Overzicht security analyses, onderzoeken en audits

Aan Begeleidingscommissie, 13 augustus 2020

Ten behoeve van de beveiliging van CoronaMelder is een breed scala aan analyses, onderzoeken, reviews en audits uitgevoerd, onder andere door verschillende (onafhankelijke externe) partijen. Hieronder staat een beknopt overzicht. Daarbij is tevens aangegeven of een audit of onderzoek nog loopt of al afgerond is.

Analyses

Eisen op het vlak van beveiliging zijn meegenomen in het ontwerp van CoronaMelder, bijvoorbeeld in de solution architecture en het cryptoraamwerk. Op basis van deze ontwerpen zijn er twee relevante analyses uitgevoerd:

- Een privacy impact assessment (of data protection impact assessment) om risico's en maatregelen op het vlak van gegevensbescherming in kaart te brengen. De Autoriteit Persoonsgegevens heeft een advies hierover uitgebracht.
- Een dreigings- en risicoanalyse op het gebied van nationale veiligheid die met hulp van de NCTV, NCSC en AIVD is uitgevoerd. In deze analyse zijn risico's op het gebied van nationale veiligheid in kaart gebracht en passende maatregelen opgenomen. Deze drie diensten hebben tevens een tussenadvies over de borging van nationale veiligheid uitgebracht. Op termijn volgt nog een eindadvies.

Onderzoeken, reviews en audits

De volgende onderzoeken (waaronder reviews, assessments, audits, etc) zijn of worden nog uitgevoerd betreffende de beveiliging van CoronaMelder:

Activiteit	Partij	Toelichting
Overkoepelend onderzoek	Fox-IT	Dit onderzoek loopt nog.
Code review CoronaMelder App	Secura	Dit onderzoek loopt nog
Code review CoronaMelder Server	Radically Open Security	Dit onderzoek loopt nog
Penetratietest website	Hack Defense	Afgerond
Code review API framework G/A	Radically Open Security	Dit onderzoek loopt in opdracht van de Europese Commissie.
Penetratietest	NFIR	Het betreft een brede penetratietest welke reeds is uitgevoerd en waar een concept rapportage van is ontvangen. Er volgt nog een tweede penetratietest door dezelfde partij voor het op basis van standaarden nalopen
Review cryptoraamwerk	Radically Open Security	Review van het cryptoraamwerk om inzicht te krijgen in de kwaliteit en veiligheid van het ontwerp.
Procedurele assessment	Prof. Paans Noordbeek	Assessment van de organisatorische en procedurele maatregelen die zijn genomen. Dit omvat tevens een toets op compliancy aan de BIO door de hosting/beheerder. Deze assessment loopt nog.
Vulnerability scans	KPN	De beheerder voert regelmatig vulnerability scans uit op diverse technische componenten om bekende kwetsbaarheden op te sporen.
Interne pentest	KPN	Na installatie voert KPN interne tests uit

Stress test	VWS	Om zeker te stellen dat de omgeving voldoende verwerkingen aan kan, worden er deze week een drietal stress tests uitgevoerd.
Verified build	Pels Rijcken	Iedere versie die beschikbaar komt, wordt gebouwd conform een zogenaamde verified build. Daarmee kan een gebruiker weten dat de app die beschikbaar is gekomen dezelfde software betreft als de open-sourcebroncode die op GitHub beschikbaar is.
Duidingsrapportage	De Winter	Deze rapportage geeft context, legt het hele model van verwerking met de aanwezige maatregelen uit en geeft een uitleg van de onderzoeken en beantwoordt de vraag: is de app vanuit informatiebeveiliging en privacybescherming fit for purpose?

Naast de toetsende activiteiten die direct gericht zijn op beveiliging worden er ook nog functionele en technische tests uitgevoerd om de kwaliteit en betrouwbaarheid van CoronaMelder te toetsen. Daar vallen onder andere ketentests en load- en performance tests onder op de verschillende technische componenten van de backend.