Maart 2009
Jaargang 13 Nummer 1

TestNet Nieuws

Vereniging TestNet p/a Diadeemstraat 91 1336 TT Almere
www.testnet.org secretris@testnet.org

Van de redactie

Door Meile Posthuma
tnn@TestNet.org

Ik weet niet of dit de all time dikste TNN is, maar over interesse voor het aanleveren van kopij hebben we de laatste tijd niet te klagen. Als redactie zijn we hier erg blij mee en met een vereniging van ongeveer 1600 leden verwachten we ook wel een beetje dat onze leden interessante testverhalen uit de praktijk aan ons aanleveren. Zo staan er in deze TNN verhalen over het elektronisch patiënten dossier, batch testen, boekrecensies van drie boeken en zijn er twee nieuwe bestuursleden. Dat houdt in dat er ook twee bestuursleden afscheid hebben genomen, maar hier leest u alles over in het stuk van onze voorzitter.

In dit nummer

Van de redactie	1
Van de voorzitter	1
Van de secretaris	2
Van de penningmeester	2
Onvolwassen en volwassen gedrag botsen	3
De dag van…	4
Werkgroep Testdata (in oprichting)	7
Werkgroep ISO 29119 (in oprichting)	8
IREB Requirements certificatie: ervaring van een cursist	9
Privacy en elektronisch patiëntendossier (EPD)	11
Thema-avond: requirements	13
Security testen met UTOPIA	14
5 Vragen aan…	19
Batch testen bij SoZaWe Gemeente Rotterdam	20
Boekrecensie: TestFrame	23
Boekrecensie: Succes met requiements	24
Boekrecensie: Testen 2.0	25
Evenementen	26

Van de Voorzitter

Door Bob van de Burgt
voorzitter@TestNet.org

Bestuurswisselingen

Op de afgelopen ALV zijn twee nieuwe leden tot het bestuur van TestNet toegetreden. Rob Baarda heeft de rol van penningmeester op zich genomen. Met zijn ervaring vanuit de kascontrolecommissie en de jarenlange bijdrage aan ons vakgebied ben ik zeer verheugd Rob in het bestuur te mogen verwelkomen. Huib Schoots zal zich op de werkgroepen gaan storten. Hij heeft zeer veel bestuurservaring bij diverse verenigingen en heeft zijn sporen in het testvak ruimschoots verdiend. Ik wens Rob en Huib zeer veel succes en plezier in hun nieuwe rol. Ik wil gelijk van deze gelegenheid gebruik maken om de twee afgetreden bestuurleden in het zonnetje te zetten. Hans van Loenhoud is op 7 mei 2000 toegetreden tot het bestuur van TestNet in de rol van 2e voorzitter en 2e penningmeester. In de verenigingjaren 2002/2003 en

Colofon

Redactie
Hylke ten Cate
Hans van Loenhoud
Meile Posthuma
Johan Vink
tnn@testnet.org

Bestuur

Bob van de Burgt	Voorzitter
Rob Baarda	Penningmeester
Meile Posthuma	Informatievoorziening & Beheer
Huib Schoots	Marktverkenning & Werkgroepen
Michiel Vroon	Vice-voorzitter, Evenementen & Thema-avonden
Bart Watertor	Secretaris, 2e penningmeester,

2003/2004 heeft hij als voorzitter de kar getrokken. Vanaf mei 2004 heeft hij zich met volle overgave op de functie van secretaris voor de vereniging gestort. Een van de hoogtepunten van Hans was zijn initiatief tot en het trekken van ons lustrumboek 10 jaar TestNet. Een welverdiende kroon op zijn werk voor de vereniging. Han Toan Lim is op 27 juni 2002 toegetreden tot het bestuur van TestNet in de rol van penningmeester. Een taaie klus die Han Toan al die jaren uitstekend heeft geklaard. Bezoekers van onze ALV herinneren zich allemaal zijn uitgebreide verhandelingen over de begrotingen en het financiële reilen en zeilen van onze vereniging. Binnen bestuursvergaderingen was Han Toan altijd tot in de puntjes voorbereid en hield hij de rest altijd scherp. Ik wil Hans en Han Toan bedanken voor hun tomeloze inzet voor TestNet en de vele en prettige bijdragen die zij vanuit het bestuur voor de vereniging hebben geleverd.

Van de Secretaris

Door Bart Watertor
secretaris@TestNet.org

In de vorige TNN heb ik maatregelen aangekondigd om de ledenadministratie soepeler te laten verlopen. Inmiddels kan ik berichten dat we met ingang van 1 januari de ledenadministratie hebben ondergebracht bij A Solution in Tiel. Door de groei die onze vereniging heeft doorgemaakt de laatste 2 jaar, is een professionelere aanpak van de administratie noodzakelijk geworden. In A Solution menen wij een partij te hebben gevonden die ons daarin kan ondersteunen.

Eveneens hebben we de procedures rondom het lidmaatschap herbezien en waar nodig aangepast. Momenteel zijn deze procedures bij het bestuur in review waarna deze van kracht zullen worden. De procedures zullen ook op de website worden gepubliceerd, zodat alle leden hier kennis van kunnen nemen.

Ondertussen groeit onze vereniging door. Ook in de eerste maanden van 2009 hebben we, ondanks de financiële crisis, al weer flink wat nieuwe aanmeldingen binnengekregen. We zien verenigingsjaar 2009 dan ook vol vertrouwen tegemoet.

Van de penningmeester

Door Rob Baarda
penningmeester@TestNet.org

De vorige penningmeester Han Toan Lim heeft na zeven jaar deze post verlaten om zich meer op zijn in de laatste jaren grotere gezin te kunnen storten. Hij heeft goed op het geld gepast en laat een rijke vereniging achter, waarvoor dank.

Mijn interesse voor de rol als penningmeester komt voort uit een enorme belangstelling voor het testvak en voor getallen: financiën en metrieken. In de afgelopen jaren was ik actief betrokken bij de TestNet werkgroep testmetrieken. Ik werk als testconsultant bij Sogeti, ben daar vaak bezig met vakontwikkeling en al vanaf het begin lid van TestNet. Regelmatig was ik kascommissielid en heb daardoor alle penningmeesters bewust mee gemaakt. Amsterdam is de woonlocatie tezamen met mijn vriendin Angelien.

De laatste tijd is TestNet enorm gegroeid en dat heeft impact op de financiën. De begroting voor dit jaar is ca 150k euro en is sluitend voor het normale verenigingsleven. Door enkele eenmalige posten, zoals de overgang van administratiekantoor en mogelijk een nieuwe website, zal worden ingeteerd op het relatief grote eigen vermogen.

Onvolwassen en volwassen gedrag botsen

Door Rik Marselis
rik.marselis@sogeti.nl

Midden februari was het negenjarige meisje Nujoud in het nieuws. Haar vader had haar uitgehuwelijkt aan een 27-jarige man. De reden was dat haar vader moest besparen en dus de kosten voor zijn kind verminderde door het kind uit te besteden.
Al snel bleek echter dat het meisje en haar echtgenoot niet goed samen konden leven. Ze hadden verschillende verwachtingen van het leven. Waar dat meestal in persoonlijke drama's eindigt trok deze Nujoud de stoute schoenen aan en ging naar de rechter om haar huwelijk te laten ontbinden. Blijkbaar maakte het optreden van de negen-jarige zo'n indruk dat ook gelijk het uithuwelijken in Jemen strafbaar gesteld is.

Waarom deze inleiding? Wel, het deed me denken aan de regelmatige mislukkingen van outsourcing en/of offshoring.
Ook daar wordt vaak om oneigenlijke redenen, zoals kostenbesparing, gekozen voor uitbesteden. En ook daar gaat het vaak mis. Al pleit ik er niet voor om outsourcing en offshoring te verbieden.
Wat echter wel voor mij als een paal boven water staat is dat de reden waarom het vaak mis gaat, erg lijkt op de situatie van Nujoud.

De betrokken organisaties hebben namelijk vaak een zodanig groot verschil in volwassenheid dat hun verwachtingen niet op elkaar aansluiten. Een CMMi-level-5 organisatie (bijvoorbeeld in India) verwacht namelijk een dergelijk niveau van documentatie en van procesmatig werken dat een CMMi-level-1 organisatie (bijvoorbeeld in Nederland) daar niet aan kan voldoen. Met als gevolg wederzijdse miscommunicatie, verwarring en irritatie, wat uiteindelijk vaak leidt tot een "scheiding".

