HOGESCHOOL PXL

Hogeschool PXL Hasselt

TOEGEPASTE INFORMATICA

Academiejaar 2019-2020

ANALYSE GEPERSONALISEERDE ADS OP INTERNET

Door:

Ian Buntinx (11800483)

Gijs Iliaens (11800551)

Hursit Tarcan (11800071)

INHOUDSOPGAVE

1. Inleiding
2. Schets het mechanisme
    2.1. Hoe komt men aan onze data?
    2.2. Cookies
        2.2.1. Hoe ziet een cookie eruit?
        2.2.2. Waar wordt dit allemaal opgeslagen?
        2.2.3. Zijn cookies legaal?
        2.2.4. Zijn cookies gevaarlijk?
        2.2.5. Zijn cookies permanent?
        2.2.6. Welke soorten cookies zijn er?
            2.2.6.1. Session cookie
            2.2.6.2. Persistent cookie
            2.2.6.3. Secure cookie
            2.2.6.4. Http-only cookie
            2.2.6.5. Same-site cookie
            2.2.6.6. Third-party cookie
            2.2.6.7. Supercookie
            2.2.6.8. Zombie cookie
3. Waarom cookies voor gebruikers?
4. Waarom cookies voor bedrijven?
    4.1. Regels voor bedrijven
5. Wat als de gebruiker deze advertenties niet wilt?
6. Besluit
7. Lijst van de geraadpleegde sites

1. INLEIDING

De meeste mensen die surfen op het internet zijn waarschijnlijk al in aanmerking gekomen met gepersonaliseerde advertenties. Dit zijn advertenties die specifiek bedoeld zijn voor persoon x, die enkele minuten op webpagina y aan het surfen was. Makkelijk gezegd, het bedrijf ziet waar de persoon interesse in toont. Daarna zorgt het ervoor dat deze persoon reclame krijgt over dingen waarin hij geïnteresseerd is. Dit proces transformeert de potentiele klant hopelijk tot een ‘echte’ klant.

In dit werk hebben Ian Buntinx, Gijs Iliaens en Hursit Tarcan een onderzoek gedaan naar hoe het proces precies in elkaar zit en hebben zij een antwoord gegeven op eerder vermelde hoofd- en deelvragen.

2. SCHETS HET MECHANISME

2.1. HOE KOMT MEN AAN ONZE DATA

De manier waarop de bedrijven aan onze data komen is door “cookies”. Wat dit precies zijn en wat ze precies doen, wordt heel uitgebreid verteld in de volgende deelvraag. Over het algemeen kan dit gezien worden als een soort kruimeltje dat je volgt op het internet. Professionele IT’ers zorgen ervoor dat dit kruimeltje je volgt en je advertenties laat zien over de producten die je recent hebt bekeken op de site van een bedrijf. Misschien was je zo al van plan om dat product te kopen bij hun, maar toch zullen ze je proberen eraan te herinneren door constant advertenties te plaatsen die speciaal voor jou bedoeld zijn. Is dit een soort van spionage? Is dit legaal? Daar gaan we dieper op in, in de van volgende deelvragen.

2.2. COOKIES

Een cookie is eigenlijk een document dat informatie opslaat over de ‘web geschiedenis’ van een bepaalde gebruiker. Stel dat persoon “X” een website opent, bijvoorbeeld “Bol.com”, en hier zoekt naar rode hakken van maat 38 voor vrouwen. Dan wordt er achterliggend op de pagina een document aangemaakt waarin staat dat persoon “X”, die waarschijnlijk een vrouw is en schoenmaat 38 heeft, op zoek is naar rode hakken met maat 38. In het begin waren deze documenten veel minder uitgebreid omdat ze opgeslagen werden op de computer, gsm, tablet van de bezoeker. Het is echter zo dat de bedrijven op die manier minder opslagmogelijkheid hebben en hierdoor minder kunnen bereiken. Daarom is het concept van ‘cookies’ aangepast. Om ervoor te zorgen dat bedrijven zo veel mogelijk kunnen opslaan moeten bedrijven in bezit zijn van het opslagmedium. IT’ers hebben ervoor gezorgd dat de gebruikers vanaf nu enkel een ‘unieke sleutel’ hoeven op te slaan op hun eigen machine (dit wordt automatisch gedaan en hier merkt de gebruiker zo goed als niks van). Deze ‘unieke sleutel’ neemt heel weinig plaats in en zorgt ervoor dat de websites deze mensen kunnen identificeren. Op deze manier kunnen de gepersonaliseerde advertenties gebruikt worden zonder opslagbeperking.

