IT-Infrastruktur

Ehrenamt – Whitepaper

Dokumenteninformationen

Herausgeber/Autoren:

Malteser Hilfsdienst e. V., Köln, zusammen.digital@malteser.org
Sven Dinglinger (Malteser), Heinz-Jörg Roling (SoCura), Kolja Scepanik (Skaylink), Sofiane Salmi (Skaylink), Sven Haase (Skaylink)

Dieses Dokument entstand im Rahmen des Programms **zusammen.digital**, welches durch das **Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)** gefördert wurde.

Inhalt

1 Management Summary

Die Digitalisierung bietet viele Vorzüge, wie etwa die stetige Verfügbarkeit von Daten und Informationen und die damit verbundenen Arbeitserleichterungen. Sie ist aber auch mit Herausforderungen verbunden, etwa im Hinblick auf Datenschutz und Fragen der Finanzierung. Vor dem Hintergrund des daraus entstehenden Spannungsfeldes hat das Projekt „IT-Infrastruktur Ehrenamt“ einen für den Malteser Verbund wichtigen Teil-Aspekt der Digitalisierung herausgegriffen, Anforderungen der Ehrenamtlichen ermittelt und denkbare technologische Lösungsszenarien entworfen und erprobt. Die Ergebnisse und Erkenntnisse haben Eingang in dieses Whitepaper gefunden.

Den Ausgangspunkt der Überlegungen bildete die bereits bestehende IT-Infrastruktur der Malteser. Im Kern handelt es sich dabei um ein Corporate Network (CN), über welches den Anwender*innen (mithilfe installierter Citrix-Client-Dienste) virtuelle IT-Arbeitsplätze mit Applikationen zur Verfügung stellt (Private Cloud) sowie zusätzlich eine Microsoft-365-Welt (Public Cloud).

Der Bedarf der Ehrenamtlichen wurde in zwei Workshops mit Helfenden erfasst. Dabei ging es um Fragen rund um die Arbeitsweise sowie die genutzten Geräte und Anwendungen. Es stellte sich heraus, dass dieser Bedarf an einigen Stellen von den Anforderungen des Hauptamtes abweicht. So besteht bei Ehrenamtlichen ein größerer Bedarf an der Offline-Nutzung von Daten und spielen privat genutzte Geräte (Stichwort BYOD – Bring Your Own Device) eine große Rolle.

Auf Basis der Ergebnisse der Anforderungsworkshops wurde eine Pilotphase geplant, in der den Teilnehmer*innen unterschiedliche Geräte (Notebooks, Tablets, Smartphones) auf Basis von Android, iOS und Windows zur Verfügung gestellt werden sollten. Die Diskussion über diverse technologische Bereitstellungsszenarien ergab am Ende vier Ansätze, die sowohl den Bedarf des Ehrenamtes erfüllten als auch den Anforderungen an eine professionell gemanagte IT-Umgebung (Supportfähigkeit, einfache Einrichtung und Handhabung, Schutz und Trennung von persönlichen und Unternehmensdaten) genügten:

- Virtueller Arbeitsplatz mit Azure Virtual Desktop
- Arbeitscontainer auf Android-Basis
- App Protection auf iOS und iPadOS
- Vollwertiges Notebook – Windows (SoCura-verwaltet)

Alle diese technologischen Ansätze entsprechen den Anforderungen der Malteser Richtlinie, die IT-Sicherheits- und Datenschutzfragen regelt.

Sie sollen auf den folgenden, ebenfalls die Anforderungen der ITK-Richtlinie erfüllenden, Microsoft-Technologien aufgebaut sein:

- Microsoft Endpoint Manager (MEM) als zentrales Client Management Tool

- Azure Active Directory (AAD) als zentraler Identitätsdienst für die Cloud-Verwaltung
- Bedingter Zugriff (Conditional Access), um alle Zugriffe gemäß einer Zugriffsdefinitionsverwaltung und einer Risikobeurteilung zu schützen
- Multi-Faktor-Authentifizierung (MFA) zur sicheren Authentifizierung und Autorisierung von Anwender*innen

Darüber hinaus mussten Lizenzierungsfragen betrachtet und bewertet werden: Eine allumfassende Lizenz von Microsoft bietet den vollen Funktionalitätsumfang (etwa auch bezüglich Sicherheit), übersteigt möglicherweise aber den finanziellen Rahmen, den die Malteser für IT im Ehrenamt vorgeben.

Die Bewertung der Pilotteilnehmer*innen nach Abschluss des Testzeitraumes fiel uneinheitlich aus. Es gibt keine eindeutig favorisierte Lösung, die wirklich alle Bedürfnisse abdeckt. In Summe decken die Szenarien die wesentlichen Anforderungen ab, wobei hierbei die – je nach Szenario teilweise erforderlichen – Lizenzerweiterungen und damit verbundene Kosten zu berücksichtigen sind.

Die aktuellen Microsoft Technologien decken grundsätzlich alle Einsatzbereiche und Bedürfnisse der Ehrenamtlichen ab. Aber erst im praktischen Einsatz der empfohlenen Lösung können Kennwerte wie Zuverlässigkeit, Umfänglichkeit, Sicherheit und Performance erfasst und Optimierungspotentiale anhand veränderter Benutzeranforderungen definiert werden.

2 Einleitung

Wie auch in allen anderen Organisationen und Unternehmen schreitet auch bei Hilfsorganisationen wie dem Malteser Hilfsdienst die Digitalisierung immer weiter fort. Mitarbeitende und Ehrenamtliche erleben Digitalisierung im beruflichen wie im privaten Umfeld, begegnen ihr mal positiv, mal vielleicht auch negativ und gestalten sie in unterschiedlichem Maße auch selbst aktiv mit. Dieses Spannungsfeld zeigt sich im Bereich der ehrenamtlichen Tätigkeiten – von den Helfenden in ihrer Freizeit erbracht – in besonderem Maße: Die Digitalisierung bietet Arbeitserleichterungen und Potenziale, ist aber auch mit Spannungen und Risiken verbunden.

Mit dem Thema IT-Infrastruktur für das Ehrenamt greift dieses Whitepaper einen grundlegenden Aspekt des Themas Digitalisierung heraus und erörtert ihn am Beispiel des Malteser Hilfsdienstes: Wie muss IT-Infrastruktur für Ehrenamtliche aussehen, damit Anforderungen erfüllt, Chancen genutzt und Risiken gesteuert werden können? Das Whitepaper basiert auf einer Zusammenarbeit des Malteser Hilfsdienstes, der SoCura – dem internen IT-Dienstleister der Malteser – und des Cloud- und Digitalisierungs-Pionier Skaylink, der Kunden messbare Mehrwerte aus der Cloud ermöglicht, für einen schnellen und sicheren Weg in die Cloud sorgt und die gesamte Cloud Journey bedient. Es gibt Antworten auf Fragen wie: Wo steht das Malteser Ehrenamt aktuell? Was sind aktuelle, aber auch zukünftige IT-Herausforderungen. Wie könnten die Lösungsansätze dazu aussehen und bewähren sich diese in der Praxis? Das Whitepaper ist aus einer Malteser-Perspektive heraus formuliert, die Ergebnisse sollen aber auch andere (Hilfs-) Organisationen unterstützen, die sich mit ähnlichen Herausforderungen konfrontiert sehen.

2.1 Wer sind die Malteser?

Die Malteser in Deutschland sind eine katholische Hilfsorganisation und Träger von stationären Einrichtungen des Gesundheits- und Sozialwesens. Mit über einer Million Mitgliedern und Förderern zählen die Malteser zu den großen karitativen Dienstleistern in Deutschland. Mehr als 80.000 Malteser – davon über 50.000 Ehrenamtliche – engagieren sich für Menschen in Notlagen. Sie leisten Erste Hilfe und kümmern sich um ältere, kranke und bedürftige Menschen. Herkunft, Religion und politische Überzeugung spielen dabei ebenso wenig eine Rolle wie die Gründe, warum die Menschen in Not geraten sind. Überwiegend ehrenamtlich geprägt sind der Zivil- und Katastrophenschutz, die Erste-Hilfe-Ausbildung, die Begleitung von alten, kranken oder benachteiligten Menschen sowie die Jugend- und Auslandsarbeit. Zu den sozialunternehmerischen Diensten gehören Rettungsdienst und Krankentransport, Hausnotruf und Menüservice. Die Malteser betreiben zudem Krankenhäuser, Altenhilfeeinrichtungen, Schulen und soziale Einrichtungen für Jugendliche, Suchtkranke und Asylsuchende.

Alle Dienste und Einrichtungen der Malteser sind gemeinnützig: Was erwirtschaftet wird, fließt zurück in die Hilfe für Menschen in Not. Die Malteser erfüllen ihren 950 Jahre alten Ordensauftrag in einer zeitgemäßen Form, die den Bedürfnissen der Menschen und den Rahmenbedingungen gerecht wird. Dazu gehört auch, dass die Malteser sich als Digitalisierungstreiber verstehen und ganz bewusst auf neue Technologien setzen, immer mit dem Ziel, Arbeitsabläufe zu verbessern und mehr Zeit für die eigentliche Kernkompetenz zu schaffen: die Arbeit mit den Menschen.

2.2 Wer ist die SoCura?

Die SoCura betreibt die gesamte IT-Landschaft der Malteser in Deutschland. Dabei betreut sie über 40.000 Nutzer*innen und leistet First-Level- bis Third-Level-Support für mehr als 200 Fachanwendungen. Die SoCura versteht sich als Vorreiter für die Wohlfahrt in Sachen Digitalisierung, Professionalisierung, Standardisierung und Zentralisierung der IT. Der Ansatz der SoCura, auf eine zentralisierte IT auf Basis hybrider Cloud-Technologien zu setzen, erleichtert nicht nur die Zusammenarbeit von Haupt- und Ehrenamtlichen, sondern hat sich auch in der Pandemie als krisensicher erwiesen. Mit Office 365 ist bei den Maltesern bereits seit 2013 ein kollaborativer Cloud-Dienst für das mobile Arbeiten im Einsatz. Die IT-Lösungen der SoCura zeichnen sich aus durch Flexibilität, Zukunftssicherheit sowie eine nachhaltige Informationssicherheitsstrategie.

Die SoCura möchte den Dienst am Menschen mit moderner Technologie, IT-Innovationen und Prozess-Know-how zielgerichtet unterstützen. Dafür gestaltet sie die Digitalisierung bei den Maltesern aktiv mit und teilt ihre Erfahrung und ihr Wissen mit anderen Wohlfahrtsorganisationen. Von diesem Austausch profitieren alle Beteiligten inhaltlich und wirtschaftlich, durch geteilte Kosten, Degressions- und Skalierungseffekte sowie größtmögliche Professionalität.

Als IT-Dienstleister für die Malteser ist die SoCura auch für die fast 50.000 ehrenamtlich Helfenden der Ansprechpartner für alle Fragen rund um die IT. Was anfänglich als begleitende Unterstützung (neben den Leistungen für die hauptamtlich Mitarbeitenden) begann, entwickelte sich immer mehr in Richtung Professionalisierung und Spezialisierung. Mit der Einstellung eines IT Business Partners (vormals Service Manager) speziell für ehrenamtliche Themen im Jahr 2016 wurde diese Entwicklung auch in personeller Hinsicht institutionalisiert und als weiterer Arbeitsschwerpunkt der Malteser IT innerhalb der SoCura etabliert. Ihre mittlerweile aus vielen Jahren resultierenden Erfahrungen im Bereich Ehrenamt lässt die SoCura tagtäglich in ihre Arbeit mit den Helfenden einfließen.

2.3 Wer ist die Skaylink?

In Skaylink haben sich vier erfahrene Cloud-Pioniere zu einem neuen europäischen Cloud und Digital Player zusammengeschlossen. Das Ziel: Den Kunden messbare, unternehmerische Mehrwerte aus der Cloud ermöglichen. Mit eigenen Frameworks, Methoden und softwaregestützten Tools sorgt Skaylink für einen schnellen und sicheren Weg in die Cloud und bedient die gesamte Cloud Journey.

Die Kunden sind so vielfältig wie die Projekte, die Skaylink realisiert: innovativer deutscher Mittelstand, Dax-40-Unternehmen, ebenso wie Bildungseinrichtungen, öffentliche Auftraggeber und gemeinnützige Organisationen, Vereine und Verbände. Kunden und Skaylink eint der Anspruch an die gemeinsame Arbeit: partnerschaftlich die angestrebten Ziele zu realisieren und die Zukunft aktiv zu gestalten – am besten durch langjährige partnerschaftliche Beziehungen.

Mit diesem Hintergrund und ihrer ausgewiesenen Cloud-Expertise ist Skaylink der ideale Partner und Impulsgeber für das im vorliegenden Whitepaper behandelte Projekt.

2.4 Die Vision: Was möchten wir erreichen?

Zukünftig sollen die von der SoCura angebotenen IT-Lösungen für Ehrenamtliche den im folgenden formulierten Ansprüchen genügen:

- Bewährte und neue, innovative Lösungen sollen sicher bereitgestellt und in den Alltag integriert werden.
- Dadurch sollen Automatisierungspotenziale genutzt werden und Arbeitserleichterungen für die ehrenamtlich Helfenden entstehen.
- Die gewählten Ansätze müssen mit den besonderen ethischen Aspekten der ehrenamtlichen Arbeit vereinbar sein.
- Oberstes Ziel ist es, mit unseres IT-Services Freiräume zu schaffen für die eigentliche Kernkompetenz der Malteser: die Arbeit mit Menschen.

Dass diese Vision nur im Zuge eines umfangreichen und dauerhaft angelegten Prozesses umgesetzt werden kann, versteht sich von selbst. Ein so großes und bedeutendes Thema wie die Neuausrichtung der IT-Infrastruktur für Ehrenamtliche ist ansonsten nicht umsetzbar. Es gilt, Lösungen für sehr unterschiedliche Aufgabenbereiche und Fragestellungen zu finden – immer vor dem Hintergrund des Spannungsfeldes von Sicherheitsaspekten, Fragen der Funktionalität und individuellen Bedarfen und Bedürfnissen. Die Lösungen müssen zu allen Beteiligten passen – zu den Helfenden, die als Anwender*innen auf unsere IT-Infrastruktur zurückgreifen, aber auch zu denen, auf die sich alle Überlegungen im Malteser Verbund konzentrieren: den Hilfebedürftigen.

Eine grundsätzliche Herausforderung ist die bei Infrastrukturlösungen zu berücksichtigende Heterogenität bei Anforderungen, Voraussetzungen und äußeren Einflüssen. Im Bereich des Ehrenamtes kommt sie in besonderem Maße zum Tragen. Ehrenamtlich Helfende tun dies in Ihrer Freizeit und in erster Linie, um Menschen zu unterstützen und ihnen zu helfen. IT-Lösungen und die dazugehörigen Infrastrukturen müssen deshalb begleitend, unterstützend und möglichst leicht und verständlich nutzbar sein, auch für nicht IT-affine Helfende. Andererseits verfügen auch viele Ehrenamtliche über digitales Wissen aus dem beruflichen und privaten Umfeld. Sie sind nicht nur bereit, digitale Lösungen auch im Ehrenamt einzusetzen, sondern wünschen sich dieses in vielen Fällen oder erwarten es sogar. Leicht bedienbar, nah an der konkreten Tätigkeit, aber ohne dabei durch zu starke Vereinfachung Potenziale zu verschenken – so der an dieser Stelle gewünschte Spagat.

Hinzu kommt eine grundsätzliche mit der Digitalisierung einhergehende Heterogenität der Herangehensweisen. Ob es um elektronische Gesundheitskarten, Kommunikationsmittel oder die Verfügbarkeit von mobilen Netzen geht, stets gibt es unterschiedliche Lösungsansätze, Produkte und Voraussetzungen. So ist das Mobilfunknetz in Deutschland noch immer nicht flächendeckend ausgebaut, was sich gerade auf das in diesem Whitepaper behandelte Thema der IT-Infrastruktur auswirkt und den erforderlichen lückenlosen und zuverlässigen Datenkreislauf erschwert. Diese Herausforderungen gilt es anzunehmen und dafür umfassende, aber gleichzeitig möglichst einfach umsetzbare Lösungen zu finden.

3 Vorgehensweise im Projekt

Im Zuge der Vorbereitung auf das Projekt haben sich zwei besondere Herausforderungen herauskristallisiert. Zum einen gilt es, von den Maltesern für das Ehrenamt bereitgestellte Hardware in die IT-Landschaft des Malteser Verbundes zu integrieren. Dabei kann nicht auf das bestehende Corporate Network zurückgegriffen werden, das die Organisationsdienststellen deutschlandweit vernetzt, da nicht jede ehrenamtliche Dienststelle daran angeschlossen ist.

Zum anderen ist eine ehrenamtliche Tätigkeit eng mit dem persönlichen Leben der Helfenden verknüpft und diese setzen häufig private Endgeräte ein (Stichwort BYOD – Bring Your Own Device). Die Kommunikationsmöglichkeiten müssen möglichst hürdenarm gestaltet sein und sich in den Alltag der Helfenden einfügen. Gleichzeitig sind – auch zum Schutz der Helfenden selbst – Sicherheitsrichtlinien und (IT-) Compliance-Vorgaben zu erfüllen. Und das alles, ohne allzu sehr in die Privatsphäre der Helfenden einzugreifen.

Dies sind beispielhaft nur zwei der wichtigsten Herausforderungen. Weitere Fragen ließen sich stellen, etwa nach der Finanzierbarkeit. In einem Umfeld, in dem Spendengelder zwar zur Verfügung stehen, in erster Linie aber ausgegeben werden sollen, um Menschen zu helfen, besteht häufig nur wenig Bereitschaft, in IT zu investieren – obwohl dies eigentlich den Hilfebedürftigen zugutekommen würde. Deshalb haben die Malteser gemeinsam mit der SoCura entschieden, ein Projekt aufzusetzen, das den aktuellen Sachstand ermittelt, Lösungen und Wege aufzeigt sowie ein Konzept für die flächendeckende Umsetzung bereitstellt, die im Anschluss an das Projekt erfolgen soll. Hier wird sich – unter Einbeziehung von Helfenden, Mitarbeitenden, der IT-Fachabteilungen, IT-Sicherheit, IT-Compliance und aller weiteren relevanten Stakeholder – endgültig zeigen, als wie praxistauglich sich das Konzept außerhalb der „Laborbedingungen“ des Projektes erweist bzw. ob Korrekturen und Nachjustierungen erforderlich sind.

3.1 Status Quo

Die IT-Infrastruktur der Malteser orientierte sich bislang an der stationären bundesweiten Dienststellen-Struktur , in der die Standorte an das Corporate Network (CN) der Malteser angebunden sind. Über das CN greifen Mitarbeitende überwiegend via Citrix auf bereitgestellte virtuelle IT-Arbeitsplätze zu (Private-Cloud-Zugriff). Dort haben sie Zugriff auf Fachapplikationen und können auch mit besonders schützenswerten Daten sicher arbeiten. Anwender*innen, die mit weniger sensiblen Daten zu tun haben – zum Beispiel auch Ehrenamtliche – arbeiten in der Public Cloud (Microsoft 365). Es kommt somit eine hybride IT-Cloud-Architektur zum Einsatz, die unter dem Namen Malteser.Cloud bekannt ist. Da für Vielnutzer*innen der Zugriff auf die Private Cloud in der Regel unverzichtbar ist, hat sich das Vorhandensein einer CN-Anbindung als zentrale Zugangsvoraussetzung zur Nutzung der Malteser IT-Infrastruktur, insbesondere der Hardware, etabliert. Die daraus erwachsenden Kosten sind nicht für jede ehrenamtliche Dienststelle refinanzierbar und die Anbindung auch nicht in allen Fällen notwendig, unter anderem auch, da im Ehrenamt häufig von zuhause gearbeitet wird. Auch in diesen Fällen kann allerdings von einer zumindest zeitweise gegebenen Verfügbarkeit eines Internetanschlusses ausgegangen werden, der zum Beispiel für die erste Einrichtung, zur Durchführung von Updates usw. verwendet werden kann. Für den Einsatz von ausschließlich über das Internet verwalteter Hardware fehlt derzeit allerdings noch die Infrastruktur. Eine solche Verwaltung würde, neben den Abrechnungsmodalitäten, den gesamten Lebenszyklus der Hardware umfassen, von Auslieferung, Einrichtung, Updates über Fehlerbehebung und ggf. Bereitstellung eines Tauschgerätes, bis hin zur

Rückgabe von Leasinggeräten bzw. deren Austausch. Alle diese Schritte sind einzeln zu betrachten und dafür die benötigten Voraussetzungen zu schaffen.

3.2 Aufgabenstellung

Das Projekt soll für den Malteser Hilfsdienst innerhalb der SoCura die Voraussetzungen für eine zukunftsfähige und kostengünstige IT-Infrastruktur für das Ehrenamt schaffen. Für alle Beteiligten sollen spürbare Verbesserung der bestehenden Situation erzielt werden. Da die Malteser, sowohl im Haupt- als auch im Ehrenamt, in vielen Bereichen bereits mit Microsoft 365 arbeiten, soll Microsoft 365 als Basis auch für die hier zu entwickelnde Infrastruktur-Lösung fürs Ehrenamt dienen. Im Rahmen des Projektes sollen die aus der ehrenamtlichen Arbeit entstehenden Anforderungen an die Infrastruktur erfasst werden, dafür passende Lösungsansätze entwickelt und anhand eines Proof of Concept (in Form einer Pilotphase) deren grundsätzliche Durchführbarkeit in der Praxis erwiesen werden. Weiterhin sollen – in einer oder in mehreren kleinen Dienststellen – „Blaupausen“ für die technische Administration geschaffen werden, mithilfe derer dann jeweils weitere Endgeräte für das Ehrenamt eingebunden werden können.

3.3 Unsere Strategie

Die Vorgehensweise lässt sich in fünf Schritte unterteilen:

- Kick-off-Workshop mit den Projektbeteiligten1: Klärung der Verantwortlichkeiten, Rollen, Aufgaben und Kommunikationswege im Projekt sowie Verschriftlichung der konkreten Zielsetzung
- Analyse- und Anforderungsworkshops: sowohl zur Ermittlung der bestehenden Infrastruktur, Prozesse und Lizenzstrukturen (Ist-Zustand) als auch des Bedarfs im Ehrenamt, gemeinsam mit Vertreter*innen aus den Fachbereichen der SoCura, des Malteser Hilfsdienstes sowie Ehrenamtlichen
- Prozess-Design: Entwickeln eines Zieldesignvorschlags (Soll-Zustand) aus den Ergebnissen der Anforderungsworkshops (Zielsetzungen, prozessuale und technische Änderungen, Reduzierung der entstehenden Mehr- und Folgekosten)
- Pilotphase: Vorbereitung, Durchführung und Nachbereitung einer einwöchigen Pilotphase an verschiedenen Standorten, als Proof of Concept konzipiert, mit technischer und prozessualer Begleitung der Pilotteilnehmer*innen sowie anschließender Anpassung (falls erforderlich) des Zieldesignvorschlags
- Planung und Angebotserstellung für die Umsetzung: Berücksichtigung aller Phasen (inkl. etwaigem Hybrid-Betrieb) bei der Einführung des definierten und in der Pilotphase erprobten Prozesses

1in diesem Zusammenhang: Programmleitung, Projektleitung, Vertreter Skaylink, Vertreter Infrastruktur SoCura, Redaktion, IT-Sicherheit und IT-Compliance

Der Projektverlauf wird begleitend dokumentiert und fließt in das vorliegende Whitepaper ein, um die Ergebnisse und Erkenntnisse auch anderen Organisationen zugänglich zu machen und diesen als Handreichung für die Entwicklung und Umsetzung eigener Lösungsansätze zu dienen. Das Whitepaper entsteht in enger Zusammenarbeit und im Austausch der Projektbeteiligten.

4 Ausgangslage

Als Startpunkt dient ein Blick auf die vorhandenen IT-Strukturen. Im Anschluss daran werden technologische Alternativen erwogen, die als Handlungsoptionen zur Verfügung stehen. Sie sind stets vor dem Hintergrund von Anforderungen aus IT-Sicherheit, Datenschutz, Compliance und existierenden Lizenzmodellen zu betrachten, auf die deshalb zum Abschluss des Kapitels eingegangen wird.

4.1 Vorhandene IT-Strukturen

Die SoCura versorgt vielfältige Anwender*innengruppen mit passenden IT-Services. Mit einem Persona-Ansatz (Definition fiktiver Personen, die für eine bestimmte Zielgruppe typische Eigenschaften, Fähigkeiten und Bedürfnisse repräsentieren) ließen sich diese zum Beispiel unterteilen in Office Worker, Information Worker und Firstline Worker, wobei diese Anwender*innengruppen ganz unterschiedliche Anforderungen an IT-Lösungen haben. Gerade für die letzte Gruppe der Firstline Worker hat IT eine ausschließlich unterstützende Funktion und stehen andere Tätigkeiten im Fokus. Hinzu kommen unterschiedliche Beschäftigungsverhältnisse, von Freelancer*innen über Festangestellte bis zu Ehrenamtlichen. Das Hauptaugenmerk lag bislang auf dem Hauptamt. Dafür stellt die SoCura verwaltete Geräte mit Anbindung an das Unternehmensnetzwerk bereit. Die laufenden Kosten werden über entsprechende Kostenstellen abgerechnet und erlauben eine solide Ausstattung, die neben der Hardware auch Fachanwendungen und andere Services wie etwa einen umfassenden Support umfasst. Auch die Einbindung von BYOD-Geräten ist möglich.

	Nutzung von MS-Office-Produkten	Nutzung einer personalisierten dienstlichen E-Mail-Adresse	Nutzung von Fachapplikationen	Teilnahme an Video-konferenzen	Arbeitsort	Tätigkeiten
Office Worker	intensiv	ja	intensiv, häufig mit mehreren Apps, Umgang mit sensiblen Daten	ja, unregelmäßig	Büro	Stark fachlich geprägte Tätigkeiten
Information Worker	intensiv	ja	selten, Zugriff auf Daten aus Fachanwendungen	regelmäßig	Mobil, an wechselnden Lokalitäten und mit wechselnden Endgeräten	Konzeptionelle Arbeit mit hohem kollaborativen Anteil
Firstline Worker	selten, hauptsächlich in Web-Anwendungen	ja	intensiv	selten	Teilweise stationär, teilweise wechselnd, auch mit privaten Endgeräten	Dienst am Menschen, wenig Arbeit mit IT

Abbildung 1: IT-Persona bei den Maltesern (Quelle: IT-Strategie für den Malteser Hilfsdienst)

Die hohe Zahl ehrenamtlich Helfender und deren abweichende Anforderungen an IT erfordern eine Neuausrichtung, mit dem strategischen Ziel, die Durchdringung der IT im ehrenamtlichen Bereich auf der Basis vorhandener IT-Strukturen und mithilfe zukunftsweisender, bereits als branchenübergreifende Standards etablierter Technologien zu stärken.

