Zorgapp aan achterzijde kwetsbaar via Google platform Firebase

Op 15 juni 2020 schreef ik dat de Britse huisartsapp Babylon videoconsulten van andere patiënten lekte toen iemand de app voor een consult gebruikte. Een softwarefout gaf het bedrijf Babylon Health als oorzaak. Door een publicatie op 19 juni 2020 op de website van het online magazine Digital Health is duidelijk geworden dat een Firebase URL technische informatie lekte over digitale zwakheden in de Babylon app. Die gebruiken huisartsen van vijf GP At Hand praktijken in Londen voor triage, (video)consulten en het regelen van medicijnvoorschriften. Firebase is een populaire dienst van Google die gebruikt wordt om informatie tussen op smartphones en tablets geïnstalleerde apps en de leveranciers ervan uit te wisselen. Op 11 mei waarschuwden cybersecurity-onderzoekers op de website Comparitech dat er grote problemen t.g.v. het gebruik van Firebase bestonden. Naar schatting 24.000 Android apps bleken gebruikersdata te lekken door blunders hij Firebase-gebruik door configuratiefouten.

Firebase

Wat doet Firebase precies? Het is software die ontwikkelaars van apps voorziet van gerichte chatberichten, meldingen van en rapportage over wat er gebeurt in de app. Firebase vormt een platform voor cloud-berichten, ontworpen voor bedrijven van elke omvang waarmee gebruikers gerichte, aanpasbare meldingen naar elk apparaat kunnen verzenden. Problematisch is dat door het nogal frequent voorkomen van configuratiefouten binnen de Firebase-databases het mogelijk blijkt dat ongeautoriseerde derden makkelijk binnen die databases persoonlijke gegevens

kunnen opsporen en toegang kunnen krijgen. Het betreft duizenden apps. Comparitech berekende wel 24.000. Men vond dat een eenvoudige verandering aan een Firebase-URL een aanval mogelijk maakt om de inhoud van kwetsbare databases in te zien en te downloaden. In het artikel van Comparitech doet de auteur Paul Bishop een dringend beroep op app-ontwikkelaars hun Firebase-configuratie te controleren op de juiste instellingen. Voor publicatie had Bishop Google al gewaarschuwd. Die zou Firebase-gebruikers erover ingelicht hebben.

Babylon

Open source technoloog Rob Dyke liet Digital Health News weten:

“At the moment they have this wide open Firebase URL which is showing debug information from the apps and this leaks information about the number of times it’s run debug tests and the times that the tests have been successful and overall successful rate, For example, we can see the test of ‘appointment details cancel appointment’ has run 159 times and has been successful 119 times, giving it a 75% success rate. So they have a dataset that is leaking the results of tests of their application which could be useful to attack the application because you can find out which bits of code could be vulnerable.”

De onderzoekers stellen geen patiëntdata gezien te hebben, maar zeggen daarbij wel dat ze daar ook niet actief naar gezocht hebben.

Reactie Babylon Health

Uiteraard was de reactie van app maker en beheerder Babylon Health op de gevonden kwetsbaarheden er één waarin men het probleem meteen minimaliseerde. Men gaf aan de door Google recent aangescherpte instellingen inmiddels geïmplementeerd te

hebben. Het neemt niet weg dat er een enorme fout begaan is door een backend-applicatie van een app die zeer gevoelige gegevens verwerkt verkeerd in te stellen.

Zeer lage CVSS-score voor Babylon

De onderzoekers bekeken ook de veiligheid van de Babylon app. Ze gebruikten daarvoor het Mobile Security Framework programma. Men gebruikte daarbij het Common Vulnerability Scoring System(CVSS). Dat is een open industrie-standaard om kwetsbaarheid-schattingen op cybersecurity-gebied. Met CVSS kan een perfecte applicatie een score van maximaal 100 krijgen. Babylon scoorde maar een magere 10 en valt daarmee in de categorie “critical risk”. Onderzoeker Rob Dyke vond in de test een onveilige random number generator, opslag van platte tekst betreffende gevoelige informatie en gekraakte encryptie-algoritmes. Ook zag hij dat men de encryptiemethoden MD5 en SHA 1 nog in de app gebruikt. Al in 2007 raadden experts het gebruik van MD5 af. Ook SHA1 wordt al jaren afgeraden voor encryptie. In een reactie zegt Babylon Health dat men SHA1 gebruikt om de ondertekening van het beveiligingscertificaat van Google Play te regelen, maar dat men verder wel 256-bits encryptie-protocollen gebruikt.

Ontkenning

Babylon Health komt dan ook met een glasharde ontkenning van de beoordeling “critical risk”. Het bedrijf zegt zich niet te herkennen in de uitslag. Men stelt dat die niet te vergelijken is met de eigen beoordelingsresultaten. Ze zien de gefundeerde kritiek van buitenaf dus niet als gratis advies maar als een regelrechte bedreiging. Een in mijn ogen nogal domme reactie.

Wat leert dit ons?

Deze hele geschiedenis leert ons dat een app niet alleen kwetsbaar kan zijn door intrinsieke fouten, slordige beveiliging etc, maar ook door de manier waarop ontwerpers

omgaan met hun testresultaten. Als die testresultaten voor de buitenwacht zichtbaar zijn op een Google-platform, dan legt men die kwetsbaarheden op een presenteerblaadje voor potentiële hackers.

W.J. Jongejan 22 juni 2020.

Afbeelding van Alexas_Fotos via Pixabay