HOE VOORKOM JE DAT?

Door organisatie, communicatie en industrialisatie.
Aan de kant van de CMMi-level-1 organisatie kun je door het anders (beter) organiseren vaak al een hoop winnen. Daarnaast moet je zorgen voor duidelijke communicatielijnen. Bijvoorbeeld "single point of contact" aan beide zijden, zodat de miscommunicatie tot een minimum beperkt raakt. En door een duidelijke aanpak van wederzijdse aanlevering van requirements enerzijds en gereed product anderzijds kun je ook het proces zodanig industrialiseren dat de communicatiebehoefte vanzelf minder wordt.
Natuurlijk weet ik ook wel dat dit allemaal niet op één dag geregeld is. Maar ach, een kind wordt ook niet op één dag volwassen. Al lijkt het in het geval van Nujoud toch wel dat haar

gedwongen huwelijk haar aangezet heeft tot zeer volwassen gedrag voor een meisje van 9!

Wil je meer over de verschillen in volwassenheid van bedrijven en hun uitbestedingpartijen weten of daarover van gedachten wisselen laten we daar dan in TestNet verband "een boom over opzetten".

PS. vind jij kostenbesparing wel een 'eigenlijke' reden, overweeg dan eens het volgende: outsourcing en offshoring zijn lange termijn beslissingen, daar moet je niet onder druk van kostenbesparing toe besluiten, het moet uit je bedrijfsstrategie voortkomen.

De dag van…

Door Paul Beving
paulbeving@kpnplanet.nl

Pensioen-GAT gedicht

Om tien voor zeven gaat de wekker en ik heb nog tien minuten voor het opstarten van mijn biologische database om het radionieuws van zeven uur te kunnen bevatten. Kort na zevenen dwarrelt de melding de slaapkamer binnen dat, na de Noordpool, nu ook Antarctica aan een door de mensheid opgelegde afslankingsoperatie bezig is. Ondanks het vroege tijdstip stel ik fluks vast dat daar maar één reactie op mogelijk is: ik moet mijn testinstinct zo spoedig mogelijk aanwenden voor een bijdrage aan een beter klimaat. Ik besluit daartoe om de diverse paden van huis naar kantoor te testen op CO2-neutraliteit. Het is mij direct duidelijk dat enkele paden voor testen in aanmerking komen, omdat die slechts leiden tot onwenselijk systeemgedrag in de vorm van een trage verwerking of zelfs uitval van het gehele systeem op lange termijn. Voor het testen van het enig overblijvende pad heb ik een uitstekende tool beschikbaar: het stalen ros dat is uitgerust met diverse hightech onderdelen.

De aanloop

Gegeven het pad per fiets (dat helaas niet geheel samenvalt met het fietspad) van Amsterdam-Oost naar -West kan ik opnieuw kiezen uit verschillende paden. Het lijkt zo eenvoudig: open de tool Google Maps versie fiets, kies voor de kortste afstand en klaar is Kees. Maar nee, er zijn nog enkele risicocriteria die ik in het fietsplan moet opnemen om ervoor te zorgen dat ik efficiënt en zonder kleerscheuren op de werkplek kom.

Uiteraard denk ik dan allereerst aan het minimaliseren van het aantal stoplichten. Die vormen weliswaar geen inbreuk op de effectiviteit van het geselecteerde pad, maar zorgen wel voor een trage verwerking door het systeem en dus voor een onnodig lang verblijf op het kritieke pad. Als tester weet je dat je dan om problemen vraagt.

Een ander risico is de batchverwerking van de enorme groep lotgenoten die,

net als ik, heeft gekozen voor een pad dwars door het hart van de stad. Met een stress test van de vele kruisingen zou ik kunnen aantonen dat Amsterdam over nog veel meer black spots beschikt dan de gemeente Amsterdam eerder zelf heeft vastgesteld.

En last but zeker not least: het risico van humeurige AJoO's ofwel Amsterdamse Juffrouwen op Omafiets. Ja, die kunnen hun woon-werktraject 's morgens letterlijk én figuurlijk dromen. In een gedwee tempo tonen ze geen begrip voor de gedegenheid van mijn testwerk. Als ik ietwat lijk te treuzelen bij een beslispunt zijn de reacties niet voor de poes.

Andere risico's die mineur van aard zijn, werk ik niet verder uit en neem ik dan ook niet op in het plan. Hierbij valt te denken aan de uiterlijke verschijningen van het weerbarstige klimaat, klussende vuilnis- en bestel-wagens, een door vorst beschadigd wegdek of een matineuze, doch nog steeds motorisch gestoorde junkie. Amsterdam holadijee!

Bij het naderen van mijn bestemming krijg ik het tevreden gevoel dat ik het tot nu toe beter heb gedaan dan de fabriekspijpen in het Westelijk havengebied: 9,75 kilometer in 32 minuten met negen stoplichten, anderhalve AJoO en… een minimum aan uitstoot.

Tot zover het CO_2-testtraject, waarvan de inhoud van het bevindingenrapport zich laat raden.

HET WOUD VAN AFKORTINGEN

Als ik op kantoor aankom moet ik nog denken aan mijn eerste werkweek. Door de bijzondere vorm van het gebouw verdwaalde ik nogal eens wat tot gevolg had dat ik voor enkele paden een exploratory test moest uitvoeren. Ofwel: er volgden enkele individuele, onvrijwillige bedrijfsrond-leidingen van paden zonder testmaat.

Op mijn werkplek merk ik meteen dat ik deze dag bepaald niet alleen zal zijn. Terwijl ik mij nog moet installeren, hebben de functioneel beheerders op de afdeling de e-mails in de inbox van de groep allang doorgeakkerd, twee testcollega's wekken bij mij de indruk dat zij al uren aan de slag zijn, terwijl de testcoördinator er juist een traditie van maakt om de laatste lege plek aan het blok te bezetten. Overigens zit ik aan een blok met uitsluitend 'externen'; ik ben de enige vaste medewerker in een gezonde mix met luitjes van SysQa en Sogeti.

De afdeling waar ik werk zorgt voor de ontvangst van alle documenten die werkgevers aanleveren voor de premieafdracht en pensioenopbouw van hun werknemers. Dit document komt binnen via een webapplicatie of een e-mail en loopt een massa van controles door. Als het bericht is goedgekeurd, wordt het vastgelegd in de database. Uiteraard houdt het systeem rekening met klanten die foutieve gegevens aanleveren. Vaak leveren ze te weinig premie aan en elke werknemer ziet natuurlijk graag dat zijn werkgever geen zooitje van zijn pensioen maakt. Daarom voeren de testers een gebruikersacceptatietest (GAT) en een productieacceptatietest (PAT) uit, nadat in de teststraat al een systeemtest en functionele acceptatie-test (FAT) is uitgevoerd. Tijdens mijn studie voor TMap Next was het verschil

tussen een FAT en een GAT mij niet zo duidelijk, maar dat is nu wel anders. Je gaat op de stoel van een gebruiker zitten en probeert het systeem als het ware te saboteren. De processen zijn zo complex dat je bevindingen, ondanks de eerder uitgevoerde FAT, een vérstrekkend effect kunnen hebben. Een gebruiker-buiten-het-systeem heeft niet in de gaten dat zijn aangeleverde gegevens door een woud van afkortingen worden geleid. Een tester moet ook daarin zijn weg weten te vinden.

HACKER

Voor het uitvoeren van de GAT had ik voor mezelf de opdracht geformuleerd: hoe kan ik de front-end controles omzeilen die de webapplicatie voor de klant standaard uitvoert bij de invoer van gegevens? Ik wil namelijk de controles testen die dieper in het systeem zijn opgenomen en daarvoor kan ik die front-end controles even niet gebruiken. In deze rol voel ik me meteen als een echte hacker, iemand die het systeem probeert te saboteren, zij het op een constructieve manier. Gelukkig heb ik een nachtje kunnen slapen over dit probleem, want een oplossing voor een goede aanpak komt niet zomaar na een treuzelig kwartiertje uit de lucht vallen. Om de gedachten wat gemakkelijker te bepalen, zou een schema zeer welkom zijn. In de functionele ontwerpen (FO's) tref ik echter geen grafische weergave aan van de processen en dus moet ik zelf de opeenvolgende stappen in kaart brengen. Gewoon tekenen en kijken waar ik een document kan vinden dat ik op de een of andere manier kan 'vervalsen' en op de juiste plaats in het systeem kan brengen. Al vrij snel is het mij duidelijk dat ik het door de klant aangeleverde document ergens in het systeem moet brengen, maar dan met 'vervalste' gegevens. Top! Het zoekproces dient wel met enkele loopjes naar de drankautomaat afgewisseld te worden. En als een greep naar de drank geen uitkomst biedt, is er nog de LHBO (laatste hulp bij onduidelijkheden): de testcoör-dinator.