Deze sleutels zijn dus uniek en verschillen per webpagina. Hierdoor is het niet direct mogelijk dat de Braziliaanse pagina die je bezocht op vakantie ook toegang heeft tot je informatie die is opgeslagen op de site van Torfs Schoenen. Het is echter mogelijk dat deze website wel toegang heeft tot je gegevens. Als voorbeeld nemen we “Bol.com” en de schoenenwinkel Torfs. Als er op de pagina van Torfs een advertentie wordt geplaatst van “Bol.com”, dan gaat Torfs ermee akkoord dat “Bol.com” ook de informatie ontvangt die aan jouw unieke sleutel verbonden is. Als jij dus op zoek bent naar ‘witte Adidas schoenen van maat 42 voor mannen’, dan wordt dit opgeslagen in de database van Torfs en wordt dit ook opgeslagen in de database van “Bol.com”. “Bol.com” kan bijvoorbeeld ook advertenties hebben op Facebook. Dat wil dus zeggen dat Facebook ermee akkoord gaat dat “Bol.com” toegang krijgt tot de informatie over de zaken waarin je bent geïnteresseerd, zoals talenvoorkeur, land waar je woont en veel meer. Op deze manier wordt dit netwerk steeds uitgebreider en is dit één van de meest succesvolle uitvindingen geweest voor bedrijven. Bedrijven hebben geautomatiseerde algoritmes die ervoor zorgen dat jij bijvoorbeeld meer advertenties ziet over ‘videogames’ terwijl je buurjongen steeds advertenties krijgt over ‘goedkope vliegtickets’.

2.2.1. HOE ZIET EEN COOKIE ERUIT?

Hier gaan we verder redeneren met Torfs Schoenen als voorbeeld. De eerste keer dat je naar de website surft, zorgt Torfs ervoor dat er een klein bestand wordt opgeslagen op het apparaat. Dit kan er dan als volgt uitzien: UserID: A9A3BECE0563982D www.torfts.be. Het middelste deel is de unieke sleutel die jij krijgt van deze website. Elke keer dat jouw apparaat verbinding maakt met de server van Torfs, vraagt het eerst of je al een unieke sleutel hebt. Als je deze code nog niet hebt, maakt de server eerst een code aan voor jou, terwijl jij je verbindt met de webpagina. Als je deze code reeds hebt dan zorgt het algoritme ervoor dat je eerst de artikels zult zien die je eerder had bekeken (op de site van Torfs of op een andere website). Het voorbeeld van de sleutel die hier te zien is, is niet de enige manier om een “cookie” op te slaan. De code kan ook langer of korter zijn.

2.2.2. WAAR WORD DIT ALLEMAAL OPGESLAGEN?

Zoals eerder vermeld, worden de documenten opgeslagen op de servers van de bedrijven. Dit geeft de bedrijven de mogelijkheid om zelf te bepalen hoeveel ze financieel willen investeren in het opslaan van gebruikersdata. Een bedrijf kan dan bepalen welke informatie ze wel of niet gebruiken (dit heeft beperkingen die later aan bod komen). Ze kunnen dit trouwens ook doen met de cookies die ze binnenkrijgen van externe bedrijven die hun links inbedden. Bijvoorbeeld, Torfs heeft advertenties op “Bol.com” en kan het dus interessant vinden naar wat voor schoenen je zoekt. Daarnaast is er ook nog de informatie over de dvd’s waarin je geïnteresseerd bent, maar daar hebben ze totaal geen interesse in, aangezien ze dit toch niet verkopen. Omdat dit volledig overbodig zou zijn, wordt het ook niet opgeslagen in hun database.

