Einführung von Microsoft Intune als Mobile Device Management Lösung

CASE STUDY IT-Beratung

Auf einen Blick:

Branche: Marketing
Mitarbeiter: ca. 1.400
Hauptstandort: München
Projektlaufzeit: 8 Monate

PAYBACK, eines der führenden Bonusprogramme und Multichannel-Marketingplattformen setzte sich zum Ziel, Microsoft 365 für die über 1.400 Arbeitsplätze vollumfänglich und unter Berücksichtigung geltender Datenschutzvorgaben einzuführen. Dies umfasste neben dem Aufbau eines Microsoft 365 Tenants und neuer Collaboration-Plattformen wie Teams und SharePoint auch die Mail- und Mobile Device Management-Migration von veralteter On-Premises-Infrastruktur in die Cloud. Im Ergebnis sollte den Mitarbeitenden ein möglichst homogener Arbeitsplatz geboten werden, dessen Tools und Features die tägliche Arbeit erleichtern. Die Einführung sollte zudem auf den „Work from Anywhere" Ansatz einzahlen, der bedingt durch die COVID-19-Pandemie stärker in den Fokus gerückt ist.

Als die matrix Mitte 2020 beauftragt wurde, die Einführung von Microsoft 365 technisch und beratend zu begleiten, hatte sich PAYBACK bereits für Microsoft Intune als neue Mobile Device Management (MDM) Lösung entschieden. Intune sollte die bisher eingesetzte MDM-Lösung von BlackBerry vollständig ersetzen und zudem an den bereits vorhandenen Microsoft Endpoint Configuration Manager (ehemals bekannt als System Center Configuration Manager, SCCM) angebunden werden. Bei der Konzeption und der Implementierung konnte der Kunde bereits grundlegendes Wissen in Bezug auf Device Management vorweisen, auf das die matrix-Berater gemeinsam mit dem Kunden aufbauen konnten.

Mit den internen Projektressourcen aus den verschiedenen Bereichen des IT-Teams des Kunden und der bereits vorhandenen Tools konnte man die unternehmensinternen Anforderungen schnell voranbringen. Dabei ging es dem Kunden vor allem um kompetente Beratung, wie eine zentrale Mobile Device Management-Plattform mit Microsoft Intune bereitgestellt werden kann. Der Kunde wollte zudem mehr über Einsatzmöglichkeiten des optisch ansprechenden Tools sowie gängige Implementierungswege und -prozesse erfahren. Ziel war es, die Administration von Intune – nach gemeinsamer Bereitstellung – selbstständig durchführen zu können.

Herausforderung

- Nahtlose Migration der unternehmenseigenen Geräte von der BlackBerry-Lösung zu Microsoft Intune
- Benutzerfreundlichkeiten bewahren trotz sehr restriktiver Auflagen der IT-Sicherheit/ Datenschutzvorgaben
- 100% Remotearbeit bedingt durch COVID-19
- Berücksichtigung von individuellen Wünschen und Anforderungen
- Begrenzter zeitlicher Rahmen

Lösung

Das Projekt wurde intern beim Kunden durch ein dediziertes Projektteam inkl. Projektmanager verantwortet. Die Experten der matrix standen mit technischem Know-how beratend zur Seite. Zudem unterstützte matrix technology im Projektverlauf auch bei der technischen Umsetzung und während der Rollout-Phasen. Die technische Projektorganisation wurde von PAYBACK selbst übernommen. Die Ressourcenplanung erfolgte durch die matrix. Der Go-Live des neuen Mobile Device Management Systems fand im Februar 2021 statt.

