

Android-telefoons lekken massaal persoonlijke data

Iedere smartphonegebruiker kent de waarschuwing: zeg nee tegen de app die je persoonlijke data wil weten. Maar ook al zeg je nee op alles, het besturingssysteem Android van Google, dat op 80% van alle mobiele telefoons is geïnstalleerd, kan ongemerkt persoonlijke gegevens blijven lekken. Dat blijkt uit een groot-schalige studie van een Spaanse onderzoeksgroep. 'Er is nu solide bewijs voor de enorme schaal waarop het gebeurt.'

→ PAGINA 26



Besturingssysteem Android lekt persoonlijke data 'op enorme schaal'

➔ **Breed Spaans onderzoek bewijst massaal datalek**

➔ Gebruikers van mobiele telefoons niet op de hoogte

➔ 'Het probleem is duidelijk niet langer onder controle'

Jan Fred van Wijnen
Amsterdam

Iedere smartphonegebruiker kent de waarschuwing: zeg nee tegen de app die je locatie wil weten. Zeg nee als de software vraagt om toegang tot foto's, contactgegevens, berichten, opslag, browsergeschiedenis, camera, microfoon, bluetooth.

Maar het helpt niet. Ook al zeg je nee op alles, het besturingssysteem Android, dat op 80% van alle mobiele telefoons is geïnstalleerd, kan ongemerkt persoonlijke gegevens blijven lekken. Dat blijkt uit een grootschalige studie van een Spaanse onderzoeksgroep.

'Gebruikers weten dit vaak niet en hebben nooit toestemming gegeven', zegt Juan Tapiador, hoogleraar computerwetenschap aan de Carlos III-universiteit in Madrid, een van de partners in het onderzoek.

Het researchcollectief schakelde een 'crowd' van bijna drieduizend telefoongebruikers uit 130 landen in. De Spanjaarden installeerden software op hun telefoons, waarmee ze een jaar lang konden monitoren welke data het apparaat uitzond naar 'derde partijen' (vooral advertentiebedrijven). Ruim een derde van de deelnemers is Europees.

'We wisten al dat Android ingebouwde privacylekken bevat', zegt Veelasha Moonsamy, onderzoeker bij de Digital Security Group van de Radboud Universiteit in Nijmegen. 'Maar met deze Spaanse studie is er solide bewijs voor de enorme schaal waarop het gebeurt.' Zelf deed ze ook onderzoek naar ingebouwde lekken in Android.

De deelnemers aan het Spaanse onderzoek gebruikten 1742 verschillende telefoontypes, van 214 fabrikanten. Een kwart van de telefoontjes was van Samsung, een vijfde van Huawei.



Datalekken in Android lopen via apps die door de telefoonfabrikant vooraf zijn geïnstalleerd. Telecombedrijven krijgen vaak korting van fabrikanten, als ze zulke apps niet verwijderen. FOTO: REUTERS

De deur van het Android-systeem blijkt wagenwijd open te staan. En dat is volgens het onderzoek al vanaf het moment dat de telefoon uit de verpakking komt en voor de eerste keer wordt aangezet.

Het probleem zit in de ongecontroleerde hoeveelheid apps die door de fabrikant worden meegeleverd. Dit is mogelijk door het 'open source'-karakter van Android. Dat maakt het voor elke fabrikant mogelijk de software aan te passen. De apps zitten als verstekeling bij het besturingssysteem, en sturen hun

data naar advertentie- en trackingdiensten van grote spelers zoals Alphabet, Facebook, Verizon, AppsFlyer en comScore.

Bij een kwart van de voorverpakte apps worden ten minste vijf soorten data verzameld, die in combinatie kunnen onthullen wie de gebruiker is. Dat kunnen unieke codes van het apparaat zijn, specifieke instellingen van de telefoon, locatie- en contactgegevens, sms-berichten en zelfs camerabeelden.

Vaak kunnen de apps niet door de gebruiker zelf worden verwijderd. Naast Google-diensten zoals YouTube of Play

Een kwart van alle apps die ongevraagd worden meegeleverd, geeft ten minste vijf soorten data prijs

Store kunnen dat gezondheidsapps zijn, of apps voor stembesturing. Veel van de 214 telefoonfabrikanten installeren apps zonder duidelijke oorsprong.

Ook weer-apps zoals AccuWeather en Weather Channel worden vaak vooraf geïnstalleerd, en verzamelen volgens de onderzoekers data over telefoon en gebruiker. Apps die wel verwijderd kunnen worden, blijven soms als spook op de achtergrond aanwezig, en sturen nog gegevens door.

De afgelopen jaren zijn veel gevallen van datadiefstal onthuld. In de zomer van 2017 staakte Amazon de verkoop van een aantal Android-telefoons, waaronder het populaire merk Blu. Er stond voorverpakte spionagesoftware op van een Chinees bedrijf. Iets eerder ontdekte consultant Check Point dat verschillende telefoonmerken werden geleverd met schadelijke virussen en 'ransomware' in het Android-systeem.

Veelasha Moonsamy publiceerde al in 2014 over BlackBerry- en Windowstelefoons die locatiegegevens blijven rondsturen, ook als gebruikers dit bewust hebben uitgezet. Twee jaar eerder onthulde ze hoe 10% van de Android-telefoons persoonlijke gegevens lekt naar advertentie- en marketingbedrijven, in een onderzoek naar ruim honderd telefoongebruikers

'Het probleem blijft groeien', zegt ze, 'en is duidelijk niet meer onder controle. Niemand roept de fabrikanten ter verantwoording. Hun gedrag begint normaal te worden, terwijl de gebruikers niet eens weten dat hun apparaat doorlopend persoonlijke data lekt.'

Privacyexpert Rob van Eijk, die onlangs in Leiden promoveerde op privacyschendingen door onlineadvertentiebedrijven, zegt dat telecombedrijven vaak korting krijgen van fabrikanten, als ze allerlei vooraf geïnstalleerde apps niet verwijderen. 'Ook het telecombedrijf zelf sluit vaak zulke contracten af, zoals met Facebook, dat daarvoor ruime vergoedingen betaalt.'