Diese Überlegungen sind immer auch vor dem Hintergrund einer Wirtschaftlichkeitsbetrachtung zu führen. Investitionen in IT gelten in diesem Zusammenhang bisher vornehmlich als Belastung und werden nicht automatisch als sinnvolles Investment wahrgenommen.

Gilt die Ausstattung von ehrenamtlichen Maltesern mit persönlicher Schutzausrüstung als selbstverständlich, ist bei Investitionsbedarf für Datenschutz und IT-Sicherheit häufig eine gegenteilige Haltung zu beobachten. Ähnlich schwierig ist es, die Anschaffung von Geräten und deren Folgekosten für Ehrenamtliche zu rechtfertigen, bei denen naturgemäß in der Regel weniger Arbeitszeit anfällt als im Hauptamt.

Vor diesem Hintergrund erscheint die Nutzung privater oder durch Drittparteien bereitgestellter Geräte naheliegend. Ohne eine Unterstützung von BYOD-Szenarien seitens der SoCura geht es nicht. Anforderungen an IT-Sicherheit und Datenschutz – bereits ein einzelner Sicherheitsvorfall kann desaströse Folgen nach sich ziehen! – setzen hier allerdings enge Grenzen. BYOD-Szenarien müssen die unterschiedlichen Schutzbedarfe erfüllen, dabei aber so wartungsarm und kosteneffizient wie möglich gestaltet sein. Teilweise gibt es auch Bedingungen, die eine passgenaue Versorgung ehrenamtlicher Malteser begünstigen könnten. So sind auch einige ehrenamtliche Dienststellen an das Unternehmensnetzwerk angebunden. Die Malteser nutzen zum Teil zentrale Dienste in Form von Web-Applikationen, die auch außerhalb des Firmennetzes sicher und performant bereitgestellt werden können.

Sporadisch ist auch das Ehrenamt auf die Nutzung von Fachapplikationen angewiesen, was zukünftige Bereitstellungsmodelle finanzierbar ermöglichen müssen. Bereits heute nutzt ein Großteil der Ehrenamtlichen die Services aus dem Microsoft-365-Spektrum (Office, Teams, SharePoint, OneDrive & Co.).

Die bis zu diesem Punkt Anwender*innenbezogene Betrachtung ist um eine gerätebasierte Perspektive zu ergänzen, insbesondere für Dienststellen-Computer und Einsatz-Tablets. Die Entwicklung von Lizenzmodellen für cloudbasierte IT-Lösungen orientiert sich zunehmend an den Anwender*innen und nicht länger an Geräten. Bei Anwender*innenbasierten Anwendungsfällen ist das kein Problem und diese kommen bei den Maltesern auch am häufigsten vor. Gerätebasierte Anwendungsfälle – wie etwa die gemeinsame Nutzung von Dienststellen-Computern und Einsatz-Tablets („Kiosk-Nutzung“)– sind jedoch kritisch zu hinterfragen, da sie eventuell nur bei gerätebasierter Lizenzierung tragfähig sind oder bleiben können. Die Malteser nutzen – über ein „Enterprise Agreement“ zwischen Microsoft und der SoCura – spezielle Lizenzprogramme für Non-Profit-Organisationen (insbesondere F3-, E3- und E1-Pläne), die zwar einige Besonderheiten bei Zugangsberechtigungen und Produktzusammenstellung aufweisen und nicht alle wesentlichen Sicherheitsfeatures in vollem Umfang abdecken (insbesondere für BYOD-Szenarien), aber zu Vorzugs-Konditionen bezogen werden.

Für das Hauptamt liegt eine IT-Securitybaseline im Entwurfsstadium vor, die zentrale Fragen bezüglich Datenschutz und IT-Sicherheit regelt und aus der voraussichtlich Festlegungen im Sinne von Minimalanforderungen auch auf das Ehrenamt übertragen werden. Die Baseline ist bei der Mindest-Lizenzierung in allen erwogenen IT-Szenarien für das Ehrenamt zu berücksichtigen, insbesondere auch bei BYOD-Szenarien. Die bestehenden Zugriffsmöglichkeiten über BYOD-Geräte aus dem Hauptamt liefern der SoCura Erfahrungswerte. Eine einheitliche Lösung gibt es hier noch nicht, zeichnet sich jedoch ab. Aktuell können Zugriffe über Cloud App Security (mit allerdings hohen

Lizenzanforderungen), den Microsoft-E5-Plan sowie mit Intune und Microsoft Endpoint Manager (MEM) abgesichert werden, auf die später noch näher eingegangen wird.

4.1.1 Zentraler Identitäts- und Zugriffsverwaltungsdienst

Der zentrale Identitätsdienst bei den Maltesern ist ein On-Premise Microsoft Active Directory (AD). Geräte werden aktuell im AD On-Premise registriert. Eine Trennung, beispielsweise in Azure Active Directory für Ehrenamtliche und Active Directory für hauptamtlich Mitarbeitende, ist in Prüfung. Allerdings sind einige Applikationen derzeit zwingend auf On-Premise-Verzeichnisdienste angewiesen. Mittelfristig werden alle Aktivitäten als automatisierbar bewertet (PowerShell oder Graph-API), was den Übergang zu cloudbasierten Verzeichnisdiensten erleichtert.

Das zentrale Malteser Active Directory verfügt über eine hierarchische Struktur, in der Informationen zu Objekten im Netzwerk gespeichert werden. Der Verzeichnisdienst Active Directory Domain Services, ADDS, stellt Methoden zum Speichern von Verzeichnisdaten bereit und macht diese für Netzwerknutzer*innen und Administrator*innen verfügbar. ADDS speichert Informationen zu Benutzerkonten, beispielsweise Namen, Kennwörter oder Telefonnummern, und ermöglicht anderen autorisierten Anwender*innen den Zugriff auf diese Informationen. Active Directory verfügt über einen strukturierten Datenspeicher für eine logische, hierarchische Organisation von Verzeichnisinformationen. Bereitgestellte Objekte resultieren aus freigegebenen Ressourcen wie Servern, Volumen, Druckern sowie Konten von Computern und Netzwerknutzer*innen.

Authentifizierung bei der Anmeldung sowie Zugriffsteuerung im Verzeichnis erhöhen die Sicherheit. Mit einer einzigen Netzwerkanmeldung können Administrator*innen Verzeichnisdaten und die Organisation im gesamten Netzwerk verwalten. Autorisierte Netzwerknutzer*innen können überall im Netzwerk auf Ressourcen zugreifen. Die richtlinienbasierte Verwaltung erleichtert die Verwaltung selbst komplexer Netzwerke.

4.1.2 Gerätebereitstellung, Geräteverwaltung und Softwareverteilung

Für die Softwareverteilung auf allen Desktop-Computer und Notebooks nutzen die Malteser aktuell Baramundi. Hauptamtliche Malteser Mitarbeitende arbeiten in den Dienststellen an über Citrix bereitgestellten virtuellen IT-Arbeitsplätzen.

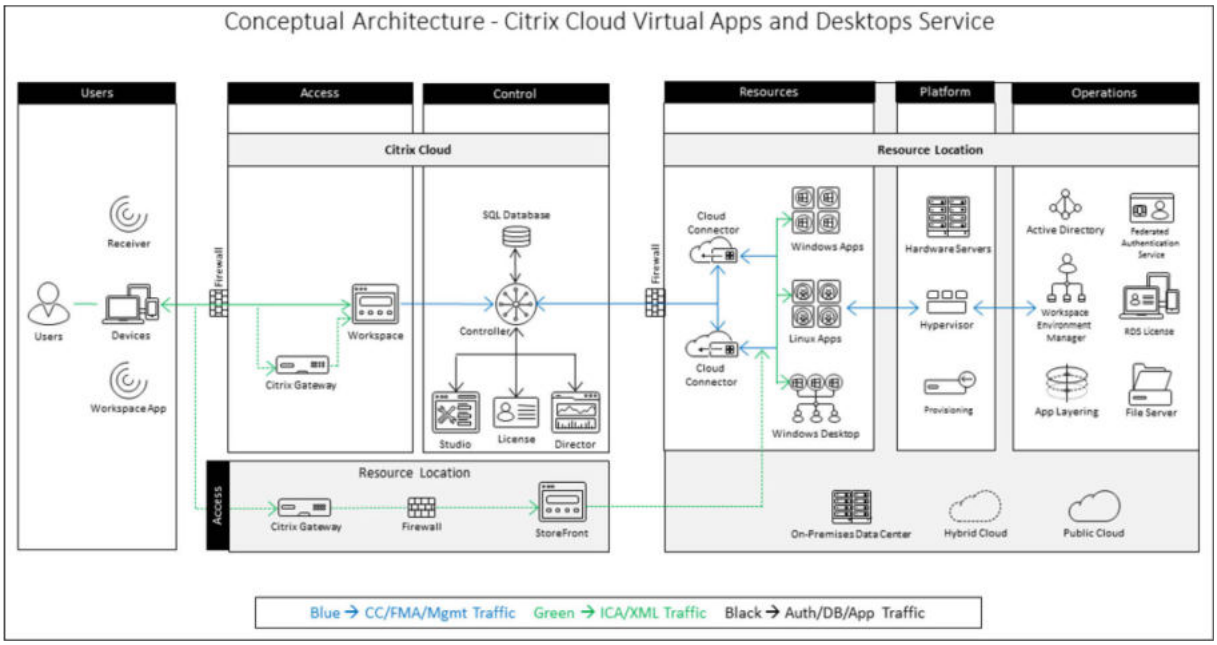


Abbildung 2:Citrix Cloud virtual Apps and Desktop Service

4.2 IT-Securitybaseline

Für das Hauptamt liegt eine IT-Securitybaseline vor, die zentrale Fragen bezüglich Datenschutz und IT-Sicherheit regelt und die – zumindest in Teilen – auch auf das Ehrenamt übertragen werden kann und muss. Einige Anpassungen und Erweiterungen erscheinen notwendig, auf die hier angesichts der sicherheitsrelevanten Thematik leider nicht detailliert eingegangen werden kann.

Übergreifend definiert die Security Baseline für die Malteser IT die folgenden Voraussetzungen:

- Microsoft Endpoint Manager (MEM) als zentrales Client Management Tool
- Azure Active Directory (AAD) als zentraler Identitätsdienst für die Cloud-Verwaltung
- Bedingter Zugriff (Conditional Access), um alle Zugriffe gemäß einer Zugriffsdefinitionsverwaltung und einer Risikobeurteilung zu schützen
- Multi-Faktor-Authentifizierung (MFA) zur sicheren Authentifizierung und Autorisierung von Anwender*innen

Darüber hinaus werden für die Proofs of Concept einige grundlegende Sicherheitsanforderungen definiert, die im Folgenden kurz vorgestellt werden.

4.2.1 IT-Sicherheit, Datenschutz und Compliance

Um beurteilen zu können, welche Funktionalitäten (und damit auch welche Lizenzpläne) erforderlich sind, sind Anforderungen aus IT-Sicherheit, Datenschutz und Compliance zu berücksichtigen, auf die im Folgenden näher eingegangen wird.

4.2.1.1 IT-Sicherheit

Die Funktionsfähigkeit und Verfügbarkeit der IT-Systeme und Netze sowie die Vertraulichkeit und Integrität der Geschäftsprozesse, Organisationsverfahren und der zugehörigen IT-Services, Anwendungen und Daten sind durch technische Fehler, Fehlverhalten, Sabotage und Ausspähen gefährdet. Dies kann zu Imageverlust, wirtschaftlichem Schaden und im Extremfall zur Gefährdung von Menschen führen. Um solchen Gefährdungen wirkungsvoll zu begegnen, müssen geeignete technische und organisatorische Maßnahmen geplant, umgesetzt und kontinuierlich verbessert werden. Zur Einhaltung gesetzlicher Vorgaben, zur Wahrung des Vertrauens der Malteser und aus Eigeninteresse kommt der Wahrung der Informationssicherheit bei der SoCura ein hoher Stellenwert zu.

Um ein adäquates Informationssicherheitsniveau zu erreichen und einzuhalten, wird ein Informationssicherheitsmanagementsystem (ISMS) gemäß der Norm ISO/IEC 27001:2013 betrieben, dass die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und Informationstechnik gewährleistet, die Belastbarkeit der Systeme und Dienste sicherstellt und die Anforderungen des Datenschutzes erfüllt.

Informationssicherheit kann nur ganzheitlich durch risikomindernde Maßnahmen in den Bereichen Organisation/Prozesse, Personal, Technik und Physische Sicherheit erreicht werden. IT-Systeme und Netzwerke müssen auf allen Ebenen, von der Hardware- bis zur Anwendungsschicht, durchgehend vor Ausfall und Missbrauch geschützt werden. Dabei kommen dem Identity und Access Management sowie dem Einsatz kryptografischer Methoden eine entscheidende Bedeutung zu. Die zunehmende Nutzung von Cloud-Diensten erfordert dabei die zuverlässige Identifikation und Klassifikation von Anwender*innen, Geräten und Informationsressourcen, um eine dynamische Zugangskontrolle auf Basis des Zero-Trust-Prinzips zu gewährleisten.

Die SoCura strebt folgende Schutzziele an:

- Die Verfügbarkeit der IT-Services, IT-Systeme, Applikationen und Daten muss gewährleistet sein.
- Die Integrität der IT-Systeme, Programme und Daten ist zu schützen.
- Der Missbrauch der IT-Services, IT-Systeme, Applikationen und Daten durch zweckwidrige Nutzung oder Nutzung durch Unbefugte ist zu verhindern.
- Vertrauliche Informationen sind unabhängig von der Art ihrer Aufzeichnung so zu handzuhaben, dass ihre Vertraulichkeit jederzeit sichergestellt ist.
- Insbesondere sind Informationswerte, die in einer Cloud-Umgebung bereitgestellt oder genutzt werden, zu schützen.
- Alle einschlägigen Gesetze und sonstigen rechtlichen Bestimmungen sind einzuhalten.
- Die Persönlichkeitsrechte von allen haupt- und ehrenamtlich Mitarbeitenden in allen Malteser Organisations- und Unternehmensteilen sind jederzeit zu wahren.

- IT-bezogene Geschäftsprozesse sind weitgehend widerstandsfähig gegen innere und äußere Störungen zu machen.

Eine ITK-Richtlinie (Informations- und Telekommunikationsrichtlinie) beschreibt konkrete Maßnahmen, die alle Mitarbeitenden (Haupt- und Ehrenamt) der Malteser unbedingt einhalten sollten, um Informationssicherheitsvorfälle zu vermeiden.

Von ihren Kunden erwartet die SoCura die Berücksichtigung von gesetzlichen Vorgaben und beim Einbringen eigener IT-Systeme und Programme die Einhaltung des Standes der Technik (wie in den nachfolgenden Punkten erläutert), um gemeinsam ein hohes IT-Sicherheitsniveau zu erreichen.

Für das vorliegende Projekt „IT-Infrastruktur Ehrenamt“ ist IT-Sicherheit ein zentraler Aspekt. Wie muss IT-Sicherheit in der IT-Infrastruktur für Ehrenamtliche aussehen, damit Informationssicherheitsanforderungen erfüllt, Chancen genutzt und Risiken beseitigt werden können? Um solchen Risiken wirkungsvoll zu begegnen, müssen geeignete technische und organisatorische Maßnahmen (TOMs) geplant, umgesetzt und kontinuierlich verbessert werden. Die Informationssicherheitsmaßnahmen müssen möglichst hürdenarm gestaltet sein und sich in den Alltag der Helfenden einfügen. Gleichzeitig sind – auch zum Schutz der Helfenden selbst – IT-Sicherheitsrichtlinien und (IT-) Compliance-Vorgaben zu erfüllen.

Im Folgenden sind einige Maßnahmen erläutert, die für IT-Infrastruktur in ehrenamtlichen Zusammenhängen zu berücksichtigen sind.

Für das Ehrenamt genutzte Systeme, Programme, Netze, Anwendungen, Skripte, Apps, Dateien, Links und deren Komponenten, die administrativ und/oder fachlich nicht in der Verantwortung der SoCura liegen, sind nach aktuellen Best Practices oder Branchenstandards der Informationssicherheit so einzurichten, dass die Sicherheit, Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Systeme, Netze, Programme, Anwendungen, Skripte, Apps, Dateien und Daten der SoCura, von anderen SoCura-Kunden sowie von Dritten nicht beeinträchtigt oder gefährdet werden.

Die IT-Sicherheit muss dem Stand der Technik entsprechen. Als Mindestanforderungen, um gemeinsam ein hohes IT-Sicherheitsniveau zu erreichen, ergeben sich daraus die nachfolgenden Punkte.

Zur Zugangskontrolle hat das Ehrenamt sicherzustellen, dass Benutzerkonten nur von Personen der eigenen Organisation genutzt werden. Ausnahmen sind mit der SoCura abzustimmen. Es ist sicherzustellen, dass Passwörter sicher und geheim gehalten werden und dass Benutzerkonten und Berechtigungen nach dem Need-to-Know- und Need-to-Use-Prinzip vergeben werden.

Für den Internetzugriff (mittels Cloud Web Access/Multi-Faktor-Authentifizierung) gilt, dass die Stabilität und Qualität der Internetverbindung zum Rechenzentrum und somit der Zugriff in die Malteser Public Cloud in der Eigenverantwortung der Ehrenamtlichen liegen und die Authentisierung, wann immer möglich, auf Basis mehrerer Faktoren (MFA) erfolgt.

Um Client-Sicherheit zu gewährleisten, dürfen eigene BYOD-Clients (z. B. PCs, Notebooks, Tablets) nur unter folgenden Bedingungen genutzt werden:

- Das Betriebssystem erhält noch Hersteller-Support.
- Es werden regelmäßig Sicherheitsupdates eingespielt.
- Ein Malwareschutz (z. B. Antivirus-Software) ist installiert und erhält regelmäßige Updates.
- Die SoCura ist berechtigt die Konfiguration mithilfe entsprechender technischer Regelwerke und automatisiert zu überprüfen und bei Verstößen angemessene Maßnahmen einzuleiten (z. B. die Sperrung des Clients).

Diese Schutzziele bilden einerseits die Basis und andererseits auch das gewünschte Niveau für Dienste, Anwender*innen und Geräte im Haupt- wie im Ehrenamt. Sie dürfen nicht unterschritten oder aufgeweicht werden.

In MS Intune läuft die Verwaltung und Überwachung aller Sicherheitsprozesse zentral, wie auch der Dienst selbst in Azure. Dies ermöglicht eine enge Verzahnung aller vorhandenen Aspekte von Gerätesicherheit, Identitätsschutz sowie Datenverschlüsselung.

Die Bereitstellung und Überwachung von Informationen wird über zentrale Dashboards gesteuert, welche die Darstellung und Kontrolle aller relevanten Sicherheits- und Compliance-Einstellungen und -Ereignisse gewährleisten.

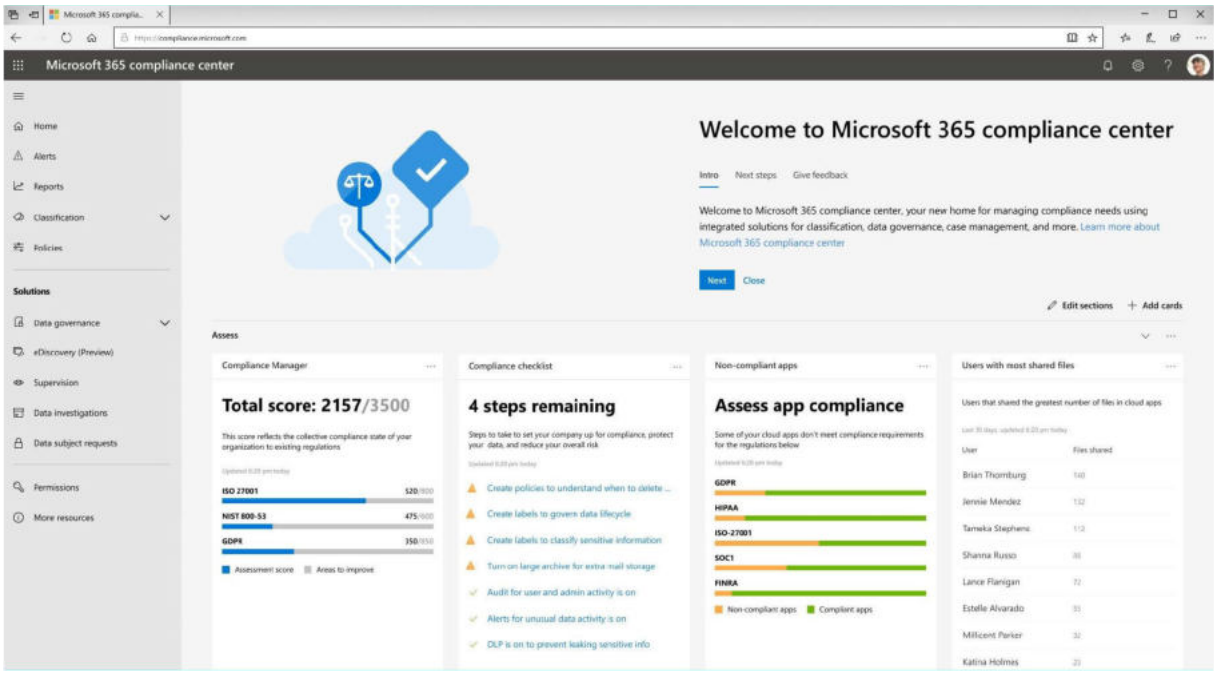


Abbildung 3: Beispiel Sicherheitscenter in M365 (Quelle: SoCura)

4.2.1.2 Datenschutz

Ähnlich wie sich die IT-Compliance der Malteser an der ITK-Richtlinie orientiert, orientiert sich der Datenschutz an einer Datenschutz-Richtlinie. Diese Richtlinie enthält neben Definitionen verschiedener zentraler Begriffe (Personenbezogene Daten, Gesundheitsdaten, IT-Service usw.) auch

Verhaltensweisen für verschiedene Situationen, wie zum Beispiel das Arbeiten im Mobile-Office, den Umgang mit Microsoft-365-Diensten oder das Verhalten bei Verstößen gegen die Richtlinie.

Hauptaufgabe des Datenschutzes ist es, mögliche Datenschutz-Risiken zu antizipieren und sich gegen diese abzusichern, ohne dabei die Umsetzbarkeit zu vernachlässigen, sodass die verschiedenen Bereiche beschwerdefrei und datenschutzkonform arbeiten können. Dabei unterliegen Sie der Kirchlichen Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (kurz: KDR-OG). Damit unterliegt der Malteser Verbund nicht dem weltlichen Datenschutzrecht, die KDR-OG steht allerdings im Einklang mit der EU-DSGVO und dem deutschen BDSG.

Der Datenschutz-Service liegt seit dem 01.04.2021 vollumfänglich bei der SoCura, die somit den zentralen Datenschutzbeauftragten stellt. Alle übergreifenden Datenschutz-Anfragen werden vom Zentralen Datenschutz-Team begleitet (in den Regionen und Betriebsgesellschaften der Malteser übernehmen dezentrale Datenschutzkoordinator*innen diese Aufgabe).

Datenschutzereignisse (Datenpannen) sind zentral an die SoCura zu melden und werden vom Service Desk bearbeitet, der 24/7 verfügbar ist.

Für den Datenschutz gelten dieselben Regeln wie für die IT-Sicherheit, allerdings sind ggf. sich aus zusätzlichen Regelwerken (z. B. dem Kirchengesetz) ergebende Erweiterungen zu berücksichtigen und je nach Bedarf als separate Konfigurationen mit den Basis-Richtlinien zu kombinieren.

4.2.1.3 Compliance

Die Compliance in Haupt- und Ehrenamt wird hauptsächlich durch die ITK-Richtlinie bestimmt. Diese ist seit dem 01.01.2018 gültig und wird jährlich an neue Gesetze und Technologien angepasst. Die Richtlinie beschreibt den Lebenszyklus von IT für die Malteser sowie Maßnahmen, die alle Mitarbeitenden (Haupt- und Ehrenamt gleichermaßen) unbedingt einhalten sollten, um Gefahrenquellen (Fehler, Cyber-Attacken, Sicherheitslücken usw.) zu vermeiden. Die Compliance im Verbund soll langfristig durch verbindliche Standards nachweisbare Daten- und IT-Sicherheit im gesamten Malteser Verbund schaffen. Gesamtverantwortlich hierfür ist der CIO der Malteser.

Die ITK-Richtlinie beschreibt aber nicht nur, was unter den verschiedenen Begriffen zu verstehen ist (Schatten-IT, BYOD, Informationssicherheit usw.). Sie gibt auch vor, wie verschiedene Ereignisse zu handhaben sind. Die IT-Compliance wiederum hat dafür Sorge zu tragen, dass diese Richtlinie eingehalten wird. Des Weiteren ist es eine der Aufgaben der IT-Compliance, die benannte ITK-Richtlinie im jährlichen Turnus zu aktualisieren. Sie prüft nicht nur die Einhaltung interner Richtlinien, sondern auch, ob Gesetze und weitere externe Rahmenbedingungen eingehalten werden.

Hauptsächlich unterstützt die IT-Compliance Haupt- und Ehrenamt aktiv bei der Umsetzung der Vorgaben aus der ITK-Richtlinie und der KDR-OG. Sie führt regelmäßig Awareness-Maßnahmen, wie z. B. Schulungen durch, um sicherzustellen, dass die Vorgaben in der gesamten Fläche umgesetzt werden, neue Vorgaben bekannt und eingehalten werden, etwa bezüglich Kennwortvorgaben, Regeln zu Speicherorten oder der konformen Nutzung der von der SoCura bereitgestellten Services. Weiterhin ist es eine Aufgabe der IT-Compliance, Anfragen zur Schatten-IT zu bewerten, prüfen und freizugeben bzw. abzulehnen.

Im Zuge des internen Proof of Concept wurden bereits erweiterte Compliance-Sets erstellt, die sich moderne Sicherheitslösungen (z. B. Windows Hello) zu Nutze machen und die allgemeinen ITK-Richtlinien um den neuen Faktor Cloud erweitern.

