Amag schützt mobile Geräteflotte mit Microsoft Intune

Innerhalb der Amag-Gruppe ist mobiles Arbeiten für Mitarbeitende und Partner zentral. Das Automobilunternehmen implementiert deshalb ein umfassendes Sicherheitskonzept für Tausende Smartphones und Tablets.

Bei der Amag-Gruppe arbeitet der überwiegende Teil der 6600 Mitarbeitenden mit privaten oder vom Unternehmen zur Verfügung gestellten Smartphones oder Tablets. Dabei kommen beispielsweise Microsofts Office 365 für E-Mail und andere Office-Funktionen und Microsoft Teams zum Austausch und zur Zusammenarbeit wie auch firmeneigene Apps zum Einsatz. Letztere digitalisieren interne Geschäftsprozesse und ermöglichen sichere Zugriffe auf Unternehmensdaten. Diese fortschrittliche Arbeitsweise hat aber auch ihre Tücken. So machte denn Arkadiusz Kucharski, Head of Infrastructure Services der Amag-Gruppe, im Zuge einer Sicherheitsüberprüfung der Informatik Mankos aus: «Unsere Digitalisierungsbemühungen sind erfolgreich. Mitarbeitende können mit speziellen Apps Arbeitsabläufe wie die Serviceannahme oder Verkaufsprozesse medienbruchfrei abwickeln und auf die Systeme zugreifen. Weil aber heute Smartphone oder Tablet Klemmbrett und Schreibzeug ersetzen, müssen wir auch in die Sicherheit unserer IT-Umgebung investieren.» Ein in Zusammenarbeit mit dem Mobile-Security-Dienstleister Nomasis durchgeführtes Assessment legte schliesslich die Defizite im Detail an den Tag: nur partielle Verfügbarkeit einer verlässlichen Unified-Endpoint-Management-Lösung mit entsprechenden Sicherheitsparametern. Die meisten Benutzer erhielten allein mit ihrer E-Mail-Adresse und dem Passwort Zugriff auf geschäftliche Daten mit ihren persönlichen Geräten. Eine Mehrfaktor-Authentifizierung, wie man sie etwa vom E-Banking her kennt, fehlte. Darüber hinaus hatten alle Benutzer dieselben Zugriffsrechte, denn eine nach Rollen definierte Rechtevergabe gab es nicht.

Digitalisierung eilt mobiler Sicherheit voraus

Damit ist die Amag-Gruppe jedoch nicht allein: Das Business wird digitalisiert, das Arbeiten mobiler. Datensicherheit und Datenschutz hingegen beschränken sich mehrheitlich noch auf die stationäre bestehende, interne Infrastruktur, während die mobile Geräteflotte neue Angriffsmöglichkeiten für Cyberkriminelle bietet. Insbesondere wenn den Mitarbeitenden gehörende oder firmeneigene Geräte, wie heutzutage üblich, für geschäftliche und private Nutzung verwendet werden, ist Vorsicht angebracht. Denn ohne strikte Trennung der beiden Bereiche können Identitäten, Daten in Apps und Geräten selbst Einfallstore für Gefahren aus dem Web darstellen, sensible Daten können gestohlen werden oder gar das Geschäft zum Erliegen kommen. Kucharski musste sicherstellen, dass die mobile Geräteflotte sicher verwaltet werden kann. Weil das Unternehmen möglichst

SÄMTLICHE DIENSTLEISTUNGEN ALS MANAGED SERVICES AUS DEM NOMASIS MOBILE OPERATIONS CENTER

Als Pionier und Marktführer für Unternehmensmobilität in der Schweiz und in Liechtenstein entwickelt und betreibt Nomasis kundenspezifische mobile IT-Infrastrukturen und setzt sich dafür ein, die Nonstop-Mobilität zu gewährleisten. Nomasis nutzt mehr als 15 Jahre Know-how und Erfahrung, um die Transformation der Unternehmensmobilität für einige der bekanntesten Unternehmen zu beschleunigen und zu inspirieren. Sämtliche Dienstleistungen von Nomasis sind seit 2020 auch aus dem Mobile Operations Center (MOC) als Managed Service erhältlich. Das MOC deckt vom Endkunden über die Sicherheit und Infrastruktur inklusive Geräteverwaltung und Geräteservices sämtliche Bereiche ab. Das MOC bietet Kunden eine zentrale Plattform, mit welcher sich früher losgelöste Services nahtlos und sicher miteinander verbinden lassen. Dies erhöht die Servicequalität und Struktur für Endbenutzer und Kunden.

Kundenspezifische Programme

Im Bereich Geräte analysiert Nomasis die individuellen Geschäftsprozesse und die Anwendungsfälle der mobilen Mitarbeitenden, um kundenspezifische mobile Programme für Managed Services zu erstellen. Unternehmen können zur Verwaltung der Mobilflotte ihre aktuelle IT-Infrastruktur mit Experten aus dem MOC für Unified Endpoint Management (UEM), Enterprise Mobility Management (EMM) und Mobile Device Management (MDM) ergänzen – inklusive Fachwissen und Erfahrung für Infrastrukturen mit Microsoft Enterprise Mobility + Security und MobileIron für Plattform-, App- und Service-Management, Monitoring und Reporting.

