Betreft: Google reCaptcha gebruiken voor Infectieradar RIVM
Van: 5.1.2e
Datum: 16 september 2020

1 Inleiding

Vanuit diverse pentesten en de code review van Infectieradar RIVM komt naar voren dat o.a. het aanmeldformulier onvoldoende beschermd is tegen het geautomatiseerd aanmaken van accounts via scripts en/of 'bots'.

Een gangbare oplossing is om hiervoor een zgn. 'captcha' in te zetten. Deze captcha beoordeelt op basis van het gedrag van de gebruiker of het daadwerkelijk een mens betreft is of dat er sprake is van een script/bot. Deze beoordeling zorgt ervoor dat de scripts/bots geblokkeerd worden.

Het gebruik van reCaptcha stuit op bezwaren m.b.t. privacy van deelnemers; er is onvoldoende onderzoek gedaan of bekend wat Google precies analyseert en wat er met deze data gebeurt.

Dit document beschrijft de probleemstelling, de onderzochte alternatieven en vraagt uiteindelijk om toestemming om reCaptcha toch in te zetten voor Infectieradar RIVM (en eventueel voor andere applicaties in de RIVM infrastructuur).

2 Probleemstelling / context

De invulformulieren (in het bijzonder de aanmeld- en inlogpagina's) van Infectieradar RIVM moeten beschermd worden tegen het geautomatiseerd aanmaken van accounts en/of geautomatiseerd inloggen via scripts.

De gangbare reCaptcha oplossing staat ter discussie. Om voortgang te houden in het project is besloten om acceptabele alternatieve oplossingen te zoeken binnen de huidige mogelijkheden van het RIVM. Een acceptabel alternatief is echter niet gevonden.

3 Onderzochte alternatieven

3.1 Captcha oplossing van de centrale netwerkbeveiliging (F5) gebruiken

Op de F5 systemen, die het netwerkverkeer scannen/beveiligen dat vanaf internet richting de RIVM webapplicaties gaat, is het mogelijk om een captcha optie te activeren. Indien er indicaties zijn dat er een script actief is in plaats van een mens, zal dit systeem een captcha aanbieden, voordat er verdere toegang verleend wordt.

Dit leek een valide oplossing, maar na onderzoek blijkt dat de F5 systemen op de achtergrond Google reCaptcha gebruiken om dit te realiseren.

3.2 Anti-bot optie activeren op de centrale netwerkbeveiliging (F5)

Het is mogelijk om op de F5 systemen de 'anti-bot' optie te activeren. Hieraan zijn wel additionele licentiekosten verbonden en er zal een extra beheerinspanning nodig zijn om deze optie te monitoren en actueel te houden.

Deze oplossing is slechts een deel van de totaaloplossing; dit zou aanvullend gebruikt moeten worden met bijvoorbeeld een captcha oplossing om het geschetste risico zover mogelijk te mitigeren.

3.3 'Rate Limiting' instellen in de applicatie

In de applicatie zelf is nu 'rate limiting' ingebouwd. Dit betekent dat er maar een beperkt aantal aanmeldingen per tijdsperiode (10 minuten) gedaan mogen worden. Als dit aantal wordt overschreden krijgt de deelnemer een melding dat er even gewacht moet worden totdat het systeem weer beschikbaar is.

Deze optie introduceert echter een extra kwetsbaarheid voor een 'denial of service' situatie. Deze optie is eigenlijk alleen bedoeld als een laatste vangnet, mochten de overige beveiligingen om de een of andere reden niet werken of omzeild worden. Als er nu een script op de applicatie wordt afgevuurd leidt dit in de huidige situatie onmiddellijk tot onbeschikbaarheid van de applicatie.

4 reCaptcha gebruiken voor beveiliging invoer Infectieradar

De onderzochte alternatieven bieden niet het gewenste beschermingsniveau of komen uiteindelijk toch weer terug bij een captcha oplossing.

Het voorstel is om toch de reCaptcha oplossing in te gaan zetten voor de additionele beveiliging van Infectieradar RIVM. Het privacyrisico moet dan worden afgewogen tegen de grote mate van zekerheid dat deze kwetsbaarheid daadwerkelijk gebruikt gaat worden bij inproductiename van de Infectieradar en leidt tot onbeschikbaarheid van de applicatie.

Enkele aanvullende punten ter overweging:

- reCaptcha is een gangbare en ook breed geaccepteerde oplossing voor deze probleemstelling.
- Vanuit de pentest én de code review wordt het gebruik van een captcha-oplossing aangeraden.
- Diverse andere applicaties binnen RIVM maken reeds gebruik van reCaptcha.
- Het gebruik van een centrale oplossing (via de reeds aanwezige F5 apparatuur) komt het algehele beveiligingsniveau van de RIVM infrastructuur ten goede en vermindert de uiteindelijke beheerinspanning.

