Buurtzorg schützt Daten im Gesundheitswesen durch das Sichern von 8.000 iPads

Die Anforderung

Die ambulanten Pflegefachkräfte von Buurtzorg Nederland (Buurtzorg) verbringen den Großteil ihrer Zeit unterwegs auf dem Weg zu ihren Patienten sowie mit deren Pflege im eigenen Haushalt. Das wichtigste Werkzeug für ihre Produktivität sind dabei firmeneigene iPads, die mit MobileIron Enterprise Mobility Management (EMM) ausgestattet sind.

Mittels der eigenen App von Buurtzog haben die Pflegekräfte auf ihren iPads Zugang zu sensiblen Patientendaten – etwa zu Pflegebewertungen oder Abrechnungen. Darüber hinaus nutzen sie häufig auch öffentliche WLAN-Netze, um weitere Anwendungen aufzurufen, die ihnen bei ihren täglichen Aufgaben helfen (z. B. bei der Bewertung von Verletzungen). Diese Anwendungsfälle stellten die Führungskräfte von Buurtzorg vor eine Herausforderung: Einerseits wollten sie ihren Beschäftigten ermöglichen, ihre iPads flexibel und möglichst effektiv einzusetzen. Gleichzeitig erkannten sie jedoch auch die Notwendigkeit, dass sie zum Schutz der Patientendaten eindeutige Richtlinien für akzeptable Anwendungen erstellen und verwalten mussten.

> „Gewisse Apps auf eine „Blacklist“ zu setzen ist sehr schwierig, da es im App Store sehr viele Anwendungen gibt. Wenn wir jedoch stattdessen nur Apps einer bestimmten „Whitelist“ zulassen, haben unsere Beschäftigten nicht mehr sehr viel Freiheit.“
>
> **Jos de Blok,** CEO und Mitgründer

BUURTZORG

Kundenprofil

Buurtzorg Nederland ist eine niederländische Organisation, die in der häuslichen Krankenpflege tätig ist. Sie ist dafür bekannt, mit selbstverwalteten Teams von Pflegefachkräften qualitativ hochwertige Pflege anzubieten. Der Name des Unternehmens bedeutet auf Deutsch übersetzt „Nachbarschaftshilfe“.

Branche: Gesundheitswesen

Mobilitätsstrategie: COPE

Die Lösung

Lookout Mobile Endpoint Security

Das Ergebnis

- Vollständige Beseitigung von mobilen Bedrohungen, durchgeführt von technisch nicht versierten Anwendern
- Produktivitätserhöhung der mobilen Pflegeteams
- Einhaltung der niederländischen Datenschutzbestimmungen bezüglich der Sicherheit privater Daten auf mobilen Geräten
- Transparenz über Netzwerk- und App-basierte Bedrohungen, die potenziell zu Datenverlusten führen könnten

Sicherheitsspezifische Herausforderungen

- Nutzung öffentlicher WLAN-Netze durch eine große Gruppe mobiler Beschäftigter bei gleichzeitiger Reduzierung des Risikos von Man-in-the-Middle-Angriffen
- Einhaltung eines niederländischen Datenschutzgesetzes, infolgedessen Unternehmen Informationen auf unterschiedlichsten Geräten schützen müssen
- Bestätigung, dass die sensiblen Daten der Kunden bei Buurtzorg in sicheren Händen sind
- Erhöhung der Transparenz über App- und gerätebasierte Sicherheitsbedrohungen (z. B. „sideloaded" Apps auf iOS-Geräten)

Den Zugriff auf den App Store generell zu sperren wäre zu restriktiv gewesen und war deshalb keine Option. Das Unternehmen entschied darüber hinaus, dass auch das Sperren bzw. Freigeben individueller Anwendungen auf Basis einer Blacklist/Whitelist keine nachhaltige Lösung darstellte. Das war der entscheidende Punkt, an dem Ecare TCS, Buurtzorgs zuverlässiger Managed-Services-Anbieter, dem Unternehmen den Einsatz von Lookout Mobile Endpoint Security vorschlug.