Im Bereich Sicherheit decken die MOC-Services alle Bedrohungen ab von Unified Threat Management, App-Analysen, Phishing, Malware, Zero Trust Security, Conditional Access, Single-Sign-on und VPN. Im Rahmen der Benutzerbetreuung umfasst das MOC 1st, 2nd und 3rd Level Support, Schulungen, Apps und Service Level Agreements etc. Oberstes Ziel ist es, Mitarbeitende zu befähigen, nicht sie mit Technologie zu überfordern. Dabei wickelt Nomasis den gesamten Lebenszyklus von der Anschaffung bis zum Recycling ab. Dies beinhaltet die Geräteprovisionierung, Bereitstellung, Handling von Zubehör, Reparaturen, Ersatzteilpool-Management und Logistik.

einheitlich auf Microsoft-Produkte setzt, lag es nahe, dafür ebenfalls auf den Redmonder Software-Konzern zu setzen. Insbesondere, weil mit dem bestehenden Office-365-Vertrag bereits ein Teil der dafür notwendigen «Enterprise Mobility + Security»-Services bezahlt, aber nicht genutzt wurde. Allerdings bedarf es bei einem solchen Unterfangen einer umfassenden Analyse der bestehenden Situation und der Bedürfnisse des jeweiligen Unternehmens. Es galt, einen tragfähigen «Blueprint» zu beschreiben, also zu formulieren, wie in den nächsten Monaten mit der mobilen Geräteflotte im Unternehmen umgegangen und die dafür nötigen Sicherheitsvorkehrungen nach und nach umgesetzt werden sollen. Darüber hinaus galt es, eine neue Grundlage zu schaffen, dass zukünftige Änderungen der Anforderungen möglichst einfach umgesetzt werden können.

Umfassende Analyse der Anforderungen

So startete Kucharski gemeinsam mit Nomasis als Erstes ein halbtätiges Security-Assessment, gefolgt von einem dreitägigen «Check-in»-Assessment. Dabei sollte herausgefunden werden, welche Einflüsse sich negativ auf das Projekt auswirken könnten. Infolge der bestehenden Herausforderungen sollten möglichst schnell Verbesserungsmassnahmen eingeleitet werden, ohne dabei das Tagesgeschäft zu beeinträchtigen. Es wurde schliesslich entschieden, dass zur Verwaltung der Geräte neben Microsoft Intune auch Apple DEP und Android Enterprise eingesetzt werden, werden doch sowohl Apple- als auch Android-Geräte verwendet. Ein weiterer Grundsatzentscheid betraf die Einführung einer Testumgebung. Schliesslich sollte mit einem Proof-of-Concept die Machbarkeit des neuen Konzepts nachgewiesen werden. Dazu gehörte unter anderem, dass die Erarbeitung eines Benutzer- und Rollenkonzepts die Sicherheit erhöht und als Basis für die Kategorisierung und die Verteilung von Apps und Profilen auf den Geräten dienen soll. Weiter wurde definiert, dass alle Geräte, die auf geschäftliche Daten zugreifen können, registriert und von der IT verwaltet werden und die Betriebssystem- sowie Sicherheits- und App-Updates kontrolliert werden müssen. Zum Konzept gehörten aber auch Zugriffskontrolle und -schutz, etwa indem mit den Regeln des bedingten Zugriffs ausserhalb des Unternehmensnetzes (z.B. in oder über die Grenzen von Europa hinaus) geregelt werden kann.

Sensibilisierung der Mitarbeitenden entscheidend

Vom ersten Workshop über den Machbarkeitsnachweis zur Überprüfung der Serviceanforderungen, der Einführung eines Pilotsystems bis hin zur Implementation der endgültigen, produktiven Umsetzung nahm das Projekt seitens des Dienstleisters rund 9 Monate in Anspruch. Seitens Amag-Gruppe waren bis zu sechs Mitarbeitende aus den Bereichen IT-Infrastruktur, -Sicherheit und -Betrieb beteiligt. Im Juni 2020 ging das System in den Live-Betrieb über. Bei allen Analysen, technischen und organisatorischen Massnahmen ist indes eines von entscheidender Bedeutung: eine klare Kommunikation gegenüber Mitarbeitenden, um in Zukunft Schatten-IT und Regelverstösse zu verhindern. Schliesslich gilt es, private Anwendungen und Daten von geschäftlichen zu trennen und dabei die Benutzerfreundlichkeit bei grösstmöglicher Sicherheit gleichwohl möglichst komfortabel zu halten. Denn die Sicherheit steht und fällt mit der Sensibilisierung der Anwender. Arkadiusz Kucharski: «Das Management von BYOD-(Bring-Your-Own-Device-)Geräten via Intune ist unerlässlich. BYOD-Geräte bieten eine umfassendere Anzahl von Angriffsvektoren, die es zuverlässig zu minimieren gilt. Dazu zählen z.B. veraltete Betriebssysteme und unüberlegt heruntergeladene Apps (z.B. Spyware). Darüber hinaus stellt die Heterogenität von BYOD-Geräten eine besondere Herausforderung für die IT dar.»