Buurtzorg beschermt gezondheidsgegevens door 8.000 iPads te beveiligen

Buurtzorg Nederland is een Nederlandse thuiszorgorganisatie die bekend is vanwege de inzet van zelfsturende wijkverzorgingsteams om hoogwaardige zorg te bieden.

De uitdaging

De zorgverleners van Buurtzorg Nederland (Buurtzorg) spenderen het grootste deel van hun tijd aan het bezoeken en verzorgen van cliënten aan huis. Ze gebruiken company-owned iPads beheerd door MobileIron Enterprise Mobility Management (EMM) als voornaamste hulpmiddel voor productiviteit.

De iPads geven de zorgverleners toegang tot gevoelige informatie van patiënten, zoals zorg assessments en administratie via de eigen app van Buurtzorg. Zorgverleners gebruiken daarnaast regelmatig openbare wifi-verbindingen om apps te gebruiken die hun alledaagse taken, zoals bijvoorbeeld het beoordelen van wonden gemakkelijker maken. Deze toepassingen vormden een uitdaging voor de leidinggevenden van Buurtzorg: zij wilden dat medewerkers de iPads op de meest productieve manier konden inzetten, maar beseften ook dat ze een beleid voor toegestane apps moesten maken om de patiëntgegevens te beschermen.

Beveiligingsuitdagingen:

- Medewerkers onderweg in staat stellen om vrij verbinding te maken met wifi bij cliënten en tegelijkertijd het risico op een man-in-the-middle-attack te verminderen;
- Naleven van Nederlandse wet, die stelt dat bedrijven hun best moeten doen om informatie op apparaten te beschermen;
- Aan klanten aantonen dat hun gevoelige informatie bij Buurtzorg in veilige handen is;
- Inzicht verkrijgen in beveiligingsdreigingen rondom apps en apparaten, zoals gesideloade apps op iOS-apparaten.

Zoals Buurtzorg zelf stelt:

„Het blokkeren van apps is erg moeilijk omdat de App Store heel veel apps bevat. Als we apps op een whitelist plaatsen, gaat dat echter ten koste van de vrijheid van onze medewerkers."

- Jos de Blok, CEO en medeoprichter

Het geheel ontzeggen van de toegang tot de App Store zou niet werken omdat dat te restrictief was. Buurtzorg concludeerde verder dat het beheren van een lijst met verboden of toegestane apps geen duurzame oplossing bood. Op dit cruciale moment suggereerde Ecare TCS, de vertrouwde aanbieder van managed services voor Buurtzorg, Lookout Mobile Endpoint Security. Omdat Ecare TCS een verlengstuk van het Buurtzorg-team vormt en ICT-diensten voor telecom, internet, hardware en software en ondersteuning biedt, is het bedrijf verantwoordelijk voor het implementeren en beheren van elke nieuwe oplossing. De suggestie was dan ook niet uit de lucht gegrepen.

Lookout

De oplossing

Om de uitdagingen op het gebied van mobiele beveiliging op te lossen, implementeerde en activeerde Ecare TCS samen met Buurtzorg, Lookout Mobile Endpoint Security op 8.000 iPads. „Dankzij de zakelijke mobiele beveiligingsoplossing van Lookout voor het detecteren van dreigingen kan Buurtzorg nu een mobiliteitsbeleid opstellen dat de zorgverleners in staat stelt om vrij internetverbindingen en apps te gebruiken, waarmee ze efficiënt hoogwaardige zorg kunnen bieden, terwijl Buurtzorg volledig inzicht heeft in dreigingen op alle iPads", stelt Jeffrey Scholten, ICT-adviseur bij Ecare TCS.

Ecare TCS en Buurtzorg implementeerden de app Lookout for Work eenvoudig via MobileIron door de app naar de apparaten van medewerkers te pushen zonder dat zij actie hoefden te ondernemen. Een andere groep medewerkers downloadde de Lookout for Work-app in één klik met een persoonlijke activeringscode. Het uitrollen verliep eenvoudig en zonder onderbrekingen voor alle medewerkers van Buurtzorg - een bewijs dat zelfs eindgebruikers zonder veel technische kennis de app van Lookout snel op hun zakelijke iPads kunnen installeren en activeren.

Criteria voor de oplossing:

- Moet iOS-apparaten kunnen beschermen tegen dreigingen vanuit netwerken en apps;
- Moet passen binnen de implementatie- en herstelfuncties van MobileIron voor apps, zodat de gedane investering in EMM wordt benut;
- Moet naleving mogelijk maken van Nederlandse privacywetgeving die bedrijven verplicht om hun best te doen om gevoelige gegevens van cliënten op mobiele apparaten te beschermen;
- Moet beschikken over een eenvoudige gebruikerservaring waardoor alle medewerkers eenvoudig zelf elke gedetecteerde dreiging kunnen oplossen.

De resultaten

Lookout Mobile Endpoint Security detecteerde in de eerste 30 dagen na de implementatie een aanzienlijk aantal man-in-the-middle-attacks en verschillende risicovolle gesideloade apps op apparaten van Buurtzorg.

Nadat er een dreiging is gedetecteerd, zijn er verschillende opties om die dreiging te verhelpen. Het team van Ecare TCS kan actie ondernemen via de EMM-oplossing van MobileIron of eindgebruikers in staat stellen om de dreiging op hun eigen apparaat op te lossen. Omdat de medewerkers van Buurtzorg voorlichting hadden gekregen over het omgaan met mobiele dreigingen die door Lookout werden gedetecteerd, werden de man-in-the-middle-detecties gemiddeld genomen in minder dan acht minuten verholpen door eindgebruikers. De gesideloade apps werden na gemiddeld zeven uur door de gebruikers zelf opgelost.

Met een herstel van 100% van de mobiele dreigingen, uitgevoerd door de eindgebruikers zelf, heeft Buurtzorg de mobiele risico's verminderd. De productieve teams waar de organisatie om bekend staat kunnen nu nóg productiever zijn. De verzorgenden van Buurtzorg hebben de vrijheid om de apps te downloaden die ze nodig hebben en kunnen zich richten op dat waar ze goed in zijn. Lookout Mobile Endpoint Security zorgt ondertussen dat hun apparaten en de persoonlijke gegevens van hun cliënten veilig zijn.

Het bedrijf heeft alle doelen gerealiseerd die aan het begin van het initiatief voor beveiliging van de mobiele apparaten werden gesteld, door te zorgen voor veilig mobiel gebruik, naleving van privacyrichtlijnen en inzicht in mobiele dreigingen.