VERGADERTIJGER

Als tester zit ik natuurlijk niet de hele dag achter een beeldscherm allerlei TMap-trucjes toe te passen. In de middag heb ik een intake voor een FO, dat slechts een onderdeel is van de vele werkprocessen die binnen het bedrijf bestaan. In zo'n sessie komen de rollen binnen het welbekende V-model bij elkaar: een projectleider, een bouwer, een informatieanalist ('een FO'er'), een FAT-tester en een GAT-tester. Het FO heb ik van tevoren gescreend op beslispunten en op de wijzigingen ten opzichte van de vorige versie. Ieder doet zijn zegje over het FO en er wordt een klein verslag gemaakt dat iedereen een uur later in zijn mailbox terugvindt.

Als ik terugkom op de afdeling heb ik een overleg met de testcoördinator en de andere testers. De testcoördinator heeft al weer de volgende klus op stapel staan: er is eind april een release gepland en daar moet een testtraject voor worden opgezet. Het is duidelijk dat van de testers opnieuw wordt verwacht waar zij goed in zijn: dat zij even snel een GAT doen. De testcoördinator heeft het gehele testproces van eind april teruggerold naar het heden en dan blijkt dat er bij een gestructureerde werkwijze

voldoende tijd zou moeten zijn voor een gedegen test.

De finale test

Het loopt al tegen half zes en ik pak mijn biezen en mijn stalen ros. De fabriekspijpen van Amsterdam-West doen het nog steeds erg goed. Het CO_2-pad had ik al getest en ik hoef mij dus geen zorgen te maken over de risico's. De dag sluit ik af met het kijken naar een reportage die het televisiejournaal losjes de woonkamer inslingert. Het gaat over het testen van een door Nederland ondersteund laboratorium op Antarctica. In de hoofdrol: Z.K.H. prins Willem-Alexander, H.K.H. prinses Máxima en testmaat-3, Zijne Excellentie Ronald Plasterk. De test blijft niet beperkt tot de ijsdikte voor een alternatieve Elfstedentocht. Er worden ook nog wat screenshots vastgelegd, zodat rond de tijd dat prinses Amalia haar rijbewijs bij het CBR kan ophalen, niet kan worden beweerd dat we het niet wisten.

Werkgroep Testdata (in oprichting)

Door Marco den Haan, Edwin van Vliet
marco.den.haan@logica.com en
edwin.van.Vliet@yacht.nl

Eindelijk werken met wettelijk geoorloofde testdata?

Je bent op het gebied van testen gestructureerd en professioneel bezig. Je werkt zorgvuldig en volledig volgens een gerenommeerde testmethodiek, hebt een testplan, de testtechnieken zijn geselecteerd en van daaruit is met behulp van een gereviewde testbasis een perfect test script opgesteld. Nu wil je gaan testen en daarvoor is testdata een vereiste.

Het organiseren van testdata in de backend systemen, zodat je kunt testen, is op zich al een uitdaging. Om dan ook nog rekening te houden met de privacy wetgeving, "Dat is toch gewoonweg onmogelijk!".

In Nederland hebben wij de WBP, Wet Bescherming Persoonsgegevens, die bepaalt wat wel en niet mag met gegevens die betrekking hebben op personen en daarmee paal en perk stelt aan het gebruik ervan. Ook voor ons als testgemeenschap is deze wet van belang; deze zou moeten dienen als uitgangspunt voor de data die wij gebruiken om mee te testen. De wet stelt onder meer dat een gegeven niet herleidbaar mag zijn naar een persoon. Duidelijke voorbeelden hiervan zijn een bankrekening, een BurgerServiceNummer (BSN), een naam als Jan Peter Balkenende. Echter ook een combinatie van postcode en huisnummer is in principe herleidbaar naar een persoon. Zijn alle testers nu criminelen?

Op deze manier lijkt het wel of je eigenlijk helemaal geen testdata kunt gebruiken, maar niets is minder waar. Een door een bank niet uitgegeven bankrekeningnummer, een vrij BSN of een combinatie van postcode en huisnummer die niet bestaan, zijn voorbeelden van gegevens die niet herleidbaar zijn naar een persoon.

Misschien is dit wel makkelijker gezegd dan gedaan: "Een niet bestaande combinatie van postcode en huisnummer", "Een BSN dat niet gekoppeld is aan een persoon". Dit zijn basisgegevens die landelijk geregeld horen te zijn. Als tester wil je

gewoonweg een lijst met testdata die je kunt gebruiken. Bestaan er geen BurgerServiceNummers voor testdoeleinden die iedereen zou kunnen gebruiken?

De TestNet werkgroep 'Testdata' gaat dit probleem aanpakken. Deze werkgroep heeft ten doel om een set "niet persoonsgebonden basisgegevens" op te leveren waar we vanuit de TestNet gemeenschap mee kunnen testen. Hiervoor zoeken wij TestNeters die mee wil denken op het gebied van testdata, liefst mensen die connecties hebben met uitgevende instanties (denk aan banken & verzekeraars, Equens, het ministerie van Binnenlandse Zaken, de belastingdienst, etc.). Ben je een dergelijk persoon en ben je geïnteresseerd in deelname aan een werkgroep op dit terrein, stuur dan een mail naar werkgroepen@testnet.org.

We nodigen je dan binnenkort uit voor een kick-off om de opzet, werkwijze en invulling van de werkgroep verder uit te werken.

Werkgroep ISO29119 (in oprichting)

Door Hans van Loenhoud
werkgroepen@TestNet.org

ISO / IEC 29119 Software Testing is een nieuwe internationale standaard die momenteel wordt ontwikkeld door de internationale ISO Werkgroep 26. Het doel van dit project is het produceren van een internationale standaard voor software testen die betrekking heeft op de gehele levenscyclus van software testen, in de analyse, het ontwerp, de ontwikkeling en het onderhoud van een software product of systeem.

Deze nieuwe ISO-norm, die volgens planning in mei 2012 ingaat, zal bestaan uit vier delen:

Concepten & begrippen

Test Proces

Test Documentatie

Test Technieken

De standaard vervangt een aantal bestaande IEEE- en BSI-normen voor software testen:

IEEE 829 Test Documentation

IEEE 1008 Unit Testing

BS 7925-1 Vocabulary of Terms in Software Testing / NEN 7925-1 woordenlijst van termen in Software Testing

BS 7925-2 Software Component Testing / Standard NEN 7925-2 Software Component Testing Standaard

Voor meer info zie www.softwaretestingstandard.org.

ISO Werkgroep 26, met de bekende testguru Stuart Reid als trekker, is bezig met het ontwikkelen van deze standaard en heeft inmiddels een aantal concepten opgesteld.

Als leidende Nederlandse testorganisatie wil TestNet uiteraard betrokken zijn bij het tot stand komen van deze nieuwe standaard. Wij staan in nauw contact met Stuart Reid en krijgen alle concepten ter review toegestuurd. Om een zo breed mogelijk draagvlak voor de nieuwe norm te creëren wil

TestNet deze review organiseren in de vorm van een werkgroep.

De werkgroep krijgt de concepten vanuit de ISO organisatie rechtstreeks aangeboden en zal per concept één of twee keer bijeenkomen om het review commentaar op te stellen en nieuwe voorstellen voor de norm aandragen. De geschatte doorlooptijd van de werkgroep is ruim een jaar. Naast de nauwe interactie met ISO zal de werkgroep ook tussentijds werken aan kennisverspreiding binnen TestNet, via TNN en op thema-avonden en/of evenementen.

