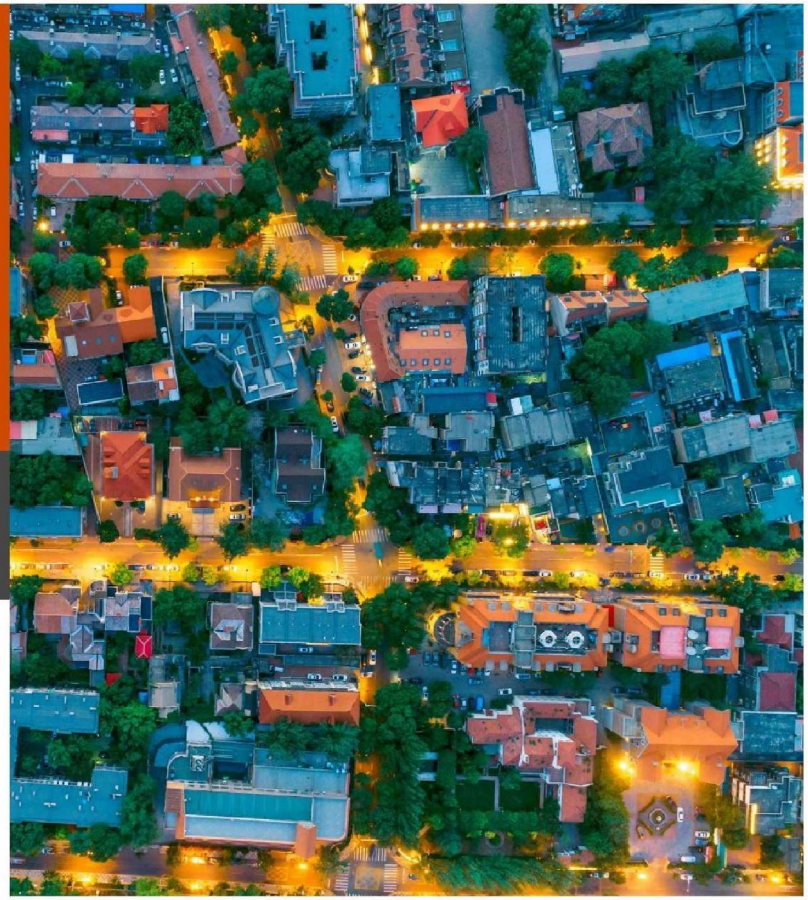
Vertrouwen borgen in de corona-apps

Actieplan eerste vier weken voor het borgen van de procesmatige, technische en juridische aspecten van de nieuwe Corona-app

DRAFT FOR DISCUSSION

pwc



De COVID-19 pandemie heeft een enorme impact op het leven van mensen, families en gemeenschappen.

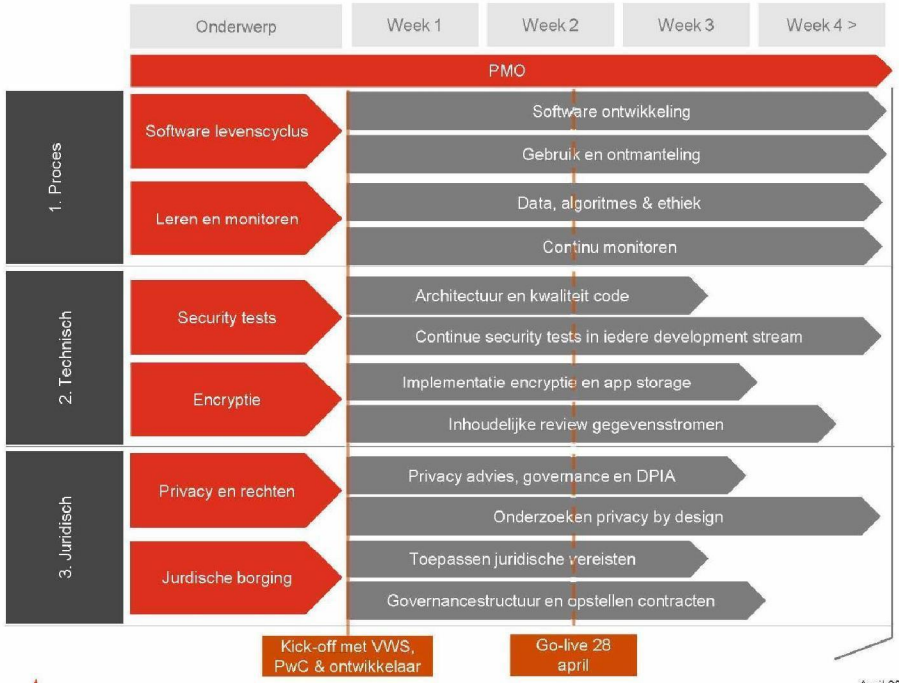
Als hulpmiddel om de verspreiding van COVID-19 tegen te gaan, worden apps gebouwd die burgers in staat stellen te identificeren in hoeverre zij in contact zijn gekomen met een positief geteste COVID-19 patiënt en een app voor zelfmonitoring.

