UNIVERSITEIT VAN AMSTERDAM

UvA-wetenschapper wijst op risico's Google Profiles
'Meer onderzoek nodig naar misbruikgevoeligheid sociale media'

Gepubliceerd op 9 juni 2011

Promovendus Matthijs Koot van de Universiteit van Amsterdam (UvA) heeft aangetoond hoe eenvoudig het is om op grote schaal gegevens van persoonlijke profielen via Google Profiles te bemachtigen. De onderzoeker stuitte in februari van dit jaar op een aantal openbare bestanden binnen Google Profiles, een dienst waar gebruikers persoonlijke informatie kunnen delen. De bestanden bevatten links naar alle 35 miljoen Google Profiles. Nog niet eerder is gebleken dat het mogelijk is persoonlijke gegevens in deze hoeveelheid te bemachtigen. Koot maakt zich vooral zorgen over het mogelijke misbruik van deze gegevens door criminelen. Hij deed de ontdekking in het kader van zijn promotieonderzoek naar de herleidbaarheid van anonieme gegevens tot individuen, dat hij uitvoert bij prof. dr. ir. Cees de Laat aan het Instituut voor Informatica en prof. dr. Michel Mandjes aan het Korteweg-de Vries Instituut van de UvA.

De publieke profielen die mensen zelf aanmaken op Google Profiles bevatten uitsluitend informatie die ze over zichzelf openbaar hebben gemaakt, zoals beroep, woonplaats, opleiding, werkervaring, en verwijzingen naar hun andere profielen op bijvoorbeeld Facebook en LinkedIn. Als een profiel is gekoppeld aan een Twitter-account maken ook Twitter-gesprekken onderdeel uit van het Google Profile. Zonder enige technische drempel of blokkade heeft Koot dus op grote schaal gegevens van Google Profiles kunnen verkrijgen. Google is door Koot geïnformeerd, maar heeft (nog) geen actie ondernomen.

Misbruik van privégegevens

Koot maakt zich vooral zorgen over het mogelijke misbruik van de persoonlijke gegevens. 'In de miljoenen profielen is het gemakkelijk om 'interessante' groepen te filteren. Wie werkt bij politie, justitie of defensie? Wie reist veel en maakt foto's met dure camera's? Criminelen kunnen verschillende profielen aan Twitter, Hyves, LinkedIn en Facebook koppelen en gebruiken voor het versturen van 'slimme' e-mails aan voor hen interessante slachtoffers. E-mails die afkomstig lijken van een bekende en je verleiden op een link te klikken naar een malafide website. Een website lijkend op die van de overheid, bank of verzekeraar, maar die ongemerkt je computer probeert te infecteren met kwaadaardige software die wachtwoorden doorstuurt of banktransacties manipuleert. Antivirussoftware helpt daar nauwelijks tegen. Bewustwording misschien wel.'

Koot gaat verder over de risico's. 'Ook toekomstige werkgevers of verzekeraars kunnen gebruikmaken van informatie die mensen nietsvermoedend op hun persoonlijke pagina's zetten. Er kunnen bedrijfjes ontstaan die deze gegevens gedurende langere tijd over je bijhouden en er informatie uit destilleren die interessant is voor banken, verzekeraars, werkgevers en overheid. Bedrijfjes die opereren buiten het Europese privacyrecht. Heb je ooit op Twitter iets gezegd over je zwakke hartkleppen of gebruik van antidepressiva? Ben je kritisch geweest over vorige werkgevers? Vormen mensen in jouw omgeving een risico?'

Controle over informatie

'Mensen zijn zich er niet van bewust dat ze geen controle meer

hebben over hun gegevens als die eenmaal op internet staan. Wanneer persoonlijke informatie uit verschillende sociale netwerken aan elkaar wordt gekoppeld, ontstaat in veel gevallen een duidelijk profiel van een persoon', aldus Koot. De onderzoeker pleit voor verder onderzoek naar mogelijke misbruikscenario's, om uiteindelijk het vertrouwen in de informatiesamenleving te versterken.

Bron: UvA Persvoorlichting
persvoorlichting@uva.nl