Voor deze werkgroep zoeken we nog enkele nieuwe leden. Gezien de complexiteit van de materie denken we vooral aan senior testers met brede kennis van standaards en ruime ervaring in het vakgebied van software testen en kwaliteit. Heb je belangstelling voor dit deel van ons vak en zin en gelegenheid om aan de ontwikkeling ervan jouw eigen bijdrage te leveren, laat dat dan weten via een mailtje werkgroepen@TestNet.org.

IREB Requirements Certificatie; ervaring van een cursist ….

Door Peter van Delft

Wat is IREB?

Binnen het vakgebied Requirements Engineering is een aantal jaren geleden de International Requirements Engineering Board (IREB) opgericht (www.certified-re.de). IREB is een internationale non-profit organisatie die zich richt op het verdere professionaliseren van het vakgebied. (Vergelijkbaar aan ISTQB op het gebied van testen.) Binnen IREB zijn onder andere requirements engineering experts zoals Chris Rupp en Suzanne Robertson actief. IREB heeft een certificatieprogramma ontwikkeld voor Requirements Engineering onderverdeeld in een drietal niveaus: Foundation, Advanced en Expert. Improve Quality Services is in Nederland geaccrediteerde tot het verzorgen van de cursus “Certified Professional for Requirements Engineering Foundation level” die volledig voldoet aan de eisen zoals deze door IREB zijn vastgesteld. De cursus behandelt zowel de internationale terminologie als standaarden, technieken en methoden ten aanzien van Requirements Engineering en Requirements Management.

Persoonlijke motivatie

Als doelgroep voor het volgen van een opleiding- en certificeringtraject zoals IREB denk je waarschijnlijk primair aan mensen uit het vakgebied waar die requirements daadwerkelijk opgesteld worden: de Informatie Analisten, Business Analisten, etc. Maar waarom zou deze training ook niet zeer geschikt kunnen zijn voor mensen uit de discipline die controleert in hoeverre die requirements ook correct opgesteld en geïmplementeerd zijn: het testen? Zelf vind ik in ieder geval dat ik uitstekend tot de doelgroep gerekend kan worden; vandaar dat ik deze IREB-training dan ook ben gaan volgen. Als testprofessional ben ik al ruim 10 jaar actief in het testvak en merk ik als externe medewerker bij diverse bedrijven steeds vaker dat er serieuzer ingezet wordt op het

verhogen van de kwaliteit 'aan de voorkant'. Vanuit het testvak roepen we al lang dat juist daar grote winst te behalen valt. Recent heb ik nog een opdracht vervuld als 'Testcoördinator Voortraject', waarbij er expliciete aandacht (vooral vanuit test) geschonken moest worden aan de specificatiefase, omdat het product daarna in een outsourcing traject 'verdween' om een hele poos later weer 'boven te komen'. Er zijn dan ook allerlei redenen te bedenken waarom juist ook daar zwaar op de kwaliteit van het 'Voortraject' in te zetten.

De opleiding

Maar goed, ik heb deze training nu dus gevolgd en het examen afgelegd. Hoe was dat nu, een 3-daagse training in het opstellen van requirements volgens de IREB-standaard? Mijn belangrijkste persoonlijke doelstelling was om na de cursus beter in staat te zijn om requirements te valideren en beter inhoudelijke feedback te kunnen geven. Aan dat persoonlijke doel is zeker invulling gegeven. De cursus is gebaseerd op de IREB-syllabus. Die geeft aan wat er binnen de context van de cursus besproken moet worden en wat er als bekend verondersteld wordt, voorbereidend op het examen en dus het kunnen behalen van het IREB Certificaat. Daarnaast is de cursus flink gevuld met aanvullende informatie, welke niet (altijd) expliciet in de syllabus wordt vermeld, maar vooral invulling geeft aan de praktische toepasbaarheid van de theorie. Binnen de cursus wordt middels een doorlopende case het hele traject van het (in 1e instantie al brainstormend) verkrijgen van requirements tot het stapsgewijs zorgvuldiger uitwerken en uiteindelijk reviewen van de requirements doorlopen. Hierbij wordt er geoefend met o.a.:

het bepalen welke stakeholders een rol spelen;

welke communicatietechnieken toegepast kunnen worden om de gewenste informatie helder te krijgen;

wat voor type requirements er zijn en hoe die te beschrijven;

het vastleggen van delen van de verkregen informatie dmv. hiervoor geschikte modelleringtechnieken.

Denk hierbij aan (grotendeel op UML gebaseerde) technieken als Use Case diagrammen, State Transition-, Activity en Sequence diagrammen, Class diagrammen en Entity Relationship Models. Ook het onderwerp 'Requirement Management Tools' komt aan de orde.

Het examen

Het afsluitend examen aan het einde van de derde dag is een 75 minuten durend multiple-choice examen, waarbij er veelal vragen zijn uit de categorie 'kies uit de gegeven mogelijkheden de 2 juiste antwoorden' en 'gerelateerd aan de beschreven case, geef van de beschreven stellingen aan of ze juist of onjuist zijn'. In totaal bestond het examen (in mijn geval) uit 45 vragen, met daarbinnen de nodige subvragen. Het examen was door alle examenkandidaten binnen de tijd af te ronden, maar wel met het gevoel dat het flink doorwerken was.

En nu nog even afwachten of ik het certificaat behaald heb…. (ik heb er al een plekje voor gereserveerd boven mijn bed…☺)

Privacy en elektronisch patiëntendossier (EPD)

Door Hylke ten Cate
tnn@testnet.org

Met het elektronisch patiëntendossier (EPD) kunnen zorgverleners medische gegevens uitwisselen. In 2009 wordt een groot deel van de huisartsenposten, huisartspraktijken, apotheken en ziekenhuizen aangesloten op het landelijk EPD.

De wettelijke verplichting voor deze zorgaanbieders om aan te sluiten op het EPD gaat waarschijnlijk begin 2010 in, afhankelijk van de wetsbehandeling door de Eerste en Tweede Kamer.

Het is belangrijk dat zorgverleners veilig en betrouwbaar relevante medische gegevens met elkaar kunnen delen. Dat maakt de kans op medische fouten kleiner en ondersteunt de samenwerking tussen artsen beter.

EERST TOESTEMMING VOOR INZAGE

Zorgverleners mogen uw medische gegevens alleen inzien als er een behandelrelatie is én het nodig is voor uw behandeling. Bovendien moet uw zorgverlener altijd eerst toestemming vragen voor inzage. Huisartsen, apotheken en specialisten kunnen via het EPD alleen gegevens inzien over de door de apotheker verstrekte medicatie. Huisartsen op de huisartsenpost kunnen een samenvatting van het dossier van uw huisarts raadplegen. Andere zorgverleners, zoals fysiotherapeuten, psychologen, bedrijfsartsen of zorgverzekeraars, kunnen uw gegevens niet inzien.

ICT-EISEN

Vanaf najaar 2008 zal het landelijk elektronisch patiëntendossier (EPD) geleidelijk aan breed worden gebruikt. De goede werking van het landelijk EPD is aangetoond door pilots die in de voorgaande periode hebben plaatsgevonden. Gegevensuitwisseling via het landelijk EPD vindt plaats op basis van het burgerservicenummer (BSN). Zorgaanbieders mogen het BSN vanaf 1 juni 2008 gebruiken. Dat is de datum waarop de Wet gebruik BSN in de zorg (Wbsn-z) in werking is getreden. Een jaar daarna is het gebruik van het BSN verplicht.

Een zorgaanbieder mag het landelijk EPD alleen gebruiken als zijn informatiesysteem aan de eisen voor een goed beheerd zorgsysteem (GBZ) voldoet. Dit betekent onder andere dat zijn zorginformatiesysteem XIS-type gekwalificeerd is. En voor het gebruik van netwerkdiensten een zorg service provider wordt gebruikt. Op deze manier is veilige en betrouwbare gegevensuitwisseling gewaarborgd.

De beide certificaten worden afgegeven door het NICTIZ. NICTIZ is het nationale knooppunt en kenniscentrum voor ICT en innovatie in de zorg.

Ook is op internet te vinden een programma van eisen voor een goed beheerd zorgsysteem. Ongetwijfeld maakt dat document deel uit van de testbasis.

http://www.infoepd.nl/ufc/file2/informatiepunt_sites/bethlehemha/8ece4c0334911dad208e1dd87b7334a8/pu/AORTA_BI_GBZ_PvE_Programma_van_Eisen_GBZ.pdf.