Doordat de bedrijven zelf het grootste deel van de informatie opslaan kunnen ze ook zelf bepalen hoeveel data ze graag willen opslaan over jou. Elk bedrijf heeft een ander budget dat ze willen investeren in cookies. De datacentra van Facebook zullen veel meer informatie bevatten dan die van Torfs, omdat Facebook veel meer investeert in opslag dan Torfs.

2.2.3. ZIJN COOKIES LEGAAL?

Het gebruik van cookies door websites staat beschreven in de wet van de Cookies. Hierin staat dat *“Alle webpagina’s die eigendom zijn van Europese bedrijven of bedoeld zijn voor Europese burgers moeten voldoen aan de cookie wet”*. In deze wet staat in het kort uitgelegd dat het bedrijf in kwestie de bezoekers op de hoogte moet brengen dat er cookies worden gebruikt op de pagina. Dit wordt meestal gedaan door een venster dat openspringt. Hierin moet de gebruiker dan aantikken of hij of zij akkoord gaat met het opslaan van zijn data. Als de gebruiker dit niet wil kan hij of zij op ‘neen’ klikken, de optie ‘neen’ is vaak niet aanwezig en dit zorgt er dan voor dat je bepaalde webpagina’s niet kunt bezoeken als je de cookies niet accepteert. Dit is dus een keuze die jij zelf moet maken.

2.2.4. ZIJN COOKIES GEVAARLIJK?

Alles is gevaarlijk als het fout wordt gebruikt. De documenten waar we het over hebben houden heel wat informatie bij, deze informatie kan natuurlijk fout worden gebruikt. Foutief gebruik van deze informatie is dan ook strafbaar, dit staat ook in de wet van de Cookies. Foutief gebruik kan niet direct grote gevolgen met zich meenemen want de informatie die vaak wordt opgeslagen is niet persé heel privé. Het is ook verboden om namen op te slaan in cookie documenten daarom is het zo dat een bedrijf alles kan weten over een persoon, maar ze weten dan toch nog niet wie die persoon is. Een cookie identificeert enkel de code die hij binnenkrijgt van de client.

2.2.5. ZIJN COOKIES PERMANENT?

Cookies zijn niet permanent, ze hebben een vervaldatum. Dit betekent dus dat ze vanzelf weer weggaan uit je apparaten. Je kan ze ook zelf verwijderen door ‘cookies’ aan te vinken bij het verwijderen van je geschiedenis in de webbrowser. Je kan de cookies die gebruikt worden op een website zien door linksboven op het slotje te klikken en daarna cookies te selecteren. Hier heb je dan ook de optie om bepaalde cookies te blokkeren of te verwijderen. Je ziet hier ook alle andere informatie, zoals bijvoorbeeld de unieke sleutel, de vervaldatum en meer.

2.2.6. WELKE SOORTEN COOKIES ZIJN ER?

2.2.6.1. SESSION COOKIE

De definitie van een session cookie is: “een cookie die wordt opgeslagen in het tijdelijke geheugen van een browsersessie en terug wordt verwijderd wanneer het browsertabblad wordt gesloten”. Als we hier bijvoorbeeld ‘Coolblue’ nemen, dan kunnen we zeggen dat in de session cookie alle data wordt opgeslagen dat de gebruiker op dat moment in zijn ‘winkelwagen’ plaats.

Omdat je bij het betalen meestal naar een andere pagina wordt gestuurd is de session cookie cruciaal. Deze zorgt er dus voor dat alles wat de gebruiker op dat moment in zijn winkelwagen had juist wordt meegestuurd naar het volgende tabblad. Als de session cookie niet bestond dan zou dit dus niet kunnen en zou je weer een lege ‘winkelwagen’ hebben bij het betalen.