Deze apps worden versneld uitgerold en dienen te voorzien in een optimale borging van gebruikersprivacy, gegevensbescherming en juridische borging.

Dit actieplan beschrijft de concrete activiteiten die wij uitvoeren om de kwaliteit van softwareontwikkeling, borging van privacy en inhoudelijke security componenten te adresseren.

Met als resultaat een app die de burger vertrouwt.

Onze aanpak kent drie kerndomeinen waar we u ondersteunen



Bovenstaande stromen werken wij uit in de volgende slides waarin de met ster gemarkeerde activiteiten door ons noodzakelijk worden geacht voor live-gang

Actieplan corona-app: procesmatige borging

1. Software ontwikkeling

- ★ De eerste stap is het analyseren van het gevolgde ontwikkelproces – welke plaats hebben risicoherkenning en -mitigatie in dit proces en hoe worden deze als requirements inclusief NFR gedefinieerd en getoetst – met specifiek aandacht voor security & privacy by design en risk assessments zoals DPIA om tot een korte cyclus te komen
- ★ Analyseren gebruik van standaarden en user stories voorstellen voor gemiste requirements op basis van good practice zoals NCSC- en AP-richtlijnen rondom tracing in het ontwerp
- Optimaliseren SDLC door tooling en best practices – zie de bijlage voor een blauwdruk

2. Gebruik & ontmanteling

- Toetsen tools, processen en werkinstructies voor na go-live zoals:
  - ★ Toetsing dat bij uitschakeling app en data volledig worden verwijderd
  - ★ Adoptieplan
  - FAQ & Helpdesk
  - Responsible disclosure programma
  - Opvolging door zorgmedewerker
  - Gebruikersbeheer
  - Functioneel beheer
  - Rechten van betrokkenen opvolgen
  - Monitoren en opvolgen van (potentiele) security incidenten
  - Disaster recovery & data breach procedure
  - Monitoring effectiviteit & procedure voor aanpassingen
  - ★ risico contact identificatie
  - ★ Anonimiseren en pseudonimisering
- Adviseren hoe de digitale oplossing intuïtief, doelgericht, en eenvoudig in het gebruik is zodat adoptie gemaximaliseerd wordt

3. Data, algoritmes & ethiek

- ★ Toetsen van inputdata op kwaliteit en representativiteit voor beoogd gebruik (zoals het tijdig melden van infectierisico aan personen)
- Valideren van proces voor ontwikkeling algoritmes
- ★ Valideren van de integriteit en vertrouwelijkheid van (tijdelijke) dataopslag
- Valideren van de processen met betrekking tot dataretentie en life cycle management
- Toetsen van de uitlegbaarheid van algoritmes en bredere accountability-aanpak richting key stakeholders

4. Continu monitoren

- Vaststellen en continu monitoren van de kpi's zoals adoptiegraad, gebruikerservaring en incident opvolging. Bijvoorbeeld door middel van social media analyse
- ★ Borging input van een burgerpanel en belangrijke stakeholders om input te verzamelen die de adoptiegraad zullen verhogen.
- Identificeren van risico's, rapporteren over de impact en adviseren over eventuele maatregelen;

Actieplan corona-app: technische borging

1. Architectuur en kwaliteit broncode

- De eerste stap is het analyseren van de systeemdocumentatie, architectuur, technisch en functioneel design van de app. Wij analyseren deze stukken en reviewen tegen best practice architecturen, zoals het three-tier model.
- De kwaliteit van de broncode analyseren wij geautomatiseerd in iedere iteratie van de app. Hierbij nemen wij security en kwaliteit mee conform ISO25010.

2. Continu uitvoeren security test

- Wij starten direct met het testen van iedere development cycle van de app, API's en servers.
- Wij gebruiken de SANS Top 25, OWASP Top 10 en OWASP API modellen.
- De backend servers testen wij vervolgens ook van uit "insider" perspectief, om te borgen dat gegevens correct zijn afgeschermd van andere omgevingen en dat de servers zijn geconfigureerd naar de meest recente en erkende beveiligingsstandaarden.
- Na livegang testen wij de omgeving continu, zodat ook toekomstige issues direct worden gedetecteerd.

3. Implementatie van encryptie en storage

- Wij testen de inhoudelijke werking en implementatie van de encryptie zoals deze door de gebruikte standaarden (zoals DP-3T) worden voorgeschreven.
- Vervolgens testen wij de beveiligde verbindingen tussen de app en de backend, door gebruik te maken van de NCSC richtlijnen voor het beveiligen van gegevenstransmissie.
- Op de telefoon zelf onderzoeken wij ook de opslag van data en welke risico's de dataopslag met zich meebrengt voor het totale aanvalsvlak van de telefoon zelf

4. Inhoudelijke review gegevensstromen

- Door een man-in-the-middle omgeving op te zetten analyseren wij welke telemetrie er exact per app (iOS, Android) de telefoon verlaat. Wij testen of de gegevens die worden verstuurd geen naar personen herleidbare informatie bevatten.
- De telemetrie van de app analyseren wij tegen de gebruikte standaard (zoals DP-3T) om te onderzoeken of de specificatie juist is geïmplementeerd.