4.2.2 Passwortrichtlinie

Ein Kennwort zum Entsperren mobiler Geräte ist eine allgemeine Voraussetzung für die Konformität mobiler Endgeräte. Nur Konforme Geräte erhalten im Microsoft Endpoint Manager weiteren Zugriff auf Informationen, Apps, Daten, E-Mails usw.

Eine Passwortrichtlinie definiert die Komplexität von Kennworten, erforderliche Änderungsintervalle und regelt Ausschlüsse zuvor bzw. zuletzt verwendeter Kennworte.

Die Kennwortvorgaben sollten immer mit anderen Systemsicherheitsvorgaben kombiniert werden, um Mitarbeitende sowie Unternehmensressourcen zu schützen.

4.2.3 Gerätekonformität

Damit mobile Endgeräte als mit dem Microsoft Endpoint Manager konform kategorisiert werden, müssen sie bestimmte, vorab definierte Anforderungen erfüllen. Beispiele für Konformitätsrichtlinien sind:

- Bestimmte Regeln und bestimmte Einstellungen, die Anwender*innen oder Geräte erfüllen müssen

- Nicht konforme Geräte von Aktionen ausschließen oder warnen, um die Unternehmensressourcen zu schützen

Wenn Konformitätsregeln nicht ausreichen, können sie zusätzlich mit bedingtem Zugriff (Conditional Access) kombiniert werden um Anwender*innen und Geräte zu blockieren.

Konformitätsrichtlinien im Microsoft Endpoint Manager bestehen aus zwei Teilen:

1. Einstellungen für Konformitätsrichtlinien – Einstellungen, die einer Konformitätsrichtlinie entsprechen, die jedes Gerät erhält. Die Einstellungen für Konformitätsrichtlinien legen eine Baseline für die Funktionsweise von Konformitätsrichtlinien in der Intune-Umgebung fest. Dazu zählt, ob Geräte, die keine Gerätekonformitätsrichtlinien erhalten haben, als konform oder nicht konform gelten.

2. Gerätekonformitätsrichtlinie – Plattformspezifische Regeln, die konfiguriert und für Gruppen von Anwender*innen oder Geräten bereitgestellt werden müssen. Diese Regeln definieren die Anforderungen für Geräte, zum Beispiel die minimalen Betriebssysteme oder die Verwendung der Datenträgerverschlüsselung. Geräte müssen diese Regeln erfüllen, um als konform eingestuft zu werden.

4.2.4 Arbeitscontainer auf Android

Für mobile Geräte (bei der Nutzung von Microsoft Exchange) gilt darüber hinaus, dass sie bei zehnmaliger falscher Kennworteingabe zurückgesetzt werden. Für die Gerätekonformität müssen Google Play Store und das Betriebssystem (als Mindestversion 8.0) vorhanden sein. Zudem muss für die Systemsicherheit die Unternehmensapp auf den Geräten installiert sein.

4.2.5 App Protection auf iOS und iPad OS

Bei App Protection für iOS-Geräte gelten von der SoCura vordefinierte Richtlinien für Outlook und Teams. Diese lassen sich als Verwaltungsfunktion für Anwender*innen (via „Push“) bereitstellen, konfigurieren, schützen, überwachen und aktualisieren.

Die IT-Securitybaseline gibt dafür die im Folgenden vorgestellten Parameter vor, die aktuell allerdings noch nicht umgesetzt sind.

Für die Outlook-App wird eine App-PIN vergeben, die eine Komplexität von 8 (numerischen) Zeichen aufweist. Die jeweils letzten sechs PINs dürfen nicht erneut vergeben werden.

Nach Verlassen der App, Geräteneustart oder Inaktivität von mindestens einer Minute ist das erneute Eingeben der PIN erforderlich. Gemäß einer Richtlinie des Microsoft Endpoint Manager wird die Applikation nach 20 Fehlversuchen gesperrt.

Für Weblinks in Outlook wird eine App-Schutzrichtline für Microsoft Edge erstellt, die das Öffnen der Links nur in einem verwalteten Edge-Browser erlaubt.

Die Geräte müssen mindestens über Betriebssystemversion iOS 15.0 verfügen.

4.2.6 Vollwertiges Notebook – Windows (SoCura-verwaltet)

Bei einem voll verwalteten Windows-Gerät (auch Full Managed Windows Client genannt) handelt es sich um einen Client mit Windows 10 oder Windows 11. Vor der erstmaligen Verwendung des Gerätes für ehrenamtliche Tätigkeiten ist einmalig eine Verbindung zum Malteser Tenant erforderlich, um das Gerät anzumelden, zu konfigurieren und benutzerspezifische Anwendungen und Berechtigungen in Form von (Geräte-)Richtlinien herunterzuladen. Die Vertrauensstellung wird dabei mittels Zertifikat zwischen Windows Client und Endpoint Manager hergestellt.

Eine Registrierung bei Microsoft Endpoint Manager kann durch Anwender*innen und Administrator*innen erfolgen. Aktuell ist der Microsoft Endpoint Manager noch nicht im Einsatz (die Geräde werden mit einem Image betankt und erhalten ihre Richtlinien und Konfigurationen via Baramundi), perspektivisch soll aber umgestellt werden.

Anwender*innen können sich selbst anmelden über einen der folgenden Wege:

- App „Microsoft Store Unternehmensportal“: Über das Unternehmensportal können die Anwender*innen dann die freigegebene Software auf ihren Computern installieren. Die Anwender*innen greifen auf Unternehmensdaten zu und können häufig anfallende Aufgaben ausführen. Darüber hinaus können sie an diesen Stellen sicher auf Unternehmensressourcen zugreifen.
- MDM-Registrierung: MDM steht für die zentrale Verwaltung mobiler Endgeräte, die in Microsoft Intune verwaltet werden.
- Anmeldung in Azure Active Directory (Azure AD): Mit der Anmeldung in Azure Active Directory (Azure AD) wird sichergestellt, dass die Anwender*innen unter Einhaltung von Sicherheits- und Konformitäts-Standards auf ihre Geräte zugreifen.

- Autopilot: Die Windows-Autopilot-Technologie ist in der Lage, neue Geräte einzurichten und im Vorfeld zu konfigurieren, um sie auf den produktiven Einsatz vorzubereiten. Daraus resultieren Vorteile, wie keinerlei Verwaltungsaufwand und die leichte Abwicklung der Services (Anwenden von Einstellungen und Richtlinien, Installieren von Apps, Ändern der Windows-Edition, die zur Unterstützung erweiterter Features verwendet werden, beispielsweise von Windows Pro zu Windows Enterprise).

Administrator*innen können Richtlinien konfigurieren, um die automatische Registrierung zu erzwingen durch:

- Eine hybride Azure AD-Verbindung: Mit dem Azure AD Hybrid Join werden Windows-10-Clients, die Mitglied in einer On-Premise-Active-Directory-Domain sind, automatisch Mitglied (Join) in Azure AD. Dies ermöglicht eine Verwaltung von Windows-10-Clients im Microsoft Endpoint Management (Intune).
- Co-Verwaltung mit Configuration Manager: Die Co-Verwaltung ist eine der wichtigsten Methoden zum Anfügen bestehender Konfigurations-Manager-Bereitstellung an die Microsoft-365-Cloud. Sie ermöglicht das Entsperren zusätzlicher Funktionen, die in der Cloud unterstützt werden (wie z. B. bedingter Zugriff)
- Device Enrollment Manager: Registrierung von bis zu 1.000 mobilen Geräten mit einem Azure-Active-Konto
- Bulk Enroll: Einbindung einer großen Anzahl von neuen Windows-Geräten in Azure Active Directory und Intune
- Registrierung von Windows IoT-Core-Geräten: Mit Intune konsistente Verwaltung von IoT Core, IoT Enterprise und anderen Windows-Geräten

4.3 Lizenzen und Lizenz-Pläne

Aktuell werden folgende Standardlizenzen durch ehrenamtliche Malteser genutzt:

- M365 E3 für Anwender*innen mit einem Zugang zur Malteser Private Cloud
- O365 F3 als Standardlizenz für die Firstline Worker
- O365 E1 als Add-on für Firstline Worker, die ein größeres Postfach brauchen.
- O365 E3 als Add-on für Firstline Worker, die eine lokale Office-Installation brauchen.
- AAD P1 als Add-on für Firstline Worker, die eine Multi-Faktor-Authentifizierung brauchen.

Die Malteser nutzen Azure Active Directory (AAD) als zentralen Identitäts- und Zugriffsdienst für die Cloud-Verwaltung. Für das Arbeiten mit Microsoft Office wird pro Anwender*in eine Office-Lizenz benötigt.

Bei der Nutzung der vorgestellten Lösungen ist folgender Minimalbedarf an Lizenzen zwingend abzudecken:

- Intune-Lizenz für die Geräteverwaltung

- Azure AD Premium P1 – für bedingten Zugriff und Multi-Faktor-Authentifizierung
- Microsoft Office 365 Apps for Enterprise – für lokale MS-Office-Installationen

Die aktuell im Lizenzplan M365 E3 enthalten Sicherheitsfeatures fasst das folgende Schaubild zusammen:

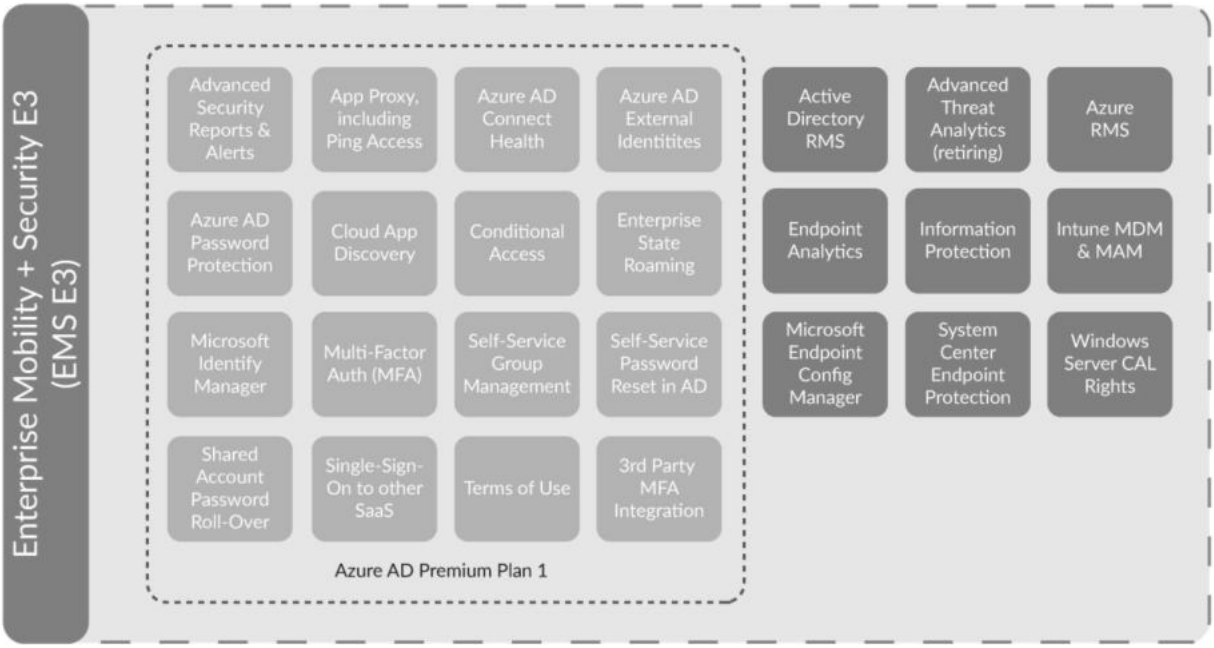


Abbildung 4: Sicherheitsfeatures in M365 E3 (Quelle: SoCura, in Anlehnung an M365Maps.com)

Microsoft trägt im Sinne des Shared Responsibility Model einen zentralen Teil der Sicherheit für ihre Kunden. Daher erfordert Sicherheit auch im gemeinnützigen Bereich ein effizientes Investment.

Eine Weiterentwicklung vom gegenwärtigen nahe Null-Tarif lizenzierten Zustand der IT im Ehrenamt stellt die Malteser vor die Entscheidung, ob und in welchem Umfang für IT-Services für das Ehrenamt mehr Geld ausgegeben werden soll, z. B. um eine höhere IT-Sicherheit oder mehr Funktionen zu erhalten. Es ist somit eine Lösung erforderlich, die ausgewogen die wirtschaftlichen und sicherheitsbezogenen Anforderungen erfüllt.

Die Lizenzangebote von Microsoft bieten grundsätzlich Lösungen für alle erkennbaren funktionalen Anforderungen der Malteser IT im Ehrenamt an. Es geht um die Frage der grundsätzlichen Machbarkeit zu vertretbaren Kosten. Dies wird im weiteren Verlauf des Whitepapers thematisiert.

So bietet Cloud App Security eine sinnvolle Erweiterung des Funktionsumfangs im Vergleich zu Intune für BYOD-Geräte mit iOS und iPadOS, erfordert aber eine E5-Lizenzierung. Dutzende weitere, ähnlich gelagerte Beispiele wären denkbar. Die Notwendigkeit, grundsätzliche Abwägungen über Lizenzmodelle und -stufen zu treffen, ist offensichtlich.

5 Anforderungsermittlung

Die Ehrenamtlichen stehen im Mittelpunkt des Projektes „IT-Infrastruktur Ehrenamt“. Alle erarbeiteten Lösungsansätze müssen zu den real vorhandenen Anforderungen aus der ehrenamtlichen Praxis passen. Um dies zu gewährleisten, führten die Projektbeteiligten gemeinsam mit Ehrenamtlichen – aus verschiedenen Organisationseinheiten und mit breit gefächerten fachlichen Profilen – zwei Anforderungsworkshops durch, die im Anschluss ausgewertet wurden. Auf Basis der daraus abgeleiteten Themenfelder und IT-Anforderungen entwickelte man insgesamt elf Design-Piloten, von denen vier für eine Pilotphase ausgewählt wurden.

5.1 Anforderungsworkshop

Da die meisten Ehrenamtlichen beruflich anderweitig eingebunden sind, fanden die (jeweils circa zweieinhalb Stunden langen) Workshops abends statt. Das Projektteam wertete die Workshops unmittelbar im Anschluss aus.

Der erste, eher technologisch und servicebasiert ausgerichtete Workshop fand mit eher IT-affinen Ehrenamtlichen statt. Zahlreiche Malteser Ehrenamtliche sind in ihren Hauptberufen in der IT tätig oder verfügen über einschlägige, teils hochqualifizierte berufliche oder akademische Ausbildungen und Erfahrungen, die sie gerne in das Projekt einbringen wollten. Am zweiten Workshop nahmen eher Kolleg*innen teil, die über keinen IT-Hintergrund verfügen und eine eigene Perspektive die derzeit vorhandenen Lösungen und deren Auswirkungen auf das Tagesgeschäft beisteuern konnten. Im Zusammenspiel beider Gruppen entstand ein umfassendes Bild der gegenwärtigen Situation und der zukünftigen Anforderungen an die IT im Ehrenamt der Malteser. Dabei ging es nicht nur um rein auf die ehrenamtliche Tätigkeit bezogene Gesichtspunkte, sondern auch um Berührungspunkte und Schnittstellen zwischen Haupt- und Ehrenamt.

Das Projektteam aus Mitarbeitenden der Malteser, der SoCura (aus IT und Projektmanagement) sowie von Skaylink erarbeiteten gemeinsam das Vorgehensmodell für die Workshops. Bereits die Vorstellungsrunde mit den Teilnehmer*innen war auf das Thema des Workshops ausgerichtet. Das Kernelement des Workshops war ein speziell auf die Ehrenamtlichen hin formulierter Fragekatalog. Die Fragen zielten ab auf alltägliche Arbeitsroutinen, die verwendete Ausrüstung (insbesondere Hard- und Software) sowie aktuelle Herausforderungen und Verbesserungswünsche der Teilnehmer*innen. Die folgende Abbildung zeigt einen Auszug aus dem Fragenkatalog.

Abbildung 5: Fragenkatalog Anforderungsworkshop (Auszug)

Die Bearbeitung der Fragen erfolgte interaktiv mithilfe von Mural, einer als Web-Applikation bereitgestellten digitalen Kollaborationsplattform für visuelle Zusammenarbeit, auf der mehrere Teilnehmer*innen gleichzeitig und gemeinsam an einer Art „virtuellem Whiteboard“ arbeiten können. Das Projektteam übertrug Antworten unmittelbar auf das Mural Board, wo sie von allen Teilnehmer*innen einsehbar waren und um Grafiken, Text oder numerische Elemente ergänzt werden konnten. Da das Projektteam die protokollarischen Aufgaben somit vollständig übernahm, konnten sich die Teilnehmer*innen ganz auf die Beantwortung der Fragen konzentrieren.

5.2 Die Top 10 Themenfelder der Ehrenamtlichen

Das Projektteam wertete die Ergebnisse im Anschluss an die Workshops aus und leitete daraus insgesamt zehn Themenfelder mit zentralen Anforderungen der Ehrenamtlichen ab, die im Folgenden näher vorgestellt werden sollen.

5.2.1 Offline-Arbeit

Es gibt eine ganze Reihe von Einsatzszenarien, in denen die Malteser auf Ausrüstung angewiesen sind, die offline funktionsfähig sein muss, etwa im Katastrophenschutz oder in der Krisenintervention. Dass es sich dabei nicht bloß um unwahrscheinliche Worst-Case-Szenarien handelt, zeigte sich zuletzt eindrucksvoll bei der Flutkatastrophe im Ahrtal, bei der die Helfenden dauerhaft ohne die von den Wassermassen zerstörte Infrastruktur arbeiten mussten. In anderen Szenarien könnte auch die geplante Deaktivierung von mobilen Datennetzen oder Mobilfunkzellen erforderlich sein, etwa bei einem Amoklauf oder vergleichbaren Krisen.

Anpassungen an der IT-Infrastruktur sollten daher Möglichkeiten der Offline-Funktionalität berücksichtigen.

5.2.2 Virtualisierte Umgebungen

Hauptamtliche Malteser Mitarbeitende arbeiten in den Dienststellen an über Citrix bereitgestellten virtuellen IT-Arbeitsplätzen. Ehrenamtliche nutzen in vielen Fällen privat eingebrachte Geräte – auch

da die internen Preismodalitäten für die Virtualisierung für ehrenamtlich geprägte und entsprechend kostensensible Organisationseinheiten aktuell wenig attraktiv bzw. nicht finanzierbar sind.

Alternative Lösungsansätze sollten die spezifischen Anforderungen des Ehrenamtes, aber auch ehrenamtliche Kostenstrukturen besser berücksichtigen. Hierbei wären andere Lösungen als Citrix denkbar, etwa der Einsatz von Technologien wie Azure Virtual Desktop mit Windows 10/11.

5.2.3 Typische Anwendungen

Einzelne monolithische, für den Arbeitsalltag der Malteser zentrale Anwendungen sind nur bei Anbindung an das Corporate Network nutzbar. Während dies für das Hauptamt in der Regel kein Problem ist, verfügen viele ehrenamtliche Dienststellen nicht über eine CN-Anbindung.

Diese Abhängigkeit vom Unternehmensnetzwerk sollte möglichst verringert werden. Viele der betroffenen Applikationen sind auch alternativ als Web-Applikationen verfügbar und sollten künftig auch auf diesem Wege bereitgestellt werden.

5.2.4 Malteser.org

Die Malteser stellen jedem Mitarbeitenden einen personalisierten Account in der Domäne malteser.org zur Verfügung. Mit diesem sind u. a. Mailbox, Chat, Dateiablage usw. nutzbar. Zurzeit verfügen noch nicht alle Ehrenamtlichen über einen solchen Account. Bereits seit einiger Zeit gibt es jedoch einen Malteser Vorstandsbeschluss, auch alle Ehrenamtlichen mit einem malteser.org-Zugang auszustatten, sodass der malteser.org-Account als Zugangsvoraussetzung zukünftig auch im Ehrenamt keine Hürde mehr darstellen sollte.

5.2.5 Top-3-Anwendungen

In den Workshops haben die Teilnehmer*innen die für ihre Arbeit wichtigsten Applikationen benannt. Ganz oben landen Microsoft-Anwendungen wie Outlook, Teams und OneDrive. Danach folgen Excel und Word sowie malteserspezifische Web-Applikationen wie ARNO, xSuite, Rew.Is und DokBox. Die hier zuletzt aufgeführten Web-Applikationen sind allerdings vorrangig bei Führungskräften und nur selten bei Ehrenamtlichen im Einsatz.

Die Versorgung mit den hier genannten Applikationen sollte unabhängig von Betriebssystemen und Bereitstellungsformen gewährleistet sein.

5.2.6 BYOD – Bring your own device

BYOD dominiert die Nutzung von IT im Ehrenamt, vor allem das Arbeiten mit privaten mobilen Endgeräten. Manche Geräte werden von Dritten verwaltet, etwa über das Mobile Device Management der Arbeitgeber der Ehrenamtlichen.

Die bei den Maltesern angebotenen Sicherheitsfunktionen – etwa die Möglichkeit eines Zugriffs für Remote Lock & Wipe – wird von den Workshop-Teilnehmer*innen überwiegend positiv bewertet und als Mehrwert verstanden. Generell ist den Ehrenamtlichen der Schutz von Daten, insbesondere auch privater Daten, sehr wichtig.

Es ist eine zentrale Erkenntnis aus den Workshops, dass die Ehrenamtlichen sich eine verbesserte Integration von BYOD-Geräten in die IT-Infrastruktur wünschen. Dabei sind fremdverwaltete ebenso wie private, nicht verwaltete Geräte zu berücksichtigen. Mit einer Unterstützung der beiden Betriebssysteme Android und iOS (bzw. iPadOS) und Windows kann man einen hinreichenden Anteil der mobilen Endgeräte abdecken.

Anwender*innen von Geräten, die nicht über die Malteser IT bezogen werden, können in der Regel nicht auf die Support-Angebote der SoCura (etwa den SoCura Service Desk) zurückgreifen bzw. werden durch diese nicht betreut. Lösungsansätze könnten der Austausch der nicht-betreuten Hardware durch von der SoCura bereitgestellte Malteser Hardware sein oder eine erweiterte Supportvereinbarung, die auch nicht von der SoCura bereitgestellte Geräte umfasst. Offen ist derzeit allerdings, wie hoch der tatsächliche Bedarf an Support-Angeboten sein könnte.

5.2.7 Multi-User-Devices

Einige ehrenamtliche Tätigkeiten erfordern, dass bestimmte Geräte durch unterschiedliche Malteser Mitarbeitende nutzbar sind (und dies auch spontan). Dies betrifft in erster Linie (aber nicht nur) sogenannte Einsatz-Tablets, die oftmals bestimmten Fahrzeugen oder Orten zugeordnet sind. In Dienststellen gibt es häufig Desktop-Computer, die regelmäßig von mehreren Anwender*innen verwendet werden.

Die Lizenzmodelle der namhaften Hersteller zielen zunehmend auf einzelne Anwender*innen bzw. Hauptanwender*innen von Geräten ab. Die Lizenzierung von Geräten über Geräte-CAL (Client Access License) ist nicht mehr üblich. Für die oben genannten Szenarien ist das ein Problem.

Für diese Lizenzierungsproblematik bei Multi-User-Devices sollte daher eine Lösung gefunden werden.

5.2.8 Budgets, Investments

Entscheidungen über IT-Investitionen im Ehrenamt werden bei den Maltesern in hohem Maße von kaufmännischen, kostenfokussierten Paradigmen bestimmt. Den lokalen Entscheidungsträger*innen stehen in der Regel nur begrenzte finanzielle Mittel zur Verfügung, die zudem häufig dezentral und zu wesentlichen Teilen über Spenden refinanziert werden. Dementsprechend angespannt ist häufig die finanzielle Lage beim Thema IT-Kosten fürs Ehrenamt.

Die für hauptamtliche Malteser flächendeckend ausgerollte Private-Cloud-Lösung mit Citrix ist für den ehrenamtlichen Bereich aufgrund der damit verbundenen Kosten aktuell so gut wie ausgeschlossen.

Hier gilt es, sinnvolle alternative Bereitstellungsformen zu finanzierbaren Preisen und mit den notwendigen wesentlichen Funktionen zu identifizieren, etwa eine kostengünstigere Lösung mit Citrix oder andere, günstigere Virtualisierungslösungen.

5.2.9 Sicherheit und Lizenzierung

Sicherheit ist im Alltag der Malteser eigentlich eine Selbstverständlichkeit, etwa wenn es um die Unversehrtheit von Einsatzkräften oder auch persönliche Schutzausrüstung und damit verbundene Kosten geht. In der IT ist diese Grundhaltung nicht im selben Maße gegeben, was für den

ehrenamtlichen Bereich noch einmal in besonderem Maße gilt. Hier fehlt es an einem tiefergehenden Verständnis der Zusammenhänge von (IT-)Sicherheit und Lizenzkosten.

IT-Sicherheit und Datenschutz sind relevante Faktoren. Die Malteser arbeiten vielfach mit sensiblen und personenbezogenen Daten. Ist dies im Falle von Patient*innendaten für die meisten noch offensichtlich, werden häufig viele weitere Daten zu Unrecht nicht als schützenswert erkannt, verstanden und akzeptiert.

Hier gibt es aktuell noch Sicherheitslücken, die vergleichsweise leicht zu beheben wären, wie etwa die außerhalb des Corporate Network noch nicht per Multi-Faktor-Authentifizierung gesicherten Zugänge.

5.3 Zusätzliche Anforderungen der Malteser internen IT

5.3.1 Zentraler Identitäts- und Zugriffsverwaltungsdienst

Die aktuelle Planung belässt die zentrale Identitätsverwaltung, -steuerung und -sicherung in der internen Infrastruktur. Damit bleiben allerdings auch administrative und effizienzsteigernde Einsparpotenziale ungenutzt, beispielsweise fehlende Azure Self-Service-Tools für die Anwender*innenverwaltung oder Synchronisierung und Rücksetzung von Passwörtern. Malteser führt bereits parallele Tests zur Erprobung und Einbindung moderner, anwender*innenfreundlicher Methoden durch, z. B. Pass-Through-Authentifizierung).

Generell ist festzuhalten, dass sich über richtlinienbasierte Verwaltung die Aufwände erheblich reduzieren lassen und komplexe Szenarien ggf. erst darüber verwaltbar werden.

