Piratenpartij Nederland
Wolvenplein 2
3512 CJ Utrecht

www.piratenpartij.nl
info@piratenpartij.nl

Piratenpartij
voor een vrije informatiesamenleving

Aan: Overheid.nl
Website internetconsultatie.nl

Afzender: Piratenpartij Nederland, Wolvenplein 2, 3512 CJ Utrecht

Datum | 20 maart 2020
Betreft | Reactie Internetconsultatie OAuth 2.0

Het idee achter OAuth is goed en heeft grote voordelen als het gaat over authenticatie. Er zitten echter ook valkuilen aan het gebruik van een externe authenticator. Zo bepleit het voorstel ten onrechte dat de implementatie van OAuth er voor zorgt dat privacy risico's, risico's op identiteitsdiefstal en misbruik van identiteitsgegevens afnemen. Deze risico's en misbruik hebben te maken met securityfouten in applicaties, zwakke wachtwoorden en het ontbreken van een degelijke 2FA en hebben niets te maken met welke methode er wordt gebruikt voor authenticatie. De acceptatie van OAuth zal samenhangen met het aantal partijen dat OAuth zal aanbieden en hun imago met betrekking tot privacy. Zeker ook omdat de OAuth-provider een profiel op kan bouwen van hoe en welke applicaties gebruikt worden. Mede om die reden is het aan te raden om beheer en ontwikkeling te scheiden. Het beheer van een OAuth-omgeving behoort niet bij een commerciële partij, maar bij één onafhankelijke en transparante non-proffit organisatie die wordt ondersteund door privacy voorvechters zoals de Piratenpartij en Bits of Freedom.

Een slechte implementatie van OAuth 2.0 kan er nog steeds voor zorgen dat er via scripting kan worden aangemeld. Het gevaar ligt op de loer dat met het toevoegen van OAuth een vals gevoel van veiligheid wordt gecreëerd. Een goed securitybeleid is veel breder dan alleen een lijstje met te gebruiken methodieken. In zo'n securitybeleid zouden bijvoorbeeld standaarden met betrekking tot sessie-tijden en refresh-tokens kunnen worden opgenomen.

Het gevaar ligt op de loer dat met het toevoegen van OAuth een vals gevoel van veiligheid wordt gecreëerd.

Het voorstel impliceert dat OAuth 2.0 alleen gaat over user-authenticatie, maar dat is niet waar. OAuth 2.0 kan ook worden gebruikt voor server-server communicatie. De Piratenpartij zou graag een beslisboom zien over wanneer je wel of niet OAuth dient toe te passen. Voor simpele data-uitwisseling waarin geen privégegevens zitten (denk bijvoorbeeld aan GIS-data) is het overdreven om een Oauth-mechanisme in te richten.

Het originele OAuth 2.0 (RFC 6749) stamt uit 2012 en is dus al acht jaar oud. De wereld verandert snel en dat geldt zeker voor authenticatie en autorisatie. Door nu OAuth 2.0 als standaard neer te leggen, wordt de weg van verbetering en innovatie nodeloos moeilijker gemaakt. Het toevoegen op de "pas toe of leg uit"-lijst is volgens de Piratenpartij dan ook niet de te volgen weg. Ja, OAuth is de *way to go*, maar niet door het om deze manier af te dwingen.

OAuth is de way to go, maar niet door het om deze manier af te dwingen.

Vriendelijke groet,

Sjoerd de Boer