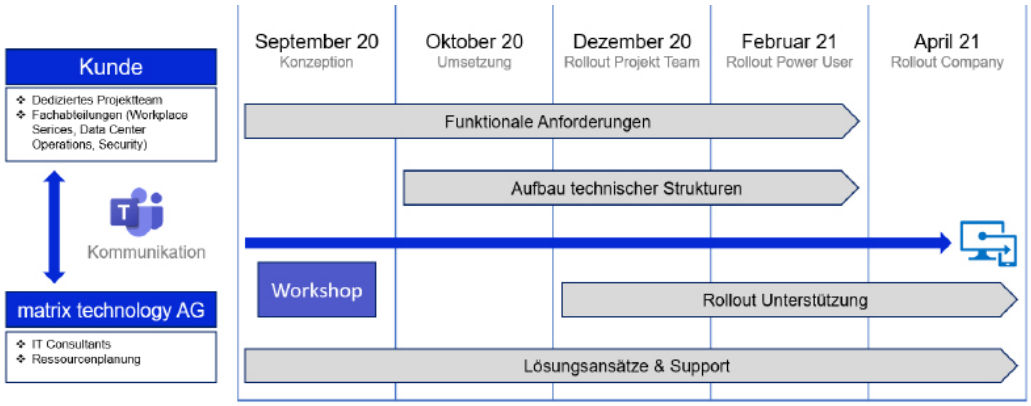

Abbildung 1: Projektablauf und Meilensteine

Technische Struktur

Intune ist eine Komponente des Microsoft-Angebots Enterprise Mobility + Security (EMS), welches ein zentraler Bestandteil von Microsoft 365 ist und in der Microsoft Cloud Azure als SaaS-basierter Dienst bereitgestellt wird. Der Zugriff für die Benutzer und Administratoren erfolgt via Anmeldung mit dem eigenen Account. Die Accounts werden aus dem On-Premises Active-Directory in die Microsoft 365-Umgebung des Kunden synchronisiert.

Mobile Device Management (MDM)

Für das Mobile Device Management wurden über 2.000 Geräte erfolgreich in Intune registriert. Darunter befanden sich neben Windows 10 Geräten auch die macOS-, Android- und iOS/iPadOS-Geräte sämtlicher Mitarbeitenden des Kunden. Neben organisationseigenen Geräten können Mitarbeitende auch ihre persönlichen Android- und iOS/iPadOS-Geräte als sogenannte BYOD-Geräte (Bring Your Own Devices) in Intune registrieren. Die Geräteregistrierung für die Windows 10 Geräte der Mitarbeitenden erfolgte automatisiert mit Hilfe von Gruppenrichtlinien (GPOs) im Hintergrund. Die Geräte der Plattformen macOS, Android Enterprise und iOS/iPadOS wurden in mehreren Phasen durch die User in Intune selbst registriert. Um die Mitarbeitenden bei dem Registrierungsprozess über die Intune Unternehmensportal-App zu unterstützen, wurden Anleitungen, Erklärvideos und ein dedizierter Support-Channel in Microsoft Teams vom Projektteam erstellt.

Für die vier Geräte-Plattformen wurden in Abhängigkeit von dem Besitzer oder der Besitzerin der Geräte (organisationseigen und persönlich) jeweils unterschiedliche Richtlinien- und Konfigurationsprofile in Intune angelegt. Diese sorgen dafür, dass die Geräte den Sicherheits- und Integritätsstandards des Unternehmens entsprechen und sich zum Beispiel automatisch mit dem unternehmenseigenen WLAN verbinden. Für die Zuweisung der Richtlinien- und Konfigurationsprofile wurden dynamische Azure Active Directory-Gruppen erstellt. Die dynamische Mitgliedschaft fügt automatisch Geräte oder Benutzer den Gruppen hinzu, wenn diese die Bedingungen für eine Gruppe erfüllen. Anhand dieser Struktur können ohne großen Administrationsaufwand sämtliche Geräteplattformen sowie innerhalb der Plattformen die unterschiedlichsten Einsatzszenarien der Geräte abgebildet werden.

Mobile Application Management (MAM)

Auf den mobilen Geräten der Mitarbeitenden erfolgte nach Abschluss der Geräteregistrierung automatisch der Download und die Installation diverser geschäftlicher Apps. Darunter befinden sich neben Outlook und Teams auch der Microsoft Authenticator, welcher für die Multifaktor-Authentifizierung (MFA) benötigt wird. Weitere geschäftliche Applikationen wie zum Beispiel OneDrive oder PowerPoint können die Mitarbeitenden im unternehmenseigenen App Store, welcher über die Intune-Unternehmensportal-App aufrufbar ist, optional herunterladen. Zum Schutz von Organisationsdaten auf Anwendungsebene dient in Intune das Mobile Application Management (MAM). Mittels sogenannter App-Schutzrichtlinien wurden die geschäftlichen Apps so konfiguriert, dass diese mit bestimmten Einstellungen gestartet oder ausgeführt werden. Hierdurch lässt sich steuern, innerhalb welcher Apps Organisationsdaten bearbeitet, gespeichert oder geteilt werden können. Ebenfalls wurde darüber sichergestellt, dass der Speicher des mobilen Geräts verschlüsselt ist und für jailbroken/rooted-Geräte der Zugriff auf Organisationsdaten blockiert wird.

Die App-Schutzrichtlinien verwenden darüber hinaus auch die Azure Active Directory-Anmeldeinformationen des Mitarbeitenden, um Organisationsdaten von persönlichen Daten zu isolieren. Meldet sich der Mitarbeitende mit seiner Organisationsidentität in der verwalteten App an, ermöglicht ihm das den Zugriff auf Daten, die seiner persönlichen Identität verweigert werden. Auf diese Weise hat die IT-Administration von PAYBACK die Kontrolle über die Organisationsdaten auf mobilen Geräten, während die persönlichen Daten des Mitarbeitenden nicht für die IT-Administration sichtbar sind und er diese selbstständig schützen und verwalten kann.

