Beoordelingsadvies

Aanmelding testaanbieder op CoronaCheck

Naam testaanbieder:
Datum rapport: 0

CoronaCheck
Ministerie van Volksgezondheid, Welzijn en Sport

Initialen toetser	AA		
KVK tekenbevoegde gecontroleerd op basis van uittreksel	Ja/Nee		
Acceptatie en ondertekening aansluitvoorwaarden?	Ja/Nee		
Is er een compleet dossier aangeleverd?	Ja/Nee		
Bevestiging via veilige mail ontvangen	Ja/Nee		
Aanbieder gebruikt NTA7516 geregistreerde mailoplossing	Ja/Nee		
Indien 7516 oplossing		*Indien geen 7516 oplossing*	
NTA7516 certificaat op naam van leverancier en Verklaring van Toepasselijkheid (VvT)	Ja/Nee/NVT	Een Verklaring van In– en Uitsluitingen NTA 7516 Criteria	Ja/Nee/NVT
Een gedocumenteerd testresultaat waaruit blijkt dat testuitslagen met multifactor wordt verstuurd via de gecertificeerde leverancier.	Ja/Nee/NVT	Een toetsing van alle NTA 7516 normen conform NCS 7516	Ja/Nee/NVT
Is gedocumenteerd testresultaat volgens tekst/format uit de implementatiehandleiding (website rijksoverheid, aansluit documentatie)	Ja/Nee/NVT	Is gedocumenteerd testresultaat volgens tekst/format uit de implementatiehandleiding (website rijksoverheid, aansluit documentatie)	Ja/Nee/NVT
Een mail naar aansluiten@coronacheck.nl waaruit blijkt dat overige ad-hoc communicatie via mail conform NTA 7516 wordt verstuurd via de gecertificeerde leverancier.	Ja/Nee/NVT	Een gedocumenteerd testresultaat waaruit blijkt dat testuitslagen conform NTA 7516 wordt verstuurd.	Ja/Nee/NVT
Let op: bij gebruik [xxxxxx] vragen aan testaanbieder om de volgende vragen schriftelijk te bantwoorden: Op welke wijze wordt door de testaanbieder voorzien in de beveiliging van de uitslag (bijzondere persoonsgegevens) in geval van: 1. Verlies van een (onbeveiligd) mobiel apparaat? 2. Gedeeld gebruik van een systeem en/of mailbox? Is er een antwoord op deze vragen gegeven?	Ja/Nee/NVT	Een mail naar aansluiten@coronacheck.nl waaruit blijkt dat overige ad-hoc communicatie via mail conform NTA 7516 wordt verstuurd.	Ja/Nee/NVT
Door naar volgende stap	Ja/Nee		