Toegang voor de patiënt tot het EPD

Om de patiënt meer regie te geven over de zorg die hij nodig heeft, maakt het programma 'Toegang voor de patiënt tot het EPD' het mogelijk dat de patiënt op termijn via elektronische weg zijn eigen medische gegevens kan inzien. Met toegang tot het elektronisch patiëntendossier (EPD) kan de patiënt bovendien zelf controleren waar gegevens over hem liggen opgeslagen, voor welke zorgverleners zijn gegevens beschikbaar zijn en wie wanneer welke gegevens over hem heeft ingezien.

Het programma realiseert voorzieningen voor toegang voor de patiënt tot zijn elektronisch patiëntendossier. Een groep softwareleveranciers en patiënten zullen deze voorzieningen uitgebreid testen, voordat ze in het hele land beschikbaar komen.

Privacy is belangrijk en daarom worden hoge eisen gesteld aan een veilige uitwisseling van medische gegevens. Met toegang tot het EPD kan de patiënt zelf controleren waar gegevens over hem liggen opgeslagen, voor welke zorgverleners zijn gegevens beschikbaar zijn en wie wanneer welke gegevens over hem heeft ingezien.

De patiënt kan bezwaar maken tegen inzage in zijn gegevens en gegevens voor zorgverleners laten afschermen. In de toekomst kan de patiënt zelf, zo mogelijk elektronisch, de toegang tot de eigen gegevens instellen. Zorgverleners dienen de patiënt dan eerst goed voor te lichten over de risico's van het afschermen van gegevens.

Daarnaast kan de patiënt in de toekomst in een zelfzorgdossier gegevens toevoegen, muteren of verwijderen. Een zelfzorgdossier kan belangrijke informatie bevatten voor zorgverleners. Een diabetespatiënt kan dan bijvoorbeeld voor zorgverleners zijn bloedsuikerwaarden elektronisch beschikbaar maken.

Privacy

Vooral problemen in de relationele of psychische sfeer zullen patiënten beperkt toegankelijk willen hebben. Normaal gesproken zal een chirurg daar niet in geïnteresseerd zijn. Een internist zal van een diabetes patiënt misschien wel willen weten, of er reden tot stress is. Die kan van invloed zijn op de bloedsuikerspiegel. Moet een apotheker een overzicht hebben over het medicijngebruik? Bij Viagra is de diagnose bekend, maar het is ook een bloeddrukverlagend middel, dat invloed kan hebben op andere medicijnen. Kan een patiënt zelf aangeven, welke gegevens hij voor slechts een deel van de zorgverleners toegankelijk wil hebben?

Testen van de systemen

Het zal zeer interessant zijn de systemen, die hiervoor ontwikkeld worden te testen. De testbasis ligt gedeeltelijk al via internet op straat. Hoe zullen uiteindelijk de eisen voor afscherming van gegevens komen te luiden? Hoe groot is het gevaar van lekken? Is na te gaan, of iemand vrijwillig inlogt?

Thema-avond Requirements

Door Hylke ten Cate
tnn@TestNet.org

Op dit drukbezochte evenement waren een tweetal duo-presentaties over requirements.

Eerste duo-presentatie

Als eerste spraken Johan Zandhuis en Jan-Jaap Cannegieter van SysQA. Zij hadden het over de mogelijkheden voor testers om de requirements te beïnvloeden.

Met cartoons toonden ze aan, dat vage requirements tot vage en onbedoelde resultaten leidden.

Requirements moeten eerst ontwikkeld worden, daarna gevalideerd en ten slotte gemanaged. De verantwoordelijkheid schuift tussen start en einde project van business naar realisatie. In de loop van de tijd moet ook de concreetheid van requirements toenemen.

Idealiter komt de tester al bij de validatie van requirements in beeld. Dan kan de correctheid van de requirements al worden beoordeeld en een beeld gevormd van acceptatiecriteria en benodigde handleidingen. Door opstellen van een prototype kan inzicht gegeven worden in het vermoedelijke eindproduct op basis van de beschikbare requirements.

Aan goede requirements moeten een tiental eisen gesteld worden. Zo moeten ze een nummer, eigenaar en prioriteit (MoSCoW) hebben; ze moeten consistent zijn met andere requirements; ze moeten meetbaar zijn en mogen dus geen vage termen bevatten.

Als de requirements goed zijn opgesteld volgens bovenstaande eisen, volgt de verificatie met management en inhoudelijke reviews, walkthroughs en inspecties. Met de verificatie begint eigenlijk al het testen. 70% van de fouten ontstaat immers door slechte requirements.

Het gaat er dus om de projectmanager ervan te overtuigen, dat dit proces tijd en geld bespaart en uiteindelijk diens status zal verhogen. De meeste winst is te behalen door fouten direct uit de requirements te halen. Bij niet gevonden fouten op requirements worden de herstelkosten hoger naarmate het langer duurt voordat een fout gevonden wordt (Boehm).

Tweede duo-inleiding

Als tweede duo spraken Ruud Harreman en Appie Pries van Qquest. Zij hadden het over het proces om van requirements tot software te komen en daarmee ook tot een teststrategie.

Business use cases moeten afgeleid worden van het verwerkingsproces. Als voorbeeld gaven ze offertetraject voor een leaseauto. Die applicatie moet snel en betrouwbaar werken, waarbij snel

en betrouwbaar precies zijn gedefinieerd.

De opdrachtgever zal meer valideren; de leverancier meer verifiëren. Zo'n proces begint met review van requirements en business use cases.

Vervolgens wordt een product risico analyse opgesteld. Hierbij wordt voor elk productonderdeel en elke business use case een viertal getallen bepaald: frequentie en impact voor de business evenals foutkans en complexiteit voor de techniek. Die getallen worden paargewijs vermenigvuldigd en opgeteld. Vervolgens wordt bepaald welke productonderdelen bij welke business user case horen. Dat levert een matrix.

Aan elk requirement zullen kwaliteitsattributen moeten worden gekoppeld.

Bij de overdracht van de realisatie naar de leverancier en bij ontvangst van het product is verificatie nodig.

Security testen met UTOPIA

Ad Keijzer
ad.keijzer@logica.com

ISA heeft al bijna tien jaar een product voor het testen van security, genaamd UTOPIA, waarvan ondergetekende product manager is. Voorafgaand aan de introductie van het product UTOPIA, zal ik eerst vertellen wat security precies inhoudt.

Security gaat over het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Deze drie kwaliteitsattributen zijn de pijlers van security of informatiebeveiliging:

Vertrouwelijkheid is de eigenschap dat informatie niet beschikbaar gesteld wordt aan ongeautoriseerde individuen, entiteiten of processen;

Integriteit is de eigenschap van het juist en de volledig zijn van informatie;

Beschikbaarheid is de eigenschap van het beschikbaar en bruikbaar zijn van informatie op het moment dat een geautoriseerde entiteit toegang vraagt.

Deze definities zijn afkomstig van de internationale standaard ISO 27000. ISO 27000 is een familie van standaarden over information security management systems (ISMS). Wanneer je dit vergelijkt met de kwaliteitsattributen zoals gedefinieerd in ISO 9126, zie je dat security een van de subattributen is van het hoofdattribuut functionaliteit. Security wordt nog wel eens gezien als een niet-functionele eigenschap; dit is dus niet terecht. De definitie van beschikbaarheid (ISO 27000) lijkt enigszins op het hoofdattribuut betrouwbaarheid (ISO 9126). De beide competences zullen wel een andere benadering kiezen bij het testen van dit kwaliteitsattribuut, zoals ik later met voorbeelden zal laten zien.

Nu we weten wat security betekent, kunnen we ons gaan verdiepen in het testen ervan. Maar laten we eerst even stilstaan bij de definitie van testen (enigszins verkort), volgens ISTQB. Testen omvat alle activiteiten rond de evaluatie van softwareproducten om aan te tonen dat ze aan de gespecificeerde eisen voldoen, dat wordt voldaan aan de doelstelling en om fouten op te sporen. In het volgende zal ik de verschillen en

overeenkomsten met security testen duidelijk maken. Wanneer ik security testen/tester (m/v) bedoel schrijf ik het ook zo. In alle andere gevallen alleen testen/tester (m/v).

