Fallbeispiel: Mobilgeräte-Management

Migration auf eine Cloud-only-Plattform

Emmi baut in der Schweiz für der Verwaltung ihrer Mobilgeräte auf eine Microsoft-only-Strategie. Der Beitrag beschreibt die Projektanforderungen der Milchverarbeiterin, den Umsetzungsprozess und die Ergebnisse.

› Jonas Hofer

Emmi ist die führende Milchverarbeiterin der Schweiz. Zum Konzern zählen allein in der Schweiz 25 Produktionsbetriebe. Knapp die Hälfte des Gruppen-Umsatzes von rund 3,9 Milliarden Schweizer Franken wird in der Schweiz erwirtschaftet. Und etwas mehr als ein Drittel der rund 9000 Mitarbeitenden arbeiten in der Schweiz. Davon benutzen rund 2000 bei ihrer täglichen Arbeit ein Mobilgerät. Dabei handelt es sich zum Grossteil um Smartphones mit dem iOS- oder Android-Betriebssystem, ein paar wenige der mobilen Helfer sind Tablets.

Mobilgeräteverwaltung

Bei den mobilen Arbeitsplatz-Services setzt Emmi mittlerweile vermehrt auf Cloud-Dienste von Microsoft. «Wir stellen fest, dass Microsoft in nächster Zeit viel in die Endpoint-Verwaltung investieren wird, und sehen Microsoft generell als strategischen Partner für Cloud-Dienste», sagt Tobias Herzog, Teamleiter Workplace Services bei Emmi Schweiz. «Darüber hinaus ist bei Emmi das Kostenmanagement ein wichtiges Thema. Aus diesem Grund setzen wir überall dort, wo Microsoft dieselbe Funktionalität wie ein bestehender Lieferant anbietet, auf eine One-Vendor-Strategie.»

Im vorliegenden Fall der Mobilgeräteverwaltung (Smartphones und Tablets) spricht vieles dafür. Denn bei der von Emmi eingesetzten Microsoft-365-Lizenz sind neben den Office-Apps, E-Mail und Kalender, Intranet und Zugriffsdiensten auf Dateien eben auch Funktionalitäten zur sicheren Geräte- und App-Verwaltung inkludiert – unabhängig davon, ob sie vom Unternehmenskunden genutzt werden oder nicht. Die Lizenz beinhaltet also nicht bloss alle wichtigen Werkzeuge und Services, sondern auch die Geräte- und Zugriffsverwaltung für alle Mitarbeitenden am Arbeitsplatz, unterwegs oder im Homeoffice.

Management in der Cloud

Mit dem Bundle können auch die Geräte und Anwendungen unterschiedlichster Art gemanagt und der sichere Zugriff auf Unternehmensdaten bereitgestellt werden. «Insbesondere sehen wir einen Vorteil, weil immer mehr Services in der Cloud betrieben werden», so Herzog. Generell sind Geräte am einfachsten da zu verwalten, wo die Services liegen. Wenn also ein Grossteil der Dienste in der Microsoft-Cloud und nicht «on-premises» im eigenen Rechenzentrum laufen, sollten die Dienste auch in der Microsoft-Cloud gemanagt werden. Erst recht, wenn die betroffenen Funktionalitäten in der bestehenden Lizenz bereits enthalten sind.

Ein ebenso schlagendes Argument sind denn auch neben der Frage des Betriebsmodells die Betriebskosten. Im Falle von Emmi sind die Einsparungen, die mit der Migration des Unified-Endpoint-Management-Systems erzielt werden können, beträchtlich. «Mit dem Wechsel auf Microsoft Endpoint Manager sparen wir allein in der Schweiz jährlich einen mittleren fünfstelligen Betrag ein.»

Projektziele

Ziel war es bei dem Projekt, innerhalb eines Jahres die Unified-Endpoint-Management-Infrastruktur vom früheren Hersteller auf Microsoft zu migrieren. Voraussetzung: Die neue Lösung sollte den Mitarbeitenden mindestens denselben Funktionsumfang wie die bestehende Lösung bieten. In der Hauptsache handelt es sich dabei um den Zugriff auf Microsoft-Office-Apps, E-Mail etc., aber auch um die Verwendung von anderen Business-Apps wie Anwendungen von SAP und Dienste-Apps von anderen Herstellern.

Die Lösung sollte geräteunabhängig sein, denn Emmi stellt firmeneigene Smartphones zur Verfügung und erlaubt nach dem BYOD-Prinzip (Bring Your Own Device) auch die Verwendung privater Devices. Das Geräte-Setup sollte dabei ohne Administrationsaufwand möglich sein, einfache Benutzeranleitungen mussten genügen. Eine weitere Anforderung war, dass die mobilen Apps nach einmaliger Authentifizierung (Single Sign-on, SSO) automatisch rollengesteuert verteilt werden und zur Verfügung stehen. Darüber hinaus sollte die Plattform auch so aufgebaut sein, dass zukünftig auch zusätzliche Anwendungsfälle aufgeschaltet werden können.