= *noodzakelijk geacht voor live-gang*

Actieplan corona-app: borging juridische aspecten

1. Privacy advies, governance en DPIA

- In eerste instantie inventariseren we de assets en entiteiten die betrokken zijn bij de verwerking van persoonsgegevens rondom de apps en gebruiken deze informatie voor begeleiding bij het opstellen van de governance structuur en het verwerkingsregister.
- ★ Fundamentele privacy-beginselen zoals toestemming van de betrokkenen en grondrechten worden in kaart gebracht en gekoppeld aan concrete, juridische actiepunten (zie stap 3 “toepassen juridische vereisten”). De DPIA is hiervoor een belangrijk instrument.
- We definiëren met welke partijen contracten en protocollen moeten worden afgesloten.

2. Onderzoeken privacy by design

- ★ We assisteren vanaf ontwerpfase tot ontmanteling bij het maken en documenteren van belangenafwegingen en keuzes over de te gebruiken persoonsgegevens, dataminimalisatie, bewaartermijnen en het delen van persoonsgegevens met derde partijen.
- In continue samenwerking met de technici, toetsen we vanuit privacy en algemeen juridisch perspectief, voorgestelde oplossingen voor doelmatigheid en gebruiksvriendelijkheid van de user interface.
- We bieden advies over de in te richten procedures voor het uitvoeren van rechten van betrokkenen en testen deze.

3. Toepassen juridische vereisten

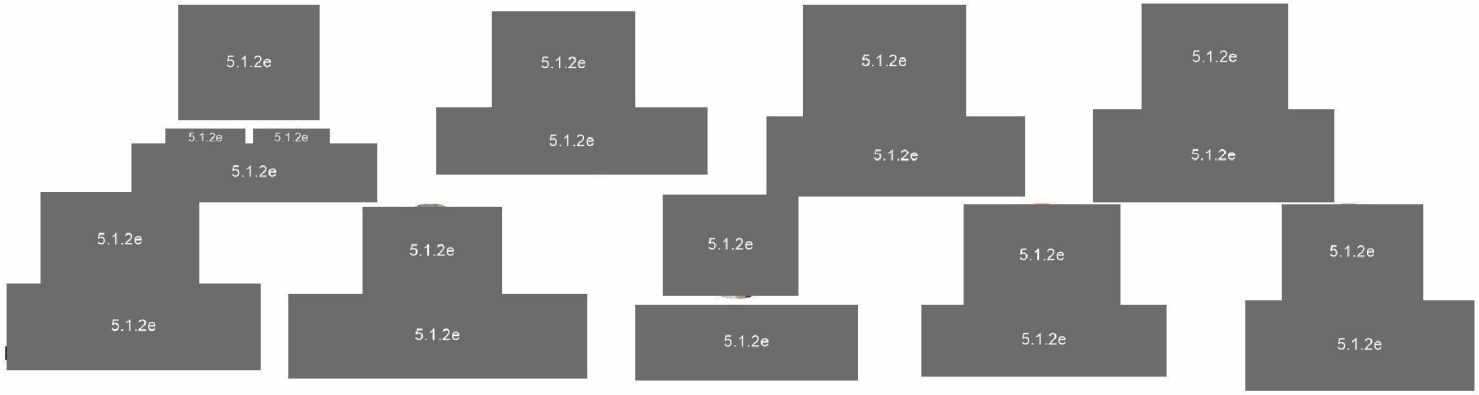
- Uit de vorige stappen is duidelijk geworden welke juridische vereisten praktisch haalbaar zijn, in welke vorm technisch implementeerbaar en hoe de lifecycle van de gegevens eruit ziet.
- We analyseren de privacyverklaringen, alsmede de toestemmingsverklaringen en assisteren bij het documenteren van de gemaakte belangenafwegingen.
- ★ We analyseren de contracten en protocollen, met oog op privacy-, aansprakelijkheids- en algemeen juridische risico’s en verplichtingen.

4. Governancestructuur en contracten

- We analyseren in samenwerking met de betrokken stakeholders de governancestructuur en adviseren over het distribueren van verantwoordelijkheden met betrekking tot monitoring van wet- en regelgeving, afhandeling van verzoeken van betrokkenen om hun rechten uit te oefenen en het protocol datalekken;
- We analyseren contracten en protocollen en bij documentatie van afspraken met (lagere) overheden en derde partijen.

PwC ★ = noodzakelijk geacht voor live-gang

Wij staan naast u als onafhankelijke en kritische partij die continu en risico-gebaseerd inzicht geeft in mogelijke kwetsbaarheden in de oplossing en u ontzorgt met praktische aanbevelingen. Hiermee zorgen we samen dat de belasting op onze zorginstellingen en GGD's wordt gereduceerd.



APPENDIX

PwC DevSecOps blauwdruk voor sterk geautomatiseerde CI/CD pipeline

Het diagram hieronder illustreert een CI/CD pipeline waarbij security geïntegreerd onderdeel is inclusief best practices en mogelijke tools.