Bij testen ligt de nadruk sterker op gespecificeerde eisen en doelstellingen, terwijl bij de security testen de nadruk sterk ligt op het opsporen van fouten en wel die fouten waarbij de vertrouwelijkheid, integriteit en/of beschikbaarheid van informatie in het geding komt. Uiteraard kunnen de gespecificeerde eisen ook security aspecten bevatten. Bijvoorbeeld authenticatie en autorisatie zijn vaak functionaliteiten die wel degelijk gespecificeerd zijn. Een voorbeeld hiervan is dat als je niet bent ingelogd als beheerder, je ook geen beheeractiviteiten mag kunnen uitvoeren. En vanzelfsprekend dienen deze zaken ook altijd getest te worden. Bij testen wordt security zeker niet uitgesloten, maar dat bleek ook al uit ISO 9126.

Bij het testen van security ligt de grootste uitdaging bij de niet gespecificeerde functionaliteit en vooral wanneer dit kan worden uitgebuit door kwaadwillige personen. En dat is waar de focus bij het testen van security ligt, het aantonen van gaten in de beveiliging. Ik illustreer dit met een eenvoudig voorbeeld.

Een tester test een verzekerings-applicatie en controleert of twee verschillende typen accounts de juiste rechten hebben in de applicatie. Account A heeft weinig rechten en mag alleen nieuwe aanvragen invoeren. Hiervoor wordt naast de inlogfunctionaliteit nog maar één andere knop in het hoofdscherm getoond. Account B heeft veel rechten en mag ook verzekeringen wijzigen en verwijderen. Naast de knoppen van account A, worden nog de knoppen wijzigen en verwijderen getoond.

Een tester gaat dit als volgt testen. Allereerst wordt er getest of de knoppen aanwezig zijn bij de juiste rechten; account A mag niet de knoppen hebben van account B. Account B moet alle knoppen hebben. Daarnaast controleert de tester of met het klikken op de knop de juiste schermen geopend worden. Naast syntactische controles is hiermee dit deel van de test afgelopen. De functionaliteit is aanwezig en werkt correct.

De security tester begint nu. De vraag is of de autorisaties te omzeilen zijn. Hoe kan een gebruiker met account A toch de functionaliteit gebruiken van account B? De tester ontdekt dat de ontwikkelaars van de applicatie alleen de knoppen wijzigen en verwijderen onzichtbaar hebben gemaakt in het account met minder rechten.

De tester logt eerst in met account B en klikt op de knop verwijderen. Hierna zet hij de URL die verschijnt in de URL-balk op zijn klembord. Daarna logt hij uit en logt hij in met account A. Hij heeft nu een sessie opgezet met het account met weinig rechten. Vervolgens plakt de tester de opgeslagen URL in de URL-balk. Het blijkt dat de applicatie dit niet afvangt en account A de handelingen kan uitvoeren van account B.

Dit is zoals vermeld een simpel voorbeeld. Een tester zou ook het omzeilen van autorisaties kunnen testen, zijn opdracht sluit dat immers niet uit. Een security tester zal na

vastgesteld te hebben dat het lijkt alsof autorisaties correct worden toegepast, direct op zoek gaan naar mogelijkheden voor misbruik. Hij zal zich verder niet bekommeren om het correct functioneren van de knoppen. En dit is pas het begin, want daarna zal de security tester trachten alle andere beveiliging te doorbreken en op zoek gaan naar zo veel mogelijk kwetsbaarheden in de software of de infrastructurele bouwstenen waaruit het testobject is opgebouwd. Omdat het onmogelijk is te weten of alle kwetsbaarheden in een testobject zijn opgespoord, zal na verloop van tijd de security test gestopt moeten worden. Wanneer dat is hangt af van de beschikbare testtijd en de professionele inschatting van de security tester. De 80/20 regel is ook hier vaak van toepassing. Het aan het licht brengen van alle publiek bekende kwetsbaarheden is beslist een haalbare kaart. Onder een publiek bekende kwetsbaarheid wordt een kwetsbaarheid verstaan waarvan bestaan is aangetoond en waarover, al dan niet gedetailleerd, is gepubliceerd.

Voor security testen is specifieke kennis over beveiligingsmethoden onontbeerlijk, bijvoorbeeld cryptografie. Als je iets wilt breken moet je weten hoe het werkt. Als laatste kenmerk van security testen noem ik het toepassen van tooling. Er zijn erg veel tools beschikbaar voor het testen van security, commercieel dan wel vrij verkrijgbaar. Dit kunnen exploit tools zijn, die gericht zijn op direct misbruik van kwetsbaarheden (die daarom ook door hackers worden gebruikt) of assessment tools die (potentiële) kwetsbaarheden alleen aantonen. Het kunnen inzetten van de juiste security tools is een waardevolle vaardigheid van de security tester.

Een security tester moet denken als hacker. Dit betekent onbetreden paden inslaan, regels breken en grenzen verkennen. Een gestructureerde security testaanpak en een uitgebreide verzameling tools helpen natuurlijk ook. Daarom heeft ISA voor het testen van security het product UTOPIA ontwikkeld. Dit product zal nu worden geïntroduceerd.

WAT HOUDT HET PRODUCT UTOPIA IN?

UTOPIA staat voor Universal Technical Organisational Procedural Internet Assessment. Het product is ontwikkeld als security assessment – zowel vanuit een technische, als organisatorische invalshoek – voor een breed scala aan informatiesystemen:

- Webapplicaties;
- Web servers en andere netwerk servers;
- Besturingssystemen;
- Databases;
- Netwerkcomponenten als firewalls en routers;
- (Wireless) netwerken.

UTOPIA is ontwikkeld in 2000 en is sindsdien voor ongeveer 40 verschillende klanten ingezet, zowel eenmalig als in abonnementsvorm.

Afhankelijk van de wens van de klant biedt UTOPIA twee producten:

- Vulnerability assessment;
- Penetration test.

Bij een vulnerability assessment worden de kwetsbaarheden in een informatiesysteem geïdentificeerd en het risico van de kwetsbaarheden geclassificeerd. Een vulnerability assessment levert dus alleen een

overzicht van aangetroffen kwetsbaarheden. Een stap verder gaat een penetratietest, want hierbij worden kwetsbaarheden vanuit de positie van een potentiële hacker bekeken en daadwerkelijk uitgebuit. Een penetratietest levert proof of concept dat de ontdekte kwetsbaarheden uitgebuit kunnen worden en is hiermee overtuigender dan een vulnerability assessment.

Aan het eind van de opdracht wordt voor de klant een rapport opgesteld waarin de bevindingen beschreven worden. Onderdeel van de rapportage is een schatting van het risico van de in het testobject geïdentificeerde kwetsbaarheden. Het risico van een kwetsbaarheid is afhankelijk van de (business) impact die misbruik van de kwetsbaarheid kan hebben en de waarschijnlijkheid dat dit zal optreden. Vanzelfsprekend wordt in de rapportage ook beschreven wat de klant kan doen om de kwetsbaarheden te verhelpen.

AANPAK

Het testen bij UTOPIA verloopt gestructureerd en kan in de volgende fasen worden onderverdeeld:

FASE 0:

Onderling afspreken van de aanpak. Zaken die in deze fase worden vastgelegd zijn scope, testtijdstippen, testmethoden (vulnerability assessment of penetratietest, white box of black box, wel of geen denial-of-service attacks) en contactpersonen bij beide partijen;

FASE 1:

Passief onderzoek: Hierbij worden passieve methoden – methoden die niet door de organisatie onder test kunnen worden opgemerkt – ingezet. Een voorbeeld van een dergelijke methode is de “Google Hacking Database”;

FASE 2:

Actief onderzoek: Actieve methoden kunnen wel worden opgemerkt door de eigenaar van het testobject, bijvoorbeeld door Intrusion Detection Systems of door analyse van log files. Methoden die hier ingezet worden zijn bijvoorbeeld port scanning, vulnerability scanning en web crawling.

FASE 3:

Analyse: In deze fase wordt de informatie die in de onderzoeksfasen is vergaard geanalyseerd. Onderdeel van deze fase is het raadplegen van externe bronnen over kwetsbaarheden (en bijbehorende exploits), zoals SecurityFocus en Secunia.

