Sicherheit die Kontrolle abhandenkommt, wenn nicht gar den Mitarbeitenden fahrlässigerweise Administratoren-

Über den gesamten Lebenszyklus hinweg verursachen mobile Geräte in vielen Abteilungen der Unternehmen versteckte Kosten.



Quelle: Nomasis

rechte auf den Arbeitsgeräten gewährt werden, damit diese selbst Konfigurationen ändern oder Apps und andere Software installieren können. Um ihren Mitarbeitenden im Angesicht der steigenden Anforderungen der Digital Natives möglichst gerecht zu werden, riskieren Unternehmen so ein erhöhtes Sicherheitsrisiko durch Kompromittierung der Geräte, Verletzungen von Datenschutzrichtlinien und nicht zuletzt einen Anstieg des Aufwands für Support und Lifecycle Management. Um alle Geräte in den Griff zu bekommen und die Zahl der Supportanfragen zu reduzieren, bedarf es unbedingt einer Verwaltung über entsprechende MDM- (Mobile Device Management) respektive UEM-Lösungen (Unified Endpoint Management). Die Einbindung aller Geräte in die Geräteverwaltungssoftware erlaubt eine effiziente Verteilung der Apps und eine Zero-Touch-Provisionierung. Support-Anfragen entfallen, weil die Anwender im Handumdrehen Zugriff auf IT-Ressourcen erhalten.

Self-Service-Portale

Selbstverständlich kann man mit Selbstbedienungsportalen gewisse Prozesse automatisieren. Allerdings funktioniert das nur für limitierte Probleme, zum Beispiel für automatisierte Supportprozesse wie das Installieren von Apps oder den Austausch von Geräten, Reparaturen, Verwaltung der Mobilfunkabonnemente, das Bestellen einer SIM-Karte oder von Zubehör et cetera. Allerdings ist in der Regel im Hintergrund immer auch jemand aus einer Unternehmensabteilung damit beschäftigt – sei dies nun im Einkauf, der Logistik, dem Personalwesen, dem Support oder gar dem Engineering. Kommt ein Nutzer aber nicht ins Netz oder eine App funktioniert nicht, wie sie sollte, dann nutzt ihm das Portal im Moment wenig. Bestenfalls kann er ein Support-Ticket absetzen und wartet dann auf die Lösung des Problems. Gerade wenn es sich um Apple- oder Android-Geräte handelt, ist dann der Support in der Regel überfordert.

Dokumentation ist ein Problem

Der Support-Mitarbeitende greift dann vielleicht auf Instruktionen zurück, die dafür irgendwann einmal erstellt wurden. Ist der Support aber nicht auf diese Geräte spezialisiert, sind solche Dokumentationen in der Regel veraltet, sodass die Anfrage zum 2nd- oder 3rd-Level-Support weitergeleitet werden muss. Denn eine App beispielsweise funktioniert auf MacOS anders als auf Windows, sie wird anders installiert und konfiguriert. Auf Smartphones und Tablets mit iOS oder Android sehen die Apps gleich nochmals anders aus. Benutzeranleitungen werden

kompliziert, sodass bei vielen Apps infolge der Fragmentierung der Dienste nicht mehr gemanaged werden kann. Für Selbsthilfeportale kann eine solche Breite an Dokumentationen auch zum Problem werden. Denn werden Apps in der Cloud geändert, ohne dass der Support davon weiss, kann es für den Nutzer schnell schwierig werden, wenn er sich mit veralteten Anweisungen selbst helfen soll. Darüber hinaus bietet der allergrösste Teil der Unternehmen nur Zugriff des Supports auf Windows-PCs, nicht aber auf andere Plattformen an. Denn was nützt es, wenn der Support auf das Smartphone, Tablet oder das Macbook zugreifen kann, sich damit aber nicht auskennt? Der Helpdesk-Mitarbeitende hat schliesslich nur wenige Minuten zur Verfügung, ein Problem zu lösen – danach muss der Fall eskaliert werden. Auf Drittsysteme spezialisierte Dienstleister können hingegen über die Integration in eine MDM-Lösung die Devices mit Software für Remote-Zugriff versorgen und schnell Hilfe bereitstellen.