Initialen toetser	AA

Eis	Afkeuren bij niet voldoen aan eis, maar eis wel van toepassing	Ratio	Bevinding
Infrastructuur wordt getest conform de Pentest Execution Standard (PTES)	Ja	Hiermee wordt een minimaal beveiligingsniveau afgedekt. De standaard helpt concreet te maken welke onderzoeken zijn	
Web applicaties worden getest conform OWASP Top 10: de 10 meest kritische kwetsbaarheden van webapplicaties	Ja	Hiermee wordt een minimaal beveiligingsniveau afgedekt. De standaard helpt concreet te maken welke onderzoeken zijn uitgevoerd.	
Web applicaties worden getest conform OWASP WSTG: standaard ten behoeve van het pentesten van webapplicaties	Ja	Hiermee wordt een minimaal beveiligingsniveau afgedekt. De standaard helpt concreet te maken welke onderzoeken zijn	
Voor API’s wordt getest conform OWASP API Security Top 10: de 10 meest kritische kwetsbaarheden van API’s.	Ja, indien er sprake is van API's.	Hiermee wordt een minimaal beveiligingsniveau afgedekt. De standaard helpt concreet te maken welke onderzoeken zijn uitgevoerd.	
Voor mobiele applicaties wordt getest conform: OWASP MSTG: standaard ten behoeve van mobiele applicatie pentesten	Ja, indien er sprake is van een eigen app.	Hiermee wordt een minimaal beveiligingsniveau afgedekt. De standaard helpt concreet te maken welke onderzoeken zijn uitgevoerd.	
Het onderzoek moet, net als bij andere onderzoeken, zo worden beschreven dat het reproduceerbaar is voor contraexpertise.	Ja	Het bewaken van het stelsel is een cruciaal onderdeel van CoronaCheck. Reproduceerbaarheid van het onderzoek zorgt dat duidelijk is bij problemen hoe onderzoek is gepleegd. Het geeft verder inzicht of onderzoek in afdoende mate heeft plaatsgevonden.	
Hoofdstukken rapportage niet exact conform PTES	Nee	Wanneer de informatie niet volledig conform de standaard is, maakt dat verificatie lastig. Het betekent echter niet dat de informatie niet is aangeleverd.	
Fase 1: Intelligence gathering aanwezig	Nee	Bij het ontbreken van intelligence gathering hoeft niet automatisch te betekenen dat geen deugdelijk onderzoek is verricht, wel is het een indicatie die vragen oproept.	
Fase 2: Threat modelling aanwezig	Nee	Het ontbreken van threat modelling kan het gevolg zijn van vooraf bepaalde threats op een systeem. Het roept wel de vraag op hoe het onderzoek is verricht, omdat het specifiek richten op dreigingen qua maatwerk beter aansluit bij de realiteit.	
Fase 3: Vulnerability analysis	Nee	Het ontbreken van een vulnerability analysis hoeft niet een probleem te zijn als de normen breed en volledig worden doorgetest. Het is wel een indicatie dat niet specifiek op de situatie	
Fase 4: Exploitation	Nee	Het niet hebben van de exploitation verhindert verificatie van het probleem. Dat is voorstelbaar als wordt gevreesd voor actief misbruik.	
Fase 5: Post-Exploitation	Nee	Het ontbreken van een post-exploitation hoeft op zichzelf geen probleem te zijn, wanneer het probleem volledig wordt verholpen. Het ontbreken betekent wel dat niet inzichtelijk is welke risico’s exact worden gelopen en welke data risico loopt. Het ontbreken van deze fase kan ook betekenen dat er nog hacking tools op systemen zijn achtergebleven.	

Fase 6: Reporting	Nee	Een ontbrekende beschrijving van het komen tot het verslag is geen probleem, omdat het verslag zelf onderdeel is van de toets.	
Fase 7: Retest	Nee	Het opnieuw checken of fouten daadwerkelijk zijn verbeterd is een belangrijke fase. Het is mogelijk dat deze in het rapport niet voorkomt, omdat de gevonden zwakheden niet zijn verholpen.	
Scope beschrijving met hostnames, ip-adressen, andere scope objecten	Ja	In deze stap wordt duidelijk wat is getest. Wanneer die duidelijkheid niet wordt verschaft is onduidelijk welke omgeving er uberhaupt is getest.	
Verloop pentest: tijdslot uitgevoerde acties, beschrijving taken per tijdsslot	Nee	Een gedetailleerde beschrijving van het verloop van de pentest geeft meer vertrouwen en inzicht in het correct uitvoeren van de test. Het ontbreken hoeft niet te betekenen dat een test niet goed is uitgevoerd.	
Rapportage kwetsbaarheden			
Lijst scopeobjecten per kwetsbaarheid	Ja	Wanneer niet duidelijk is welke zwakheid op welk object invloed heeft, is de ernst niet te bepalen.	
Gebruik CvSS v3 of geen vectorstring	Ja	Wanneer er geen CVSS v3 is aangemaakt is niet duidelijk wat de echte gevolgen van een kwetsbaarheid zijn. Wanneer de vectorstring ontbreekt, is niet te volgen hoe tot de score is gekomen en daarmee is het niet mogelijk de bevinding te controleren of kost dit onredelijk veel moeite. De pentest heeft geen	
Gedetailleerde beschrijving van de kwetsbaarheid of het risico	Ja	Zonder een goede uitleg zijn de gevolgen van een zwakheid niet in te schatten.	
Gedetailleerde reproductiestappen van de kwetsbaarheid	Ja	Zonder dat duidelijk is hoe de zwakheid vorm krijgt, is de bevinding niet te controleren.	
Gedetailleerde impactbeschrijving van de kwetsbaarheid of het risico	Ja	Zonder een beschrijving van de impact is niet navolgbaar hoe tot een risicoinschatting is gekomen.	
Gedetailleerde oplossingsrichting van de kwetsbaarheid of te nemen mitigerende maatregelen bij het risico	Nee	Hoe belangrijk het hebben van oplossingsrichtingen op zichzelf ook is, toch hoeft het ontbreken ervan niet direct een showstopper te zijn. Het is denkbaar dat er al een oplossing gevonden is of de organisatie zelf in staat is gebleken het probleem te	
Bijlagen rapport			
Scanresultaten per uitgevoerde scan, opgemaakt in leesbaar formaat	Ja	Zonder scanresultaten is niet te volgen wat is getest en wat de uitkomst was.	
Eindoordeel			
Eisen die niet direct leiden tot afkeuring leiden tot afkeuring wanneer er drie of meer niet voldoen.		Deze eisen zijn een indicatie van verhoogde risico’s of een gebrekkig inzicht in de risico’s die voor aansluiting gelden. Wanneer dat op verschillende punten het geval blijkt te zijn, is het zaak eerst de pentest beter uit te voeren.	
		Bij livegang mogen er geen bevindingen zijn met een CVSS-score van hoger dan 4 en moet een hertest hebben plaatsgevonden.	
	Aantal niet compliant onderdelen van de pentest	**Aantal openstaande bevindingen met een CVSS 3.0 score van hoger dan 4**	**Eindoordeel**
SLOTSOM	13	0	