Die Lösung

Um die mobilen Sicherheitsprobleme zu lösen, arbeitete Ecare TCS mit Buurtzorg zusammen: gemeinsam stellten sie Lookout Mobile Endpoint Security auf 8.000 iPads bereit und aktivierten es. „Jetzt, da wir die Lösung von Lookout für mobile Sicherheit im Unternehmen implementiert haben, kann Buurtzorg entsprechende Mobilitätsrichtlinien erstellen. Diese ermöglichen es den Pflegeteams, Internetverbindungen und Anwendungen für eine effiziente und hochwertige Patientenversorgung nach Belieben zu nutzen. Gleichzeitig haben wir nun auch vollständige Transparenz über die Bedrohungen, mit denen die iPads der Pflegekräfte in Berührung kommen", erklärt Jeffrey Scholten, IT-Berater für Ecare TCS.

Für einen Teil der Beschäftigten konnten Ecare TCS und Buurtzorg die „Lookout for Work-App" via MobileIron bereitstellen. Dabei wurde die Anwendung direkt auf die Geräte übertragen, ohne dass die Beschäftigten etwas tun mussten. Ein weiterer Teil der Beschäftigten konnte die „Lookout for Work-App" über einen persönlichen Registrierungscode mit einem einzigen Klick herunterladen. Die Einführung verlief für alle Beschäftigten von Buurtzorg mühelos und störungsfrei. Dies beweist, dass auch technisch nicht versierte Anwender die Lookout-App auf ihren Firmen-iPads schnell installieren und aktivieren können.

Lösungskriterien

- Muss in der Lage sein, die iOS-Geräte vor Netzwerk- und App-basierten Bedrohungen zu schützen
- Muss sich in MobileIron für die App-Bereitstellung und Gerätefehlerbehebung integrieren lassen, um das EMM-Potenzial voll auszuschöpfen
- Muss die Einhaltung der niederländischen Datenschutzgesetze ermöglichen, die Unternehmen dazu verpflichten, sensible Kundendaten auf mobilen Geräten zu schützen
- Muss eine einfache Benutzeroberfläche aufweisen, die es auch technisch nicht versierten Beschäftigten leicht macht, erkannte Bedrohungen selbst zu beseitigen

Das Ergebnis

Lookout Mobile Endpoint Security erkannte eine beträchtliche Anzahl von Man-in-the-Middle-Angriffen und einige risikoreiche „sideloaded" Apps auf den Geräten von Buurtzorg innerhalb der ersten 30 Tage nach der Bereitstellung.

Wenn ein Angriff erkannt wird, gibt es nun mehrere Möglichkeiten, die Bedrohung zu beseitigen: Das Ecare TCS-Team kann entweder mittels seiner MobileIron EMM-Lösung Maßnahmen ergreifen oder aber dem User ermöglichen, die Bedrohung auf dem eigenen Gerät selbst zu beseitigen. Da die Beschäftigten von Buurtzorg damit vertraut waren, wie sie mit von Lookout erkannten mobilen Gefahren umgehen sollten, wurden die erkannten Man-in-the-Middle-Bedrohungen von den Endanwendern in durchschnittlich weniger als 8 Minuten beseitigt. Wurden „sideloaded" Apps erkannt, erfolgte die Beseitigung durch die User nach durchschnittlich 7 Stunden.

Indem 100 % der mobilen Bedrohungen durch technisch nicht versierte Anwender beseitigt wurden, konnte Buurtzorg das Risiko durch mobile Bedrohungen für die Organisation deutlich verringern. Außerdem ermöglichte die Organisation ihren hoch-produktiven Pflegeteams auf diese Weise, ihre Leistung noch weiter zu verbessern. Die Pflegefachkräfte von Buurtzorg haben jetzt die Freiheit, alle Apps herunterzuladen, die sie brauchen, und können sich auf ihre wesentlichen Aufgaben konzentrieren. Gleichzeitig sorgt Lookout Mobile Endpoint Security dafür, dass ihre Geräte und die vertraulichen Daten ihrer Kunden jederzeit geschützt sind.

Das Unternehmen hat jedes der Ziele erreicht, die am Beginn der Initiative für mobile Sicherheit definiert wurden: Es hat für die Sicherheit mobiler Plattformen gesorgt, die Einhaltung der niederländischen Datenschutzbestimmungen sichergestellt und dem Unternehmen Transparenz über mobile Bedrohungen verschafft.