6 Handlungsempfehlung

Für das Hauptamt haben sich drei wesentliche IT-Bereitstellungsformen etabliert, die auch einen großen Teil der Ehrenamtlichen abdecken:

- Vollwertiges Notebook – Windows mit Azure VPN Anbindung (SoCura-verwaltet)
- Virtueller Cloud Arbeitsplatz
- Mobilgerät mit iOS und iPadOS
- Mobilgerät mit Android

Für den Bereich Ehrenamt kommt eine weitere Bereitstellungsform mit großer Bedeutung hinzu: die Nutzung privat eingebrachter Geräte (BYOD) für die ehrenamtliche Tätigkeit als Malteser. Dabei handelt es sich um private Geräte der Ehrenamtlichen, aber auch um Geräte, die den Ehrenamtlichen von anderen Arbeitgebern zur Verfügung gestellt werden. Für das Ehrenamt haben wir es somit mit insgesamt vier typischen Bereitstellungsformen zu tun, die unabhängig von Rollen, Profilen oder Personen im Einsatz sind.

Unter Berücksichtigung dieser Ausgangslage wurden für die Pilotphase des hier beschriebenen Projektes vier Proof-of-Concept-Szenarien ausgewählt:

6.1 Virtueller Arbeitsplatz mit Azure Virtual Desktop

Hauptschwerpunkt sind die Abdeckung der Themfelder:

- Virtualisierte Umgebung
- Nicht unterstütze Geräte
- BYOD
- Typische Anwendungen
- Multi-User-Devices
- Zentraler Identitäts- und Zugriffsverwaltungsdienst

Im Vergleich zwischen Citrix On-Premise, Citrix on Azure, Azure Virtual Desktops (AVD) sowie Windows 365 sind aufgrund der durchgeführten Workshops die Anforderungen mit AVD ebenso abdeckbar wie mit einer On-Premise Citrix Farm. Durch die Nutzung von AVD im MultiMode ist es zusätzlich möglich, eine virtuelle Maschine für mehrere gleichzeitig aktive Benutzer*innen bereitzustellen. Im Hinblick auf die Cloud First Strategie wäre hier die Wahl auf AVD empfehlenswert, da es vom Aufbau und Betrieb, bis auf aktuelle Hybrid Identitäten, unabhängig von der lokalen Infrastruktur aufgebaut und flexibel erweitert werden kann. Zudem unterstützt es verwaltete und nicht verwaltete Endgeräte, da lediglich das Bild des Desktops übertagen wird. Auf den Endgeräten sind nur

Eingabegeräte erlaubt, dadurch sind problemlos auch BYOD Geräte nutzbar. Bei genauerer Betrachtung sollte nochmals geprüft werden, ob nicht auch Windows 365 – Cloud PC ebenfalls ausreichend wäre.

Für die passwortfreie Authentifizierung in Verbindung mit Conditional Access kann Windows Hello for Business eingesetzt werden. Diese Technologie unterstützt die Kategorie „Office- und Information Worker“.

6.2 Arbeitscontainer auf Android-Basis/ App Protection auf iOS und iPadOS

Hauptschwerpunkt sind die Themfelder:

- Offline-Arbeit
- BYOD
- Typische Anwendungen/Top 3 Anwendungen
- Multi-User-Devices
- Zentraler Identitäts- und Zugriffsverwaltungsdienst

Für den mobilen Bereich sollten Geräte mit Arbeitscontainern (Android) oder App Protection (IOS) eingesetzt werden.
Für Geräte mit ständig wechselnden Benutzer*innen eignet sich der Betrieb Multi Device Mode.
Für die Nutzung typischer Unternehmensanwendungen eignet sich Microsoft VPN Tunnel für Intune.
Diese Technologie unterstützt die Kategorie „Information- und Firstline Worker“.

6.3 Vollwertiges Notebook mit Windows mit Azure VPN Anbindung

Hauptschwerpunkt sind die Themfelder:

- Offline-Arbeit
- Typische Anwendungen/Top 3 Anwendungen
- Multi-User-Devices
- Zentraler Identitäts- und Zugriffsverwaltungsdienst

Für die Kategorie „Office Worker, empfiehlt sich der Einsatz von vollwertigen Notebooks als Azure AD Clound-only. Durch eine VPN Anbindung mittels Azure VPN Gateway sind Zugriffe auf Netzlaufwerke sowie die Nutzung lokaler Ressourcen möglich. Die Azure VPN Anbindung wird vollständig über die Microsoft Geräteverwaltung konfiguriert. Im Cloud-only Betrieb lassen sich auch Absicherungen über das Conditional Access in Verbindung mit dem Azure AD einrichten.

Für eine passwortfreie Authentifizierung existieren mehrere Authentifizierungsmethoden. Für die Offline Arbeit empfiehlt sich Microsoft Information Protection, speziell für Datenablage und -verwaltung. Alternativ können vollwertige Notebooks auch als Multi-User Devices mit einem Device VPN Tunnel über das Azure VPN Gateway konfiguriert werden.

7 Design-Pilot

Die aus der Aufnahme der Ist-Situation, den Workshops zu den Schlüsseltechnologien Intune bzw. Endpoint Manager sowie den Workshops mit den Ehrenamtlichen gewonnenen Erkenntnisse bilden die Grundlage für die Auswahl von verschiedenen Design-Piloten.

Insgesamt wurden elf alternative Szenarien für den Design-Piloten betrachtet. Jeder bietet einen eigenen Lösungsansatz in Form einer bestimmten Technologie oder Bereitstellungsform, der sogenannten Best Practices (bewährten Standardlösungen) der Branche entspricht.

Für die Pilotphase hat man die vier Ansätze ausgewählt, die die erfolgversprechendsten Lösungsansätze für wesentliche Anforderungen der Malteser im Ehrenamt bieten. Die folgenden sieben Szenarien sind erst einmal zurückgestellt, könnten aber in Zukunft wieder aufgegriffen werden:

- Windows 365
- Citrix on Azure
- Microsoft Cloud App Security
- Microsoft Information Protection
- Windows fully managed device with always-on VPN
- Android App Protection
- Citrix Workspace

Die vier im Rahmen der Pilotphase weiter verfolgten Ansätze sind:

- Virtueller Arbeitsplatz – Azure Virtual Desktop
- Arbeitscontainer auf Android
- App Protection auf iOS und iPadOS
- Vollwertiges Notebook – Windows (SoCura-verwaltet)

Die elf einzelnen Pilotansätze lassen sich nicht einfach als jeweils qualitativ bessere oder schlechtere Lösungen beschreiben. Sie repräsentieren vielmehr ein knappes Dutzend einzelner Bausteine einer zu einem späteren Zeitpunkt möglichen Gesamtlösung. Allerdings sind einzelne Pilotansätze für die Anforderungen bestimmter Anwender*innengruppen besser oder schlechter geeignet.

Alle in den Workshops im Detail aufgenommen Anforderungen ergeben zusammengenommen ein vollumfängliches, allerdings nicht im Rahmen des vorliegenden Projektes realisierbares (Wunsch-)Bild – die sprichwörtliche „eierlegende Wollmilchsau“. Ein Blick auf Anforderungen liefert wertvolle

Erkenntnisse und Anregungen. Mit Blick auf eine pragmatische, unter den gegebenen Möglichkeiten realistische Vorgehensweise ist es allerdings erforderlich, die Bausteine, die möglichst viele der erarbeiteten Anforderungen adressieren, einzeln herauszugreifen und umzusetzen.

Aus diesen Gründen hat man für die Pilotphase dieses Projektes einen MVP-Ansatz gewählt. Dieser Minimum Viable Product Ansatz zielt darauf ab, möglichst schnelle und einfache, mit geringem Ressourceneinsatz umzusetzende Lösungen zu erstellen, die minimal funktionsfähig (Minimum Viable) sind und für die Anwender*innen bereits einen ersten spürbaren und sinnvollen Nutzen bieten. Dafür wurden vier der oben genannten Szenarien ausgewählt, die sich in wenigen Tagen und mit überschaubaren Lizenz- und Gerätekosten bis zur Testbereitschaft aufbauen lassen.

In technischer Hinsicht war die Pilotphase ein Erfolg. Die vier ausgewählten Proof-of-Concept-Szenarien deckten die wesentlichen Bedürfnisse an die IT-Struktur für das Ehrenamt weitgehend ab. Die Bewertung der Pilotteilnehmer*innen fiel allerdings uneinheitlich aus. Eine favorisierte Lösung, die wirklich alle Bedürfnisse (etwa von Offline- und Online-Arbeitenden gleichermaßen) abdeckt, gibt es nicht. Auch sind hierbei die – je nach Szenario teilweise erforderlichen – Lizenzerweiterungen, von O365 F3 in M365 F3, bis hin zur Nutzung einer E5-Lizenz (notwendig bei Nutzung von Cloud App Security) und die damit verbundenen Kosten zu berücksichtigen und abzuwägen.

Das Projekt hat gezeigt, dass Microsoft für alle diese Szenarien geeignete Mobile-Device-Management-Lösungen zur Bereitstellung und Verwaltung von Geräten bietet. Mit ihnen gehen weitreichende Potenziale für die Zukunft einher, insbesondere für die weitere Verschlankung von Prozessen, eine leichtere und zentralisierte Verwaltung sowie mit Blick auf eine allgemeine Modernisierung der IT.

Als Nachteil bzw. Problem ist neben den teilweise hohen Kosten für die Lizenzierung insbesondere auch der zur hinreichenden Absicherung erforderliche Eingriff in private Geräte (beim BYOD-Szenario) anzusehen. Viele der Teilnehmer*innen empfanden diese Eingriffe als zumutbar. Der Testzeitraum war allerdings relativ kurz, sodass eine tiefergehende Auseinandersetzung mit zusätzlichen Sicherheitsvorgaben und weiterreichenden Anforderungen aus dem ehrenamtlichen Arbeitsalltag erforderlich ist.

Im Detail ist deshalb ein Ausbau der ausgewählten Szenarien im Vergleich zu den in den Piloten gestellten Test-Umgebungen erforderlich, insbesondere mit anspruchsvolleren Sicherheitseinstellungen. Es bleibt abzuwarten, ob die Anwender*innen die Verwaltung der Geräte und deren Absicherung dann spürbarer als Eingriff „von außen“ und ggf. auch als leichte Beeinträchtigung erleben werden.

Für die Pilotphase hatte man im laufenden Projekt insgesamt elf Szenarien erwogen, die sich nicht gegenseitig ausschließen, sondern als einzelne Bausteine einer möglichen Gesamtlösung zu verstehen sind. Auch hier bieten sich Ansätze für ein mögliches Folgeprojekt, in dem einzelne dieser Szenarien technisch ermöglicht und erprobt werden könnten – ggf. in Abstimmung mit anderen, für den hauptamtlichen Bereich laufenden Initiativen rund um die Malteser IT-Infrastruktur.

7.1 MVP 1 – Virtueller Arbeitsplatz – Azure Virtual Desktop

Hierbei wird ein vollwertiger Arbeitsplatz als sogenannter Virtual Desktop bereitgestellt. Die Anwender*innen können die eigene Ausstattung nutzen und benötigen keine zusätzliche Hardware, müssen allerdings über eine Internetverbindung verfügen. Sie können dann mit einem vollwertigen Arbeitsplatz mit Maus, Tastatur und eigenem Desktop-Betriebssystem arbeiten, unabhängig davon, welches eigene Betriebssystem sie verwenden. Die Malteser können die Benutzerprofile zentral verwalten. Der virtuelle Desktop wird in einer Sandbox auf dem Gerät der Anwender*innen sicher ausgeführt, wobei die Malteser nicht auf das Gerät der Anwender*innen zugreifen können. Eine VPN-Verbindung ist hierfür nicht erforderlich.

Dieses Szenario ist für Desktop-PCs, Notebooks und Tablets gleichermaßen geeignet, unabhängig vom Betriebssystem der Geräte. Es wird ein HTML-Browser benötigt. Fehlendes oder nicht ausreichendes Zubehör (etwa zu kleine Monitore, nicht vorhandene Maus, Tastatur usw.) können die Nutzbarkeit beeinträchtigen. Der wesentliche Nachteil: Eine Internetverbindung ist zwingend erforderlich, offline kann nicht gearbeitet werden.

7.2 MVP 2 – Arbeitscontainer auf Android

Hierbei wird auf einem mobilen Endgerät ein Arbeitsbereich als sogenannter Arbeitscontainer bereitgestellt. Die Anwender*innen benötigen dazu ein eigenes, durch die Malteser oder von einem Dritten bereitgestelltes Smartphone oder Tablet mit Android-Betriebssystem. Das Arbeiten mittels gesichertem Container ermöglicht eine klare Trennung zwischen persönlichen bzw. privaten Daten und Applikationen und solchen, die vom Unternehmen bereitgestellt werden.

Die Containerlösung hat den Vorteil, dass die Einhaltung von Firmen-Richtlinien auf die Applikationen und Daten beschränkt werden kann, die vom Unternehmen bereitgestellt werden. Im Offline-Modus können die Anwender*innen mit den im Hintergrund geladenen Daten weiterarbeiten.

Im Eingriff der Malteser IT auf private Endgeräte kann man (muss man aber nicht) ggf. einen Nachteil sehen.

7.3 MVP 3 – App Protection auf iOS und iPadOS

Bei dieser Variante werden mithilfe einer sogenannten App Protection Policy für jede Applikation einzeln der Zugriff und die Verarbeitungsmöglichkeiten von Firmendaten detailliert geregelt. Der Zugriff auf die Daten ist dann – im Rahmen der Festlegungen der App Protection Policy – prinzipiell von jedem Ort und zu jeder Zeit möglich, auch etwa von einem privaten iPhone oder iPad.

Ein wesentlicher Vorteil besteht in reduzierten Aufwendungen für die vergleichsweise hochpreisigen Geräte mit iOS und iPadOS. Die Malteser müssten beispielsweise keine gesonderte Hardware für Ehrenamtliche kaufen, sofern diese ein BYOD-Gerät nutzen möchten.

Aus Anwender*innensicht kann auf ein zusätzliches Gerät verzichtet werden und auch die Unterteilung auf verschiedene Bereiche (wie es bei einer Container-Lösung der Fall wäre) entfällt. Anwender*innen können Apps mit mehreren verschiedenen Accounts nutzen. Sollten zwei oder mehr

Accounts unterschiedlich starke Richtlinien mit sich bringen, so greift i. d. R. die weiterreichende Richtlinie bei der Nutzung der App, und zwar unabhängig vom jeweils genutzten Account.

Die Anwender*innen erfahren eine vergleichsweise hohe Flexibilität, insbesondere bei der Nutzung von Office-Apps, Teams und Outlook. Diese Apps von Microsoft sind via Multi-Account nutzbar und deshalb für die Tests prädestiniert.

Allerdings ist die Verwaltung einer App Protection Policy mit relativ hohem Aufwand verbunden. Die Kontrolle kann sich als schwierig erweisen und eine vergleichsweise geringere Datensicherheit kann daraus resultieren. Beispielsweise erschwert die DSGVO die Kontrolle in manchen Anwendungsfällen. Viele private Daten sind sprichwörtlich tabu, private Bilder, Nachrichten, E-Mails, Browserverläufe usw. sind in besonderem Maße zu schützen. Nicht alle Apps sind Multi-User fähig, sondern auf die Nutzung mit nur einem Account ausgelegt.

7.4 MVP 4 – Vollwertiges Notebook – Windows (SoCura-verwaltet)

Auf einem von der Malteser IT bereitgestellten und verwalteten Notebook wird ein vollwertiger Arbeitsplatz bereitgestellt. Die Anbindung an das Corporate Network der Malteser ist möglich, ebenso wie das Arbeiten im Offline-Modus. Es gibt keine Einschränkungen hinsichtlich der Produktivität.

Als Nachteil ist zu nennen, dass hohe Kosten anfallen für Hardware und Lizenzen, Administration, Verwaltung und Konfiguration, Support und Austausch der bereitgestellten Geräte.

8 Pilotphase

Das Projektteam führte einen Proof of Concept mit Ehrenamtlichen der Malteser durch. Die insgesamt rund 50 freiwilligen Teilnehmer*innen stammen aus zehn Gliederungen. In einem Zeitraum von zehn Tagen (mit zwei vollen Wochenenden) testeten die Ehrenamtlichen jeweils einen oder mehrere Piloten. Das folgende Kapitel erläutert den Verlauf der Pilotphase sowie die daraus abgeleiteten Erkenntnisse.

8.1 Ablauf

Die Geräte für den Testzeitraum wurden durch die Malteser gestellt und verblieben anschließend bei den Gliederungen, deren Mitarbeitende sich an den Pilottests beteiligen. Die Tester*innen wurden sporadisch vom Projektteam angerufen und angeschrieben. Technischer Support war in den üblichen Zeitfenstern verfügbar und auch das Projektteam jederzeit erreichbar. Die Tests erfolgten entlang eines strukturierten Fragenkatalogs, freie Tests waren aber ebenso möglich und auch erwünscht. Ihr Feedback konnten die Ehrenamtlichen über eine Microsoft-Forms-Umfrage einreichen, also einen weiteren strukturierten Fragenkatalog in einem Webtool (die Abbildung unten zeigt einen Auszug aus dem Fragenkatalog).

Die Teilnehmer*innen konnten ihr Feedback selbstständig abgeben, sich für Unterstützung aber auch an das Projektteam wenden. Die Mitglieder des Projektteams dokumentierten während der Pilotphase auch abseits der strukturierten Feedback-Kanäle eingehendes Feedback.

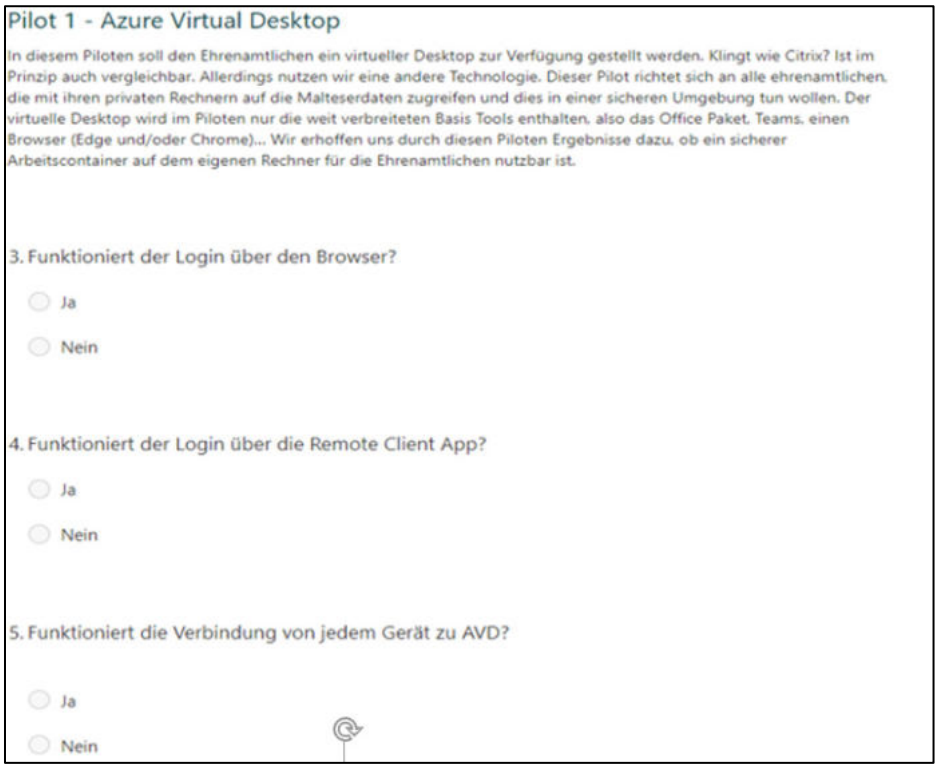


Abbildung 6:Auszug aus der Feedback Abfrage

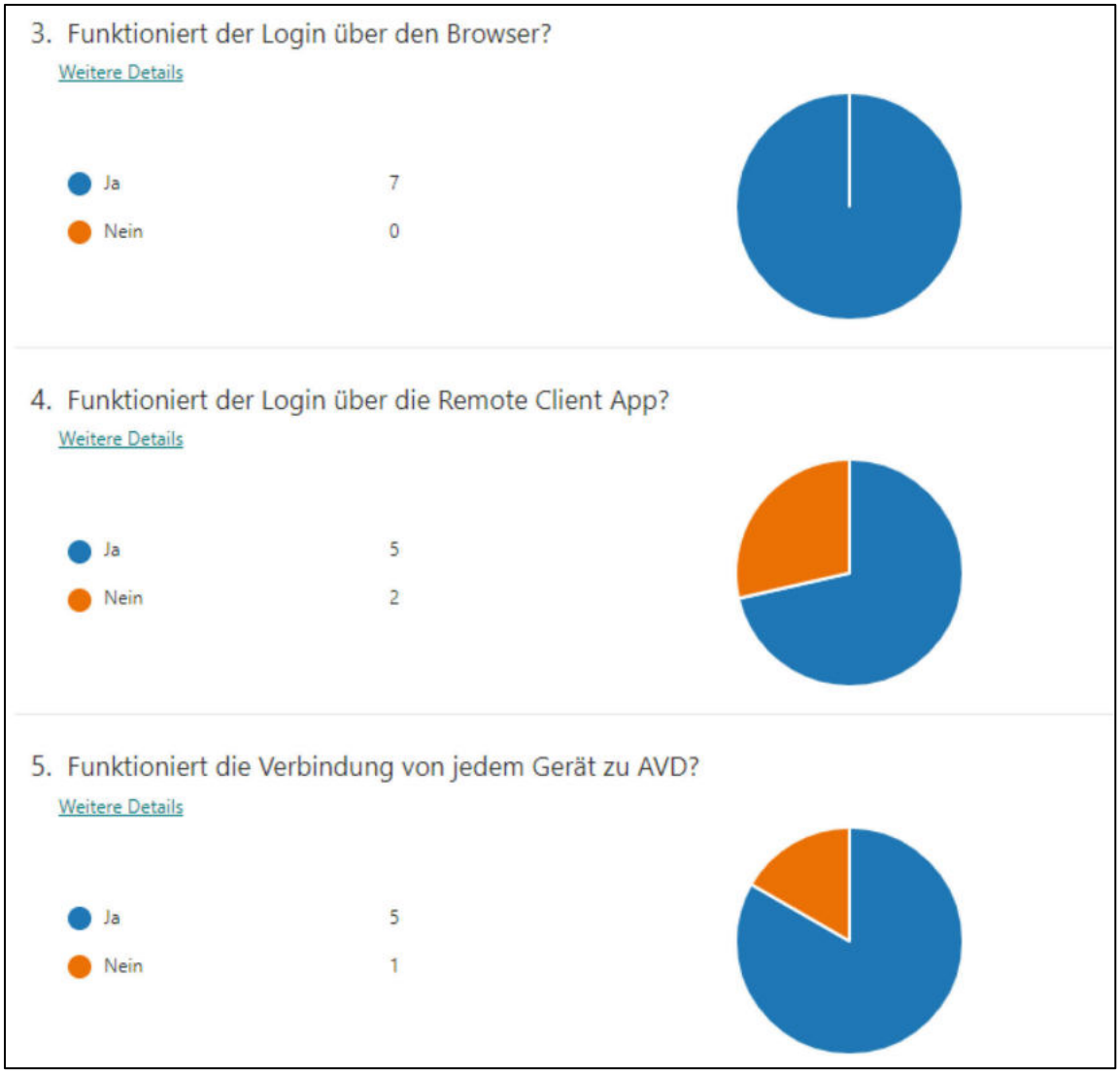


Abbildung 7: Auszug der Feedbackauswertung (Quelle: SoCura)

Die Teilnehmer*innen konnten entweder mit eigener Hardware oder mit gestellten Geräten an der Pilotphase teilnehmen. BYOD war als Teil des Pilotszenarios ausdrücklich erwünscht, da die Nutzung eigener Hardware denkbaren späteren Anwendungsfällen tendenziell am nächsten kommen dürfte. Die Teilnehmer*innen, die für den Piloten eigene Endgeräte einsetzen wollten, wurden bereits im Rahmen der Kick-Off-Veranstaltung gebeten, Datensicherungen durchzuführen oder alternativ auf die gestellte Hardware zurückzugreifen.

Nach dem Aufbau der Piloten wurden die Teilnehmer*innen tageweise versetzt freigeschaltet, um allen am Test beteiligten Ehrenamtlichen unmittelbar zu Testbeginn ausreichende Support-Kapazitäten anbieten zu können.

Die während der Pilotphase gewonnenen Erkenntnisse wurden mit den in den Anforderungsworkshops aufgenommenen Anforderungen abgeglichen und bilden die Grundlage für die weitere Entwicklung von Ansätzen und Ideen, Ableitung von Entwicklungspotenzialen sowie kurz- bis mittelfristige Handlungsoptionen.

9 Erkenntnisse/Ergebnisse

Die Ergebnisse aus den Workshops zeigten, dass die Arbeitsweise von Ehrenamtlichen sich einem (oder auch mehreren) der folgenden Profile bzw. Arbeitsweisen zuordnen lassen:

- Vollwertiger virtueller Arbeitsplatz ohne vorgegebene Hardware
- Überprüfung und kurze Check-ins von Aufgaben/Informationen von Unterwegs
- Vollwertiger Arbeitsplatz mit Hardware und Offline-Arbeit

Die Pilotphase hatte das Ziel, die verschiedenen Profile über einen oder mehrere Proofs of Concept abzudecken.

Unabhängig von diesen Profilen sind folgende Anforderungen übergreifend von Bedeutung:

- Support durch die SoCura
- Einfache Einrichtung und Handhabung
- Trennung von privaten Daten und Malteser Daten
- Kein Eingriff der Malteser IT auf persönliche Geräte

9.1 Virtueller Arbeitsplatz – Azure Virtual Desktop

Für den Test wurde allen Pilotteilnehmer*innen sowohl ein Windows-10- als auch ein Windows-11-Desktop bereitgestellt.

9.1.1 Bereitstellung/Login

In Azure Virtual Desktop (AVD) besteht die Möglichkeit, sich sowohl über den HTML-Browser als auch, bei Unterstützung vom Betriebssystem, über den Remote-Desktop-Client einzuwählen. Bei Android, MacOS und iOS steht über den jeweiligen Store ebenfalls eine Remote-Desktop-App zur Verfügung.

