Een kijkwijzer voor apps

Wie: Susanne Barth
Waar: Enschede
Wat: Serious apps
Waarom: Privacy en security

Het is verleidelijk om apps tijdens de installatie toegang te geven tot privégegevens, maar dat is niet altijd verstandig.

De technische specs van smartphones doen nauwelijks onder voor die van computers. Maar waar we onze desktops en laptops dichtmetselen met antivirusprogramma's en firewalls, zijn we op onze smartphones een stuk zorgelozer. Een app is in een opwelling snel geïnstalleerd, zeker als die gratis is. En dat de makers ervan wat gulzig zijn in het vragen van toegang tot privégegevens nemen we dan maar voor lief. Wat vreemd is, want als er één apparaat is dat alles over ons weet, is het onze smartphone wel. Al onze vrienden, familie en bekenden staan in de contactenlijst. En ook onze locatie is bekend dankzij de gps. Waarom klikken we dan zo snel op Accepteren? Susanne Barth van de Universiteit Twente hoopt ons bewuster te maken van de risico's.

Zijn smartphonegebruikers te onvoorzichtig?

"Ja. Zo zijn volgens ESET begin maart de Instagram-accounts van 1,5 miljoen Instagramgebruikers gekaapt. Al die personen hadden een app geïnstalleerd die hen zou helpen om meer volgers te krijgen. Via een nep-Instagram-inlogscherm werden hun inloggegevens gestolen. Dit is een extreem voorbeeld, maar los daarvan geven gebruikers over het algemeen veel te gemakkelijk toestemming voor gebruik van hun contactgegevens, locatie of camera. Ook wanneer dat helemaal niet nodig is om een app te laten functioneren. We nemen regelmatig willens en wetens een beslissing waarvan we eigenlijk weten dat die niet rationeel is. Zo kiezen mensen vaak liever voor een gratis app die privégegevens verzamelt dan een betaalde app die de privacy van gebruikers respecteert. Ook als ze hun privacy wel degelijk belangrijk vinden. Worden we bij dit soort keuzes verblind door de korte-termijnvoordelen van het installeren van een gratis app? Of onderschatten we de langere-termijnrisico's van het lukraak geven van permissies?"

Foto: Arjan Reef.

Wat heb je aan die kennis?

"Ik wil graag een soort kijkwijzer voor apps maken. Die zou moeten verschijnen tijdens de installatie van een app en gebruikers in één oogopslag duidelijkheid moeten geven over de risico's die ze op het punt staan te nemen. Maar niet alleen gebruikers moeten hun leven beteren. Dat geldt ook voor de makers van apps. Daarom gaan wij een lijst van eisen opstellen waaraan veilige apps moeten voldoen. Dat gaan we overigens voorlopig eerst alleen doen voor het Android-platform."

Gaan appmakers naar jullie luisteren?

"We richten ons vooral op 'serious apps'. Dat zijn apps die worden gemaakt door bedrijven of overheden. Denk aan apps voor online bankieren, apps om medische gegevens te delen met zorgverleners, of overheidsapps voor bijvoorbeeld het aanvragen van een nieuw paspoort. Daarmee worden vaak bijzonder privacygevoelige gegevens verwerkt. Volgens de nieuwe Europese privacywetgeving die op 28 mei in werking treedt, moeten dit soort apps voldoen aan 'privacy by design'. Ze mogen niet méér toegang tot persoonsdata vragen dan strikt noodzakelijk is en moeten data goed beschermen door deze te versleutelen en waar mogelijk te anonimiseren. Het ministerie van Veiligheid en Justitie wil onze aanbevelingen gaan toepassen, net als onderzoeksinstituut TNO en het ict-bedrijf Centric. Het zou mooi zijn wanneer in de toekomst alle apps in Google Play aan onze aanbevelingen voldoen. We hebben nog een lange weg te gaan, maar hopelijk is dit onderzoek daarbij een stap in de goede richting.".

Tekst: Jolein de Rooij

SITES

- http://scs.ewi.utwente.nl/staff/BarthS/
- https://tinyurl.com/jb4fobr
- www.wodc.nl

Oproep

Doet u iets bijzonders met uw pc? Of hebt u een handige softwareoplossing voor uw hobby bedacht? Stuur dan een e-mail met als onderwerp **'Creatief met de pc'** naar **redactie@computeridee.nl**. Wie weet komt u ermee in Computer Idee.