To: (10)(2e) [(10)(2e)@icloud.com]; (10)(2e))[(10)(2e)@minvws.nl]
Cc: (10)(2e))[(10)(2e)@minvws.nl]; (10)(2e) [(10)(2e)@dictu.nl]; (10)(2e) .
((10)(2e))[(10)(2e)@minvws.nl]
From: (10)(2e)
Sent: Fri 7/3/2020 8:15:57 AM
Subject: Re: Graag offerte back en penetratie test laten tekenen.
Received: Fri 7/3/2020 8:16:14 AM

Hallo,

Gelet op de urgentie heb ik (10)(2e) en (10)(2e) ook in de CC gezet.

Geen probleem om die onderbouwing te leveren.

Vooropgesteld: NFIR is al getekend. PMP zit op(10)(1c) euro dus valt daar buiten. Secura zit op (10)(1c) euro. Die zou ik graag al hebben, want daar zit een deel van de druk.

Afbreukrisico: als de handtekeningen niet komen dan vervallen opties en vallen er gaten. Gaten zou betekenen dat zaken niet worden afgetest of we met mindere goden moeten werken (denk kaliber probleem infectieradar met hun pentest). In de arena van het maatschappelijk debat zal dit zeer problematisch uitwerken voor de draagkracht. Bovendien als wij 'domme' steken laten vallen dan is dat dodelijk voor de reputatie. Daarnaast vrees ik dan dat ook de Autoriteit Persoonsgegevens weer gaan opvlammen in hun kritische houding. We bouwen heel voorzichtig vertrouwen op en ik vecht tegen een last van andere projecten en het verleden. Er is een grens in wat ik in de relationele sfeer kan blijven regelen.

In het algemeen zijn de selectiecriteria:

1. Het centrale doel is publiekelijk mensen te overtuigen.

2. De rapportage dienen om openbaar te maken. Dat betekent dat sommige partijen al afvallen (Deloitte is een mooi voorbeeld).

3. Er is gekozen om per onderdeel een ander bedrijf te kiezen. Daarmee krijgen wij niet alleen een breder beeld, maar is er ook over de onderdelen heen druk op kwaliteit. Een voorbeeld is dat een codereview dingen kan vinden, die je ook soms vindt in een penetratietest. De codereview van de client ziet dingen in relatie tot de server en omgekeerd. Kortom: de bedrijven zijn bang dat hun concurrent het beter doet. Dat effect is al merkbaar, omdat NFIR zes mandagen extra levert zonder kosten in reactie op dit plan. Daarnaast is hier een andere gedachte: er is veel wantrouwen naar de App. Door verschillende partijen in te zetten ontstaat er een breed beeld van goedkeuring. Dat wekt meer vertrouwen dan een bedrijf waar altijd iemand weer tegen kan zijn.

4. Over alle onderdelen heel maakt Fox-IT een overall verslag. Zij helpen daarmee het beeld goed te schetsen en helpen verder met toetsen of ik de juiste onderzoeksvragen heb neergelegd. Zo laten we geen steken vallen. Fox-IT is gekozen, omdat (10)(2e) graag Fox-IT heeft.

5. Niet alle bedrijven kunnen ons bedienen door een gebrek aan tijd. Ik ben in mei begonnen en vraag veel van bedrijven. Normaliter zijn wachttijden van 3-6 maanden geen uitzondering.

6. De bedrijven die ik heb benaderd, hebben allemaal een goede reputatie en zijn vertrouwendwekkend. Ik heb gezocht naar best of breed. Immers dat heeft de minister gezegd. We zetten de beste partijen in. Daarnaast is de harde voorwaarde geweest dat het partijen in de Nederlandse markt zijn, die als bedrijf Nederlands of Europees zijn. Per bedrijf loop ik ze

langs:

