de Correspondent

Update

23.05.2014 • Leestijd 7 - 9 minuten

Gisteren schreef ik over de enorme hoeveelheid data die via je smartphone weglekt naar bedrijven die je niet kent. In deze update zeven praktische tips hoe je je persoonlijke gegevens op je telefoon beter kunt beschermen. Oplopend van makkelijk naar ingewikkeld. Heb je zelf ook tips? Deel die dan vooral!

Zeven manieren om je smartphone beter te beveiligen

Correspondent
Hacken

Dimitri **TOKMETZIS**

Om je meteen te ontmoedigen: het is onbegonnen werk om álle datalekken in je smartphone te dichten. Ik heb sinds oktober vorig jaar veel verschillende apps geprobeerd (op Android-toestellen) en er bestaat geen enkele die een combinatie biedt van totale controle over datastromen én gebruikersgemak.

Dit gezegd hebbende, je kunt wel degelijk wat doen om de controle over je toestel te heroveren. Ik zet mijn belangrijkste bevindingen hieronder uiteen, oplopend van eenvoudig tot ingewikkeld. Als jullie nog tips en aanvullingen hebben, dan hoor ik dat graag. De meeste technische tips zijn van toepassing op Android-toestellen.

1. Verbeter de operationele beveiliging

Met een aantal simpele stappen kun je je gegevens al aardig beschermen. Zet bijvoorbeeld een wachtwoord op je smartphone en ook op enkele apps. Kies in dat geval wel goede wachtwoorden. Dus niet Naamvanjekind-geboortedatum. Of 1234567890. Dat soort wachtwoorden zijn makkelijk te kraken. Gebruik het liefst ook verschillende wachtwoorden, dus niet je pincode voor het ontgrendelen van je scherm.

En dan wordt het natuurlijk moeilijk. Probeer al die ingewikkelde en verschillende wachtwoorden maar eens te onthouden. Om je daarbij te helpen is er LastPass, een app waarmee je eenvoudig wachtwoorden kunt opslaan. Met één 'moederwachtwoord' kun je ze allemaal stuk voor stuk ontsluiten. De wachtwoorden worden lokaal en versleuteld opgeslagen, veilig dus. Je kunt deze LastPass op verschillende toestellen gebruiken, zoals smartphone, tablet en pc.

2. Kies veiligere instellingen

Een simpele stelregel is: als je iets niet gebruikt, zet het dan uit of haal het van je smartphone. Stel je gebruikt alleen gps als je verdwaald bent, zet het dan uit als je niet verdwaald bent. Als je bluetooth nooit gebruikt, schakel het dan uit. Als apps werkeloos op je smartphone blijven, verwijder ze dan. Je kunt ze altijd weer installeren.

Let daarnaast op je Google Instellingen. Google gebruikt sinds kort een advertentie-ID, een uniek nummer aan de hand waarvan adverteerders je kunnen volgen. Deze staat standaard aan. Je kunt hem uitzetten door naar de Google Instellingen-app te gaan -> Advertenties -> Afmelden. In Google Instellingen kun je ook onder het kopje Zoeken Google Now deactiveren. Vooral Google Now gebruikt erg veel persoonlijke data om gerichte aanbevelingen te doen.

3. Verkrijg inzicht in je apps

MyPermissions is een app die je snel een overzicht geeft van welke data andere apps willen gebruiken. Je kunt bijvoorbeeld makkelijk zien welke apps toegang vragen tot je Twitter-account (en dus data kunnen onderscheppen). MyPermissions zendt wel geanonimiseerde gebruikersdata naar een eigen server.

Clueful doet in grote lijnen hetzelfde en waarschuwt bij het installeren van een app wat het mogelijke privacygevaar is. Deze app is nuttig om alert te blijven op wat je installeert.

4. Gebruik 'permission managers'

En nu wordt het een stukje moeilijker. Als je op Android een app installeert, vraagt die app allerlei toestemmingen, bijvoorbeeld of hij gebruik mag maken van je locatiegegevens, of informatie mag opslaan in het geheugen. Helaas is het slikken of stikken. Als een van de toestemmingen je niet zint, moet je de hele app weigeren. Het zou mooi zijn als je selectief permissies kunt intrekken. Er is een aantal apps die dat kunnen, maar dan moet je je smartphone wel *rooten*; toegang krijgen tot het besturingssysteem.

Dat is op zich niet zo moeilijk, maar als je dat doet, vervalt de garantie van je smartphone. Als het rooten dus mislukt en je smartphone loopt helemaal vast, heb je een probleem. Het XDA Developer platform heeft echter een aantal hele goede en duidelijke instructiefilmpjes (en betrouwbare software) over hoe je je telefoon kunt rooten. Ik kan het niet beter uitleggen.

Als het je eenmaal is gelukt je smartphone te rooten, kun je een paar goede apps installeren.

XPrivacy houdt datastromen niet tegen, maar geeft nep-informatie

Zelf ben ik erg onder de indruk van de app XPrivacy. Hiermee kun je instellen wat voor soort data een app mag opvragen en exporteren. Het is bijvoorbeeld niet nodig dat een zaklamp-app je locatiegegevens opvraagt. XPrivacy houdt dit soort datastromen niet tegen, maar geeft nep-informatie (bijvoorbeeld dat je je op Christmas Island begeeft). Doordat de apps wel informatie krijgen, blijven ze goed werken.

Een nadeel van XPrivacy is dat de app vrij veel inzet vergt om in te stellen. Er zijn honderden potentiële lekken en soms is een toestemming echt noodzakelijk voor een goede werking. Ik heb zelf al een paar keer gehad dat ik de toegang tot een app te veel beperkte, waardoor de app het niet meer deed. Dan is het even zoeken naar welke geblokkeerde toestemming het probleem veroorzaakt.