Co-Management

Da der Kunde bereits Microsoft Endpoint Configuration im Einsatz hat, wurde die Co-Verwaltung mit Intune evaluiert, getestet und für den produktiven Einsatz aktiviert.
Die Co-Verwaltung ermöglicht die Verwaltung von Windows 10-Geräten mithilfe von Configuration Manager sowie Intune und erweitert die vorhandene Infrastruktur um neue nützliche Funktionen wie zum Beispiel die moderne Bereitstellung mit Windows-Autopilot und dem bedingten Zugriff abhängig von dem Konformitätszustand des Gerätes. Zudem werden auch die Windows 10-Updates durch Intune verwaltet und überwacht.

Apple Business Manager & Android Zero-Touch

Die Bereitstellung von neuen organisationseigenen Android-, iOS/iPadOS- und macOS-Geräten erfolgt zukünftig automatisiert über Android Zero-Touch und Apples Automated Device Enrollment (ADE). Um ADE nutzen zu können, wurde bei Apple ein Apple Business Manager (ABM) beantragt, welcher benötigt wird, um nach der Verknüpfung mit Intune die Bereitstellung von neuen Apple-Geräten zu automatisieren. Darüber hinaus wird das webbasierte Portal von Apple Business Manager durch den Kunden genutzt, um die Apple-IDs der Mitarbeitenden und das Programm für Volumenlizenzen (VPP) zu verwalten. Für die Android Zero-Touch-Funktionalität wurde ein Managed Google Play-Account angelegt und mit Intune verbunden.

Die Hardware-IDs aller neu gekauften mobilen Geräte werden zukünftig direkt vom vertraglichen Telekommunikationsdienstleister/Hardwareverkäufer des Kunden im Apple Business Manager und Zero-Touch-Portal hinterlegt. Dadurch können die neuen Geräte direkt an die Mitarbeitenden ausgegeben werden. Während der Ersteinrichtung findet die Registrierung in Intune statt. u Die Geräte werden zudem automatisch mit Richtlinien, Konfigurationsprofilen und geschäftlichen Apps versorgt. Sobald der Mitarbeitende die Ersteinrichtung abgeschlossen hat, kann er sofort sein neues Gerät sicher für geschäftliche Zwecke nutzen.