Alle Teilnehmer*innen empfanden die Einwahl über den Browser oder über die verschiedenen Apps als einfach und selbsterklärend.

Einzelne Teilnehmer*innen hinterfragten die Häufigkeit der Kennwortabfragen. Ein Vergleich mit der bestehenden Citrix-Umgebung steht noch aus. Um die Anzahl der Kennwortabfragen zu reduzieren, wäre Single-Sign-On ein natürlicher Lösungsansatz.

9.1.2 Performance/Qualität

Die Übertragungs- und Reaktionsgeschwindigkeit der Desktops wurden von den Teilnehmer*innen als flüssig wahrgenommen, auch das Verhalten der Apps diesbezüglich gelobt. Einige Teilnehmer*innen empfanden die Umgebung performanter als die derzeit verwendete Citrix-Umgebung.

Ein Teilnehmer empfand die Desktopauflösung als unscharf und äußerte Bedenken in Bezug auf eine intensivere Nutzung über einen längeren Zeitraum.

Im Bereich Teams-Telefonie über Citrix gab es von einigen Teilnehmer*innen die Rückmeldung, dass Telefonate immer wieder abbrachen und der Ton nicht mehr funktionierte. Im Vergleich dazu hat die Umgebung mit Azure Virtual Desktop besser funktioniert (auch mit besserer Tonqualität).

9.1.3 Auswahl von Desktop und Applikationen

Zahlreiche Teilnehmer*innen bemängelten, dass Ihnen für weiterreichende und aussagekräftigere Tests und Vergleiche mit bestehenden virtuellen Arbeitsplätzen Applikationen fehlten, wie etwa:

- Videokonferenz-Tools (z. B. WebEx, Zoom)
- Grafikbearbeitung (z. B. Inkscape, Gimp)
- Mindmap (z. B. Xmind)
- PDF-Viewer
- DokBox
- ARNO
- Xviewer

Ein Teilnehmer (der IT-Verantwortlicher ist), wünschte sich lokale Administrationsrechte, um weitere Administrator*innen-Apps zu installieren:

- Power Apps
- Administrator Tools

9.1.4 Verfügbarkeit

Die Verfügbarkeit wurde von allen Teilnehmer*innen als gut bewertet. Bei den meisten kam es zudem sehr gut an, dass die virtuellen Desktops auch außerhalb der regulären Arbeitszeiten hochgefahren werden (im ausgeschalteten Zustand, aber dennoch automatisiert), sobald man sich mit einem Desktop verbinden möchte.

9.1.5 Performance – Netzwerk und Umgebung

Die Netzwerkqualität wurde mit gut bewertet. Auch hier gab es mehrfach die Rückmeldung, dass die AVD-Umgebung stabiler und besser lief als die aktuell verwendete Citrix-Umgebung.

Einige Teilnehmer*innen haben mehrfach bestätigt, dass insbesondere für Hauptamtliche Zugriff auf malteserinterne Netzwerke wichtig wäre, um auf lokale Ressourcen und Applikationen auch aus der AVD-Umgebung zugreifen zu können.

9.2 Arbeitscontainer auf Android

Für den Test wurde Hardware an die Teilnehmer*innen ausgeteilt. Einige erhielten Smartphones, andere Tablets mit Android OS. Den Teilnehmer*innen wurde freigestellt, zusätzlich (oder auch ausschließlich) eigene Geräte einzubringen. Letztlich nahm etwa jeder zweite beteiligte Ehrenamtliche mit einem privaten Geräte teil.

9.2.1 Allgemein

Die Teilnehmer*innen fanden es gut und wichtig, dass die persönliche von der Malteser Umgebung getrennt wurde. Viele von ihnen hatten Bedenken darüber geäußert, dass eine fremde IT (wie etwa die Malteser IT) Zugriff auf ihre privaten Geräte erhalten könnte. Arbeitscontainer empfanden sie als eine gute Möglichkeit, die oben genannte Trennung herbeizuführen, da sie den Anwender*innen durch die sichtbare Trennung im Arbeitscontainer subjektiv ein Sicherheitsgefühl vermitteln und sie diese Art des Zugriffs als wenig invasiv empfanden. Einige Teilnehmer*innen gaben an, dass ihre Hemmschwelle gesunken sei und sie sich vorstellen könnten, eine solche Lösung zukünftig zu nutzen.

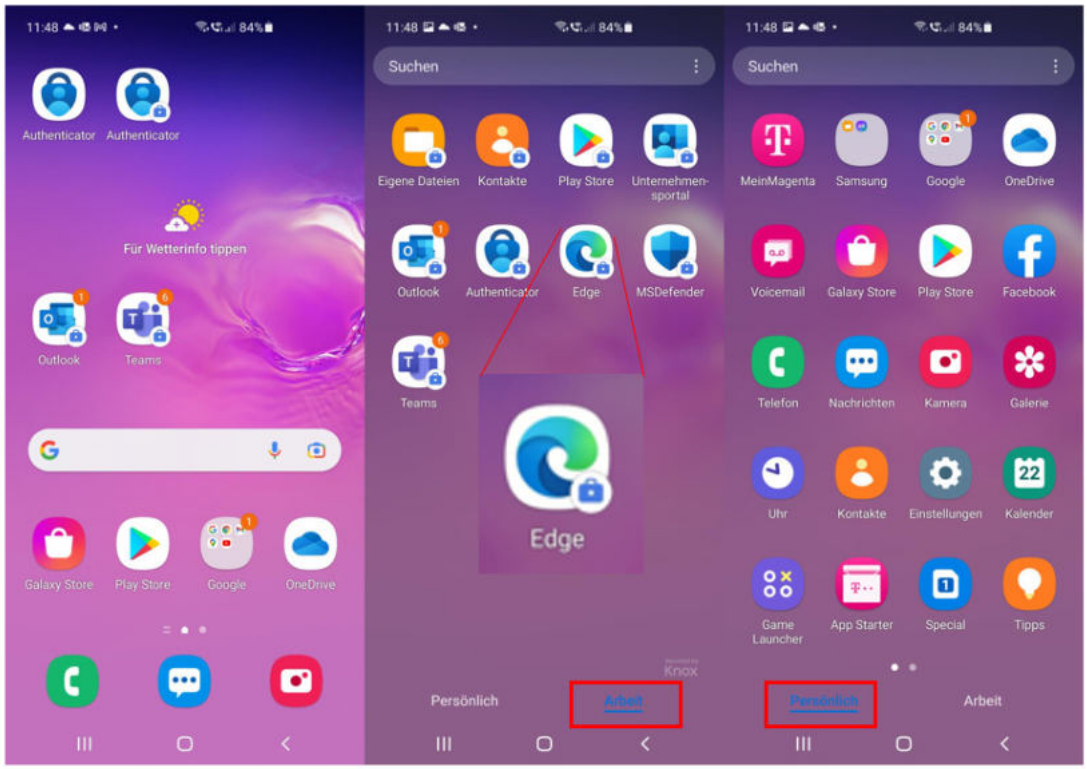


Abbildung 8: Sichtbare Trennung von persönlicher und geschäftlicher Umgebung (Quelle: Skaylink)

9.2.2 Bereitstellung/Login

Die Einrichtung der Containerlösung nahmen die Tester überwiegend als gut und schnell wahr, maßen der bereitgestellten Schritt-für-Schritt-Anleitung zur Ersteinrichtung aber dennoch eine hohe Bedeutung bei.

Einzelne Teilnehmer*innen hatten das Problem, dass auf ihren privat eingebrachten Geräten nicht mehr ausreichen freier Speicher für den Arbeitscontainer verfügbar war.

9.2.3 Performance

Die Performance wurde uneingeschränkt als gut bewertet. Unterschiede im Vergleich zur bisherigen Arbeitsform auf Geräten mit Android OS ohne Arbeitscontainer wurden erwartungsgemäß nicht erkannt.

9.2.4 Auswahl an Applikationen

Die wichtigsten Apps standen im privaten Playstore der Unternehmensumgebung zur Verfügung und wurden auch automatisch im Hintergrund installiert. Einige Applikationen, die bei einer produktiven Umgebung für die Arbeit und dementsprechend auch für den Testlauf wichtig gewesen wären, fehlten hierbei. Genannt wurden in diesem Zusammenhang:

- OneDrive
- Zoom
- Skype
- Planner
- ToDo
- OneNote
- Office Lens
- SharePoint
- Arno
- Vivendi
- Power Alarm
- CovPass
- aPager Pro

Die Teilnehmer*innen empfanden die erneute Installation von Apps als sinnvoll. Zwar seien diese damit doppelt vorhanden, gleichzeitig sei dies im Sinne einer leichten und transparenten Trennung von Privatem und Beruflichem. Dadurch sinke die Hemmschwelle, berufliche Accounts auch privat, bzw. private Accounts für das Ehrenamt zu nutzen. Die Teilnehmer*innen sahen in der Containerlösung das Potenzial, die Bereitschaft zu steigern, Geräte in BYOD-Szenarien zu nutzen.

Als nachteilig wurde bewertet, dass durch die automatisierte und erzwungene Installation der Apps nach der Einrichtung des Arbeitscontainers Probleme mit der Speicherplatzkapazität entstehen könnten.

9.2.5 Verfügbarkeit

Das Arbeiten mit den Apps und die Offline-Funktion wurden als sehr gut bewertet.

9.2.6 Netzwerk

Die Netzwerkqualität wurde (abhängig von der vorhandenen Bandbreite der Mobilfunkkarte) ebenfalls mit gut bewertet.

Einige Teilnehmer*innen wünschten sich, dass bestimmte WLAN-Einstellungen von Organisationseinheiten bzw. Liegenschaften der Malteser im Arbeitscontainer ebenfalls schon vorkonfiguriert sein sollten.

9.3 App Protection auf iOS und iPad OS

Die Teilnehmer*innen erhielten Tablets mit iPadOS oder nutzten private Geräte mit iOS oder iPadOS.

Die Rückmeldung war insgesamt positiv. Die Zugriffsmöglichkeit auf Unternehmensressourcen ohne zusätzliches Endgerät wurde dabei wiederholt hervorgehoben. Insbesondere die Trennung von privaten Daten in den Apps durch App Protection Policies erhöhte das Vertrauen in ein sicheres Arbeiten mit Unternehmensdaten.

9.3.1 Einrichtung/Login

Ersteinrichtung und Log-in funktionierten problemlos, kritische Rückmeldungen gab es hierzu nicht.

9.3.2 Performance

Einige Testteilnehmer*innen sahen eine enorme Verbesserung der Anwender*innenfreundlichkeit im Vergleich zur Arbeit mit einem Windows-Laptop. Mobilität bringt im Arbeitsalltag der Helfenden sehr viel, da zur Not auch das Smartphone ausreicht, um kleine Änderungen vorzunehmen.

Als besonders angenehm wurden von einigen Teilnehmer*innen die Kommunikationsmöglichkeiten zwischen den Geräten (etwa mit geräteübergreifenden Zwischenablagen) und auch die Handover-Funktion bewertet. Hier böten sich Möglichkeiten für ganz neue Workflows.

Auch wurde eine Verbesserung des Schutzes von sensiblen Informationen erkannt.

9.3.3 Auswahl an Applikationen

Einige Applikationen, die bei einer produktiven Umgebung für die Arbeit und dementsprechend auch für den Testlauf wichtig gewesen wären, fehlten. Genannt wurden in diesem Zusammenhang:

- OneDrive
- Zoom
- Skype
- Planner
- ToDo

- OneNote
- Office Lens
- SharePoint
- Arno
- Vivendi
- Power Alarm
- CovPass
- aPager Pro

9.3.4 Verfügbarkeit

Das Arbeiten mit den Apps und die Offline-Funktion wurden als sehr gut bewertet.

9.3.5 Netzwerk

Die Netzwerkqualität wurde (abhängig von der vorhandenen Bandbreite des Mobilfunkkarte) ebenfalls mit gut bewertet.

Einige Teilnehmer*innen wünschten sich, dass bestimmte WLAN-Einstellungen von Organisationseinheiten bzw. Liegenschaften der Malteser im Arbeitscontainer ebenfalls schon vorkonfiguriert sein sollten.

9.4 Vollwertiges Notebook – Windows (SoCura-verwaltet)

Die Teilnehmer*innen erhielten ein von der SoCura verwaltetes Notebook.

9.4.1 Bereitstellung/Login

Die Teilnehmer*innen haben diesen Punkt mit gut bewertet.

9.4.2 Performance

Fast alle Teilnehmer*innen haben diesen Aspekt als gut bewertet. Einige bemängelten jedoch, dass Performance und Stabilität beeinträchtigt wurde, sobald mit dem Notebook innerhalb der aktuellen Citrix-Umgebung gearbeitet wurde. Ein produktives Arbeiten sei dann nur noch eingeschränkt oder schwer möglich gewesen.

9.4.3 Auswahl an Applikationen

Alle Teilnehmer*innen haben diesen Punkt als gut bewertet. Ein Teilnehmer bemängelte die fehlenden Administrator*innenberechtigungen, um zum Beispiel Teamviewer oder andere lokal gewünschte Programme installieren zu können.

9.4.4 Verfügbarkeit

Zu diesem Punkt gab es keine Rückmeldungen.

9.4.5 Netzwerk

Zu diesem Punkt gab es keine Rückmeldungen.

9.5 Zusätzliche Entwicklungspotenziale

9.5.1 Virtueller Arbeitsplatz – Azure Virtual Desktop

Bereitstellung/Login

Um zu vermeiden, dass – wie bemängelt wurde – häufig das Passwort abgefragt wird, könnte man ein Single-Sign-On über den ADFS-Server einrichten. Alternativ bestünde die Möglichkeit, den ADFS-Server abzuschaffen oder in Verbindung mit Windows Hello for Business zu erweitern. Damit würde nicht nur die Eingabe des Passwortes vereinfacht, sondern diese zugleich abgesichert.

Performance

Um eine bessere bzw. höherer Bildschirmqualität einstellen zu können, bedarf es der Möglichkeit, die Optimierungen der virtuellen Maschinen anzupassen. Diese sind bei der Einrichtung im Leistungszustand konfiguriert und können zentral über die Administrator*innen auf bessere Bildqualität (mit dem Nachteil einer Leistungsverringerung) eingestellt werden.

Auswahl Desktop und Applikationen und Netzwerk

Alle bemängelten fehlenden Apps sollten in der Arbeitsumgebung zentral zur Verfügung gestellt werden. Da bei einigen Apps eine Verbindung zum Corporate Network der Malteser bestehen muss, sollte hier im Hintergrund eine Verbindung zwischen dem Microsoft-Rechenzentrum und den Malteser Rechenzentren aufgebaut werden. Damit wäre sichergestellt, dass alle Applikationen und Ressourcen erreichbar sind.

9.5.2 Arbeitscontainer auf Android und App Protection auf iOS und iPad OS

Auswahl an Applikationen

Alle bemängelten fehlenden Apps sollten in der Arbeitsumgebung zentral zur Verfügung gestellt werden. Da bei einigen Apps eine Verbindung zum Corporate Network der Malteser bestehen muss, sollte bei allen Geräten ebenfalls eine appgesteuerte VPN-Verbindung im Hintergrund zum Rechenzentrum der Malteser aufgebaut werden. Diese Technologie wird auch durch den Microsoft Endpoint Manager unterstützt und kann als Erweiterung konfiguriert werden.

Des Weiteren sollten keine Apps für die Installation erzwungen werden, da dies insbesondere bei älteren Smartphones zu Speicherproblemen führen könnte.

10 Technischer Anhang

Im Folgenden werden Lösungen, Technologien und Best Practices beschrieben, die Alternativen zu den in der Malteser IT-Landschaft eingesetzten Infrastrukturlösungen bieten.

10.1 Gerätebereitstellung – Windows Autopilot

Eine Alternative zur Bereitstellung eines modernen IT-Arbeitsplatzes bietet Microsoft Endpoint Manager (MEM). MEM umfasst Dienste und Tools für die Verwaltung und Überwachung mobiler Endgeräte, von Desktop-Computern, virtueller Maschinen, eingebetteter Geräte und Server. Mit Blick auf die Malteser IT ist der Windows Autopilot relevant.

Windows Geräte können mit Windows Autopilot bereitgestellt werden. Windows Autopilot ist eine Sammlung von Technologien zur Einrichtung und Konfiguration neuer Geräte. Windows Autopilot kann auch zum Zurücksetzen, Ändern und Wiederherstellen von Geräten verwendet werden, z.B. nach einem Virenbefall. Die Neuinstallation kann dabei aus der Ferne erfolgen. Diese Lösung minimiert Aufwände und erforderliche Infrastruktur und führt effizient und schnell zum gewünschten Ergebnis. Es vereinfacht den Windows Gerätelebenszyklus für die IT und die Endbenutzer*innen von Bereitstellung bis Ende der Lebensdauer. Zusammengefasst ergeben sich für die IT Abteilung die folgenden Vorteile bei der Verwendung vom cloudbasierenten Windows Autopilot:

- reduziert die Zeit, die die IT für die Bereitstellung, Verwaltung und Einstellung von Geräten aufwendet.
- reduziert die für die Wartung der Geräte erforderliche Infrastruktur.
- Maximiert die Benutzerfreundlichkeit für alle Arten von Endbenutzer*innen.

Übersicht über das Verfahren zum Lifecycle und Bereitstellung mittels Windows Autopilot

Bereitstellung:

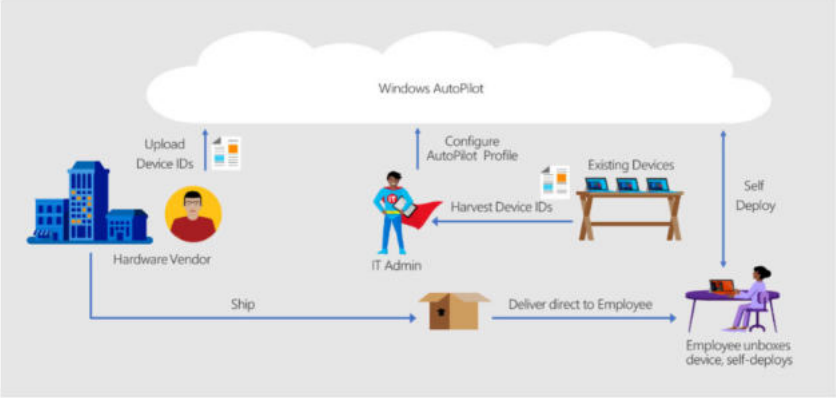


Abbildung 9: https://docs.microsoft.com/de-de/mem/autopilot/images/image2.png

Wenn durch den Auftraggeber zugelassen, kann der Hardwarelieferant schon während des Bestellvorgangs neue Geräte automatisiert im Firmentenant registrieren. Alternativ kann der Administrator auch über eine manuelle Registrierung die Geräte im Firmentenant aufnehmen. Sobald

der Anwender seine Hardware startet, muss er nur noch die Sprache und das Tastatur-Layout auswählen und den Client mit dem Internet verbinden.

Nach erfolgreicher Internetverbindung prüft der Client mittels Hardware ID, ob er für eine Organisation registriert wurde. Da die Hardware ID des Client vorab im Tenant eingepflegt wurde, akzeptiert der Client automatisch die zugewiesene Organisation. Benutzer*innen werden zur Anmeldung mit einer Organisations-E-Mail-Adresse und Passwort aufgefordert. Anschließend wird das Gerät im Azure AD und in Intune registriert und erhält die zugewiesenen Richtlinien und Software. Einem Admin ermöglicht Windows Autopilot die entfernte Vorbereitung eines Geräts, sodass der Mitarbeiter dieses Gerät nach kurzer Installationsphase sofort verwenden kann. Mit Hilfe von Intune und AutoPilot lassen sich Geräte vorkonfigurieren, zurücksetzen, wiederverwenden und wiederherstellen (Device Lifecycle). Es lassen sich Anpassung vornehmen und die Einstellungen ohne erneutes Imaging bereitstellen, was viel Zeit und natürlich finanzielle Mitten erspart. Windows Autopilot verwendet die OEM-optimierte Version von Windows 10/11. Diese Version ist auf dem Client vom Hersteller schon vorinstalliert, sodass nicht für jedes Gerätemodell dedizierte Images und Treiber verwaltet werden müssen. Anstatt ein Gerät neu zu installieren, kann die vorhandene Windows 10-Installation Richtlinien neu einrichten und Software erneut installieren.

Nach Abschluss der Bereitstellung lässt sich entweder Intune, Configuration Manager oder andere Tools zum Verwalten dieser Clients verwenden. Kurz gesagt, Windows Autopilot kann verwendet werden, um das vorhandene Windows-Betriebssystem anzupassen und kein völlig neues Betriebssystem bereitzustellen.

Die Autopilot-Lösung ermöglicht es dem Unternehmen, dies mit wenig bis gar keiner zu verwalteten Infrastruktur zu erreichen. Seit Windows 10 1809 ist auch ein Beitritt in das lokale Active Directory möglich, entweder im internen Unternehmensnetzwerk oder entfernt mittels Azure VPN Gateway. Hier benötigt man aber eine Windows Enterprise als vorinstallierte Windows OEM Version.

Lebenszyklus:

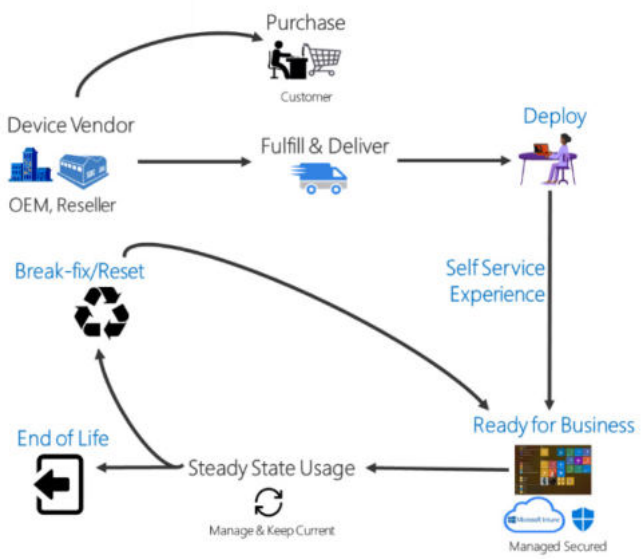


Abbildung 10: https://docs.microsoft.com/de-de/mem/autopilot/images/image1.png

Intune unterstützt bei der Verwaltung der Geräte über den gesamten Lebenszyklus: Von der Registrierung über die Konfiguration und den Schutz bis hin zur Abkopplung des Geräts. Beispiel: Ein unternehmenseigenes Windows Notebook muss zunächst mit dem Microsoft Intune-Konto des Unternehmens registriert werden, damit es verwaltet werden kann. Anschließend muss es den Vorgaben des Unternehmens entsprechend konfiguriert werden. Die von Benutzer*innen auf dem Gerät gespeicherten Daten müssen vor Angriffen, Manipulation und Datenklau geschützt werden. Schlussendlich müssen zum Ende des Lebenszyklus oder beim Wechsel der Benutzer*in alle vertraulichen Daten abgekoppelt oder zurückgesetzt werden. Durch modulare Konfigurationen, Richtlinien oder Softwarepakete nach dem Baukastenprinzip lassen sich diese immer wiederverwerten.

Lifecycle-Prozess:

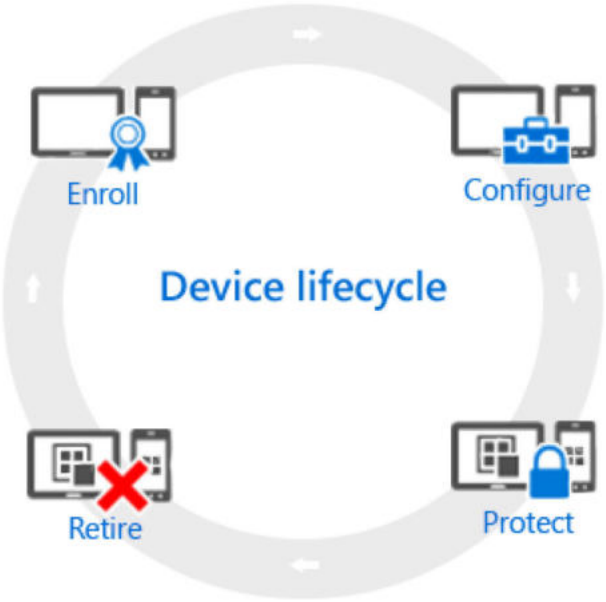


Abbildung 11: https://docs.microsoft.com/de-de/mem/intune/fundamentals/device-lifecycle

Nach der Bereitstellung mit Windows Autopilot können Windows Geräte verwaltet werden mit:

- Microsoft Intune
- Windows Update for Business
- Microsoft Endpoint Configuration Manager
- Andere ähnliche Tools

10.2 Geräteverwaltung und Softwareverteilung – Microsoft Intune

Für die Geräteverwaltung und Softwareverteilung bietet Microsoft Intune für die Malteser geeignete Funktionen.

Microsoft Intune ist ein cloudbasiertes Mobile Management Device und Mobile Application Management für alle Apps und Geräte und Betriebssysteme (Windows 10/11, Android, iOS, iPadOS, macOS), das sich in Azure Active Directory und die mobile Bedrohungsabwehr integrieren lässt.

Architektur Smartphone:

Abbildung 12: Intune high-level Architektur

Diese Referenzarchitektur zeigt Optionen für die Integration von Microsoft Intune in der Azure-Umgebung mit Azure Active Directory.

