Mobil und angreifbar

Amag Das Automobilunternehmen implementiert ein Sicherheitskonzept für Tausende Smartphones und Tablets.

PASCAL MEYER

Der überwiegende Teil der 6600 Amag-Mitarbeitenden arbeitet mit privaten oder vom Unternehmen zur Verfügung gestellten Mobiltelefonen oder Tablets. Dabei kommen beispielsweise Microsoft Office 365 für E-Mail und andere Office-Funktionen und Microsoft Teams zum Telefonieren wie auch firmeneigene Apps zum Einsatz.

Die Apps digitalisieren interne Geschäftsprozesse und ermöglichen sichere Zugriffe auf Unternehmensdaten. Diese fortschrittliche Arbeitsweise hat aber auch ihre Tücken. So machte Arkadiusz Kucharski, Head of Information Technology bei Amag, 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 bei der Sicherheit investieren.»

Zugriffe zu wenig geschützt

Ein mit dem Mobile-Security-Dienstleister Nomasis durchgeführtes Assessment legte schliesslich die Defizite im Detail an den Tag: Zur Verwaltung von Endgeräten (Unified Endpoint Management) war nur partiell eine verlässliche Lösung mit entsprechenden Sicherheitsparametern verfügbar. Die meisten Benutzer erhielten mit ihren persönlichen Geräten allein mit ihrer E-Mail-Adresse und dem Passwort Zugriff auf geschäftliche Daten. Eine Mehrfaktor-Authentifizierung wie etwa beim E-Banking fehlte. Darüber hinaus hatten alle Benutzer dieselben Zugriffsrechte; eine nach Rollen definierte Rechtevergabe gab es nicht.

Damit ist die Amag-Gruppe jedoch nicht allein: Das Business wird digitalisiert, das Arbeiten mobiler. Datensicherheit und -schutz 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 Geräte selbst Einfallstore für Gefahren aus dem Web darstellen, sensible Daten können gestohlen werden oder das Geschäft könnte zum Erliegen kommen.

Kucharski musste dazu sicherstellen, dass die mobile Geräteflotte sicher verwaltet werden kann. Weil das Unternehmen möglichst 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 Unternehmens. Es galt einen tragfähigen Blueprint zu beschreiben. Darüber hinaus galt es, eine neue Grundlage zu schaffen, auf der zukünftige Änderungen der Anforderungen möglichst einfach umgesetzt werden können.

So startete Kucharski gemeinsam mit Nomasis als Erstes ein halbtägiges 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.

Wichtig ist die Kommunikation gegenüber den Mitarbeiterinnen und Mitarbeitern.

Weil sowohl Apple- als auch Android-Geräte verwendet werden, wurde entschieden, dass zur Verwaltung der Geräte neben Microsoft Intune auch Apple DEP und Android Enterprise eingesetzt werden. Ein weiterer Grundsatzentscheid betraf die Einführung einer Testumgebung. Schliesslich sollte mit einem Proof of Concept die Machbarkeit des neuen Konzepts nachgewiesen werden.

Weiter definierte man, 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 (etwa in oder über die Grenzen von Europa hinaus) geregelt werden kann.

Sensibilisierung der Mitarbeitenden

Vom ersten Workshop über den Machbarkeitsnachweis zur Überprüfung der Serviceanforderungen und die Einführung eines Pilotsystems bis hin zur Implementation der endgültigen, produktiven Umsetzung nahm das Projekt seitens des Dienstleisters rund neun Monate in Anspruch. Von der Amag 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 Eines von entscheidender Bedeutung: eine klare Kommunikation gegenüber Mitarbeitenden, um in Zukunft Schatten-IT und Regelverstösse zu verhindern. Denn es gilt, private Anwendungen und Daten von geschäftlichen zu trennen und dabei die Benutzerfreundlichkeit bei grösstmöglicher Sicherheit möglichst komfortabel zu halten. Denn die Sicherheit steht und fällt mit der Sensibilisierung der Anwender.