- NFIR is steengoed in pentesten. Zij werken conform open standaarden en daarmee genormeerd. Daarnaast leveren zij verslaglegging met positieve testen. Daarmee bedoel ik dat zij aangeven wat ze exact getest hebben. Niet alleen aangeven wat niet goed is (dat doen namelijk de meeste). Ons doel is te laten zien dat we alles hebben afgecheckt. Het kwaliteitsverschil tussen bedrijven is groot. Dat hebben we gezien met infectieradar waar Ordina dit voor de handliggende lek niet heeft getest. Belangrijk is de inzet van (10)(2e) een groot expert op het gebied van pentratietesten en daarop ook op gecertificeerd.
- Secura heb ik gekozen op basis van hun reputatie op codereviews. Zij hadden beperkt tijd en kunnen alleen de apps testen. Belangrijk bij hen is de inzet van (10)(2e), die een groot expert om anonimisering/pseudonimisering is.
- Radically Open Security heb ik gekozen op basis van hun reputatie. Zij hebben goede cryptografen in dienst en zijn sterk in het doen van codereviews. Zij testen de backend alsmede controleren zij het cryptodocument.
- Voor het opzetten van de backend server worden de procedurele zaken nog uitgezet. Er loopt via de Belastingdienst nog uitvraag bij de Audit Dienst Rijk om te checken dat aan die kant alles conform afspraken verloopt.
- Er komt nog een bugbounty als de app live is om eventuele oversights alsnog gekanaliseerd tot ons te krijgen.
- We gaan op de community leunen voor de open-sourcesoftware peer-review.

Is dit voldoende om nu verder te kunnen?

Nogmaals wil ik erop wijzen dat we dankzij Corona en de inschikkelijkheid van klanten van de betrokkenen partijen ruimte kunnen creeeren om bediend te worden. Als die Windows of Opportunity sluiten dan vrees ik dat de kwaliteitsborging een lastig proces wordt.

Met vriendelijke groet,

(10)(2e)

06- (10)(2e)

On 7/3/20 9:47 AM, (10)(2e) wrote:

> Weet even dat hier wel een enorme druk op staat. En er al andere partijen zijn afgehaakt in het heel pen-test traject.
>
> @ (10)(2e), Stuur jij die motivatie nog even naar (10)(2e)?
> Dank.
>
> (10)(2e)
> +316 (10)(2e)
>
> > On 3 Jul 2020, at 09:44, (10)(2e)
> > <(10)(2e)@minvws.nl> wrote:
> >
> > Ha (10)(2e),
> >
> > Ik ga deze in gang zetten. Echter, omdat dit een bedrag > (10)(1c) betreft moet e.e.a. via de HIS (Haagse Inkoop Samenwerking) verlopen. Om dit rechtmatig te kunnen doen heb ik nog een aantal aanvullende gegevens nodig, te weten:
> >
> > 1. De offerte-opvraag (mag afschriftje zijn van de door (10)(2e) uitgezette mail);
> > 2. Een motivering waarom voor deze partij (en niet voor andere partijen) is gekozen (graag iets meer inkleuring dan hieronder wordt gegeven);
> >
> > Parallel zal ik achter akkoord van (10)(2e) (10)(2e) aangaan, de administratieve afhandelingen doen en de dienstverleningsovereenkomst opstellen. Afhankelijk van de actiesnelheid door de HIS kan de overeenkomst aansluitend uit.
> >
> > Ik hoor graag,

Dank en groet,
(10)(2e)

-----Oorspronkelijk bericht-----
Van: (10)(2e) <(10)(2e)@icloud.com>
Verzonden: donderdag 2 juli 2020 08:17
Aan: (10)(2e)) <(10)(2e)@minvws.nl>; (10)(2e))
<(10)(2e)@minvws.nl>
CC: (10)(2e) <(10)(2e)>
Onderwerp: Graag offerte back en penetratie test laten tekenen.

Goedemorgen (10)(2e) en (10)(2e),

Kunnen jullie de ondertekening van bijgesloten offerte verzorgen.

De offset betreft de crypto en code review van de backend applicatie.

Prijs en activiteiten zijn marktconform.
(10)(2e) heeft nog wel (10)(1c) van de oorspronkelijke offerte af weten te krijgen :-
).
Deze nieuwe is de finale prijs.

Sturen jullie mij en (10)(2e) even een cc zodra deze is getekend?

Dank dank,

(10)(2e)
+316 (10)(2e)

--
Trek lessen uit andermans fouten. Luister iedere week de BNR-podcast 'De Onderzoeksraad der Dingen':
https://bnr.nl/onderzoeksraad