Mit Android Workprofile und iOS App Protection sind folgende Einstellungen möglich:

- Konfigurationsrichtlinien
- Konformitäts-Status
- Rollout/Installation der Unternehmensapps
- Integration in Conditional Access und Azure AD
- Defender (Endpoint)
- Intune/MEM Console zur Verwaltung
- Inventarisierung und Monitoring der Geräte

Architektur Windows Geräte / Clients

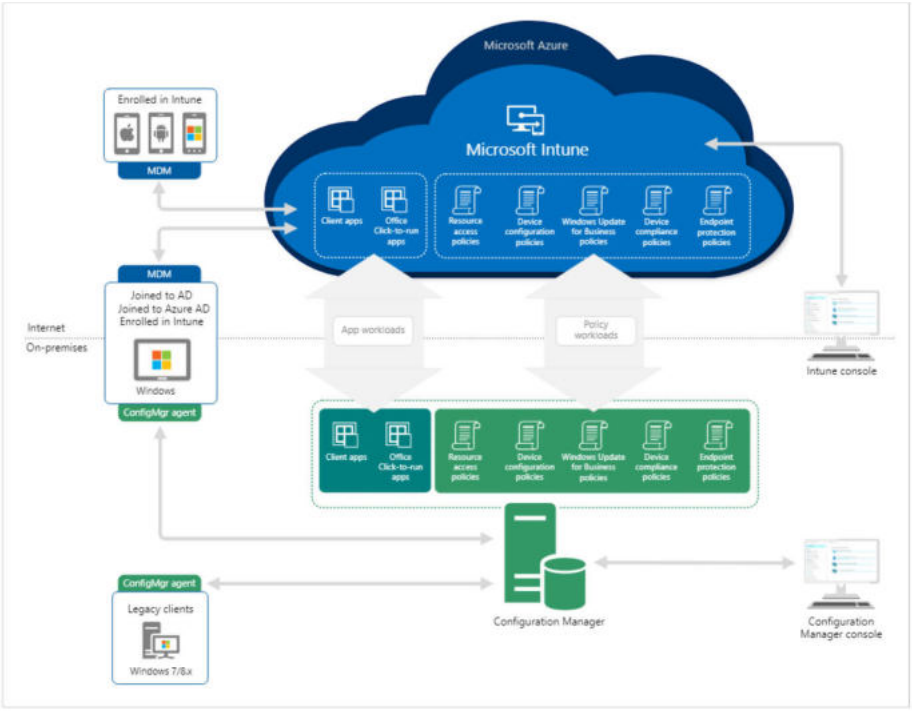


Abbildung 13: https://docs.microsoft.com/en-us/mem/configmgr/comanage/media/co-management-overview.svg

Diese Referenzarchitektur zeigt Optionen für die Integration von Microsoft Intune und Co Management eines Windows Geräts in der Azure-Umgebung mit Azure Active Directory.

Unterstützung von Android:

- Konfigurationsrichtlinien
- Konformstatus
- Rollout/Installation der Unternehmensapps
- Integration in Conditional Access und Azure AD
- Defender (Endpoint) Firewall/Bitlocker/Antivirenprogramm
- Intune/MEM Console zur Verwaltung
- Inventarisierung und Monitoring der Geräte

10.2.1 Kioskmodus für Multi-Device Geräte

Single-App-Kiosk: Eine einzelne App wird im Vollbildmodus auf dem Sperrbildschirm ausgeführt. Die User, die den Client verwenden können somit nur den Kiosk und nur diese App sehen und verwenden. Das besondere, sobald die Kiosk-App geschlossen wird, wird sie automatisch neu gestartet. Sobald ein User die Verbindung trennt, kann der Kiosk-mode so konfiguriert werden, dass dieser sich im Protokollbildschirm automatisch zurückmeldet.

Es ist Erbfalls möglich im Shell Launcher zu starten, um ein Kioskgerät zu konfigurieren, auf dem eine Windows-Desktopanwendung als Benutzeroberfläche ausgeführt wird.

Multi-App-Kiosk: Hier kann wahlweise eine oder mehrere Apps vom Desktop ausgeführt werden. User, die den Kiosk verwenden, wird ein benutzerdefiniertes Startmenü angezeigt, in dem nur die Kacheln oder Apps für die zulässigen Apps angezeigt werden.

10.2.2 Windows Multi-Device Geräte

Windows 10/11-Geräte lassen sich für den Einzel-App-Kioskmodus konfigurieren. Windows 10 Geräte unterstützen zusätzlich den Multi-App-Kioskmodus. Windows 10/11-Geräte können als Multi-User Geräte verwendet werden; sie werden dann als freigegebene Geräte bezeichnet und sind Teil einer mobilen Geräteverwaltung (Mobile Device Management, MDM).

Mit Microsoft Intune können sich Benutzer*innen mit einem Gastkonto bei freigegebenen Geräten anmelden, dann aber nur die für Sie zugelassenen Funktionen nutzen. Ein Intune-Administrator kontrolliert und konfiguriert die Richtlinien.

10.2.3 Android Multi-Device Geräte

Android Enterprise und iOS unterstützen bei unternehmenseigenen Geräten die Verwendung des Shared Device Mode (Multi-User Mode) für gemeinsam genutzte mobile Devices. Solche Geräte werden für einen einzigen Zweck verwendet, z. B. die digitale Beschilderung, das Drucken von Tickets oder die Bestandsverwaltung. Die Administratoren können so verschiedenen Usern eine schnelle Anmeldung und so Zugriff auf die nötigen Unternehmensresscourecen ermöglichen. Für freigegebne Geräte wird eine Identätsgeschützte Verwaltung ermöglicht. Nach der Abmeldung ist das Gerät sofort für den nächsten user Einsatzbereit. Administratoren können die Nutzung installierter Apps beschränken. Ebenso können Benutzer*innen daran gehindert werden, Einstellungen zu verändern oder neue Apps zu installieren.

Benuter benötigen die Rolle des Cloud-Geräteadministrator um Geräte mithilfe der Authentifcator-App in den freigegebenen Modus zu versetzen.

Geräte können auf zwei Arten in Intune registriert werden:

10.2.3.1 Android Enterprise-Standardgerät ohne Benutzerkonto

Diese Geräte werden ohne ein Benutzerkonto in Intune registriert und sind keinem Endbenutzer zugeordnet. Diese Geräte sind nicht für personalisierte Anwendungen oder Apps mit benutzerspezifischen Kontodaten vorgesehen, wie z. B. Outlook oder Gmail.

10.2.3.2 Android Enterprise-Standardgerät mit Azure AD-Modus für gemeinsame Nutzung

Android Enterprise-Standardgeräte mit Azure AD-Modus werden bei Registrierung automatisch durch Microsoft Authenticator für eine gemeinsame Nutzung eingerichtet. Diese Geräte werden ohne ein Benutzerkonto in Intune registriert und sind keinem Endbenutzer zugeordnet. Sie werden im Azure AD-Modus für freigegebene Geräte verwendet und unterstützen Single-Sign-On (SSO).

10.2.4 iOS Multi-Device Geräte – Microsoft Intune

Microsoft Endpoint Manager unterstützt zwei Arten von Lösungen für gemeinsam genutzte Geräte für iOS und iPadOS:

10.2.4.1 Freigegebene iPads

Freigegebene iPads sind für die Verwendung durch mehrere Benutzer*innen eingerichtet. iPads unter iPadOS 13.4 und höher können als „Gemeinsam genutztes iPad“ bereitgestellt werden, wenn sie mithilfe der automatisierten Geräteregistrierung ohne Benutzeraffinität registriert wurden. Ein gemeinsam genutztes iPad besteht aus einer vordefinierten Anzahl von Benutzerpartitionen. Durch Benutzerpartitionen wird sichergestellt, dass die Apps, Daten und Einstellungen der einzelnen Benutzer*innen separat auf dem gemeinsam genutzten iPad gespeichert und in iCloud gesichert werden können (sofern vom Administrator zugelassen). So wird ein nahtloser Übergang zwischen mehreren gemeinsam genutzten iPads gewährleistet. Durch einen Verbund der AAD-Instanz Ihrer Organisation mit Apple Business oder School Manager kann sich eine Benutzer*in mit ihrem AAD-Benutzernamen und -Kennwort an einem gemeinsam genutzten iPad anmelden. So wird bei der ersten Anmeldung automatisch eine verwaltete Apple-ID für die Benutzer*in erstellt, die dem AAD-Benutzernamen entspricht. Außerdem richtet die Benutzer*in bei der ersten Anmeldung an einem gemeinsam genutzten iPad einen alphanumerischen Passcode für die Benutzerpartition ein, und die dem Gerät zugewiesenen Apps werden auf der Benutzerpartition installiert. Wenn die Benutzer*in das nächste Mal auf ein gemeinsam genutztes iPad zugreift, muss er nur die verwaltete Apple-ID (identisch mit dem AAD-Benutzernamen) und den alphanumerischen Passcode angeben.

10.2.4.2 Modus für gemeinsam genutzte Geräte

Mitarbeiter in Service und Produktion verwenden für ihre Arbeit häufig ein gemeinsam genutztes mobiles Gerät. Diese gemeinsam genutzten Geräte können Sicherheitsrisiken darstellen, wenn Benutzer*innen Kennwörter oder Pins absichtlich oder versehentlich teilen, um auf Kunden- und Geschäftsdaten auf dem gemeinsam genutzten Gerät zuzugreifen. Im Modus für gemeinsam genutzte Geräte kann ein Gerät mit iOS 13 oder höher einfach und sicher für die gemeinsame Nutzung durch mehrere Mitarbeiter konfiguriert werden. Mitarbeiter können sich anmelden und schnell auf Kundeninformationen zugreifen. Nach Abschluss der Aufgaben können sie sich auf dem Gerät abmelden, das dann sofort für den nächsten Mitarbeiter einsatzbereit ist. Der Modus für gemeinsam genutzte Geräte ermöglicht auch eine auf Microsoft-Identitäten basierende Verwaltung des Geräts. Diese Funktion verwendet die Microsoft Authenticator-App, um die Benutzer*innen auf dem Gerät zu verwalten und das Microsoft Enterprise SSO-Plug-In für Apple-Geräte zu verteilen.

Das Microsoft Enterprise SSO-Plug-In für Apple-Geräte ermöglicht einmaliges Anmelden (Single Sign-On, SSO) für Azure Active Directory-Konten (Azure AD) auf macOS-, iOS- und iPadOS-Geräten und für alle Anwendungen, die das Feature Enterprise Single Sign-On von Apple unterstützen. Das Plug-In ermöglicht einmaliges Anmelden (SSO) auch für ältere geschäftskritische Anwendungen, die aber noch nicht die neuesten Identitätsbibliotheken oder -protokolle unterstützen. Microsoft hat bei der Entwicklung dieses Plug-Ins eng mit Apple zusammengearbeitet, um die Nutzbarkeit Ihrer Anwendung zu erhöhen, während gleichzeitig bestmöglicher Schutz gewährt wird.

Das Enterprise SSO-Plug-In ist derzeit ein in die folgenden Apps integriertes Feature:

- Microsoft Authenticator: iOS, iPadOS
- Microsoft Intune-Unternehmensportal: macOS

Mit dem Microsoft Enterprise SSO-Plug-In für Apple-Geräte ergeben sich folgende Vorteile:

- SSO für Azure AD-Konten und alle Anwendungen, die das Feature „Enterprise SSO“ von Apple unterstützen
- Kann für jede MDM-Lösung (Mobile Device Management, Verwaltung mobiler Geräte) aktiviert werden
- Weitet einmaliges Anmelden (SSO) auf Anwendungen aus, die noch keine Microsoft Identity Plattform-Bibliotheken nutzen
- Weitet einmaliges Anmelden (SSO) aus Anwendungen aus, die OAuth2, OpenID Connect und SAML nutzen

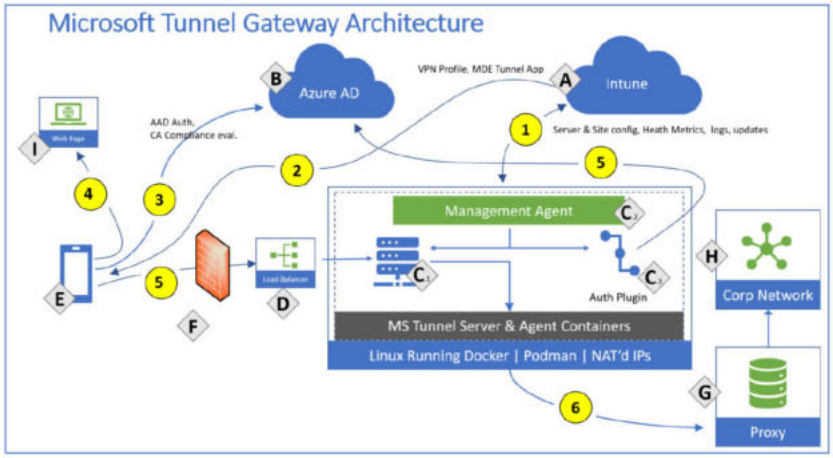
Die bisher genannten Dienste unterstützen den Geräteschutz, Datenschutz und die Risikominimierung. Darüber hinaus unterstützt Microsoft Endpoint Manager die Administration über den gesamten Lebenszyklus bei Verfügbarkeitsprüfung, Leistungsmessung, Inventarisierung und dem Asset Management der zentralen Identitätsplattform Azure Active Directory Informationen über den Zustand der Geräte und steuert den bedingten Zugriff (Conditional Access).

10.3 Microsoft Tunnel VPN

Während der Transformation vom On-Premise Rechenzentrum zur Cloud Infrastruktur ist in der Regel eine Übergangsphase für geschäftskritische, nicht-cloudfähige Anwendungen notwendig. Zur Unterstützung mobiler Android oder iOS Clients kann Microsoft Tunnel VPN über Microsoft Intune genutzt werden.

Microsoft Tunnel ist eine VPN-Gatewaylösung für Microsoft Intune, die als Dockercontainer unter Linux unter ausgeführt wird und für iOS-/iPadOS und Android Enterprise-Geräte den Zugriff auf lokale Ressourcen mit moderner Authentifizierung und bedingtem Zugriff ermöglicht.

MS Tunnel Gateway Architektur:



Komponenten

A	Microsoft Intune
B	Azure Active Directory (AD)
C	C.1: Microsoft Tunnel-Gateway C.2: Verwaltungs-Agent C.3: Authentifizierungs-Plug-In
D	öffentliche IP-Adresse oder FQDN der Tunnel Instanz
E	Mobile Geräteverwaltung (MDM) registriertes Gerät
F	Firewall
G	Interner Proxyserver (optional)
H	Unternehmensnetzwerk
I	Öffentliches Internet

Abbildung 14: Intune Microsoft Tunnel Übersicht

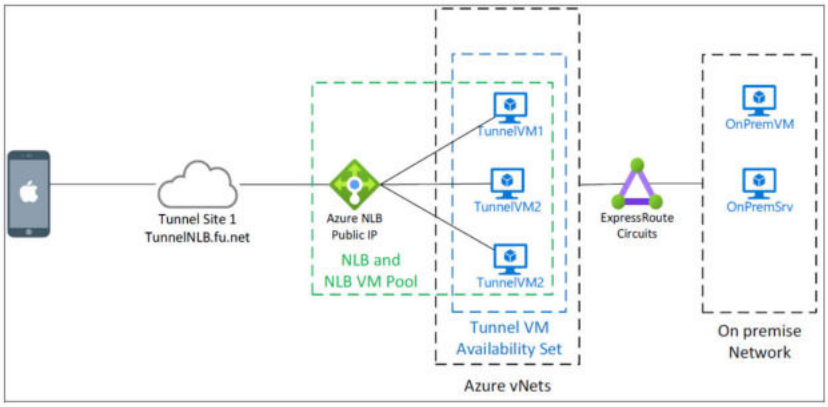


Abbildung 15: Dokumentation zu MS-Tunnel-Gateway_Deployment_Guide_v2

Microsoft Tunnel unterstützt die Verwendung multipler VPN Profile. Zu den Funktionen der VPN-Profile gehören:

- Ein Anzeigename für die VPN-Verbindung, der Endbenutzer*innen angezeigt wird
- Der Standort, mit dem der VPN-Client eine Verbindung herstellt
- VPN-Konfigurationen pro App, die definieren, für welche Apps das VPN-Profil verwendet wird, und ob dieses „always-on“ ist. Wenn „always-on“ festgelegt ist, stellt das VPN automatisch eine Verbindung her und wird nur für die von Ihnen definierten Apps verwendet. Wenn keine Apps definiert sind, bietet die Always-on-Verbindung Tunnelzugriff für den gesamten Netzwerkdatenverkehr des Geräts
- Manuelle Verbindungen mit dem Tunnel, wenn eine Benutzer*in das VPN startet und Verbinden auswählt
- Bedarfsgesteuerte VPN-Regeln, die die Verwendung des VPN zulassen, wenn Bedingungen für spezifische FQDNs (vollqualifizierte Domänennamen) oder IP-Adressen erfüllt sind (iOS/iPadOS)
- Proxyunterstützung (iOS/iPadOS, Android 10 und höher)

Mit dem Einsatz von Microsoft Tunnel VPN wird sichergestellt, dass mobile Endgeräte (iOS/ IpadOS und Android Enterprise) beim Zugriff auf geschäftliche Ressourcen immer sicher und richtlinienkonform sind.

10.4 Microsoft Azure VPN Gateway

Microsoft Azure VPN Gateway stellt eine Verbindung zwischen Cloud Infrastruktur und On-Premise Welt bereit. Mit Azure VPN Gateway (Point-to-Site VPN - P2S-VPN) werden sichere standortübergreifende Verbindungen zwischen virtuellen Netzwerken in Azure und der lokalen IT-Infrastruktur hergestellt. Die Always On VPN Funktion ist unabhängig von der Infrastruktur und ermöglicht damit verschiedene lokale und cloudbasierte Anwendungsszenarien. In Microsoft Azure kann das Azure-VPN-Gateway so konfiguriert werden, dass es Windows 10 Always On-VPN-Clientverbindungen unterstützt. Als Authentifizierungstyp wird dabei die Azure AD-Authentifizierung verwendet. Über Intune wird das entsprechende Always-On VPN-Profil aktiviert. Die VPN-Einbindung erfolgt dann über einen User-VPN Tunnel. Die native Azure AD-Authentifizierung garantiert die Authentizität der Identitäten, die mittels benutzerbasierter Richtlinien, kontrolliertem Zugriff und mehrstufiger Authentifizierung für Point-to-Site-VPNs erreicht wird. Die native Azure AD-Authentifizierung verlangt sowohl die Integration des Azure-VPN-Gateways als auch eine neue Version von Azure VPN Client, um Azure AD-Tokens beziehen und überprüfen zu können.

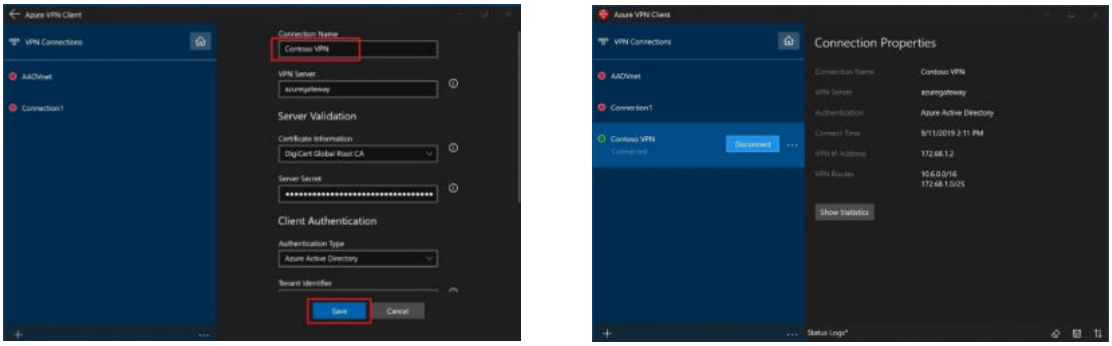


Abbildung 16: Azure VPN Gateway Einrichtung

Architektur: Azure VPN mit Azure AD-Authentifizierung im VPN-Gateway

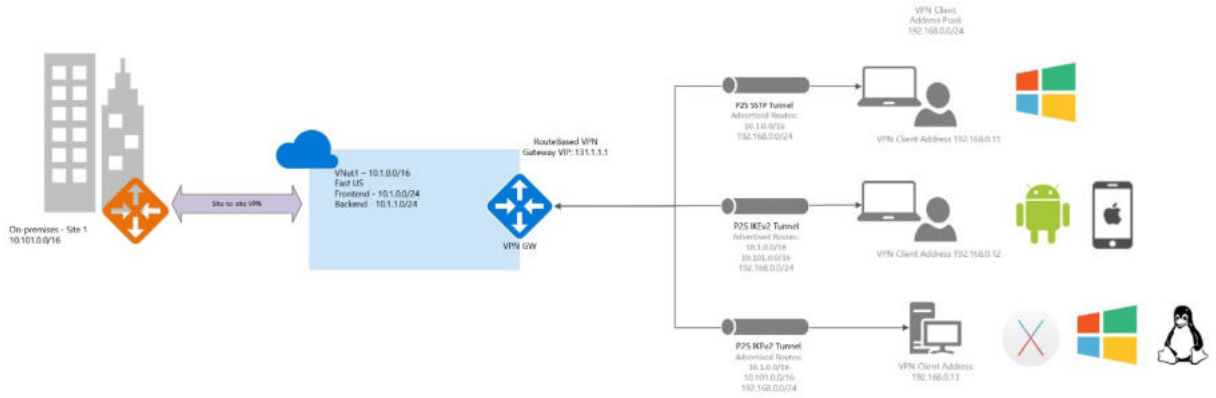


Abbildung 17: Azure VPN Gateway Point-to-Site Routing

Durch die Konnektivität zum Corporate Network mittels Azure VPN P2S können Cloud-only Azure AD Join Geräte weiterhin auf Netzlaufwerke und lokale Ressourcen zugreifen. Voraussetzung ist dabei auch eine Site-to-Site (S2S) VPN Verbindung zwischen dem On-Premise Rechenzentrum und der Azure Region.

10.5 Azure Active Directory für Cloud-Umgebungen

Azure Active Directory, kurz Azure AD oder kürzer AAD, ist ein cloudbasierter Identitäts- und Zugriffsverwaltungsdienst von Microsoft. Bei der Einführung von Microsoft 365 erweitert es die Identitäten der lokalen Umgebung aus dem Active Directory (AD) und verknüpft sie über das Azure Active Directory mit den Identitäten in der Microsoft Cloud. Das hat den Vorteil, dass Mitarbeitende sich mit ihrer Active-Directory-Identität anmelden und auf externe Ressourcen wie Microsoft 365, das Azure Portal und Tausende anderer Software-as-a-Service-Ressourcen zugreifen können. Bei einer entsprechend konfigurierten Verbindung kann damit auch auf interne Ressourcen, etwa Anwendungen im Netzwerk bzw. im Intranet des eigenen Unternehmens oder selbst entwickelte Cloud-Apps, zugegriffen werden.

10.6 Bedingter Zugriff – Conditional Access

Moderne Sicherheitsparameter beziehen nicht mehr nur das Netzwerk einer Organisation mit ein, sondern auch die Anwender*innen- und Geräteidentitäten. Organisationen können diese Identitätssignale für Entscheidungen in Bezug auf die Zugriffssteuerung nutzen. Azure Active Directory setzt hier auf den sogenannten bedingten Zugriff (Conditional Access) als Kern der neuen identitätsbasierten Steuerungsebene, indem die o. g. Identitätssignale zunächst zusammengeführt werden. Aus der Summe der Signale können intelligente Entscheidungen abgeleitet werden. Solche Entscheidungen können beispielsweise das Blockieren eines Zugriffs oder das Gewähren eines Zugriffs auslösen. Auf diesem Wege können verdichtete kleinste Signale zur automatisierten Durchsetzung von Organisationsrichtlinien genutzt werden.

Die einfachsten Richtlinien für den bedingten Zugriff sind Wenn-Dann-Anweisungen: Um auf eine Ressource zugreifen zu können, müssen Anwender*innen eine Aktion ausführen.

Für Administrator*innen einer Organisation ergeben sich daraus zwei zentrale Vorteile für die Zugriffssteuerung:

- Schaffen von Bedingungen für Anwender*innen, unter denen sie an jedem Ort und zu jeder Zeit produktiv sein können
- Schützen der Ressourcen einer Organisation

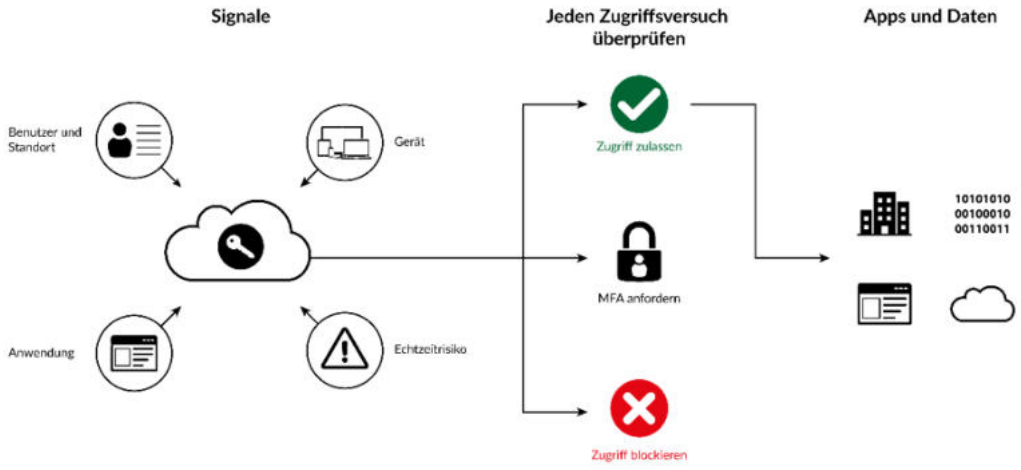


Abbildung 18: Identitätsbasierte Steuerungsebene – Conditional Access (Quelle: SoCura)

Darüber hinaus spielt der bedingte Zugriff eine wichtige Rolle im Konzept der Security Baseline sowie bei der Cloud-Absicherung und der Zugriffssteuerung auf Unternehmensressourcen. Erst im Zusammenspiel aller Microsoft-Cloud-Komponenten lässt sich das volle Potenzial des bedingten Zugriffs als Identitäts- und Zugriffsdienst abrufen.

10.7 Microsoft Information Protection – Datenverschlüsselungen und externe Zugriffe

Eine besondere Herausforderung der Malteser IT-Landschaft ist es, auch nicht verwaltete Geräte und offline arbeitende Ehrenamtliche abzudecken, diesen die für ein effizient-produktives Arbeiten benötigten Daten zur Verfügung stellen zu können, dabei aber weiterhin die Unternehmensdaten ausreichend zu schützen. Die Szenarien für innerhalb des Unternehmensnetzwerkes verwaltete Geräte (einheitliche und strukturierte Datenklassifizierung mit entsprechenden Vertraulichkeitsstufen; Labeling und Zugriff auf Daten über das Berechtigungssystem der Dateiablagen) sind hierfür nicht ausreichend. Eine geeignete Lösung könnte Microsoft Information Protection (MIP) sein. Es bietet die Möglichkeit, vertrauliche Informationen und Unternehmensdaten zu finden, klassifizieren und zu schützen, und zwar auch dann, wenn sich die Daten und Anwender*innen außerhalb des Unternehmens und der verwalteten Geräte befinden – ideal für Szenarien mit dem Einsatz von BYOD-Geräten.