Kucharski zufolge ist das Management von BYOD-(Bring-your-own-device-)Geräten via Intune unerlässlich. «BYOD-Geräte bieten eine umfassendere Anzahl von Angriffsvektoren, die es zuverlässig zu minimieren gilt. Dazu zählen zum Beispiel veraltete Betriebssysteme und unüberlegt heruntergeladene Apps wie etwa Spyware. Darüber hinaus stellt die Heterogenität von BYOD-Geräten eine besondere Herausforderung für die IT dar.»

Pascal Meyer, Program Manager Microsoft, Nomasis, Langnau a. A.

HOW-TO

Der Projektablauf in Kürze

1. Security Assessment (organisatorisch und technisch)
– Identifizierung der internen Anforderungen an die mobile Sicherheit und deren Benutzerfreundlichkeit

2. Check-in Assessment (technisch)
– für das Reduzieren von bestehenden Risiken, Beschleunigen der Implementierung und Vermeidung von heutigen kritischen Blockern

3. Aufbau Test als Proof of Concept (technisch)
– nach Vorgaben aus Security Assessment und gefundenen Verbesserungen aus dem Check-in Assessment

4. Überführung in ein produktives System (technisch)

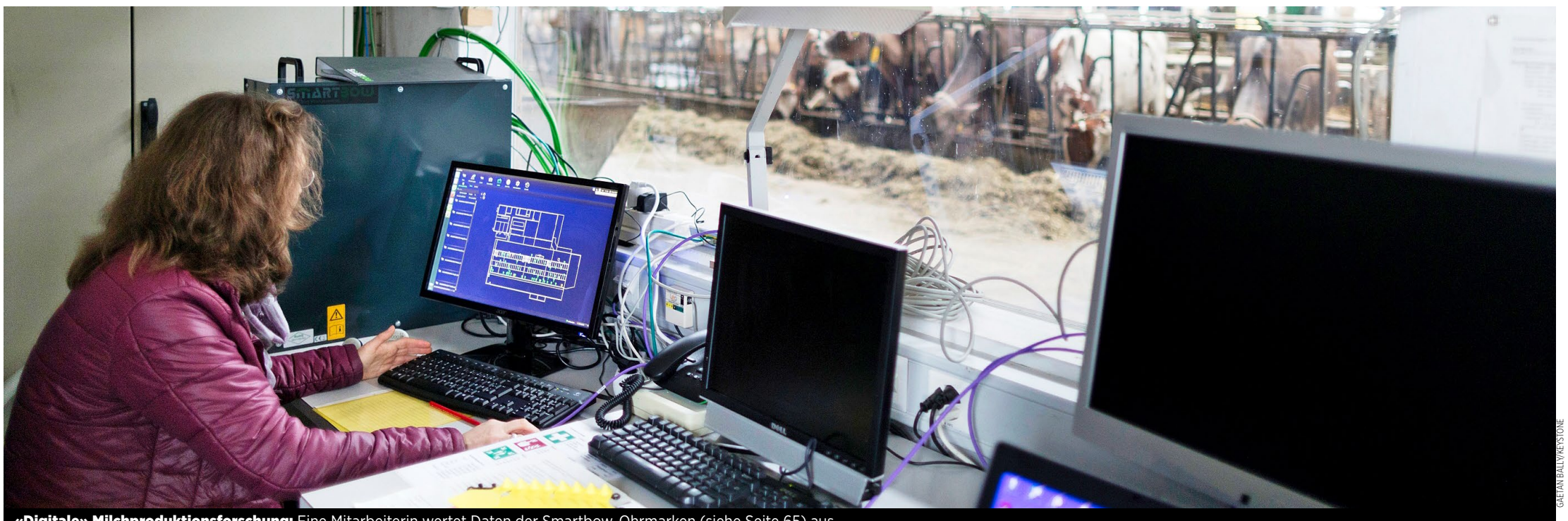
5. Enduser Pilot (organisatorisch und technisch)
– Finalisierung des produktiven Systems
– kontinuierliche Serviceverbesserung nach Rückmeldung

6. Operational Readiness (Beratung) für 1st-, 2nd- und 3rd-Level-Support unter Einbezug des Plattform- und Service-Managements (organisatorisch)
– Betriebshandbuch
– Endbenutzerbestimmung in D/F/I
– Benutzer-Guides in D/F/I
– Training für Mitarbeitende im 1st-, 2nd- und 3rd-Level-Support

7. Migration (organisatorisch und technisch)
– Device-Migrationsstrategie

8. Benutzer- und Device-Migration (organisatorisch und technisch)
– Go-Live mit potenziell 4500 Geräten

9. Projektfinalisierung (organisatorisch und technisch)



GAETAN BALLY/KEYSTONE

«Digitale» Milchproduktionsforschung: Eine Mitarbeiterin wertet Daten der Smartbow-Ohrmarken (siehe Seite 65) aus.

