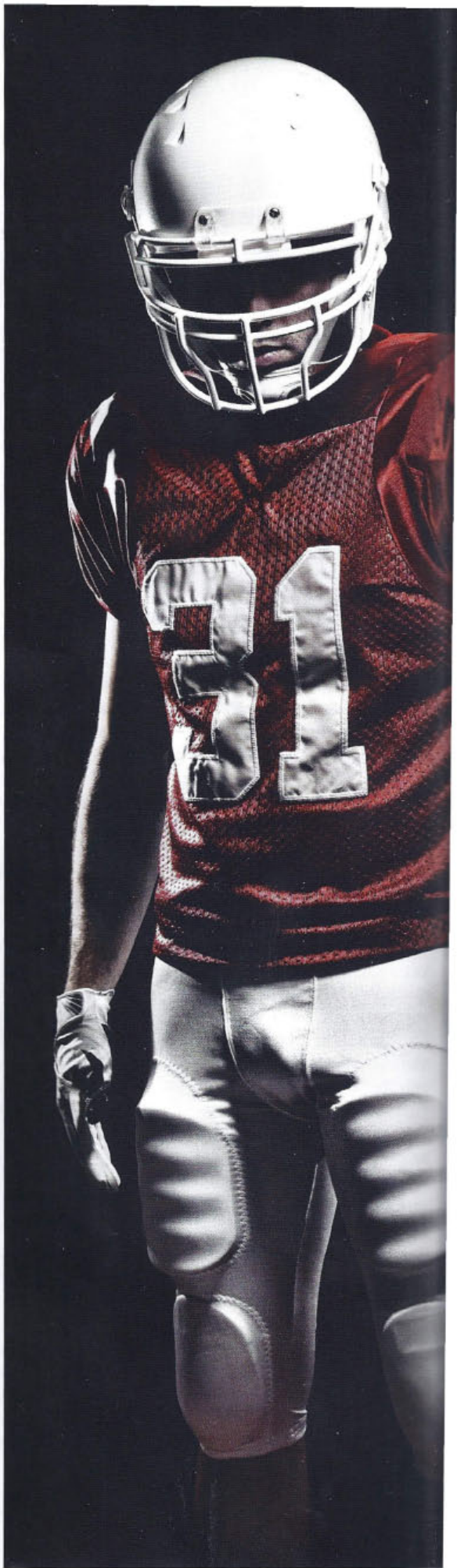

ANGEBOTSERSTELLUNG MIT SICHERHEIT SCHNELLER

Der größte Sicherheitsdienstleister in Deutschland, Securitas, hat den Prozess der Angebotserstellung mittels einer CRM-App beschleunigt. Um ein sicheres Geräte- und App-Management zu gewährleisten, wurde ein Mobile Device Management implementiert.

Securitas operiert mit 300.000 Mitarbeitern in 51 Ländern. Aus einem breiten Spektrum spezialisierter Sicherheitsdienstleistungen, technologischer Komponenten sowie Beratung und Ermittlung entwickelt das Unternehmen auf die jeweiligen Kundenbedürfnisse zugeschnittene Sicherheitslösungen. Mit 120 Niederlassungen in den drei Geschäftsbereichen Spezialisierte Sicherheitsdienste, Mobile Dienste und Alert Services ist Securitas Deutschlands größter Sicherheitsdienstleister und der einzige international arbeitende Konzern der Branche.

Relativ früh setzte man auf neue mobile Endgräte: Die Geschäftsführung und der Vertrieb des Bereichs Mobile Dienste nutzen bereits seit zwei Jahren iPads ergänzend zu Notebooks. Anfang 2012 entschloss man sich im Unternehmen dann, den zeitaufwendigen, klassischen Prozess der Angebotserstellung mit Hilfe der Tablets zu beschleunigen: Während des Kundengesprächs sollten die Vertriebler direkt mit dem iPad auf Dokumente im Firmennetz und auf die Kundendaten der von Securitas eigenentwickelten CRM-App iKnow zugreifen können, um passende Angebote elektronisch vor Ort erstellen und den Kunden direkt per E-Mail zum Unterzeichnen vorlegen zu können.

Das Angebot direkt auf dem Tisch

Über einen geschützten Zugriff auf die Datenbank sollten die erhobenen Daten ins Firmennetz zurückgeschrieben werden. Im ersten Schritt sollten dafür 100 iPads mit iKnow ausgestattet

Angebotserstellung auf dem iPad beim Kunden vor Ort

Damit die Vertriebler Angebote direkt beim Kunden auf Tablets erstellen können, musste Securitas-IT-Leiter Antonio Valls Ruiz in Sachen Mobile Device Management aktiv werden.

werden, später dann der deutschlandweite Rollout der CRM-Software erfolgen. Die Leitung des Projekts übernahm Stefan Schenke, IT-Leiter Division Mobil in Zusammenarbeit mit Antonio Valls Ruiz, IT-Leiter Deutschland und Verantwortlicher für Datensicherheit bei Securitas.

