NRCHANDELS
WOENSDAG 21 JANU

Hebberige apps happen naar je data

Privacy Via machtigingen vraagt een app toegang tot onderdelen van je smartphone, zoals adresboek of camera. Soms onnodig.

Door **Herbert Blankesteijn**

AMSTERDAM. Machtigingen vormen een handig overzicht van de privacyaspecten van een app. In een paar regels geven ze een overzicht van de informatiekranen die worden opengezet. Op de iPhone en de iPad kun je zelf bepalen welke informatie je aan een app gunt (zie kader). Bij Android heb je dat gemak niet. In de Play Store kun je de machtigingen inspecteren voordat je een app installeert. Als je het met één machtiging niet eens bent, moet je je bezwaren inslikken, of de hele app afwijzen.

Een nadeel van de manier waarop toestemming wordt gevraagd, is dat nooit wordt gemeld waar een machtiging voor nodig is - laat staan dat beloofd wordt hem alleen voor dat doel te gebruiken. Aan de machtigingen van één app kun je vaak niet zien welke noodzakelijk zijn. Maar bekijk je er een paar die ongeveer hetzelfde doen, dan is een machtiging die ze niet allemaal vragen blijkbaar niet echt nodig.

Hongerige apps

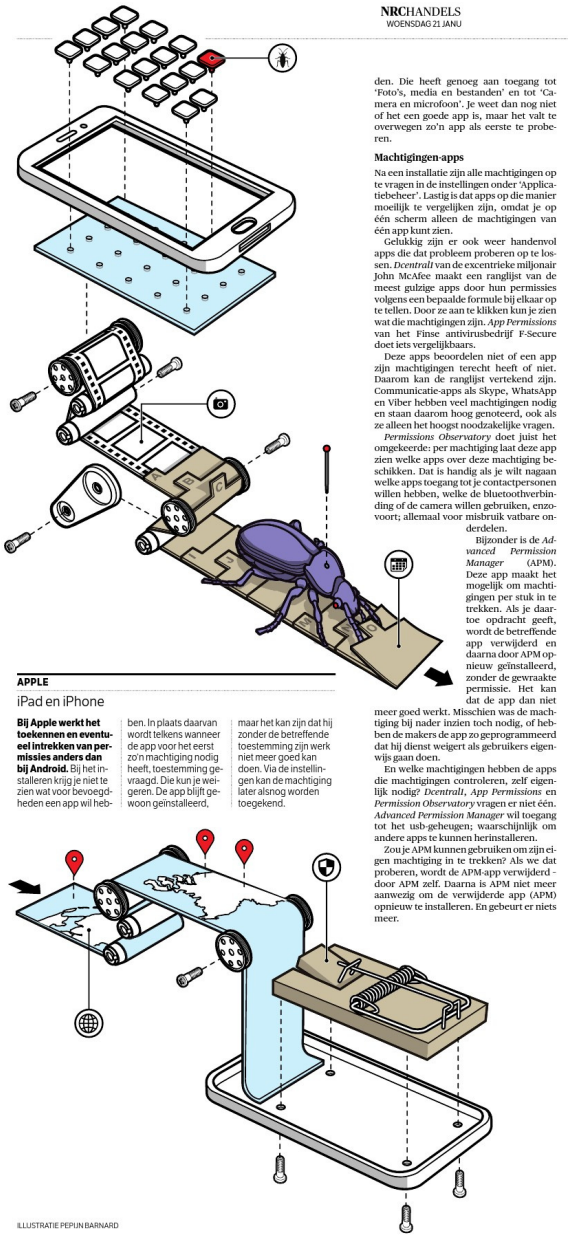
Apps kunnen goede redenen hebben om veel machtigingen te vragen. Neem bijvoorbeeld Skype. Deze razend populaire bel-app vraagt bij installatie een hele waslijst aan machtigingen, je contacten, je berichten, je locatie, foto's en video's maken, geluid opnemen, het gaat maar door. Heeft Skype dat allemaal nodig? Het meeste wel. Zonder toegang tot je contacten kun je vanuit Skype niet iemand bellen van wie het nummer gewoon in je adresboek staat. Zonder toegang tot 'geluid opnemen' kan Skype jouw geluid niet naar de ander sturen. Enzovoort.