Session cookies zijn ook de enige soort van cookies die geen vervaldatum hebben. Dit zorgt ervoor dat de browser dit soort cookies kan onderscheiden van de andere soorten. Dit soort cookies wordt ook wel non-persistent cookies genoemd.

2.2.6.2. PERSISTENT COOKIE

Als we deze soort vergelijken met de hierboven besproken soort. Dan is het grootste verschil dat persistent cookies wel een vervaldatum hebben. En er wordt geen data verwijderd wanneer de gebruiker zijn browsertabblad sluit.

Een persistent cookie is eigenlijk een document dat veel data opslaat over de interesses van de gebruiker zodat de site bijvoorbeeld bij het laden alle interessante items vanboven kan plaatsen.

2.2.6.3. SECURE COOKIE

Een secure cookie is een cookie die enkel werkt bij een geëncrypteerde verbinding. Dit wil niet direct zeggen dat in een secure cookie veel gevoelig informatie zit. De data die bewaard wordt is hetzelfde, het enige verschil is dat deze documenten veel beter beveilig zijn dan non-secure cookies. Een cookie wordt geïdentificeerd als secure als de beheerder deze 'flag' toevoegt aan de code. Een flag is dus eigenlijk een extra eigenschap die wordt meegegeven.

Als we het gemakkelijk willen houden, dan kunnen we in het kort zeggen dat secure cookies enkel mogelijk zijn bij servers die HTTPS gebruiken.

2.2.6.4. HTTP-ONLY COOKIE

Een http-only cookie is een cookie die niet gezien kan worden in client-side browserscripts. Deze maatregel zorgt ervoor dat hackers die goed zijn met XSS (Cross-site Scripting) deze cookies niet kunnen zien in de scripts van de pagina. Hierdoor wordt het veel moeilijk voor hun om aan de data in de cookies te geraken. Dit wordt ook gedaan door het gebruik van een 'http-only flag'.

De cookies kunnen natuurlijk wel gezien worden bij server-side scripts.

2.2.6.5. SAME-SITE COOKIE

Een same-site cookie is een cookie die ervoor zorgt dat de data die opgeslagen wordt niet wordt gedeeld met externe servers. Dit wil zeggen dat bijvoorbeeld als er een Facebook link is op de site van Torfs, dat de data in deze specifieke cookie niet wordt doorgestuurd met de andere data. Dit is een nieuwe vorm van data beschermen.

2.2.6.6. THIRD-PARTY COOKIE

Dit zijn de cookies die eerder ook al besproken zijn. Third-party cookies zorgen ervoor dat de verkregen data ook wordt gedeeld met andere websites als er gebruik van wordt gemaakt. Dus als Torfs een link van Facebook heeft op hun site. Dan zorgen deze cookies ervoor dat de data die opgeslagen wordt in de cookies van Torfs ook word doorgestuurd naar de servers van Facebook.

Dit proces gebeurt enkel als er een link, afbeelding, video of een andere soort document wordt ingebed. Voor de cookies die wij hiervoor hebben besproken (dus de same-site cookies) geldt dit proces niet.

2.2.6.7. SUPERCOOKIE

Een supercookie is een cookie dat de bedoeling heeft om 'permanent' opgeslagen te worden op de computer van de gebruiker. Deze cookies mogen niet gebruikt worden, ze worden meestal alleen gebruikt door kwaadaardige beheerders om privé data te krijgen zoals inloggegevens en meer. Hierdoor worden deze cookies door de meeste bekende browsers ook direct geblokkeerd.

2.2.6.8. ZOMBIE COOKIE

Deze cookie wordt gebruikt bij sites die gebruik maken van de Quantcast technologie. Dit zorgt er dan voor dat deze cookies niet verwijderd kunnen worden omdat de sleutels meerdere back-ups hebben op gebruiker zijn apparaat. Bij het verwijderen worden de cookies opnieuw tot leven gebracht, daarom de naam zombie.