Die Fünf-Minuten-Kühlschrank-Werbepause

Streaming-Dienste Werbung soll die Einnahmen und die Reichweiten erhöhen. Abo-Modelle dürften sich damit ausdifferenzieren.

MATTHIAS NIKLOWITZ

Auch wenn sämtliche Kinos während des Lockdowns geschlossen waren (etliche sind es weiterhin) – auf Filme verzichten musste niemand: Alleine Netflix hält ein Angebot von 36 000 Filmstunden, entsprechen vier Jahre Nonstop-Schauen, bereit. Viele Hollywood-Streifen sind auf Disney+ zu sehen. Mubi, Sky Show, Myfilm und weitere Streamer bringen ebenfalls Filme und mit Amazon Prime Video sowie Apple TV+ gibt es Player mit der erforderlichen finanziellen Stärke, um attraktive Filme und Serien zu verbreiten.

Marktführer unter den bezahlten Diensten ist indes weiterhin Netflix, das in der Schweiz gemäss jüngsten Zahlen zwei Millionen Haushalte erreicht.

Gemäss dem Marktforschungsunternehmen Statista wird Youtube in der Schweiz am meisten genutzt: Rund zwei Drittel aller Schweizer schauen hier regelmässig Filme, deutlich mehr als bei Netflix sowie den Diensten der grossen Telekom-Netzbetreiber in der Schweiz. Amazon kommt auf 7,3 Prozent, Netzkino auf 2,8 Prozent.

Typischerweise haben Haushalte zwei bis drei Streaming-Dienste abonniert. Sie verlieren indes gemäss den Analysten der Investmentbank Bernstein nicht nur langsam die Übersicht über das, was sie sehen. Jetzt drängen sich auch erste Gratisdienste, die sich über Werbung finanzieren, in den Markt. Werbeeinnahmen gelten unter den Streaming-Verbreitern auch als potenzielle weitere Einnahmequelle, um im sich verschärfenden Wettbewerb bei attraktiven neuen Inhalten mitzuhalten. Aus der Sicht der Werbetreiber sind solche Angebote ebenfalls interessant, denn nicht jede Firma will sich den Reputationsrisiken der Youtube-Inhalte aussetzen. Wegweisend ist auch hier Asien: In China ist das werbefinanzierte Streaming das Standard-Geschäftsmodell. Youku von Alibaba, Iqiyi von Baidu und Tencent Video kommen auf je eine halbe Milliarde Zuschauer.

Ob die Rechnung dabei aufgeht und die Zuschauenden mehr als lediglich ihre Augenbrauen über ihren rechteckigen Augen leicht heben, wenn Gratis-Streaming kommt, ist offen. Zwar zeigt die Marktforschung eine Sättigung bei der Anzahl der Dienste und gemäss Umfragen ist ein Drittel der Kunden bereit, für niedrigere Abo-Kosten oder für ein Gratisangebot Werbung zu ertragen (oder diese Zeit für den Gang zum Kühlschrank zu nutzen). Laut den Bernstein-Analysten wird es für den Erfolg dieser Angebote aber entscheidend sein, ob und wie lang die Werbezeit im Verhältnis zum Programm ist. In den USA und in Italien erreicht die Werbung 15 bis 20 Minuten pro Stunde. Werbefinanzierte Angebote haben laut den Analysten lediglich eine Chance, wenn sie unter und bis maximal 5 Minuten bleiben.

Unter Analysten gilt es als ausgemacht, dass sich der Gigant Amazon mittelfristig in einer Poleposition befindet. Denn beim besonders zukunftsträchtigen Contextual Shopping, also dem Einkauf von Produkten beim Zuschauen von Sendungen, ist man besonders gut positioniert.