Secura

Statement of Work
IT-BEVELIGINGSONDERZOEK RIVM
voor
RIVM

5.1.2e

20121088.v1.1-OFF-MinisterieVWS-Designreview+scans bij RIVM
Versie 1.0
22-12-2020

VERTROUWELIJK

SAMENVATTING

Binnenkort starten in Nederland de inentingen tegen het Coronavirus (COVID-19). Het RIVM speelt hierin een centrale rol omdat zij de gegevens van alle vaccinaties ontvangen van partijen zoals o.a. huisartsen en verpleeghuizen. Het is zeer belangrijk dat alle gegevens van burgers op een veilige (security) en vertrouwelijke (privacy) wijze worden verzonden, verwerkt en opgeslagen. Het gebruik van de benodigde IT-infrastructuur brengt veiligheidsrisico's met zich mee.

5.1.2e heeft daarom aan 5.1.2e van Secura gevraagd om een opdrachtbevestiging te maken voor het op korte termijn uitvoeren van een security assessment op de RIVM omgeving die gebruikt wordt voor het vastleggen van de Corona vaccinaties. Deze opdracht is urgent en moet op zeer korte termijn uitgevoerd worden.

Project overzicht	
Projectnaam:	IT-beveiligingsonderzoek RIVM
Doel:	Secura zal de effectiviteit van de geïmplementeerde beveiligingsmaatregelen testen, kwetsbaarheden identificeren en heldere adviezen geven ter verbetering.
Scope:	De It-omgeving bij het RIVM die gebruikt wordt voor het verwerken en opslaan van de vaccinatie gegevens m.b.t. de komende Corona inentingen. Definitieve URL's en/of IP-adressen worden nog afgestemd.
Onderzoeksmethode:	Designreview van de IT-architectuur en scans van de externe omgeving.
Bijzonderheden:	Deze opdracht is urgent en moet op korte termijn uitgevoerd worden. Secura en het Ministerie van VWS hebben daarom besloten om op een praktisch manier met elkaar deze opdracht uit te voeren. Dit Statement of Work dient als opdracht bevestiging. Ook de uitvoering van het onderzoek is gebaseerd op wat haalbaar is gezien de zeer korte termijn, beschikbare resources en eventuele onduidelijkheden. Belangrijk is dat er een eerste indruk moet komen over de digitale veiligheid van de RIVM omgeving die gebruikt wordt voor de vaccinatie gegevens.
Deliverable:	Na ons security assessment ontvangt u als resultaat een memo per email met daarin onze bevindingen. Hiervoor is in gezamenlijk overleg gekozen i.v.m. de urgentie en doorlooptijd van het onderzoek.
Planning & Uitvoering:	Secura zal op verzoek het onderzoek direct opstarten. Het onderzoek inclusief voorbereiding, uitvoering, rapportage en kwaliteitscontrole heeft een omvang van 7 mandagen
Prijs (vaste prijs)	5.1.1c excl. BTW

Als u naar aanleiding van dit voorstel vragen of aanvullingen heeft, neem dan gerust contact met mij op. In alle gevallen zien we uit naar uw reactie en het vervolg op dit voorstel.

VERTROUWELIJK

Met vriendelijke groet,
Namens Secura,

5.1.2e

5.1.2e

5.1.2e

BEGROTING

Aan de hand van de informatie uit de intake heeft een securityconsultant van Secura een inschatting gemaakt van de benodigde tijd voor het project. Hieronder vindt u de daarbij behorende begroting.

Security Assessment	Totaal
IT-beveligingsonderzoek RIVM inclusief: • Voorbereiding • Rapportage en toelichting • Projectmanagement en kwaliteitscontrole	5.1.1c
Totaal (vaste prijs)	

Bovenstaande begroting is gebaseerd op de kennis en ervaring van Secura en de beschikbaar gestelde informatie door RIVM. Wanneer (bij een vaste prijs voorstel) door onvoorziene omstandigheden significante delen van de scope niet onderzocht kunnen worden, zal Secura hierover met RIVM overleggen.

VRIJWARING

Met het ondertekenen van deze SoW of het verstrekken van een inkooporder verstrekt RIVM toestemming aan Secura tot het uitvoeren van dit onderzoek. Tevens vrijwaart RIVM Secura voor mogelijke schadeclaims – inclusief claims van derden – voor directe en indirecte schade als gevolg van het uitvoeren van deze opdracht.

Indien de te onderzoeken systemen geen eigendom zijn van RIVM, dient de eigenaar van de systemen ook toestemming voor uitvoering van het onderzoek en vrijwaring te geven. RIVM is verantwoordelijk voor het verkrijgen van de toestemming en vrijwaring van de eigenaar van het systeem en van eventuele derden.

OVEREENKOMST EN ONDERTEKENING

Deze offerte is 30 dagen geldig vanaf de datum van ondertekening door Secura. Alle genoemde prijzen zijn in Euro, inclusief reiskosten binnen Nederland, exclusief B.T.W. en gebaseerd op het werken tijdens normale kantoortijden (tussen 08:00u-18:00u). Bij dit aanbod zijn de kosten voor het gebruik van tooling en kantoorkosten inbegrepen.