In Bijlage A is informatie opgenomen met betrekking tot Google reCaptcha.

5 Gewenste besluitvorming

- Akkoord om Google reCaptcha in te zetten voor de additionele beveiliging van Infectieradar RIVM in afstemming met de Privacy Officer RIVM.

- Een puntoplossing voor Infectieradar implementeren of meteen centraal inrichten via de F5 beveiligingsapparatuur?

Bijlage A: Google reCaptcha achtergrondinformatie

Wat is een Captcha?

Een **captcha** (een afkorting van '**c**ompletely **a**utomated **p**ublic **T**uring test to tell **c**omputers and **h**umans **a**part') is een reactietest die in de gegevensverwerking wordt gebruikt om te bepalen of er al dan niet sprake is van een menselijke gebruiker.

Hoe werkt reCaptcha

Op basis van het gedrag van een websitebezoeker (scrollen, klikken, snelheid van invullen, etc.) en andere factoren (IP-adres, eerder geplaatste cookies, etc.) krijgt dit gedrag een risicoscore. Uit de risicoscore maakt Google vervolgens op of ze te maken hebben met een legitieme bezoeker of een bot.

Een echte bezoeker hoeft bij de reCaptcha v2 dan alleen op een vinkje te klikken, waarmee diegene bevestigt geen robot te zijn. Bij twijfel moet de bezoeker een plaatjespuzzel oplossen.

Google reCaptcha v3 is onzichtbaar. Je ziet dus geen captcha op je website. De techniek, voor zover deze relevant is voor de privacy van de bezoeker, is hetzelfde als bij reCaptcha v2.

ReCaptcha verzamelt dus persoonlijke informatie van gebruikers om te bepalen of het gaat om een mens of een robot.

Welke informatie verzameld reCaptcha?

Als eerste controleert reCaptcha of er al eerder een cookie van Google is geplaatst op de computer. Vervolgens wordt er een reCaptcha cookie toegevoegd aan de browser van de gebruiker en er wordt een volledige snapshot gemaakt van het browservenster. Elke pixel wordt daarbij vastgelegd.

Voor een goede analyse verzamelt Google browser- en gebruikersinformatie en deze omvat onder andere:

- Alle cookies die Google in de afgelopen 6 maanden heeft geplaatst op het systeem van de gebruiker
- Hoeveel muisklikken de gebruiker in het browservenster heeft gemaakt (of heeft aangetikt als het gaat om een aanraakapparaat)
- Het scrolgedrag van de gebruiker
- Het CSS van de webpagina
- De systeemdatum en -tijd van de gebruiker
- Het IP-adres van de gebruiker
- Of de gebruiker op dit moment is ingelogd in diens Google account
- De ingestelde taal van de browser van de gebruiker
- Alle invoegtoepassingen die in de browser van de gebruiker zijn geïnstalleerd
- Alle Javascript-objecten
- De snelheid waarmee de gebruiker het formulier invult

Google Servicevoorwaarden voor reCaptcha

Door toegang te zoeken tot de reCaptcha-API's of deze te gebruiken, ga je akkoord met de gebruiksvoorwaarden van Google API's, de gebruiksvoorwaarden van Google en de onderstaande aanvullende gebruiksvoorwaarden. Zorg ervoor dat je de van toepassing zijnde voorwaarden en al het van toepassing zijnde beleid hebt gelezen en begrepen voordat je toegang zoekt tot de API's.

Servicevoorwaarden voor reCaptcha

Je erkent en begrijpt dat de reCaptcha-API werkt door informatie over hardware en software te verzamelen, zoals apparaat- en app-gegevens, en deze gegevens voor analyse naar Google te verzenden. De in verband met je gebruik van de service verzamelde informatie wordt ingezet voor de verbetering van reCaptcha en voor algemene beveiligingsdoeleinden. De informatie wordt niet door Google gebruikt voor gepersonaliseerd adverteren. Op grond van sectie 3(d) van de servicevoorwaarden voor de Google API's, stem je ermee in dat als je de API's gebruikt, het jouw verantwoordelijkheid is de benodigde meldingen weer te geven en toestemming te verkrijgen om deze gegevens te verzamelen en te delen met Google. Voor gebruikers in de Europese Unie geldt dat jij en je API-client(s) moeten voldoen aan het beleid ten aanzien van toestemming van gebruikers in de Europese Unie.

Bron: https://www.google.com/recaptcha/admin/create