Gemeente Amsterdam

Evaluatie DUTO-scan Pilot

Auteur: Rick Scholten
Datum: 28-02-2019

Evaluatie DUTO-scan pilot

Een van de doelen van de pilot was het toetsen of de (vertaalde) DUTO-methodiek in de praktijk werkt en zodoende ook op andere gewenste (doel)applicaties/ werkprocessen kan worden toegepast. Om tot een antwoord op deze vraag te komen is er, tijdens het uitvoeren van de DUTO-scan, ook de tijd genomen om de methodiek te evalueren. In deze evaluatie werden zowel een aantal punten die betrekking hebben op de subvragen benoemd alsmede een aantal punten die meer slaan op de methodiek in z'n algemeenheid. De verbeterpunten en aanbevelingen die uit de scan zijn gekomen staan in een apart rapport beschreven[1].

De methodiek en opzet van de scan
In het onderzoeksvoorstel voor het uitvoeren van de pilot DUTO-scan is beschreven dat wij met verschillende rollen, zowel aan de beheerders als gebruikerskant, aan tafel wilden hebben. De gedachte hierachter was dat wij op deze manier gezamenlijk tot inzichten hoopten te komen hoe BlueDolphin zich als applicatie houdt tot de in het onderzoeksrapport opgestelde eisen en welke verbetermaatregelen er getroffen kunnen worden om de duurzame toegankelijkheid van de applicatie te optimaliseren. Door met zowel de beheerders als de gebruikers aan tafel te zitten was bovendien de business eveneens vertegenwoordigd tijdens de scan.

Het was een nieuwe ervaring om met verschillende rollen om de tafel te zitten. Tijdens het evalueren was iedereen het er echter anoniem over eens dat de DUTO-methodiek en de opzet door met verschillende rollen aan tafel te zitten van meerwaarde is. De deelnemers aan de scan gaven aan dat een bredere blik op de zaak werd geboden, waardoor zij op ideeën kwamen die ze anders niet bedacht zouden hebben. Het werd bovenal ook als een leerzame ervaring beschouwd om eens van elkaar te kunnen horen hoe er tegen bepaalde zaken wordt aangekeken. Dat de verschillende bloedgroepen, zowel aan de beheerders- als gebruikerskant, elkaar beter gaan begrijpen werd dan ook als een mooie bijvangst beschouwd.

Het uitvoeren van een DUTO-scan werd met name geschikt geacht voor applicaties waarvan het bekend is dat deze op de korte termijn vervangen zullen worden. De te vervangen applicatie zou in dit geval aan de opgestelde eisen kunnen worden getoetst middels het uitvoeren van een DUTO-scan. De uitkomsten/bevindingen die hieruit komen kunnen vervolgens worden gebruikt als input voor een programma van eisen (pve) voor een nieuwe applicatie.

Een aandachtspunt dat werd meegegeven is het toevoegen van een blanco stemoptie tijdens de individuele beoordeling van de applicatie in relatie tot de eisen. Deze beoordelingen hebben een meerwaarde als het gaat om het rangschikken van de eisen op basis van prioriteit. Ook geeft het een inzicht in eventuele verschillende beoordelingen tussen de verschillende rollen wat vervolgens weer een belangrijk aanknopingspunt kan zijn tijdens de discussie. Een punt van aandacht is echter dat, met betrekking tot bepaalde eisen, de kennis voor bepaalde rollen voor een weloverwogen beoordeling ontbreekt. Deze individuele beoordelingen wegen echter wel mee in de uiteindelijke beoordeling wat betreft de eisen die het meeste prioriteit verdienen tijdens de scan. Door een blanco stem aan de stemopties toe te voegen zal de impact van een individuele beoordeling minder groot zijn voor het vaststellen de uiteindelijk rangschikking (indien specifieke kennis voor een weloverwogen beslissing ontbreekt). Een andere aanbeveling wat betreft het rangschikken van de eisen is om de deelnemers tegelijk te laten stemmen (zonder dat ze dit van een ander

[1] Zie 'Aanbevelingsrapport DUTO-scan BlueDolphin'.

kunnen zien) zodat de deelnemers aan de scan niet door elkaar beïnvloed kunnen worden tijdens het beoordelen van de applicatie in relatie tot de opgestelde eisen.

De eisen en geformuleerde subvragen
Zoals beschreven in de introductie van dit rapport werden er ook een aantal punten benoemd die betrekking hebben tot de opgestelde eisen en de geformuleerde subvragen.

Een eerste opmerking heeft betrekking op het scherper formuleren van het doel/ de achterliggende gedachte van de eisen. Iets wat naar voren kwam tijdens de uitvoering van de scan was dat de verschillende rollen aan tafel soms een andere taal spreken. Eis 2 kan dit illustreren. De eis luidde: 'de informatie is vindbaar en beschikbaar'. De Information Security Officer beoordeelde deze eis als groen (BlueDolphin voldoet aan de eis) aangezien de applicatie technisch altijd beschikbaar is geweest en dat er geen storingen hebben plaatsgevonden. De informatiebeheerder die deelname aan de scan beoordeelde deze eis echter als rood (BlueDolphin voldoet totaal niet aan deze eis) aangezien heel veel velden in BlueDolphin simpelweg niet zijn ingevuld. Iets wat hier mee in verband staat is dat het onderscheid tussen gegevens (technische focus) en informatie (procesfocus) soms niet eenduidig was te herleiden aan de hand van de eisen. Een oplossing die werd geopperd om de eisen (en doelen) scherper te formuleren tijdens de uitvoering van een DUTO-scan is om deze eisen in de vorm van 'user stories' te formuleren.

Voor elke eis zijn ook enkele subvragen geformuleerd om een idee te geven aan wat voor zaken gedacht kan/ moet worden bij de invulling van de eis. Het is niet zo dat de geformuleerde subvragen in beton gegoten zijn en dat er op elke vraag een antwoord moet worden gegeven. De ene subvraag is voor de ene applicatie relevanter dan voor de andere. De subvragen zijn met name bedoelt om richting te geven aan de discussies tijdens de behandeling van de eisen. Wat dit punt betreft hebben de vragen ook hun meerwaarde bewezen tijdens de uitvoering van de DUTO-scan. Door met meerdere rollen aan tafel te zitten komt men er echter ook achter dat bepaalde vragen ontbreken, terwijl deze wel betrekking hebben op de duurzame toegankelijkheid van de applicatie. Zo kwam tijdens de evaluatie van de scan naar voren dat de subvragen uitgebreid kunnen worden. Tijdens de evaluatie werd onder andere geopperd dat:

- Subvragen uitgebreid kunnen worden met vragen over functionaliteit (business rules);
- Met betrekking tot eis 2 een subvraag kan worden toegevoegd over een audit trail.
- Enkele vragen over beveiligingsmaatregelen/ beheersmaatregelen omtrent vertrouwelijkheid (met name eis 5):
    - Aandacht voor AVG-eisen;
    - Aandacht voor autorisatiebeheer;
    - Aandacht voor de classificatie van informatie;
    - Aandacht voor het gebruik van wachtwoorden;
    - Functiescheiding: scheiding taken en verantwoordelijkheidsgebieden;
    - Beveiligingsmaatregelen die komen kijken bij externe inhuur indien er wordt gewerkt met data.