Sicherheit im Home Office und von unterwegs verbessern

Mit dem Trend zur Verlagerung von Rechenkapazitäten in die Cloud verändern sich auch die Sicherheitsanforderungen. Hier kommt bei der Arbeit im Home Office oder unterwegs das Zero-Trust-Prinzip zum Tragen. Mit der erwähnten Verwaltung aller Geräte mit MDM- und UEM-Lösungen kann zum Beispiel das Smartphone als «Trust-Anker» für die sichere Authentifizierung der Nutzer und als Perimeter für die sichere Kommunikation mit den Unternehmensdaten verwendet werden. Denn wenn Mitarbeitende von ausserhalb auf Systeme mit Unternehmensdaten und -Ressourcen zugreifen, verlieren die Firmen die Kontrolle über die Einhaltung der Sicherheitsanforderungen. Private Netze, öffentliche WLANs oder Netze in nicht firmeneigenen Büros wie Coworking-Spaces können jederzeit zum Ziel von Cyberangriffen werden. Bei einer Cloud-First-Strategie, oder selbst wenn nur Teile der Unternehmens-IT in die Cloud ausgelagert werden, macht es aus technischer Sicht keinen Sinn, Methoden wie beispielsweise VPNs (Virtuelle private Netze) einzusetzen. Den Netzwerkverkehr über VPN in die Firmeninfrastruktur und wieder retour ins Home Office oder das Coworking-Büro zu leiten, ist überflüssig.

Vom Unternehmen oder spezialisierten Dienstleistern verwaltete Zugangspunkte ins Internet über ein Smartphone oder auch einem extra fürs Home Office bereitgestellten Router erlauben es, die Sicherheitsanforderungen des herkömmlichen Büroarbeitsplatzes auch darüber hinaus zu gewährleisten. Die Mitarbeitenden benötigen keine technischen Vorkenntnisse. Damit können private und Unternehmensdaten einfach getrennt und die Kontrolle der Netzwerkleistung beibehalten werden. Denn während in der Pandemie von Endkunden oder Mitarbeitenden noch verziehen wurde, wenn die Performance beim Datenverkehr schwächelte, wird heute erwartet, dass die Leistung der Infrastruktur unabhängig vom Aufenthaltsort der Mitarbeitenden besteht. Weder die Unternehmensleitung noch der Support kann Zeitverluste durch Arbeitsausfälle wegen mangelnden Services, unzufriedenen Mitarbeitenden oder verärgerten Kunden gutheissen.

Viele gute Gründe für Outsourcing

Während früher die Benutzer keine grossen Erwartungen an die IT hatten, sind Digital Natives heute viel anspruchsvoller. Es ist Support für Nutzer, nicht für die IT selbst, gefragt. Denn während früher über mobile Geräte bestenfalls auf E-Mail und Kalender zugegriffen wurde, gehören heute Apps für Businessprozesse zum Alltag. Multiplattformsupport für verschiedene Hersteller und Gerätetypen ist gefragt. Schlecht konzipierte Mobilitätslösungen – von der Geräteauswahl bis hin zum Anwendungsdesign, der Netzwerkleistung und der Support-Infrastruktur – haben Schatten-IT, Gefährdung durch Cyberattacken, Störung der Arbeitsabläufe, Arrbeitsausfälle, vermehrte Support-Anfragen, unzufriedenes Personal und nicht zuletzt ein Vertrauensverlust bei den Endkunden der Unternehmen zur Folge. All das führt zu versteckten Kosten. Unternehmen ihrerseits können über die genannten Verbesserungen hinaus vom Skaleneffekt des Dienstleisters profitieren und mit umfassenden, auf die Bedürfnisse der Firma abgestimmten DaaS-Leistungen ihre Beschaffungskosten hin zu Betriebskosten verlagern. Damit lassen sich Investitionsrisiken minimieren und die Ausgaben flexibel an die Budgets anpassen. Spezialisierte IT-Dienstleister haben deshalb viele gute Verkaufsargumente im Köcher. Von der Übernahme der Support-Dienste für Nicht-Windows-Systeme bis hin zu umfassenden Device-as-a-Service-Angeboten können sie die vorhandenen Lücken schliessen. ■

Der Autor

Patrick Trevisan ist Mobile Security Consultant und Head of Product Management bei Nomasis, einem auf Lösungen und Services für Cybersecurity und Enterprise Mobility spezialisierten Schweizer Dienstleister. Das Unternehmen bietet Managed Services in den Bereichen Cyber Security, Modern Workplace, Infrastruktur, Cloud- und End-User-Services an. Vor seiner Zeit bei Nomasis war Trevisan unter anderem bei der Zürcher Kantonalbank und bei Swiss Re als System Engineer und Business Engineer tätig.