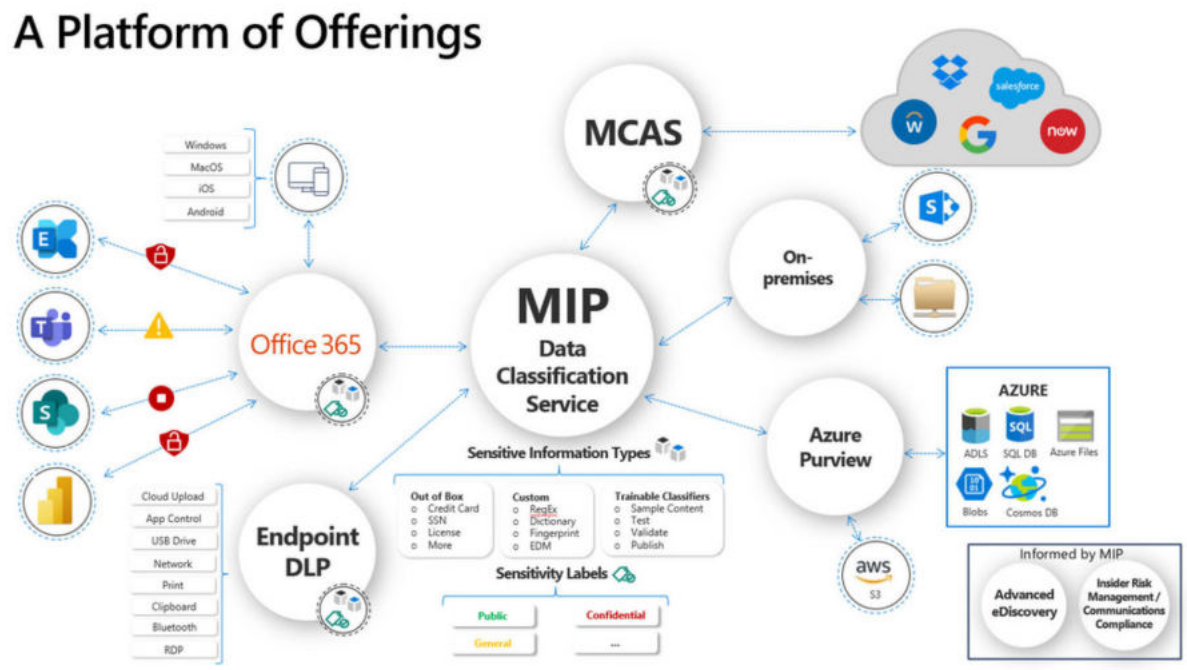


Abbildung 19: Azure Cloud On-Premise Integration

10.8 Passwortlose Authentifizierung

Microsoft empfiehlt den Einsatz kennwortloser Authentifizierungsmethoden wie Windows Hello, FIDO2-Sicherheitsschlüssel oder die Microsoft Authenticator-App. Obwohl sich Benutzer*innen mit anderen gängigen Methoden wie „Benutzername“ und „Kennwort“ anmelden können, sollten perspektivisch Kennwörter durch sicherere Authentifizierungsmethoden ersetzt werden.

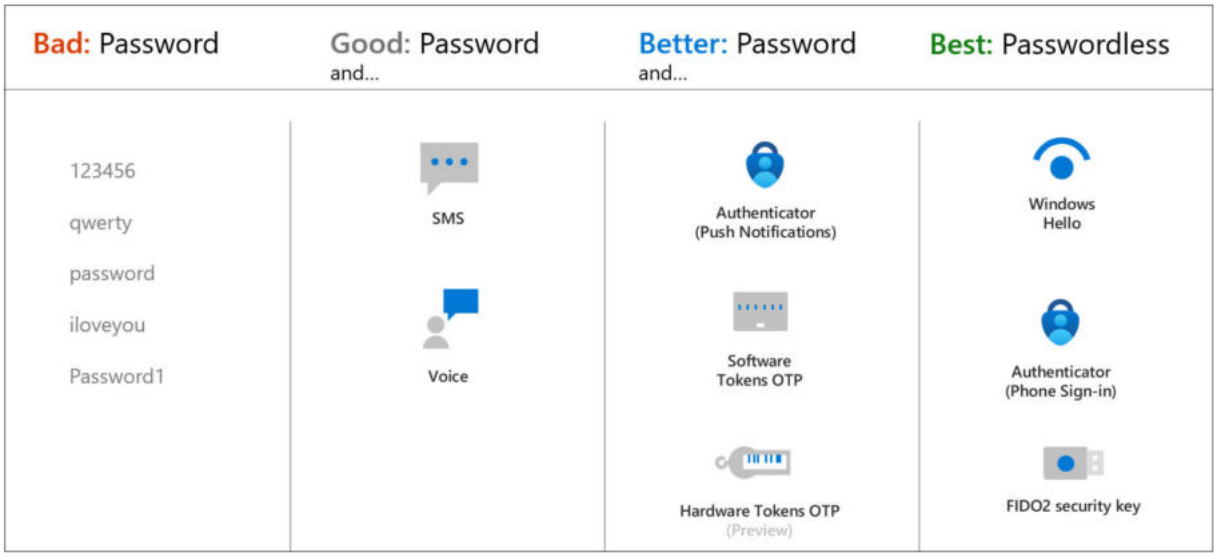


Abbildung 20: Authentifizierungsmethoden

Methoden zur mehrstufigen Authentifizierung (Multi-Factor Authentication, MFA) erhöhen die Sicherheit im Anmeldeprozess signifikant. Der Austausch passwortbasierter Verfahren gegen fälschungssichere Methoden erhöht die Sicherheit. In Frage kommen beispielsweise biometrische Merkmale oder Rückfragen auf mobile Geräte, Benutzer*innen stehen diesen Verfahren aber häufig aufgrund des Mehraufwands ablehnend gegenüber.

Jede Organisation hat unterschiedliche Anforderungen in Bezug auf die Authentifizierung. In die globale Microsoft Azure-Plattform und Microsoft Azure Government können drei Optionen für eine kennwortlose Authentifizierung integriert werden:

- Windows Hello for Business
- Microsoft Authenticator-App
- FIDO2-Sicherheitsschlüssel

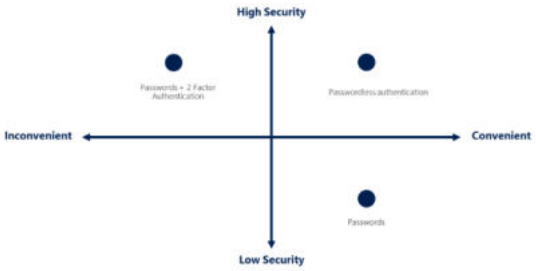


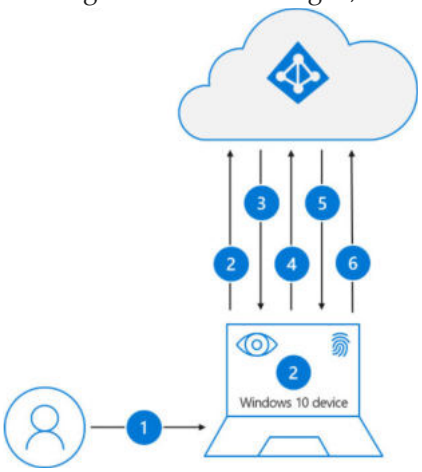
Abbildung 21: Authentifizierungsmethoden im Quadrant

10.8.1 Windows Hello for Business

Windows Hello for Business eignet sich ideal für Benutzer*innen mit eigenem Windows-PC. Die biometrischen und PIN-basierten Anmeldeinformationen sind direkt mit dem PC des Benutzers

verknüpft, wodurch ein fremder Zugriff verhindert wird. Mit PKI-Integration (Public Key-Infrastruktur) und integrierter Unterstützung für einmalige Anmeldung (Single Sign-On, SSO) bietet Windows Hello for Business eine praktische Methode für den nahtlosen Zugriff auf Unternehmensressourcen lokal und in der Cloud.

Die folgenden Schritte zeigen, wie der Anmeldevorgang mit Azure AD funktioniert:



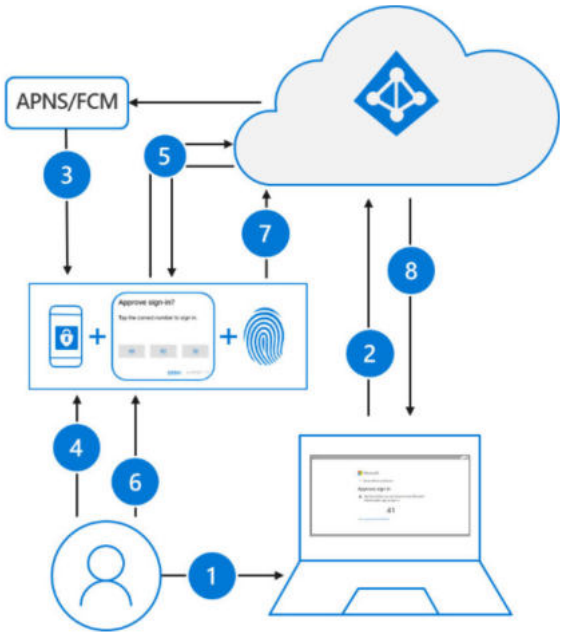
1	Cloudauthentifizierungsanbieter fordert eine Nonce vom Azure AD an
2	Azure AD gibt einen 5 Minuten gültigen Nonce zurück
3	Cloudauthentifizierungsanbieter signiert Nonce mit dem privaten Schlüssel des Users und gibt es anschließend dem Azure AD wieder zurück
4	Azure AD überprüft das signierte Nonce und erstellt ein Primary Refresh Token (PRT) und gibt es dem Cloudauthentifizierungsanbieter zurück
5 6	Cloud-AP-Anbieter erhält das PRT und entschlüsselt. Cloudauthentifizierungsanbieter gibt an Windows die erfolgreiche Authentifizierung zurück. Der Benutzer kann nun sowohl auf Windows-Anwendungen als auch auf Cloudanwendungen und lokale Anwendungen zugreifen, ohne dass eine wiederholte Authentifizierung erforderlich ist (SSO)

Abbildung 22: Azure Authentifizierungsmethoden

10.8.2 Microsoft Authenticator-App

Die Microsoft Authenticator App unterstützt auf jedem iOS oder Android Telefon die sichere, kennwortlose Anmeldung (ausgenommen die Windows Anmeldung). Benutzer können sich bei jeder beliebigen Plattform oder jedem beliebigen Browser anmelden, indem sie eine Benachrichtigung auf ihrem Telefon erhalten, eine auf dem Bildschirm angezeigte Zahl mit der Zahl auf dem Telefon abgleichen und dann ihre biometrischen Daten (Touch oder Gesicht) oder ihre PIN zur Bestätigung verwenden.

Das Grundprinzip der kennwortlosen Authentifizierung mit Authenticator App ist dasselbe wie bei Windows Hello for Business. Sie ist etwas komplizierter, da der Benutzer identifiziert werden muss, damit Azure AD die verwendete Version der Microsoft Authenticator-App herausfinden kann:



1	Azure AD erkennt, dass der Benutzer über sichere Anmeldeinformationen verfügt, und startet den Strong Credential-Flow (Ablauf für sichere Anmeldeinformationen)
2	Über den Apple Push Notification Service (APNS) bei iOS-Geräten bzw. Firebase Cloud Messaging (FCM) bei Android-Geräten wird eine Benachrichtigung an die App gesendet
3	Der Benutzer erhält die Pushbenachrichtigung und öffnet die App
4	Die App ruft Azure AD auf und erhält eine Proof-of-Presence-Abfrage sowie eine Nonce
5	Der Benutzer beantwortet die Abfrage durch Eingabe von biometrischen Daten oder einer PIN, um den privaten Schlüssel zu entsperren
6	Die Nonce wird mit dem privaten Schlüssel signiert und an Azure AD zurückgesendet
7	Azure AD überprüft den öffentlichen/privaten Schlüssel und gibt ein Token zurück
8	Der Benutzer gibt seinen Benutzernamen ein

Abbildung 23: Azure Authentifizierungsmethoden

10.8.3 FIDO2-Sicherheitsschlüssel

Die FIDO-Allianz (Fast Identity Online) fördert offene Standards für die Authentifizierung und trägt zur Reduzierung der Verwendung von Kennwörtern als Authentifizierungsmethode bei. FIDO2 ist der aktuelle Standard, der den Webauthentifizierungsstandard (WebAuthn) beinhaltet.

FIDO2-Sicherheitsschlüssel sind eine Phishing-resistente, standardbasierte Methode zur kennwortlosen Authentifizierung, die in jedem Formfaktor verfügbar sein kann. Fast Identity Online (FIDO) ist ein offener Standard für die kennwortlose Authentifizierung. Dank FIDO können Benutzer und Organisationen den Standard nutzen, um sich ohne Benutzername oder Kennwort mit einem externen Sicherheitsschlüssel oder einem in ein Gerät integrierten Plattformschlüssel bei ihren Ressourcen anzumelden.

Benutzer können einen FIDO2-Sicherheitsschlüssel registrieren und dann auf dem Anmeldebildschirm als Hauptauthentifizierungsmethode auswählen. Bei diesen FIDO2-Sicherheitsschlüsseln handelt es sich in der Regel um USB-Geräte, es können aber auch Bluetooth- oder NFC-Geräte sein. Mit einem Hardwaregerät, das für die Authentifizierung sorgt, erhöht sich die Sicherheit eines Kontos, da es kein Kennwort gibt, das verfügbar gemacht oder erraten werden kann.

FIDO2-Sicherheitsschlüssel können verwendet werden, um sich bei in Azure AD oder Azure AD Hybrid eingebundenen Windows 10-Geräten anzumelden und das einmalige Anmelden für den Zugriff auf cloudbasierte und lokale Ressourcen zu nutzen. Benutzer können sich auch bei unterstützten Browsern anmelden. FIDO2-Sicherheitsschlüssel sind eine gute Option für Unternehmen, die sehr sicherheitsbewusst sind oder deren Mitarbeiter nicht bereit oder in der Lage sind, ihr Telefon als zweiten Faktor zu nutzen, oder aber bei denen andere entsprechende Szenarien vorliegen.

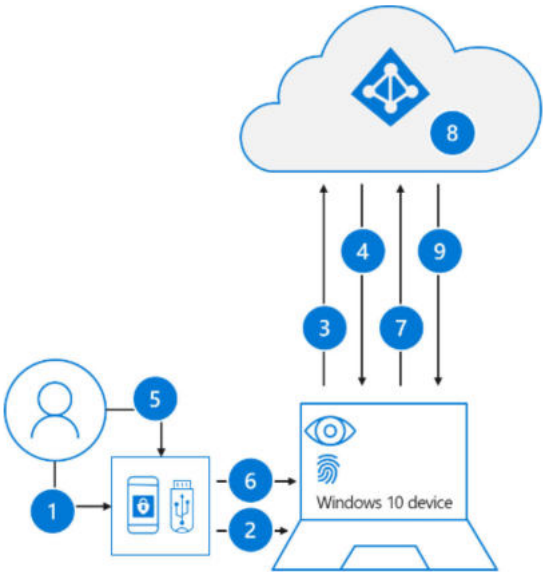


Abbildung 24: Azure Authentifizierungsmethoden

1	Der Benutzer steckt den FIDO2-Sicherheitsschlüssel in seinen Computer
2	Windows erkennt den FIDO2-Sicherheitsschlüssel
3	Windows sendet eine Authentifizierungsanforderung
4	Azure AD sendet eine Nonce zurück
5	Der Benutzer führt eine Geste aus, um den privaten Schlüssel freizuschalten, der in der sicheren Enclave des FIDO2-Sicherheitsschlüssels gespeichert ist
6	Der FIDO2-Sicherheitsschlüssel signiert die Nonce mit dem privaten Schlüssel
7	Die Anforderung des primären Aktualisierungstokens (PRT) mit signierter Nonce wird an Azure AD gesendet
8	zure AD überprüft die signierte Nonce mit dem öffentlichen FIDO2-Schlüssel.
9	Azure AD gibt das PRT zurück, um den Zugriff auf lokale Ressourcen zu ermöglichen

10.8.4 Bewertung der Authentifizierungsmethoden in der Praxis

Persona	Szenario	Environment	Kennwortlose Technologie
Administrator	Sicherer Zugriff auf ein Gerät für Verwaltungsaufgaben	Zugewiesenes Windows 10-Gerät	Windows Hello for Business und/oder FIDO2-Sicherheitsschlüssel
Administrator	Verwaltungsaufgaben auf Nicht-Windows-Geräten	Mobilgerät oder Nicht-Windows-Gerät	Anmelden ohne Kennwort mit der Microsoft Authenticator-App
Information-Worker	Produktive Arbeit	Zugewiesenes Windows 10-Gerät	Windows Hello for Business und/oder FIDO2-Sicherheitsschlüssel
Information-Worker	Produktive Arbeit	Mobilgerät oder Nicht-Windows-Gerät	Anmelden ohne Kennwort mit der Microsoft Authenticator-App
Mitarbeitern im Kundenkontakt	Terminals in Fabriken, im Einzelhandel oder zur Dateneingabe	Gemeinsam genutzte Windows 10-Geräte	FIDO2-Sicherheitsschlüssel

Abbildung 25: Bewertung der Authentifizierungsmethoden

10.9 Microsoft Defender for Cloud App

Microsoft Defender for Cloud App (vormals bekannt unter dem Namen Microsoft Cloud App Security) ist ein Tool für die Vermittlung von weiteren Diensten (z. B. API-Connectors, Reverse-Proxy, Protokollsammlung). Es kann Unternehmensdaten rund um die Uhr analysieren und Bedrohungslagen in allen Microsoft-Cloud-Diensten zügig identifizieren und bekämpfen. Es sorgt für den Zugriff auf Unternehmensdaten, aber auch für den Schutz kritischer Daten. Das Tool fungiert als Gatekeeper und

vermittelt in Echtzeit den Zugriff zwischen Anwender*innen und den von ihnen verwendeten Cloud-Ressourcen – unabhängig davon, wo sich diese Anwender*innen befinden und welches Gerät sie verwenden.

Es verfügt über eine breite Palette von Funktionen, um Anwender*innen und vertrauliche Daten vor möglichen Hackerangriffen zu schützenüber die folgenden Säulen hinweg:

- Transparenz: Erkennung aller Cloud-Dienste und Zuweisung einer Risikoeinstufung; Identifikation aller Anwender*innen und Apps von Drittanbietern, die sich anmelden können
- Datensicherheit: Identifizierung und Kontrolle sensibler Informationen; Reaktion auf Empfindlichkeitskennzeichnungen von Inhalten
- Bedrohungsschutz: Adaptive Zugriffskontrolle; Bereitstellung von Anwender*innen- und Entitätsverhaltensanalysen; Entschärfung von Malware
- Compliance: Bereitstellung von Berichten und individueller Dashboards zur Cloud-Governance; Unterstützung der Bemühungen zur Einhaltung der Data Residency- und Compliance-Anforderungen

Nicht alle Microsoft-Lizenzen enthalten alle CAS-Funktionen. Dies ist zurzeit erst ab der höchsten Lizenz EMS E5 der Fall. Diese bietet darüber hinaus automatische Datenklassifizierung und Datenklassifizierung und -kennzeichnung sowie Mobile Device Management und Mobile App Management zum Schutz von Unternehmens-Apps und Daten auf jedem Gerät und für jede Erst- und Drittanbieter-App.

Defender for Cloud Apps bietet ein besonders transparentes Monitoring für Cloudlösungen durch:

- Cloud Discovery zur Zuordnung und Identifikation von Cloudumgebung und Cloud-Apps
- Sanktionierung von Cloud-Apps
- App-Connectors (die Anbieter-APIs nutzen) zur Gewährleistung der Sichtbarkeit und Governance von Apps

- App-Control-Schutz mit bedingtem Zugriff, für Echtzeittransparenz und Zugriffskontrolle in Cloud-Apps

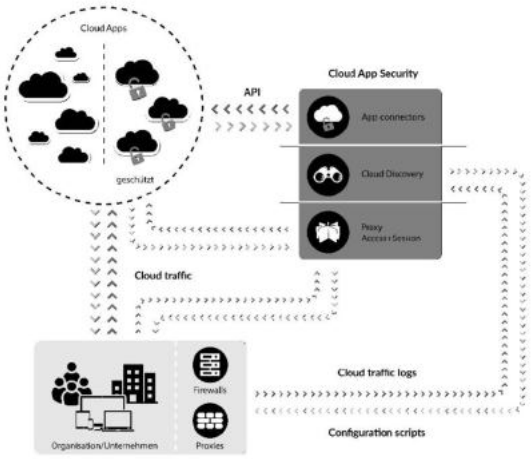


Abbildung 26: Sicherheitsarchitektur von Cloud App Security (Quelle: SoCura)

10.10 Azure Virtual Desktop

Bei Azure Virtual Desktop handelt es sich um einen cloudbasierten Dienst für eine flexible VDI-Plattform (Cloud Virtual Desktop Infrastruktur) zur Desktop- und App-Virtualisierung. Azure Virtual Desktop kann geräteübergreifend verwendet werden – einschließlich Windows, Mac, iOS und Android – und enthält voll funktionale Apps für den Zugriff auf Remotedesktops und -Apps. AVD bietet folgende Vorteile :

- Bereitstellung und Zugriff auf die Ressourcen:
    - Geräteunabhängiges Zugreifen auf RemoteApps- und Desktops – auch mit BYOD Geräten
    - Containerbasierendes Profilmanagement mittels FSLogix für schnelle und dynamisches Anmeldung mit einem nativen Benutzerprofil
- Verbesserte Sicherheit:
    - Zentrale Sicherheitsverwaltung für Desktops von Benutzern mit Azure Active Directory (Azure AD)
    - Benutzersitzungen sind sowohl in Umgebungen mit einer als auch mit mehreren Sitzungen isoliert (Multimode oder Singlemode)
    - Höhere Sicherheit durch den Einsatz von umgekehrter Verbindungstechnologie (Reverse Connect), wo es sich beim Verbindungstyp um ein RDP mit höherer Sicherheit handelt, da aus des Virtuellen Maschinen keine eingehenden Ports für die Sitzungshost geöffnet werden
    - Sichere Authentifizierung durch moderne Ansätze wie Smartcards, FIDO2, oder Windows Hello for Business und zukünftige Funktionen.

- Vereinfachte Verwaltung:
    - Bereitstellung von Tools für die Automatisierung von VM-Bereitstellungen, die Verwaltung von VM-Updates sowie die Bereitstellung der Notfallwiederherstellung
    - Azure Monitoring für Überwachung und Benachrichtigungen um auf diese Weise Probleme über eine einzige Oberfläche schnell zu erkennen
- Verwalten der Ressourcenleistungen:
    - Optionale Lastenausgleichsmodelle für Hostpools (sind Sammlungen von VMs mit derselben Konfiguration, die mehreren Benutzern zugewiesen werden). Im Breitenmodus werden Benutzer für Ihre Arbeitsauslastung nacheinander in die breite der vorhandenen Hostpools zugeordnet. Im Tiefenmodus wird der erste Host Pool befüllt (nur im Multimode Bereich) bis dieser voll ist um den nächsten Host Pool zu befüllen.
    - Skalierung durch Automatische Bereitstellung zusätzlicher VMs, wenn die eingehende Nachfrage einen bestimmten Schwellenwert überschreitet.
    - Azure Virtual Desktop ermöglicht die Verwendung von Windows 10 Enterprise für mehrere Sitzungen, das einzige auf dem Windows-Client basierende Betriebssystem, das mehrere gleichzeitige Benutzer auf einem einzigen virtuellen Computer (VM) aktiviert. Azure Virtual Desktop bietet auch eine konsistentere Erfahrung mit breiterem Anwendungssupport vergleichen mit Windows Server-basierten Betriebssystemen.
- Weitere:
    - Bereitstellung virtueller Windows-7-Desktops mit kostenlosen erweiterten Sicherheitsupdates für das anderweitig nicht länger unterstützte Betriebssystem
    - Anwendungen mithilfe von MSIX App Attach bereitstellen. MSIX App Attach ist eine Technologie zur Anwendungsbereitstellung, die Anwendungen und deren Zustand vom Betriebssystem trennt und den Benutzern Anwendungen dynamisch zuweist.

Azure Virtual Desktop vereinfacht die Verwaltung von virtuellen Desktops im Vergleich zu vorhandenen Remotedesktopdiensten (RDS) oder virtuellen Desktopinfrastrukturumgebungen (VDI). Administratoren müssen keine Server und Serverrollen bereitstellen, wie Gateway, Verbindungsbroker, Diagnose, Lastenausgleich oder Lizenzierung.