In andere gevallen is het minder duidelijk waarom apps toegang willen tot allerlei onderdelen van je smartphone. Zo zijn er apps die je helpen een gitaar te stemmen. In principe hoeft zo'n app alleen toegang tot de microfoon. Toch vragen van tien bekeken apps er drie om de machtiging voor 'In-app-aankopen'. Dat stelt ze in staat muzikale producten te verkopen en zo geld te verdienen aan een gratis app. En waarom de *Guitar Tuner Workpail* je locatie wil weten, is een raadsel.

Of neem apps voor het lezen van QR-codes, die tweedimensionale streepjescodes die veel op etiketten, posters en in advertenties staan. De *QR Code Reader* wil toegang tot je locatie. Dat heeft zo'n app niet nodig, wat alleen al blijkt uit het feit dat van de zes bekeken apps er maar twee om die locatie vragen. De *QR Droid Code Scanner* hoeft geen locatie maar wil weer wel je bij je contacten kunnen.

Het hongerigst zijn de *QR & Barcode Reader* en de *Barcode & QR Scanner*, die allebei een lijst van zeven machtigingen opeisen. De *QR Droid Private* is het meest bescheiden. Die heeft genoeg aan toegang tot 'Foto's, media en bestanden' en tot 'Camera en microfoon'. Je weet dan nog niet of het een goede app is, maar het valt te overwegen zo'n app als eerste te proberen.

Aan één app kun je niet zien welke machtigingen nodig zijn. Controleer ook welke machtigingen andere apps vragen die hetzelfde doen



ILLUSTRATIE PEPIJN BARNARD

Machtigingen-apps

Na een installatie zijn alle machtigingen op te vragen in de instellingen onder 'Applicatiebeheer'. Lastig is dat apps op die manier moeilijk te vergelijken zijn, omdat je op één scherm alleen de machtigingen van één app kunt zien.

Gelukkig zijn er ook weer handenvol apps die dat probleem proberen op te lossen. *Dcentrall* van de excentrieke miljonair John McAfee maakt een ranglijst van de meest gulzige apps door hun permissies volgens een bepaalde formule bij elkaar op te tellen. Door ze aan te klikken kun je zien wat die machtigingen zijn. *App Permissions* van het Finse antivirusbedrijf F-Secure doet iets vergelijkbaars.

Deze apps beoordelen niet of een app zijn machtigingen terecht heeft of niet. Daarom kan de ranglijst vertekend zijn. Communicatie-apps als Skype, WhatsApp en Viber hebben veel machtigingen nodig en staan daarom hoog genoteerd, ook als ze alleen het hoogst noodzakelijke vragen.

Permissions Observatory doet juist het omgekeerde: per machtiging laat deze app zien welke apps over deze machtiging beschikken. Dat is handig als je wilt nagaan welke apps toegang tot je contactpersonen willen hebben, welke de bluetoothverbinding of de camera willen gebruiken, enzovoort; allemaal voor misbruik vatbare onderdelen.

Bijzonder is de *Advanced Permission Manager* (APM). Deze app maakt het mogelijk om machtigingen per stuk in te trekken. Als je daartoe opdracht geeft, wordt de betreffende app verwijderd en daarna door APM opnieuw geïnstalleerd, zonder de gewraakte permissie. Het kan dat de app dan niet meer goed werkt. Misschien was de machtiging bij nader inzien toch nodig, of hebben de makers de app zo geprogrammeerd dat hij dienst weigert als gebruikers eigenwijs gaan doen.

En welke machtigingen hebben de apps die machtigingen controleren, zelf eigenlijk nodig? *Dcentrall*, *App Permissions* en *Permission Observatory* vragen er niet één. *Advanced Permission Manager* wil toegang tot het usb-geheugen; waarschijnlijk om andere apps te kunnen herinstalleren.

Zou je APM kunnen gebruiken om zijn eigen machtiging in te trekken? Als we dat proberen, wordt de APM-app verwijderd – door APM zelf. Daarna is APM niet meer aanwezig om de verwijderde app (APM) opnieuw te installeren. En gebeurt er niets meer.

APPLE

iPad en iPhone

Bij Apple werkt het toekennen en eventueel intrekken van permissies anders dan bij Android. Bij het installeren krijg je niet te zien wat voor bevoegdheden een app wil hebben. In plaats daarvan wordt telkens wanneer de app voor het eerst zo'n machtiging nodig heeft, toestemming gevraagd. Die kun je weigeren. De app blijft gewoon geïnstalleerd, maar het kan zijn dat hij zonder de betreffende toestemming zijn werk niet meer goed kan doen. Via de instellingen kan de machtiging later alsnog worden toegekend.