De reden dat deze cookies werden gebruikt was om gebruikers online te kunnen volgen. Dit gaf bedrijven de kans om persoonlijke informatie van gebruikers te verkrijgen. Omdat dit een schending van privacy is en omdat er in de ‘Cookie wet’ staat dat er geen data mogen opgeslagen worden waarmee personen geïdentificeerd kunnen worden zijn deze cookies ook sinds 2010 verboden.

3. WAAROM COOKIES VOOR GEBRUIKERS?

Hoewel de meeste mensen het vreemd vinden dat bedrijven dit doen en ze zeggen dat dit enkel voordelig is voor bedrijven, kan het eigenlijk ook erg handig zijn voor de gebruiker zelf. Sommige mensen vinden het nu eenmaal leuk als ze advertenties krijgen die gepersonaliseerd zijn. Voor andere mensen is het juist helemaal niet leuk en kan het zelfs irriterend zijn. Het is natuurlijk ook niet leuk als je steeds dezelfde reclame krijgt over iets wat je helemaal niet (meer) interesseert.

4. WAAROM COOKIES VOOR BEDRIJVEN?

Het echte voordeel van cookies ligt bij de bedrijven. Zij kunnen op deze manier meer data binnenkrijgen over hun potentiële klanten en op deze manier hopelijk meer verkopen. Dit is natuurlijk een groot voordeel voor de bedrijven. Neem als voorbeeld een reclamebord langs de straatkant, waarop een poster over een nieuwe parfum voor mannen geplakt wordt. Het bedrijf dat de reclame maakt beperkt zich op verschillende vlakken. Ten eerste sluiten ze de vrouwelijke klanten uit, er staat tenslotte een mannenparfum en de meeste vrouwen gaan hier niet geïntresseerd in zijn. Ten tweede sluiten ze ook de mannen uit die niet van dit soort parfum houden, elke persoon heeft zijn eigen interesses en niet iedereen ruikt dus graag hetzelfde. Zoals je ziet heeft het bedrijf zichzelf eigenlijk onnodig beperkt in de grootte van hun doelpubliek. Ze zouden veel meer klanten krijgen als ze bijvoorbeeld een bord hadden dat eerst identificeerde wie ervoor stond en dan het bord aanpaste naar een gepersonaliseerde reclame.

Dus als er een vrouw voor het bord stond, dan zou er een parfum voor vrouwen op komen te staan en als er een man voor stond, één voor mannen. Als er een aziatische vrouw voor stond zou het algoritme ervoor zorgen dat er een parfum werd getoond dat meer voldoet aan de eigenschappen die de aziatische vrouwen verkiezen. Op deze manier kunnen er via één middel (het reclamebord) meerdere mensen aangesproken worden. Dit zorgt dan voor een hogere omzet voor het bedrijf en dit is dus ook het globale idee van cookies en gepersonaliseerde ads op het internet.

4.1. REGELS VOOR BEDRIJVEN

Bedrijven gevestigd in Europa of buitenlandse bedrijven die clients hebben uit de Europese Unie zouden zich moeten houden aan alle regels die verklaard zijn in de Cookies wet. De Cookies wet valt onder de wet van ‘The General Data Protection Regulation’. Hierin staan onder andere de regels over hoe alles opgeslagen moet worden, wat opgeslagen mag worden en wat niet, dat het verplicht is om duidelijk te weergeven dat er gebruik gemaakt wordt van cookies en veel meer. Als er niet wordt voldaan aan deze regels, kunnen er straffen worden uitgedeeld door de Europese Unie. Dit kan bijvoorbeeld een geldboete zijn die het bedrijf moet betalen.

5. WAT ALS DE GEBRUIKER DEZE ADVERTENTIES NIET WILT?

Als een gebruiker helemaal geen advertenties wil, kan dit heel gemakkelijk opgelost worden door een google extensie te installeren. Een ‘AdBlocker’ zorgt ervoor dat er geen advertenties meer worden getoond in de browser. Natuurlijk kunnen er websites zijn die geen toegang verlenen voordat je deze “AdBlocker” uitzet. In dit geval ligt de keuze weer bij de gebruiker.

