

**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) @minvws.nl]  
**From:** (10)(2e) (10)(2e) @minvws.nl]  
**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 handtekening 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 vertrouwenswekkend. 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