In onderstaande video leg ik uit hoe je XPrivacy kunt installeren.

Je kunt ook een firewall installeren, bijvoorbeeld DroidWall. Daarmee kun je bepaalde internetadressen, bijvoorbeeld van advertentieplatformen, afsluiten. DroidWall is alleen niet zo makkelijk in het gebruik. Je moet zelf nog handmatig softwarecode in de app toevoegen.

5. Beveilig je browser en mail

Je kunt ook betere browsers gebruiken dan het standaardmerk dat met de smartphone wordt meegeleverd. Orbweb is een zeer veilige browser, waarmee je ook anoniem kunt surfen. Orweb is ontwikkeld door The Guardian Project, dat apps ontwikkelt die privacy- en securityvriendelijk zijn. In combinatie met de app Orbot kun je op smartphone

gebruikmaken van het TOR-netwerk. Orweb blokkeert cookies en houdt standaard géén zoekgeschiedenis bij.

The Guardian Project heeft ook nog een aantal andere fraaie apps ontwikkeld, waaronder ChatSecure (voor beveiligd chatten) en PixelKnot. Met die laatste app kun je boodschappen in foto's verstoppen: een soort cryptografisch trucje.

Je kunt ook de Firefox-browser gebruiken en die optuigen met een aantal privacy-plugins. Veel websites zijn *responsive*: ze passen zich automatisch aan aan het formaat van de drager. De Correspondent, maar ook sites als Nu.nl zijn bijvoorbeeld prima via de browser op je smartphone te lezen. Je kunt er dus voor kiezen om de app van Nu.nl te verwijderen en de site voortaan via je browser te bekijken. Je kunt dan via je browser alle *trackers* blokkeren.

In Firefox kun je je cookie- en trackingvoorkeuren instellen (Menu -> Instellingen -> Privacy). Daarnaast kun je de Ghostery-plugin installeren. Die blokkeert cookies van adverteerders (Menu -> Extra -> Add-ons). Mijn ervaring is wel dat als je veel trackers blokkeert via Ghostery, je browser erg traag wordt. ABP is een programmaatje dat opdringerige reclame (en hun cookies) tegenhoudt.

Als je op een gastnetwerk zit, bijvoorbeeld in een café of in de trein, dan kun je beter een Virtual Private Network (VPN) gebruiken. Met zo'n VPN stuur je alle data door een beveiligde tunnel. Een app die ik heel gebruiksvriendelijk vind, is Private Tunnel VPN. Je kunt de app op al je devices installeren. Je krijgt 100MB dataverkeer gratis. Als je 50 gigabyte aan data wilt verzenden, kost dat twaalf dollar: goed te betalen dus, en je kunt er lang mee doen.

K-9 Mail is een mailprogramma dat het mogelijk maakt om versleuteld te mailen vanaf je smartphone met behulp van de veelgebruikte PGP-software. Het is heel gebruiksvriendelijk.

6. Installeer een ander besturingssysteem

Je kunt nog een stap verder gaan. Je smartphone krijgt het besturingssysteem mee van de fabrikant en meestal biedt dat weinig mogelijkheden tot persoonlijke aanpassingen. Als je de installatie van XPrivacy niet al te ingewikkeld vond, kun je er ook eens aan denken om een ander besturingssysteem te installeren. Er zijn veel ontwikkelaars actief die alternatieve opensourcebesturingssystemen ontwerpen, waarin al veel privacyfeatures zijn ingebakken.

Het heeft me twee avonden en het nodige gevloek gekost om het

Een veel gebruikt besturingssysteem is CyanogenMod. Het heeft me twee avonden en het nodige gevloek gekost om het systeem te installeren. Het is niet risicovrij. Als je een grote fout maakt, loopt je smartphone vast. Het is dus heel belangrijk om een *backup*te

gevaak gekost om het systeem te installeren

maken.

Maar de moeite en het risico worden beloond. Je kunt met CyanogenMod volledig wegblijven van Google apps en je smartphone in grote mate personaliseren. Daarnaast heeft CyanogenMod standaard een privacyguard ingebouwd die erg lijkt op de permissionmanager van de iPhone. Je kunt daarmee hele categorieën data uitsluiten van gebruik, zoals contactgegevens of locatiegegevens. Je kunt dat ook per app instellen.

7. Neem een andere smartphone

Nog een stap verder: neem een andere smartphone. Het is moeilijk te zeggen of een smartphone meer of minder privacyvriendelijk is. Apple ziet strenger toe op wat app-aanbieders en adverteerders van je smartphone plukken. Maar de mogelijkheden om zelf te klussen en de fabrieksinstellingen te wijzigen zijn bij Apple beperkt. Android is veel opener, de software is makkelijker aan te passen. Als je enige technische kennis hebt en het leuk vindt om aan je smartphone te klussen, zou ik Android nemen. Voor de gewone gebruiker is een iPhone (van Apple dus) wellicht privacyvriendelijker.

Daarnaast komen er voor de fijnproevers enkele alternatieve smartphones op de markt. De meest markante is de Blackphone, ontwikkeld naar aanleiding van de Snowden-onthullingen. De Blackphone werkt op Android, maar heeft heel veel ingebouwde privacyfeatures, zoals versleuteld mailen en bellen. KPN zal deze smartphones binnenkort verkopen.

Tot slot wordt in Engeland op dit moment de zogenoemde indie Phone ontwikkeld. Deze smartphone belooft de gebruiker maximale controle over zijn data te geven. Het project is nog in ontwikkeling. Het is nog te vroeg om te zeggen of deze mooie belofte kan worden nageleefd.