FASE 4:

Penetratie: Hierbij worden de kwetsbaarheden die zijn ontdekt uitgebuit om – afhankelijk van de afspraken met de klant – aan te tonen dat vertrouwelijke informatie kan worden blootgelegd, informatie op de site kan worden gewijzigd of onbeschikbaar gemaakt.

FASE 5:

Rapportage: Bevindingen en aanbevelingen worden op schrift gesteld en aan de klant aangeboden.

Bij het penetratietesten vormen tools een belangrijke aanvulling op de vaardigheden van de testers. Dit

kunnen tools zijn waarvoor licentiekosten verschuldigd zijn, maar uiteraard worden ook veel vrij verkrijgbare "hack" tools gebruikt, bijvoorbeeld de network mapper Nmap. Een tool die al verscheidene jaren gebruikt wordt is WebInspect van HP (voorheen van SPI Dynamics). WebInspect is een geautomatiseerde test tool voor webapplicaties. Omdat geautomatiseerde tools voornamelijk de meer fundamentele kwetsbaarheden detecteren, blijft handmatig testen noodzakelijk. Ontwerpfouten bijvoorbeeld, zijn lastig te detecteren met tools.

KWETSBARE WEBAPPLICATIES

De laatste jaren blijken onze klanten vooral geïnteresseerd te zijn in technisch assessment van webapplicaties. Webapplicaties zijn wijdverbreid; welke organisatie heeft geen site of web-portal via welke diensten worden aangeboden aan klanten, medewerkers of partners. Een hack van een website kan erg schadelijk zijn, zeker voor het vertrouwen en de reputatie van de organisatie. Over dit soort gebeurtenissen is regelmatig te lezen in de media. Volgens een rapport van Gartner (Now is the Time for Security at the Application Level) van eind 2005 vindt 75% van de hacks van websites plaats via de webapplicatie (de rest via infrastructuurcomponenten, zoals netwerk, database of server). Er is geen reden om aan te nemen dat dit percentage tegenwoordig lager zou moeten zijn. De applicatie is verreweg het meest kwetsbare onderdeel van een site of web portal. Hoe komt dat?

Webontwikkelaars geven functionaliteit meestal veel meer aandacht dan security. Security wordt vaak gezien als "iets van die andere afdeling" of wat achteraf nog even moet worden gedaan. Webapplicaties worden ook regelmatig gewijzigd en worden vaak niet onderworpen aan grondige tests gedurende de software development life cycle. Kortom, genoeg momenten waarop kwetsbaarheden de webapplicatie kunnen binnensluipen. Aan wat voor kwetsbaarheden moet je dan denken?

Om een idee te krijgen van kwetsbaarheden in webapplicaties werkt een bezoek aan de site van OWASP (www.owasp.org) verhelderend. OWASP (The Open Web Application Security Project) is een open community die zich tot doel heeft gesteld organisaties te helpen bij het ontwikkelen en onderhouden van webapplicaties die veilig zijn. Een van de projecten van OWASP is het Top 10 Project, die een ranglijst bijhoudt van de meest voorkomende kwetsbaarheden in webapplicaties. Ik zal de "winnaar" en nummer 2 eens nader toelichten:

NUMMER 1:

Cross Site Scripting (XSS). Deze kwetsbaarheid treedt op wanneer een applicatie door gebruikers aangeleverde data accepteert en dit naar de browser stuurt zonder validatie. XSS stelt een hacker in staat scripts uit te voeren in de browser van het slachtoffer, waardoor bijvoorbeeld sessies kunnen worden gekaapt.

Nummer 2:

Injectie. Kwetsbaarheden met betrekking tot injectie, waarvan SQL injectie de bekendste is, komen veel voor. SQL injectie gebeurt wanneer door gebruikers aangeleverde data direct, zonder filtering, worden doorgestuurd naar de database en daar als SQL commando kunnen worden uitgevoerd. De aanvaller is dan in staat via de browser databasecommando's te geven en zo data op te vragen of te wijzigen.

Dat SQL injectie zoveel voorkomt bewijzen verschillende berichten in de media van de laatste maanden waar melding werd gemaakt van massale SQL injectie aanvallen. Deze aanvallen hadden tot doel malware te "implanteren" in websites om bezoekers van die websites mee te infecteren (drive-by downloads). De massaliteit (het gaat hier over duizenden geslaagde aanvallen) kan worden verklaard doordat via Google eerst een groot aantal (potentieel) kwetsbare sites werden geïdentificeerd, waarna geautomatiseerd de malware-implantaties werden uitgevoerd.

Business cases

Klanten kiezen er meestal voor te testen vlak voordat een webapplicatie live gaat. Maar uiteraard is het veel verstandiger security assessments uit te voeren tijdens de gehele software development life cycle. Verscheidene klanten sloten een abonnement af, wat als voordeel heeft dat security regelmatig getest wordt. Security assessments blijven momentopnamen tenslotte. Dat security assessments noodzakelijk blijven bewijzen ook de cijfers. Volgens hetzelfde rapport van Gartner heeft in 2009 80% van de bedrijven een security incident gehad met betrekking tot webapplicaties.

Als je meer wil weten over security testen, neem dan gerust contact op.

5 vragen aan…

Door: ing. René Menninga
R.Menninga@cimsolutions.nl

Ik vind testen een leuk vak want…

Ik vind testen een leuk vak want het is veelzijdig. De dynamiek van het testen zorgt voor uitdagingen die professioneel opgelost dienen te worden. Je hebt te maken met diverse partijen zoals de klant, eindgebruikers, ICT medewerkers in verschillende rollen, eventueel een externe leverancier. Dit vergt dat je als tester op verschillende wijze met deze partijen moet communiceren en hierbij een goede relatie behoudt, ook als de boodschap die je te melden hebt minder positief is. Daarnaast ben je bezig om de kwaliteit van het product, dat we met zijn allen realiseren, inzichtelijk te maken. Dit resulteert in een advies om het product al dan niet op te leveren. Is het product opgeleverd aan de klant, dan kan het voorkomen dat de klant toch nog een ernstig incident meldt waardoor deze de hoogste prioriteit krijgt en geanalyseerd moet worden. Vaak wordt

de tester bij de eerste analyse betrokken. Het geeft mij voldoening om te zien dat de kwaliteit van het product gedurende het project steeds beter wordt.

Het grootste misverstand over testen is…

Het grootste misverstand over testen is dat het pas aan het eind van een project aan bod komt. Indien de ontwikkelfase uitloopt wordt vaak bespaard op de testfase door de testperiode in te korten. De einddatum van de oplevering is een gegeven en blijft staan. Als tijdens het testen blijkt dat het product niet aan de requirements voldoet, krijgt de tester "de schuld" toegewezen. De tester wordt verantwoordelijk gesteld voor de eventuele uitloop (foutherstel periode) of dat de klant het product met problemen ontvangt (advies van de tester om niet op te leveren wordt niet opgevolgd). Dit heeft gevolgen voor de relatie met de klant (en eindgebruikers). Dit misverstand komt wel steeds minder vaak voor omdat bedrijven beseffen dat testen belangrijk en noodzakelijk is. Een goede relatie met de klant wekt vertrouwen en zorgt voor continuïteit. Er wordt geïnvesteerd in testen.

Over 5 jaar zie ik mijzelf in de functie van…

Over 5 jaar zie ik mijzelf in de functie van ervaren testconsultant of testcoördinator. Of dit in een industry-omgeving of in een business-omgeving is maakt me niet zo veel uit. Ik vind beide omgevingen interessant en een testmethode (bijv. TMap Next, ISTQB) kun je in beide omgevingen toepassen. Echter bij het toepassen moet je er wel rekening mee houden dat elke omgeving zijn specifieke eigenaardigheden heeft. Ook lijkt het me leuk om eens aan een project in het buitenland (bijv. Azië) te werken.

Een tester moet zeker beschikken over de vaardigheid of kennis om…

Een goede tester dient te beschikken over een combinatie van vakinhoudelijke kennis en persoonlijke vaardigheden. Met vakinhoudelijke kennis is de tester in staat om: requirements te beoordelen op testbaarheid, een testontwerp te realiseren op basis van requirements. De tester dient communicatief vaardig, kritisch, nauwkeurig en flexibel te zijn.

Bij communicatie met een andere partij dient de tester het behoud van een goede relatie in acht te nemen, zowel bij positief als minder positief resultaat. Bij veranderingen in het project dient de tester snel om te kunnen schakelen en eventuele gevolgen, met betrekking tot het testtraject, in kaart te brengen.