Für Nomasis als externen Dienstleister hatte man sich entschieden, weil das Unternehmen langjähriger Partner von Emmi im Bereich Sicherheit und Verwaltung von mobilen Endgeräten ist. Herzog: «Weil Nomasis uns bereits mit der Geräteverwaltung unterstützt hat, kannte man die Situation gut.»

Schrittweise Umsetzung

Zur Umsetzung des Projekts wurde das Nomasis-Standardvorgehen angewendet: Es begann mit zwei Workshops von je einem Tag im Abstand eines Monats. Zu Beginn des eigentlichen Projekts wurde ein Security Assessment Workshop (1,5 Tage) durchgeführt, gefolgt von einem Check-in Assessment (drei Tage), woraus sich der Aufbau des technischen Proof of Concept ergab (acht Tage). Dieser Ansatz wurde ausgiebig getestet. Anschliessend wurde das Produktivsystem aufgebaut und in einer Pilotphase bei Geräten von IT-Mitarbeitenden bei Emmi eingesetzt.

Danach wurden die weiteren erforderlichen Dienste nacheinander aufgebaut und pilotiert. Parallel dazu erfolgte auf der Microsoft-Plattform die Planung der Migration der im Vorgängersystem registrierten Geräte. Zusätzlich wurde definiert, welche Geräte in welchem Modus wann von wem aktiv zur neuen Plattform migriert, also vom alten System abgekoppelt und am neuen System registriert werden. Dieser Wechsel der Geräte begann im Januar 2021 und konnte bereits im Mai 2021 abgeschlossen werden. Dank Nutzung des Microsoft-Frameworks für Apps, Authentifizierung und Gerätemanagement haben heute 2000 Angestellte Single Sign-on für ihre mobilen Apps mit den firmeneigenen oder BYOD-Geräten.

Einheitliches Plattformsystem

«Das Projekt ist reibungslos verlaufen. Wir wurden viel schneller fertig als geplant», sagt Herzog. Dieser Umstand sei einerseits auf die gute Kenntnis der Gegebenheiten von Nomasis aus früheren Projekten bei Emmi zurückzuführen. Andererseits auch, weil man gemeinsam mit Nomasis eine sehr gute Benutzeranleitung für die Migration bereitgestellt habe. «Wir wussten aufgrund der Einträge im Vorgängersystem, wie viele der unterschiedlichen Geräte im Einsatz sind und konnten die Anleitungen für die Geräte optimieren, die die grösste Verwendung haben.» Dies war nötig, weil insbesondere bei den Android-Smartphones die Art und Weise der Einstellungen von Hersteller zu Hersteller variiert.

«Alles in allem waren wir dank der guten Vorbereitungen mit weniger Support-Tickets bei der Migration konfrontiert und konnten das Vierfache an Geräten pro Woche einplanen», bestätigt Herzog. Auch nach der Migration würden weniger Tickets anfallen als früher. «Das System läuft heute reibungsloser als früher. Wir führen das hauptsächlich darauf zurück, dass wir heute Microsoft-Apps über eine Microsoft-Plattform statt über ein Drittsystem zur Verfügung stellen.» Denn heute wird der Microsoft Endpoint Manager über Azure Active Directory integriert. Mit dem Vorgängersystem war dies nicht möglich.

Weitere Use Cases folgen

Die Lösung soll in Zukunft ständig weiterentwickelt werden. Zum Beispiel soll auch die «Deskless Workforce», also Mitarbeitende ohne Desktop-Arbeitsplatz, auf die neue Plattform migriert werden, ebenso Staplerterminals in der Logistik. Und man arbeitet an einem Proof of Concept, um technischen Werkstattmitarbeitenden Tablet-Computer zur Verfügung stellen zu können, damit diese für ihre Arbeit nicht fix an einen Bedienungsort an den Maschinen gebunden sind. Auch diese würden dann an die neue Lösung angebunden. «

Porträt

Jonas Hofer
Mobile Security Consultant, Nomasis

Jonas Hofer ist Mobile Security Consultant bei Nomasis, einem Service-Anbieter für mobile, sichere IT-Arbeitsplätze. In der Umsetzung von mobilen IT-Infrastrukturen betreut Nomasis über 200 aktive Kunden aus der Finanz- und Versicherungsbranche, den öffentlichen Diensten, Industrie, Gesundheitswesen, Handel und Bildung.

Kontakt

jonas.hofer@nomasis.ch
www.nomasis.ch