„Natürlich sind wir in der IT immer offen für Neuerungen, aber Sicherheitsvorkehrungen haben bei uns oberste Priorität – auch bei mobilen Geräten", betont Antonio Valls Ruiz. Folglich hat der IT-Leiter nach einem Mobility-erfahrenen IT-Beratungshaus für die möglichst schnelle Umsetzung des anspruchsvollen Projekts gesucht, das sowohl eine sichere Mobile-Device-Management-Infrastruktur aufbauen als auch eine zuverlässige App für den sicheren, mobilen Dateizugriff per Fileserver-Anbindung anbieten und integrieren kann. Im Juni 2012 beauftragte Valls Ruiz die EBF GmbH.

Im ersten Schritt installierten und konfigurierten die Kölner Mobility-Experten das Mobile-Device-Management-System MobileIron. Dessen IT-Komponenten Sentry und Virtual Smartphone Platform (VSP) wurden als virtuelle Images vollständig in die bestehende Microsoft-Umgebung von Securitas integriert. Die VSP baut automatisch die Verbindungen zu den MDM-Anwendungen und den erforderlichen Securitas-Systemen wie LDAP, Lotus Notes, ActiveSync und zu den unterschiedlichen Zertifizierungsstellen auf. In der zentralen VSP-Managementkonsole richtete der Dienstleister die Konfigurationsprofile für die Benutzergruppen ein, z. B. die Passwortrestriktionen, die Sperrcode-Regeln und die Jailbreak Detection.

Kein unnötiger Papierkram mehr

Im zweiten Schritt richtete EBF den Securitas Enterprise AppStore mit Hilfe der MobileIron App Storefront ein. Somit ist der Securitas-AppStore per Zertifikat gesichert, nicht richtlinienkonforme Tablets erlangen keinen Zutritt zum App-Katalog von Securitas. Das Deployment der CRM-App iKnow auf die ersten 100 iPads wurde automatisiert über den Enterprise App-Store ausgeführt, sodass die Securitas-Vertriebler fortan sicher auf Kundendaten zugreifen können. Auf die gleiche Weise hat das IT-Beratungshaus die selbst entwickelte Business-App EBF.Connector auf den angeschlossenen iPads verteilt. Mit dieser Software ist jederzeit ein sicherer Lesezugriff via iPad auf Dokumente auf einem dedizierten Fileserver im Securitas-Netzwerk möglich. Dabei werden keine Kopien von Dokumenten auf den Tablets gespeichert. Kritische Unternehmensdaten bleiben also immer in der sicheren Netzwerkumgebung und können direkt aus dem Connector heraus präsentiert werden.

„Vorher arbeitete unser Vertrieb mit klassischen Mitteln, erst Beratung und Präsentation beim Kunden und dann die Angebotserstellung im Büro. Seit Mitte dieses Jahres können die Vertriebsmitarbeiter der Division Mobil im Dialog mit den Kunden die gewünschten Produkte und Dienstleistungen bereits während des Gesprächs auf dem iPad zusammenstellen", berichtet Securitas-Projektmanager Stefan Schenke und er fährt fort: „Den Vertrag erhalten unsere Kunden sofort per E-Mail. Lästiger Papierkram und Zeitverlust gehören der Vergangenheit an."

Besonders wichtig ist für Securitas die Sicherheit und Effizienz der zentralen MDM-Lösung. Die überwacht permanent Apps, Inhalte und Geräte und verfügt über eine Jailbreak-Detection: Es stellt über Ortungsdienste selbstständig fest, ob ein Tablet vom Benutzer gejailbreakt wurde und sperrt dann die Verbindungen ins Unternehmensnetzwerk. Zudem können die Administratoren unerwünschte Apps definieren. Installiert ein Benutzer eine potentiell gefährliche App wie Dropbox oder Apps mit rechtsradikalen Inhalten, Sex, Gewalt oder Ähnlichem auf seinem iPad, bleibt das gesamte Gerät so lange blockiert, bis er die App löscht. Nicht zuletzt besteht für Besitzer mobiler Geräte bei Securitas die Pflicht, einen mindestens sechsstelligen alphanumerischen Sperrcode festzulegen. Geht ein iPad verloren, kann die IT das Gerät zentral per Remote Lock sperren oder die Unternehmensdaten Wund -Apps per selektiven Remote Wipe vom Tablet entfernen.

Als Nächstes möchten die IT-Verantwortlichen – basierend auf den bisherigen Erfahrungen – die User Policies erweitern. Diese werden intern publiziert und dann mittels der MDM-Lösung auf den iPads durchgesetzt. „Bei Sicherheitsverstößen wird künftig automatisch jeder Zugriff auf Netzwerk, Apps und Inhalte gesperrt", kündigt der IT-Leiter an. ■

MARINA BÄDER