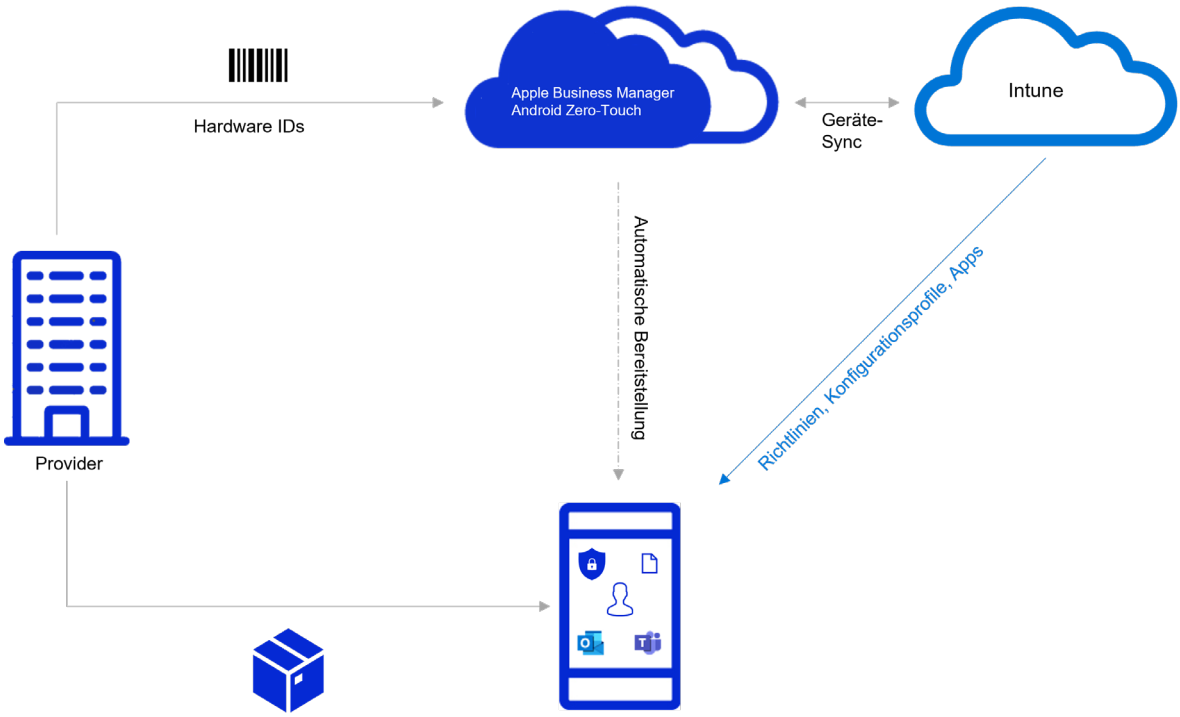

Abbildung 2: Lösung - grafische Darstellung

Customer Statement

„Mit Hilfe der matrix technology und dem dort vorhandenen Fachwissen haben wir es geschafft, unsere Mobile Device Management Landschaft auf den neusten technologischen Standard zu heben. Unter der definierten Timeline und den aktuellsten Sicherheitsstandards wurde eine State-of-the-Art Lösung bereit gestellt, welche uns in Zukunft bestmöglich in unserem Arbeitsalltag unterstützt. Die matrix stand uns stets mit Rat und Tat zur Seite und hat durch kontinuierlichen Austausch maßgeblich mitgewirkt, dass die Plattform in Zukunft problemlos ohne Mühen betrieben werden kann. Die Zusammenarbeit mit matrix technology war zu jeder Zeit geprägt von Vertrauen und Unterstützung, wo sie gebraucht wurde.

Alexander Stauber
Projektleiter
PAYBACK GmbH

Projektergebnis – Nutzen für den Kunden

Das Projekt konnte innerhalb des vorgegebenen Zeitraums erfolgreich umgesetzt werden. Mit Hilfe der matrix Experten gelang es, innerhalb kurzer Zeit die alte On-Premises Mobile Device Management-Lösung abzuschalten und Microsoft Intune einzusetzen. Der Kunde hat fundiertes Intune Know-how aufgebaut und ist nun in der Lage, das Mobile Device Management eigenverantwortlich zu administrieren und weiterzuentwickeln

Die wesentlichen Vorteile für PAYBACK lauten:

- Verwaltung von über 2.000 mobilen Geräten, plattformübergreifend und zentralisiert aus der Microsoft Cloud
- Steigerung der Effizienz und Benutzerfreundlichkeit durch neue Applikationen und Funktionen (einfachere Geräteregistrierung, Microsoft 365 Apps, eigener Unternehmens App Store)
- Zugriff auf Mail, Kalender, Kontakte und Collaboration-Tools von allen Geräteplattformen möglich, ohne Aufbau einer VPN-Verbindung
- Gesteigerte Gerätesicherheit (Gerätekonformitätsstatus, bedingter Zugriff, Multifaktor-Authentifizierung)
- Schutz von Organisationsdaten auf allen mobilen Geräten durch Intune Mobile Application Management
- Automatisierte Bereitstellung von neuen mobilen Geräten durch Apple Automated Device Enrollment und Android Zero-Touch
- Mehr Flexibilität und zusätzliche Funktionen für die Verwaltung von Windows 10-Geräten durch das Co-Management

matrix technology GmbH
Nymphenburger Str.1, 80335 München
Telefon +49 89589395-600
Telefax +49 89589395-711

Über PAYBACK

PAYBACK ist eines der führenden deutschen Unternehmen in den Bereichen Bonusprogramme und Marketing-Plattformen. Als Tochtergesellschaft eines des größten börsennotierten amerikanischen Finanzdienstleisters American Express bietet das Unternehmen seinen Kunden ein attraktives Bonusprogramm und gleichzeitig die größte Multichannel-Marketingplattform Deutschlands.

Über matrix

Die matrix technology GmbH gehört mit mehr als 2000 erfolgreich abgeschlossenen Projekten zu den führenden Spezialisten für Planung, Aufbau, Steuerung und Betrieb der IT für internationale Konzerne und den anspruchsvollen Mittelstand. Mit Leidenschaft, fachlicher Kompetenz und technologischem Know-how stellen sich die über 200 Mitarbeiter täglich der Herausforderung, unternehmenskritische IT-Systeme bedarfsgerecht und mit höchster Qualität zu konzipieren, aufzubauen und zu betreiben.

Das Portfolio der matrix umfasst Leistungen in den Bereichen IT-Services und IT-Beratung. Insbesondere bei der Entwicklung von IT-Strategien und deren Umsetzung, der Migration in die Cloud sowie dem Betrieb im Rahmen des IT-Outsourcings verhilft die matrix Unternehmen zu Höchstleistungen. An ihrem Hauptsitz in München sowie weiteren Standorten in Deutschland und Europa erbringt die matrix IT-Dienstleistungen für Kunden weltweit.

Kontakt

matrix technology GmbH
Telefon +49 89 589395-600
Telefax +49 89 589395-711

Web: www.matrix.ag
E-Mail: kontakt@matrix.ag