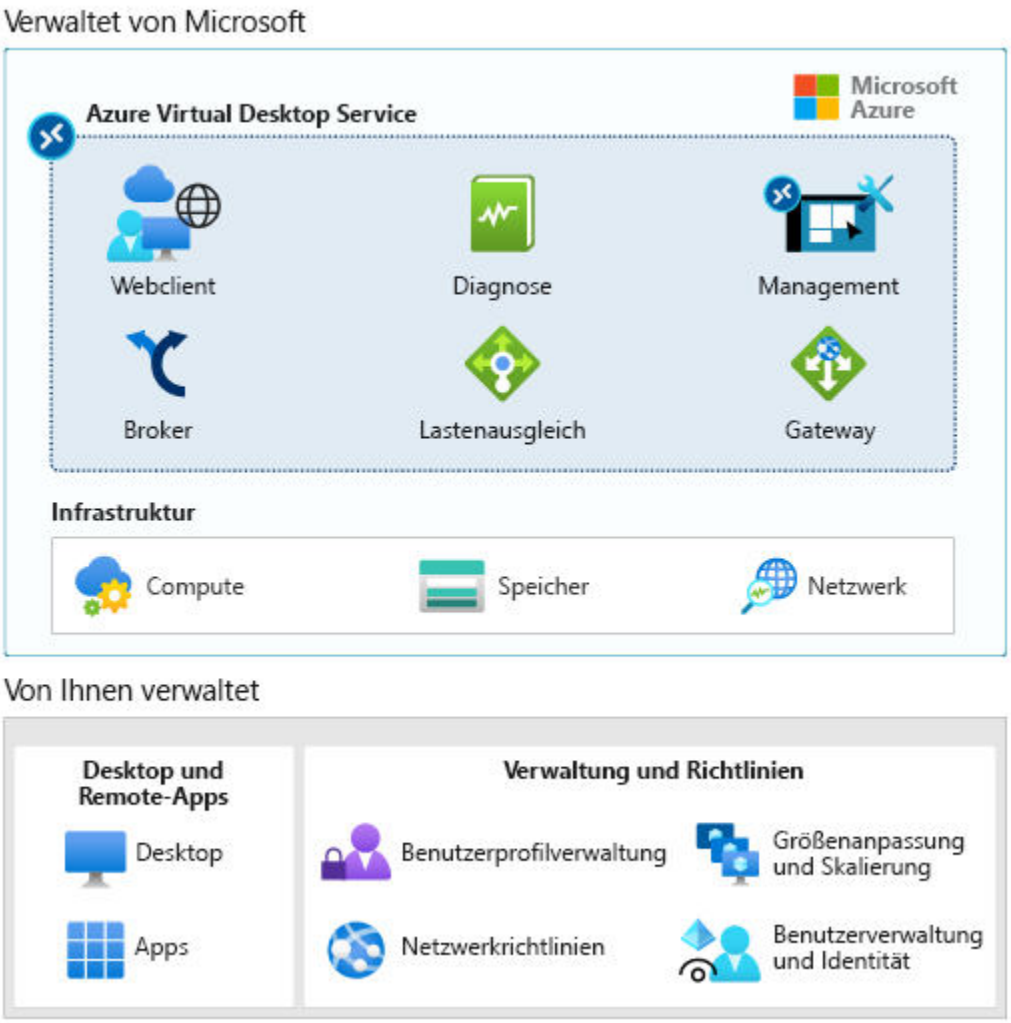


Abbildung 27: Azure Virtual Desktop Service

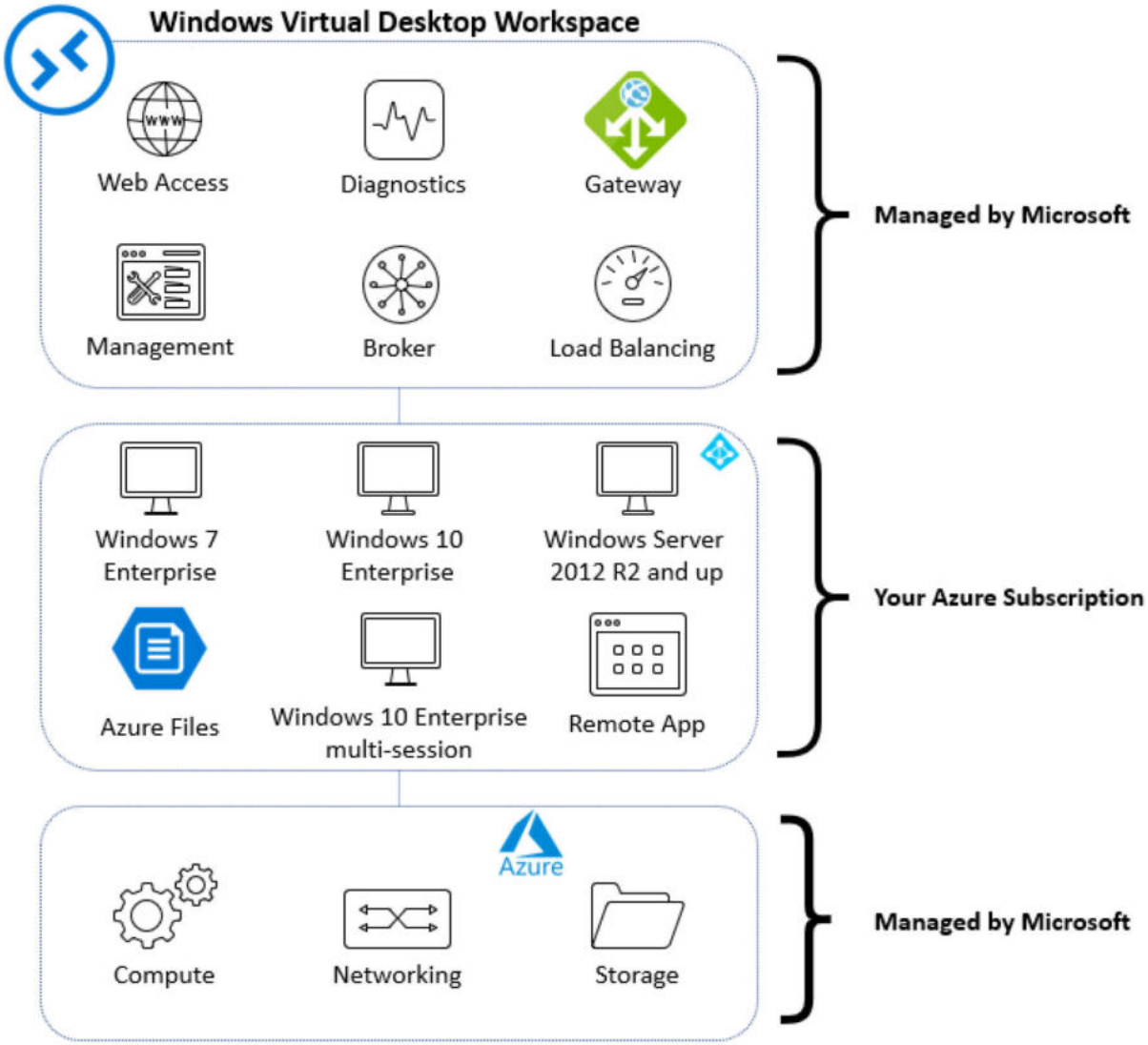


Abbildung 28: Citrix mit Windows virtual Desktop

10.10.1 Azure Virtual Desktop – Cloud-Only

AVD unterstützt sowohl die Cloud-only Variante, in der die VM nur im Azure AD verbunden und in Microsoft Intune des eigenen Tenants registriert und verwaltet wird. Vorteil ist die unabhängige und schnelle Bereitstellung von AVD ohne eigenen Active Directory Domaincontroller oder Active Directory Domain Services. Eine Integration mit der eigenen On-Premise Umgebung kann weiterhin durch ein Azure VPN Gateway mittels Site-to-Site-Verbindung realisiert werden. Der Azure AD-Domänenbeitritt für Azure Virtual Desktop bietet einen modernen Ansatz für Smartcards, FIDO2, Authentifizierungsprotokolle wie Windows Hello for Business und zukünftige Funktionen. Auch bietet der Azure AD-Domänenbeitritt die Möglichkeit, Active Directory außer Betrieb zu nehmen, da Azure Virtual Directory-Hostpools kein Active Directory mehr benötigen.

10.10.2 Azure Virtual Desktop – Hybrid AD Modus

Als weitere Alternative kann AVD auch im Hybrid AD Modus bereitgestellt werden. Die VM kann zum eigenen Active Directory Domaincontroller oder ein Active Directory Domain Services in Azure

verbunden werden. Auch hier können die VM’s in Intune registriert und verwaltet werden, Es wird aber zusätzlich eine AD Konfiguration über den AD Connect notwendig; die direkte Registrierung über das Deployment Portal in Intune ist nicht möglich.

Die Konfiguration und Verwaltung über Intune spart Administratoren die Erstellung, Aktualisierung sowie den Rollout der neuen VM’s über ein Masterimage. Es gelten alle Konfigurationen, Aktualisierungen und Softwareinstallationen für beide Umgebungen.

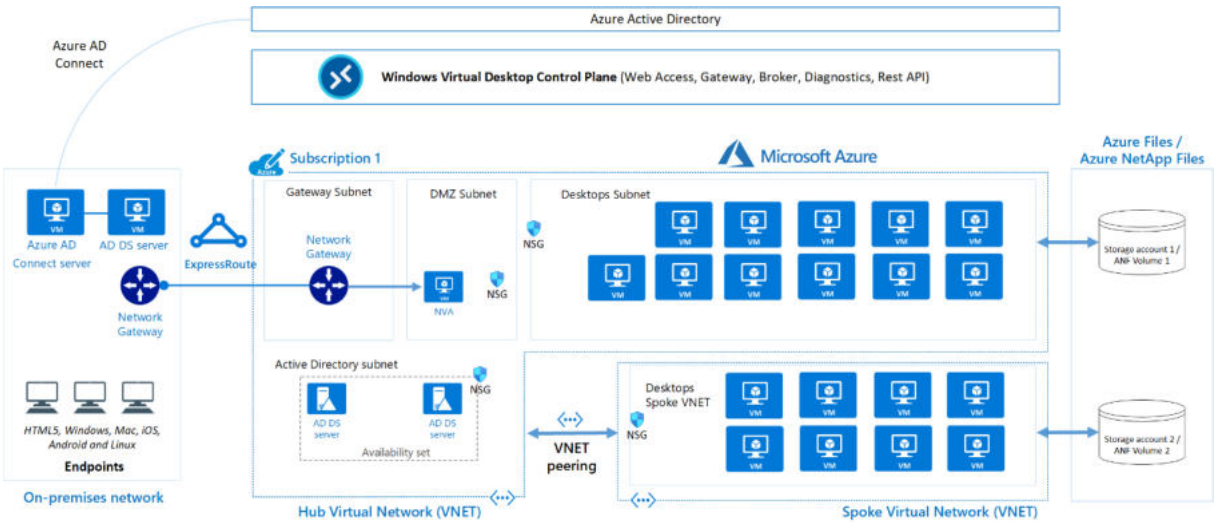


Abbildung 29: Architektur Azure Virtual Desktop (AVD)

10.10.3 Windows 365 – Cloud-PC

Windows 365 Cloud-PC´s sind hochverfügbare, optimierte und skalierbare virtuelle Maschinen (VMs), die den Endanwender*innen die Nutzung einer umfangreichen Windows-Desktopversion ermöglichen. Sie werden im Windows-365-Dienst gehostet und sind von überall aus und auf jedem Gerät zugänglich.

Endanwender*innen können über https://windows365.microsoft.com eine Verbindung mit ihrem Cloud-PC herstellen. Der browser- oder appbasierte Zugriff ist über Windows-, iOS- und Android-Geräte möglich.

Windows 365 ist ein auf einer stark vereinfachten Azure-Virtual-Desktop-Technik basierender Cloud-Dienst, der für Endanwender*innen automatisch neue Windows-VMs erstellt, die immer nur einem Anwender oder einer Anwenderin zugewiesen sind und für diese damit zum dedizierten Windows-Gerät werden. Es bietet die gleichen Vorteile hinsichtlich Produktivität, Sicherheit und Zusammenarbeit wie Microsoft 365.

Windows 365 und Microsoft 365 unterscheiden sich darin, dass Windows 365 einen PC virtuell bereitstellt. Microsoft 365 stellt hingegen bestimmte Applikationen bereit.

Windows 365 gibt es in zwei Editionen:

- Windows 365 Business - die Business Variante richtet sich an Kunden bis zu 300 Mitarbeiter.

- Windows 365 Enterprise - die Enterprise an größere Unternehmen

Windows 365 Business ist die wesentlich einfachere Version. Es sind weder technologische Voraussetzungen erforderlich, noch braucht das Unternehmen ein Azure-Abonnement oder einen Active Directory Domaincontroller. Alles funktioniert nativ mit Azure AD als Identitätsplattform und die Ressourcen und Komponenten hierfür werden im Hintergrund über die Microsoft Cloud bereitgestellt und betrieben. Für den Administrator sind bis auf die Lizenz alle technischen Ressourcen der VM transparent. Im M365-Admin-Center können die Lizenzen und Userzuordnungen verwaltet werden.

Windows 365 Enterprise ist etwas anspruchsvoller und bietet ein breiteres Spektrum an Tools und Funktionen für Wartung und Sicherheit. Dazu zählen Funktionen wie:

- Image-Management
- Anpassung Netzwerkeinstellungen
- Monitoring durch Endpoint Analytics

Im Vergleich zur Business Variante ist es komplett in den Microsoft Endpoint Manager integriert und wird auch darüber verwaltet und konfiguriert. Der Administrator kann im Azure Portal die Netzwerkkonfiguration anpassen, allerdings wird dazu ein zusätzliches Azure Abonnement benötigt. Bei vorhandener Site-to-Site VPN Verbindung zwischen dem lokalen On-Premise Rechenzentrum und der Azure Region kann mit der Enterprise Variante auch auf On-Premise Ressourcen zugegriffen werden.

Auch hier gibt es wie bei AVD die Möglichkeit eines AD Hybrid Joins oder einem Cloud-only Betrieb mittels Azure AD.

Abbildung 30: Endpoint Analytics Infrastruktur

10.10.4 Citrix Cloud on Azure

Citrix Virtual Apps and Desktops Standard for Azure (CVAD Standard) ist die einfachste und schnellste Möglichkeit, Windows-Apps und Desktops von Microsoft Azure bereitzustellen. Dieser Service bietet cloudbasierte Verwaltung, Bereitstellung und ermöglicht die Bereitstellung virtueller Apps und Desktops auf jedem Gerät. Die Lösung umfasst:

- Cloudbasierte Verwaltung und Bereitstellung von Citrix-gehosteter Azure Virtual Desktops und Apps von Multi- und Single Session-Computern
- Hochauflösende Anwender*innenerfahrung auf einer Vielzahl von Geräten, bei Verwendung der Citrix-Workspace-App
- Vereinfachte Workflows zur Image-Erstellung und -Verwaltung sowie für Citrix vorbereitete Windows- und Linux-Images für Einzelsitzungen und mehrere Sitzungen, auf denen der neueste Citrix Virtual Delivery Agent (VDA) installiert ist
- Absicherung des Remotezugriffs von jedem Gerät aus, mit globalen Präsenzpunkten des Gateway-Dienstes Citrix Gateway Service
- Erweiterte Überwachungs- und Helpdesk-Verwaltungsfunktionen
- Verwaltete Azure IaaS, einschließlich Azure-Rechen-, Speicher- und Netzwerkfunktionen für die Bereitstellung virtueller Desktops
- Remote-Verwendung physisch vorhandener Computer (etwa im Büro) über die Citrix-Remote-PC-Zugriffsfunktion, mit den besten Ergebnissen bei Verwendung von Citrix HDX

CVAD ist ein Dienst der Citrix Cloud, einer Plattform für das Hosting und Management von Citrix-Cloud-Diensten.

Die Kombination von Citrix Cloud und Microsoft Azure ermöglicht es, neue virtuelle Citrix-Ressourcen mit größerer Geschwindigkeit und Elastizität aufzubauen und deren Nutzung an sich ändernde Anforderungen anzupassen. Virtuelle Maschinen in Azure unterstützen alle Steuerungs- und Arbeitslastkomponenten, die für eine Dienstbereitstellung von CVAD erforderlich sind. Citrix Cloud und Microsoft Azure verfügen über gemeinsame Steuerelemente-Integrationen, die Identität, Governance und Sicherheit für globale Abläufe festlegen.

Da diese Lösung auch in Hybridszenarien einsetzbar wäre, könnte Citrix Cloud on Azure eine Alternative zu bestehenden Lösungen sein. Hybridfähig bedeutet hier, dass die aktuell vorhandene lokale Citrix-Umgebung durch die Citrix Cloud erweitert und neue Desktops über die Cloud bereitgestellt werden oder die vorhandenen lokalen Desktops weiter betrieben werden können. Die zentralen Zugriffs- und Steuerungselemente laufen in der Citrix Cloud. Eine solche Lösung würde den Vorteil bieten, dass die gesamten lokalen Citrix-Komponenten als Infrastrukturdienste abgebaut und somit auch die Verwaltungsaufwände für Administrator*innen verringert werden könnten. Die neuen Infrastruktur-Komponenten würden dann in der Citrix Cloud als Platform-as-a-Service-Dienst (PaaS) laufen, bei dem Citrix im Hintergrund alle Dienste administriert, sodass die Administrator*innen sich

nur noch um die Bereitstellung, Verwaltung und Konfiguration der Desktops und Apps bemühen müssten.

Architektur einer Bereitstellung in einem eigenen verwalteten Azure-Abonnement

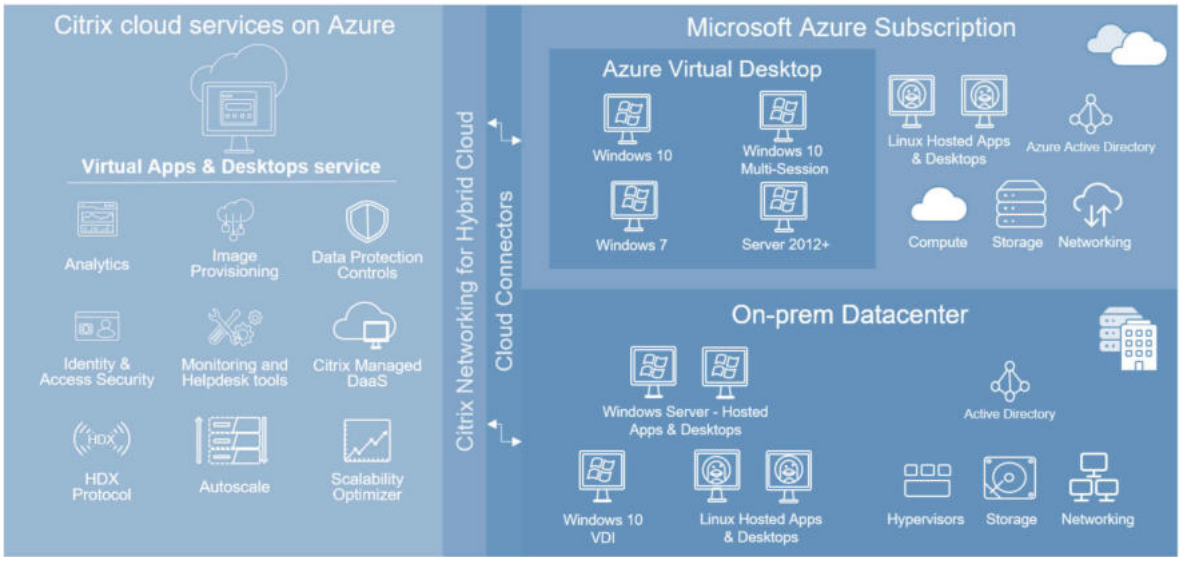


Abbildung 31: Citrix virtual App Desktops for Azure

Die untere Darstellung verwendet ein eigenverwaltetes Azure-Abonnement. Die Möglichkeit eines Citrix Managed Azure-Abonnement besteht als Alternative, diese Option wird in diesem Dokument aber nicht thematisiert.

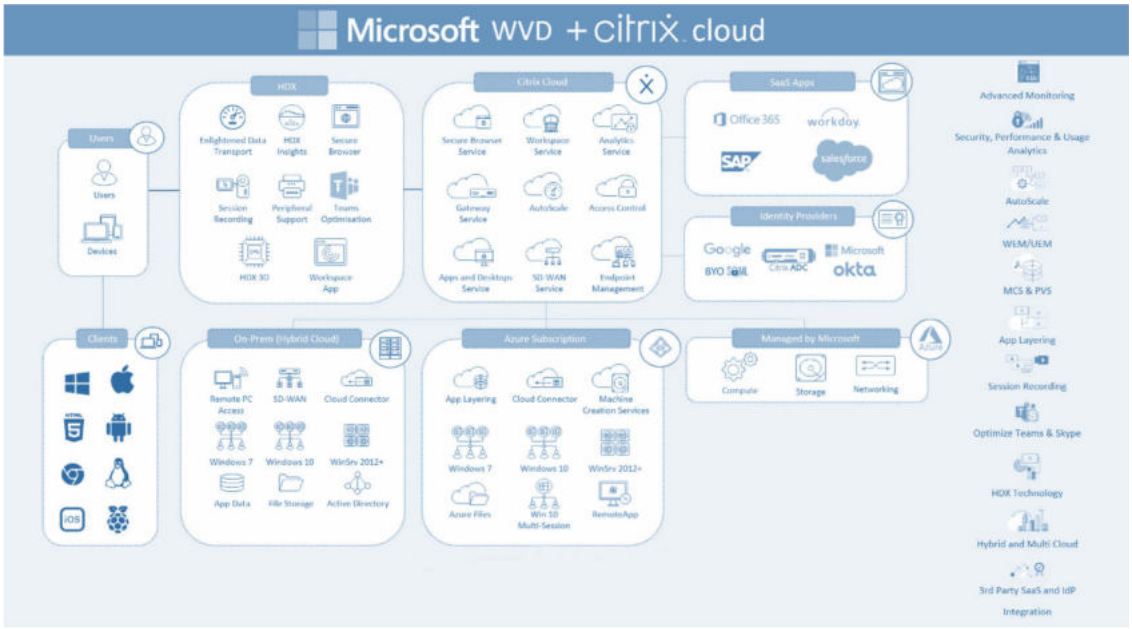


Abbildung 32: Citrix Windows virtual Desktop value-add

10.10.5 Vergleich der Terminalserver und virtuelle Desktop-Infrastrukturen

	Cloud PC – Windows 365 Enterprise	**Cloud VDI – Azure Virtual Desktop**	**Hybrid VDI - Citrix on Azure mit eigenem Azure-Abonnement**
Schwerpunkt	Auf Einfachheit optimiert	Auf Flexibilität optimiert	Vereinfachte und optimierte Konfiguration für anspruchsvollere Anforderungen und Hybridfähigkeit
Arten von Desktops	Windows 10/11 personalisierte Desktops	Windows 10/11 oder Windows Server im Multi- oder Single Desktop Mode	Windows 10/11 oder Windows Server im Multi- oder Single Desktop Mode
Streaming von Remote Apps	nein	Ja	ja
App Layering	nein	Teilweise nur mit MSIX App Attach	ja
Maschinenerstellungsdienste für nicht persistente Desktops	Nein	Nein	ja
Azure On-Demand-Provisioning	Nein	Nein	ja
Verwaltung/Konfiguration	Eingeschränkt über Microsoft Endpoint Manger	Volle administrative Steuerung über das Azure Portal	Volle administrative Steuerung über das Citrix Cloud
Zugriff	Mittels Browser oder App	Mittels Browser oder App	Mittels Browser oder Workspace App (erweiterte Funktionen innerhalb der App)
Schützt Ihre Umgebung vor versehentlichem oder böswilligem Datenverlust	Ja, durch Erweiterung von Microsoft Information Protection	Ja, durch Erweiterung von Microsoft Information Protection	Ja, durch Citrix App Protection innerhalb des Workspaces – alternativ auch durch Erweiterung von Microsoft Information Protection
Teams Optimierung	Ja	Ja	ja

Erweiterbar durch Einbindung/Nutzung von Citrix oder VMware	nein	ja	-
Grafik intensive oder HPC Workloads	nein	Ja, allerdings kein Support von speziellen simulierten Eingabegeräten	Ja, auch die Unterstützung von simulierten Eingabegeräten und sonstiger Peripherie
Hybrid-Cloud-Management (Desktops in der Cloud + on Prem)	nein	nein	ja
Know-how	Wenig bis kein VDI Know-how erforderlich	Know-how in der Azure Landing Zone und VDI erforderlich	Know-how in der Azure Landing Zone, VDI sowie Citrix Technologie erforderlich
Kostensteuerung	Nicht steuerbar - Einfach Abrechnung pro User – pro Lizenz	Steuerung flexibel möglich durch automatische Abschaltung, Skalierung und weiten Tools	Steuerung flexibel möglich durch automatische Abschaltung, Skalierung und weiten Tools
Weitere Vorteile	keine	Ja, aber alles muss erstmal im Azure Portal konfiguriert werden Monitoring – LogAnalytics Automatisierung – DevOps ….	Erweitertes Remotedesktop-Protokoll – HDX Möglichkeit der Aufnahme von Sitzungen Erweiterte vorabeingebaute Admintools z.B. erweitertes Monitoring, zeitgesteuerte Provisionierungsaufgaben zum Updaten oder zur Erstellung von VM‘s

11 Abbildungsverzeichnis

12 Glossar

A

Active Directory · *Active Directory ist ein Microsoft-Produkt zum Organisieren von IT-Assets wie Benutzer, Computer und Drucker.*

Active Directory Domain Services, ADDS
: ADDS stellt Methoden zum Speichern von Verzeichnisdaten bereit und macht diese für Netzwerknutzer*innen und Administrator*innen verfügbar. · 9

AD On-Premise
: Active Directoy (AD) On-Premises zu betreiben, heißt, dass die Verzeichnisdaten auf eigenen Servern gehostet werden. · 8

Asset Management
: Software zur Verwaltung von Softwarelizenzen. · 9

Azure Active Directory · *Azure Active Directory (Azure AD) ist der cloudbasierte Identitäts- und Zugriffsverwaltungsdienst von Microsoft, mit dem sich Mitarbeiter anmelden und auf bestimmte Ressourcen zugreifen können*

B

Baramundi
: Mit der Baramundi Management Suite können beliebig viele Geräte ortsunabhängig über LAN oder Internet zentral verwaltet werden. · 9

BYOD · *Bring your own device* ist die Bezeichnung dafür, private mobile Endgeräte wie Laptops, Tablets oder Smartphones in die Netzwerke von Unternehmen oder Schulen, Universitäten, Bibliotheken und anderen Institutionen zu integrieren.

C

CAS
: Cloud App Security (CAS) ist Teil von Microsoft Defender für Cloud-Apps, die eine verbesserte Sichtbarkeit und Kontrolle für Office 365 ermöglicht. · 12

Citrix
: Citrix ist eine Terminalsoftware-Lösung, mit der über eine Client-Software auf dedizierte virtuelle Desktops zugegriffen werden kann · 5

Citrix HDX
: Mittels der Citrix HDX-Technologie können Anwender hochauflösende virtuelle Desktops und Anwendungen nutzen. · 13

Conditional Access
: Unter Conditional Access versteht man die Kontrolle, welche Clients auf Daten des Unternehmens wie zugreifen können. Speziell das Arbeiten auf fremden oder unsicheren Clients kann so über weitere Faktoren bei der Anmeldung abgesichert werden. · 26

Corporate Network · Ein Corporate Network dient der Vernetzung räumlich verteilter Einzelnetze einer Organisation miteinander. Ein CN ist ein geschlossenes und privates Kommunikationsnetz.

D

G

M

P

S

X

xSuite · xSuite ist ein Programm zur Erfassung und Verarbeitung von Eingangsrechnungen.