Door naar volgende stap Ja/Nee

Initialen toetser	AA
Is er een NEN-certificaat	Ja/Nee
Bij gaan NEN-certificaat is er een eigen verklaring?	Ja/Nee
Analyse verklaring	
Afdoende NEN-7510 afgedekt?	Ja/Nee
Door naar volgende stap	Ja/Nee

Initialen toetser	AA
DPIA Aanwezig	Ja/Nee
Doel beschreven	Ja/Nee
Noodzaak en proportionaliteit beschreven	Ja/Nee
Analyse risico's voor de betrokkenen	Ja/Nee
Risico's uit preambule 75 benoemd of geanalyseerd?	Ja/Nee
Technische en organisatorische maatregelen benoemd	Ja/Nee
Informatie met betrekking tot de door Aanbieder geïmplementeerde procedurele maatregelen ten aanzien van door Aanbieder ingeschakelde medewerkers en facilitaire diensten.	Ja/Nee
Autorisatie Matrix voor toegang tot de Teststraat applicatie en Lokale IT omgeving	Ja/Nee
Beschrijving van fysiek testkit proces en koppeling met Teststraat applicatie	Ja/Nee
Beschrijving proces koppeling testkit aan identiteit van burger, uitgifte van testkit, uitvoering van de test en het transport van de test naar de ruimte waar de test verder wordt verwerkt:	Ja/Nee
Overige verwerkingen (als die er zijn) benoemd	Ja/Nee
FG aanwezig	Ja/Nee
Advies FG aanwezig	Ja/Nee
DPIA niet door FG uitgevoerd	Ja/Nee
Door naar volgende stap	Ja/Nee

Initialen toetser	AA
Zelfverklaring NTA7516 aanwezig en rechtsgeldig ondertekend	Ja/Nee
Zelfverklaring websites en e-mailadressen aanwezig	Ja/Nee
Door naar volgende stap	Ja/Nee

Initialen toetser	AA
Website conform W3C	J/N
Score internet.nl 100%	J/N
Akkoord bevonden	J/N

Uitzondering: geen IPv6 is toegestaan

FINAAL OORDEEL

Concept advies toelating IB&P	J/N

Eind oordeel CSPO	
Datum	
Toetsing onderdelen	
Positief advies toelating tot CoronaCheck stelsel	Ja/Nee