Secura factureert RIVM na het opleveren van het (concept)rapport, of maandelijks bij advies- of detacheringsopdrachten. In geval van meerjarig contract wordt per kwartaal gefactureerd. De betalingstermijn is 30 dagen na factuurdatum.

Keuze	Beschrijving
☒	Assessment zoals beschreven, inclusief projectmanagement en kwaliteitscontrole.

Op deze overeenkomst zijn de General Terms and Conditions van Secura B.V., zoals gedeponeerd bij de Kamer van Koophandel op 25 juni 2018 onder nummer 17126968, van toepassing.

Voor akkoord:

RIVM	Secura B.V.
Datum:	Datum: 22-12-2020
Naam:	Naam: Dirk Jan van den Heuvel
Functie:	Functie: Managing Director
Handtekening:	Handtekening: 5.1.2e

20121088.v1.1-OFF-MinisterieVWS-Designreview+scans bij RIVM 22-12-2020

Secura

APPENDIX A. GEFASEERDE AANPAK BIJ SECURITYASSESSMENTS

Bij alle security assessments volgt Secura een gefaseerde aanpak. Eerst vindt de voorbereiding van het onderzoek plaats, daarna wordt informatie over de systemen, componenten en applicaties verzameld, vervolgens wordt het assessment uitgevoerd en tot slot wordt het rapport geschreven. Optioneel kan een heronderzoek worden uitgevoerd om onafhankelijk de effectiviteit van geïmplementeerde beveiligingsmaatregelen te testen die zijn gedaan naar aanleiding van eerdere bevindingen.

Fase 1: Voorbereiding en informatievergaring

Een goede voorbereiding is essentieel en zorgt voor een tijdsefficiënte uitvoering van de opdracht.

De activiteiten in deze fase zijn:

- Bepalen van een volledig overzicht van de doelsystemen in de scope (bijv. IP-adressen en URL's).
- Opstellen en verifiëren van een vrijwaringsverklaring (indien derde partijen betrokken zijn).
- Aanwijzen en vastleggen van technische en operationele contactpersonen.
- Valideren dat inloggegevens zijn opgeleverd (indien van toepassing).

Door zoveel mogelijk informatie te verzamelen (onder andere door gebruik te maken van gegevens uit publiek beschikbare bronnen) krijgen we een volledig beeld van de systemen in de scope.

De informatie die verzameld wordt bestaat onder andere uit:

- Systemen binnen de scope;
- TCP- en UDP-poorten met actieve diensten;
- Bekende kwetsbaarheden bij onderliggende diensten;
- Applicatie of gebruikte frameworks;
- (Sub-)domeinen;
- Functionaliteit (geauthentiseerde) van gebruikers rollen (indien relevant)
- Benaderbare webservices en/of API's;
- Mogelijke externe koppelingen;

Het resultaat van deze fase is een goed voorbereidde aanpak die zorgt voor een efficiënte testmethode.

Fase 2: Test en analyse

In deze fase onderzoekt Secura welke kwetsbaarheden geïdentificeerd kunnen worden door het uitvoeren van een onderzoek door een ervaren securityspecialist. De kracht van het onderzoek is de manier waarop wij onze technische kennis en logica gebruiken om kwetsbaarheden te vinden (zie de in de bijlage beschreven aanpak van het onderzoek). Om zo efficiënt mogelijk te werken maken we hierbij ook gebruik van tools en scripts die deels door Secura zelf zijn ontwikkeld. Het onderzoek levert ruwe data en mogelijke kwetsbaarheden op die daarna in een analyse handmatig worden gecontroleerd op 'false positives[1]'.

[1] *Een 'false positive' lijkt een kwetsbaarheid te zijn, maar is dat niet in werkelijkheid.*

Fase 3: Rapportage en toelichting

Deze fase bestaat uit het schrijven (zie voor de details hiervan hoofdstuk 3.3) en reviewen van het rapport Wanner u dat wenst, bespreken wij graag het rapport met u en nemen we de bevindingen samen door.

Fase 4: Optioneel heronderzoek

Secura biedt de mogelijkheid om tot zes maanden na afloop van ons beveiligingsonderzoek een heronderzoek te doen. Op deze manier kan RIVM controleren of onze aanbevelingen correct zijn verwerkt door de organisatie. Zo is RIVM verzekerd van een onafhankelijk en scherpe toetsing van de kwaliteit van de correcties en aanpassingen met als doel de beveiliging te verbeteren.

Na afloop van het heronderzoek schrijven wij een toevoeging (addendum) op het originele rapport. Hierin zal per eerder aangetroffen kwetsbaarheid worden aangegeven of deze is opgelost. Als Secura tijdens het heronderzoek nieuwe kwetsbaarheden aantreft worden deze aan RIVM gecommuniceerd. Bij het addendum zullen wij een nieuwe managementsamenvatting schrijven die de eindsituatie goed weergeeft.