Wens begeleidingscommissie

Meer betrouwbare statistiek met betrekking tot het aantal mensen dat naar aanleiding van een notificatie een test aanvraagt.

Suggestie begeleidingscommissie

Genereer na notificatie een *meldcode* die tijdens de testaanvraag moet worden. (Noot: de bcie vraagt niet om een testaanvraag te weigeren als iemand een code vervalst, en gaat ervanuit dat de test capaciteit voldoende is om geen meldingen te hoeven tegenhouden ; wel is het wenselijk dat we dat kunnen detecteren om de statistiek te corrigeren).

Mogelijke oplossingen

1. 'Validated Feedback' in GAEN

Cryptografisch dichtgetimmerde manier om te kunnen bewijzen dat je een notificatie hebt gehad, met behoud van privacy.

- **Haalbaarheid**: laag, vereist medewerking apple/google (voorstel is op 20 mei ingediend, 5.1.2e achterhaald momenteel status)
- **Privacy impact**: laag, protocol uitbreiding is privacy preserving.
- **Waterdichtheid**: hoog, vrijwel niet te vervalsen
- **Impact bouwteam:** Relatief eenvoudig aan app kant, vereist uitbreiding backend (call om ontmoeting te valideren en bijhouden extra (niet publieke) data per key)
- **Impact GGD:** Hoog: GGD afspraken site/callcenter moet een portal/extra veld krijgen waarin de meldcode kan worden ingevoerd (en eventueel gevalideerd).

2. Ophalen 'test voucher' met gebruik van push notificatie

Op het moment dat de app een notificatie triggert, vraagt hij via een API call een voucher op. Om te voorkomen dat iedereen de APi handmatig aanroept, wordt het resultaat gedistribueerd via een push noticficatie, die alleen tussen server en officiele app kan worden uitgewisseld.

- **Haalbaarheid**: redelijk.
- **Privacy impact:** hoog, push gaat via Apple/Google servers, dus decoys zijn nodig om te verbloemen dat iemand een notificatie heeft gehad. Voor push is bovendien een zogenaamd 'device token' nodig, dat een pseudoniem creeert.
- **Waterdichtheid**: hoog, vrijwel niet te vervalsen omdat apple en google de verzending van push goed beveiligd hebben.

- **Impact bouwteam:** Medium. Vereist een API call die vouchers uitgeeft, een implementatie van push notificaties, en een wijziging aan de app kant.
- **Impact GGD:** Hoog: GGD afspraken site/callcenter moet een portal/extra veld krijgen waarin de meldcode kan worden ingevoerd (en eventueel gevalideerd)

3. Genereren pseudo-meldcode geïnspireerd door DP-3T, met shared secret

DP-3T heeft een voorstel voor het genereren van een code na notificatie, waarbij die code gebaseerd is op een hash van de datum van risicovol contact en een shared secret.

- **Haalbaarheid:** goed
- **Privacy impact:** laag, de code is niet herleidbaar
- **Waterdichtheid:** laag. De shared secret is niet volledig secret te houden (ofwel onderdeel van code, ofwel geïnjecteerd in build proces; indien dat laatste, dan ook impact op verified builds/reproducible builds). Een slim iemand kan het secret achterhalen en een site maken die geldige codes genereert. Deze zou dan jurisch bestreden moeen worden.
- **Impact bouwteam:** Laag, geen backend wijziging nodig, app kan deze pseudocode zelf genereren.
- **Impact GGD:** Hoog: GGD afspraken site/callcenter moet een portal/extra veld krijgen waarin de meldcode kan worden ingevoerd (en eventueel gevalideerd) en evt een veld voor invoeren datum risicovol contact

4. Genereren pseudo-meldcode obv 'proof of work'

Door de app regelmatig iets te laten ophalen wat je nodig hebt voor een code (bijv bij de decoys of manifest telkens een 'woord' uit een 'reeks') kun je een code genereren die hierop gebaseerd is. Dit maakt dat een fake site meer moeite moet doen om codes te genereren.

- **Haalbaarheid:** goed
- **Privacy impact:** laag, de code is niet herleidbaar
- **Waterdichtheid:** laag. Alhoewel het meer moeite kost om fake codes te genereren zijn ze nog steeds gebaseerd op publieke info..
- **Impact bouwteam:** Hoog, backend krijgt een feature om woorden uit een reeks in volgorde uit te geven, app moet worden aangepast om deze woorden om te zetten naar een code.
- **Impact GGD:** Hoog: GGD afspraken site/callcenter moet een portal/extra veld krijgen waarin de meldcode kan worden ingevoerd (en eventueel gevalideerd) en evt een veld voor invoeren datum risicovol contact

5. Genereren 'light' pseudo-meldcode zonder shared secret, obv tijd

5.1.2e uit de bcie heeft eerder een light versie voorgesteld waarbij er een hash gegenereerd wordt obv de datum van risicovol contact en het moment waarop het scherm met de code wordt geopend (na een minuut sluit hij automatisch). Hierdoor genereer je een code met een korte geldigheid.

- **Haalbaarheid:** goed
- **Privacy impact:** laag, de code is niet herleidbaar
- **Waterdichtheid:** laag. Alhoewel de codes een korte geldigheid hebben, is obv de open source code eenvoudig een website te maken die geldige codes genereert. Deze zou dan jurisch bestreden moeen worden.
- **Impact bouwteam:** Laag, geen backend wijziging nodig, app kan deze pseudocode zelf genereren.
- **Impact GGD:** Medium: GGD afspraken site/callcenter moet een portal/extra veld krijgen waarin de meldcode kan worden ingevoerd (en eventueel gevalideerd) en een veld voor invoeren datum risicovol contact. Makkelijker dan voorgaande methode is dat een tijd gebaseerde code makkelijk kan worden gegenereerd zonder koppeling met de coronamelder backend.

6. Geen meldcode, maar als drempel vragen om datum contact en datum notificatie.

Schijnbaar in andere landen een succesvolle bestrijding van aantal keren dat test wordt aangevraagd obv notificatie.

- **Haalbaarheid:** uitstekend
- **Privacy impact:** medium, je vraagt een test-aanvrager om 2 extra gegevens.
- **Waterdichtheid:** laag. Je kunt eenvoudig 2 datums verzinnen (er is geen manier om te controleren of ze kloppen) - maar dat weten de bellers niet.
- **Impact bouwteam:** Geen
- **Impact GGD:** Medium, voor het registreren van deze 2 gegevens moeten velden worden toegevoegd (volgens 5.1.2e zit dit echter al in de pijpliijn).

7. Niets doen. (Geen meldcode, en geen drempel)

Onder het motto 'misbruik werd in Ierland na verloop van tijd vanzelf minder'

- **Haalbaarheid:** uitstekend
- **Privacy impact:** geen.
- **Waterdichtheid:** zeer laag, geen enkele controle / drempel om een test aan te vragen met 'notificatie' als reden..
- **Impact bouwteam:** Geen
- **Impact GGD:** Geen.

Te nemen beslissing

Gaan we het advies van de begeleidingscommissie uitvoeren en bouwen we een meldcode in?

Concrete deelvragen:

1) Willen we een meldcode introduceren om drempel te vergroten / statistiek te verbeteren?
2) Accepteren we dat dit niet waterdicht is? 5.1.2e 5.1.2e 5.1.2e kunnen daarna de 'meest waterdichte methode' uitwerken)
3) Hoe gaan we om met de niet-waterdichtheid (afbreukrisico 'de coronamelder is gehackt') en met aanpak eventuele fake sites.
4) Kunnen we in het test aanvraag proces de juiste wijzigingen doen.