Als een gebruiker bepaalde cookies niet wil, kan hij deze blokkeren of niet accepteren bij het laden van de pagina of links boven bij de browser. Dit kan ervoor zorgen dat (zoals in voorgaande alinea) de pagina geen toegang verleent tot je de bepaalde cookies accepteert. Dit kan irriterend zijn, maar de keuze ligt bij de gebruiker zelf.

Als de gebruiker cookies wil blokkeren maar dit niet bij elke site speciaal wil doen, dan kan dit bij de instellingen van de meeste browsers worden ingesteld. De gebruiker kan ervoor kiezen dat cookies automatisch geblokkeerd worden. Dit kan er dan wel weer voor zorgen dat je bepaalde sites niet kunt betreden voordat je de bepaalde cookies accepteert.

Bij instellingen zoals scholen waar het beheer geen cookies wilt. Kunnen ze ervoor zorgen dat de IT’ers alle sites automatisch blokkeren die bepaalde cookies hebben. Dit kunnen ze doen voor alle computers op het netwerk, dit zou er wel voor zorgen dat er veel beperkingen komen omdat veel websites toegang weigeren als er geen cookies worden geaccepteerd.

6. BESLUIT

Het gebruik van gepersonaliseerde advertenties is natuurlijk heel fijn voor sommige mensen, maar het heeft ook zijn nadelen. De meningen zijn er verdeeld over. Voor bedrijven is dit natuurlijk één van de beste uitvindingen van de afgelopen jaren, aangezien zij er het meeste voordeel uithalen. Voor klanten kan het natuurlijk ook voordelig zijn, maar klanten kunnen zich er natuurlijk ook aan irriteren. Omtrent de gevaren van cookies kunnen we zeggen dat cookies in normale omstandigheden niet bedoeld zijn om slecht gebruikt te worden. Bedrijven kunnen hier misbruik van maken, maar als ze gepakt worden dan worden ze hier ook zwaar voor gestraft.

Over het algemeen kunnen we concluderen dat een ‘gewone gebruiker’ zich niet teveel zorgen moet maken om zijn gegevens. Daarnaast is het regelmatig verwijderen van de geschiedenis en het gebruiken van een ‘AdBlocker’ een goede oplossing.

7. LIJST VAN DE GERAADPLEEGDE SITES

EnveritasGroup. 21 mei 2018. *Every Move You Make… I'll Be Watching You: How Personalised Ads Work*. Geraadpleegd op 11 oktober 2019 via https://enveritasgroup.com/campfire/why-am-i-seeing-this-ad-how-personalized-ads-work/

Adversitement. 21 juni 2012. *What is a cookie?*. Geraadpleegd op 11 oktober 2019 via https://www.youtube.com/watch?v=I01XMRo2ESg

M. Brain. *How Internet Cookies Work*. Geraadpleegd op 11 oktober 2019 via https://computer.howstuffworks.com/cookie1.htm

T. Rankin. 20 augustus 2018. *The Real Story on Cookies: Dispelling Common Myths About the GDPR and Consent*. Geraadpleegd op 15 oktober 2019 via https://torquemag.io/2018/08/cookie-law-and-consent/

Techopedia. *Session Cookie*. Geraadpleegd op 15 oktober 2019 via https://www.techopedia.com/definition/4910/session-cookie

Cookies.org. *What are session cookies used for?*. Geraadpleegd op 15 oktober 2019 via https://www.allaboutcookies.org/cookies/session-cookies-used-for.html

Netsparker. 2019. *Using the Same-Site Cookie Attribute to Prevent CSRF Attacks*. Geraadpleegd op 16 oktober 2019 via https://www.netsparker.com/blog/web-security/same-site-cookie-attribute-prevent-cross-site-request-forgery/

Techopedia. *Super Cookie*. Geraadpleegd op 16 oktober 2019 via https://www.techopedia.com/definition/27310/super-cookie

Techopedia. *Zombie Cookie*. Geraadpleegd op 16 oktober 2019 via https://www.techopedia.com/definition/25736/zombie-cookie