In de toekomst hoop ik dat binnen het test vakgebied is veranderd, omdat…

Ik hoop dat in de toekomst het imago van het test vakgebied naar de buitenwereld toe verder toegenomen is. Nog vaak wordt testen gezien als iets wat saai en dom werk is. De tester krijgt vaak het stempel als een lastig persoon want hij/zij heeft altijd wel ergens een opmerking over. Op zich is dit goed, want daarvoor ben je tester. Echter door ook de zaken te benoemen die wel goed gaan verdwijnt dat stempel voor een groot deel en wordt de tester van toegevoegde waarde

gezien. Het resultaat is dat er meer van de opmerkingen van de tester wordt opgepakt.

IK GEEF DE VRAAG DOOR AAN …, OMDAT…

Ik geef de vraag door aan Jaap Boumans, omdat ik veel van hem heb geleerd gedurende de periode dat ik met hem heb samengewerkt. Jaap heeft veel ervaring in het test vakgebied en ik hecht waarde aan zijn mening.

Batchtesten bij SoZaWe, Gemeente Rotterdam

Door Dew Persad
persad@inqa.nl

Nieuw bij SoZaWe

De sociale dienst SoZaWe van de gemeente Rotterdam heeft op 1 januari met succes een nieuw uitkerings-systeem voor de bijstandswet e.d. in gebruik genomen. Aan dit nieuwe systeem zijn ongeveer 55 batch-processen gekoppeld. Deze moeten uiteraard allemaal een keer getest worden.

RISICO'S

De introductie van een nieuw uitkeringssysteem kent een paar nachtmerrie scenario's:

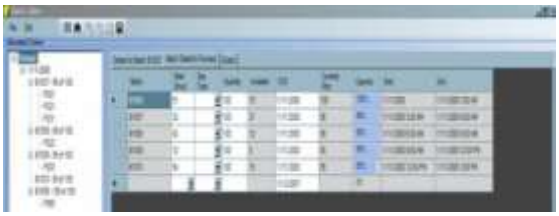
Tienduizenden uitkeringsgerechtigden die hun geld niet op tijd ontvangen

Duizenden verkeerde aanmaningen verstuurd

Miljoenen euro's teveel betaald aan een derde partij

U ziet het voor u: grote krantenkoppen, boze klanten, miljoenen schade.

Genoeg redenen dus om het testen zeer serieus op te pakken.



EEN BATCH? WAT IS DAT?

Een gegooglede definitie: "A batch job is […] a sequence of commands to be executed by the operating system which is listed in a file (often called a batch file, command file, or shell script) and is submitted for execution as a single unit."

De batch queue van SoZaWe, een sequentiële reeks van batches, is gescheduled om te draaien na kantoortijd. Alle batches leveren per batchrun een logfile en verschillende outputbestanden op zoals XML-bestanden, duizenden brieven of acceptgiro's, betaalbestanden, etc.

SOCRATES

Zo heet het nieuw geïmplementeerde uitkeringssysteem van SoZaWe Rotterdam. Het is een bestaand systeem dat al tien jaar in gebruik is in Den Haag en As-Is werd overgenomen. Hier was dus sprake van een pakket-implementatie waarin naast een omvangrijke en complexe dataconver-sie met name de stuurdata moest worden ingericht; ook moesten de procesinstructies voor de medewerkers aangepast worden. Daarnaast is er een tiental nieuwe batchprocessen aangemaakt.

BATCHTESTEN BIJ SOZAWE

Het testen van de batchprocessen maakt onderdeel uit van de Ketenintegratietest (KIT) die op haar beurt weer onderdeel uitmaakt van de ProductieAcceptatieTest (PAT). Het batchtesten vereist een multi-disciplinair team met expertise op het gebied van de technische infra-structuur, database, ontwikkeling, testen en de business processen. Binnen het reguliere testteam was er een speciaal batchtestteam samen-gesteld.

HARDE DEADLINE

De deadline was onverbiddelijk. Per 1 januari moesten ongeveer 40 van de 55 batchprocessen in productiegenomen worden. De overige 15, het jaarwerk, zijn pas na de "Go Live"-datum opgeleverd en hoefden voorlopig niet te worden getest. Veel batches maken onderdeel uit van koppelingen met externe systemen zoals die van Equens, ING, de Belastingdienst, Eneco, etc. Het testen van deze batches vergde extra aandacht vanwege de specifieke formats die de externe partijen gebruiken.

We hebben de deadline – just in time! – gehaald. Tijdens de PAT hebben we alle te testen batches in de testomgeving kunnen draaien en valideren. Na de Go-Live hebben we vervolgens een proefrun gedraaid op basis van een halve dag mini-productie op 2 januari. En tenslotte hebben we de eerste 'echte' batches, met name het aanmaken van het betaalbestand, nog eens onder het vergrootglas gelegd alvorens de output door te sturen. Alles OK!

COMPETENTIES

Om te kunnen batchtesten moet je:

- het desbetreffende business proces door en door kennen om de juiste input te genereren
- precies weten wat de batch hoort te doen
- een dekkende testset aanmaken om de batch zowel technisch als functioneel end-to-end te testen; zo'n testset bestaat niet uit één, maar uit een hele, vaak samenhang-ende, reeks van testgevallen.

PFFFF…

Stel je voor dat je, net als het mij overkwam, onderstaand format van een outputbestand met 360 records ter analyse voor je neus gedrukt krijgt.

```
00472320500091312120010030000000000

00232080870091462220010033310012 00

..

00535089240092391450010021470351 51
```

Je begrijpt dat het even zweten was om te achterhalen of er iets fout aan was. Via internet kon ik uiteindelijk achter-halen dat hier onder andere klantcodes, datums en bedragen moeten staan. Met die informatie konden we vervolgens de vergelijking met de database maken.

OUTPUT ANALYSE

De output beoordelen is een verhaal op zich. Als je, net als wij bij SoZaWe, gebruik maakt van uit productie afgeleide testdata (dus met tien-duizenden testgevallen), is het vaak

onmogelijk om een exacte output-voorspelling te maken. Output analyses richten zich op vergelijking met vorige batchruns, op steekproeven en op het oordeel van gebruikers over waarschijnlijkheden.

Als er indicaties worden gevonden van mogelijke problemen moet er geanalyseerd worden of:

- de input correct was
- de juiste batch parameters waren meegegeven bij het triggeren van de batch
- welk deel van de technische infra-structuur het probleem zich voordoet
- welk deel van de uitkeringsappli-catie en welk deel van de database geraakt wordt door de batch.

BATCHTESTEN MEER DAN TESTEN

Vooral de diepgaande multidisciplinaire kennis, vereist bij het batchtesten, maakt de benodigde expertise erg schaars. Als je het reguliere testen zou kunnen vergelijken met het lopen van een marathon, dan is batchtesten gelijk aan een triatlon. Bijzonder uitdagend dus en zeer geschikt voor ervaren testers om hun kennis zowel in de breedte als diepte uit te bouwen.

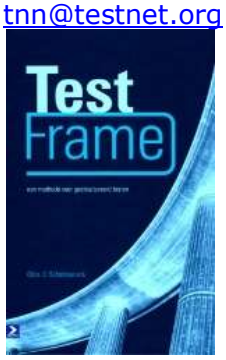
ER WAS EENS…

Batchprocessen zijn er geweest vanaf het begin van het ICT-tijdperk en zullen er zeer waarschijnlijk tot het eind nog blijven bestaan evenals het batchtesten zelf. Doordat er vaak ketenintegratieaspecten een rol spelen is de complexiteit groot en de expertise schaars. Over de toekomst hoeft de batchtester zich dus geen zorgen te maken.

Boekrecensies:

TestFrame
Een methode voor gestructureerd testen

Door Hans van Loenhoud
tnn@testnet.org



Uitgeverij: *Academic Service*
ISBN-nummer: *978-90-12-12596-3*
Auteur(s): *Chris C. Schotanus e.a.*

'Jemig, een echt boek!' Dat schoot als eerste door mijn hoofd toen ik het nieuwe TestFrame boek in handen kreeg gedrukt. Bijna 10 jaar geleden was de eerste druk een paperback van bijna 200 pagina's; deze nieuwe, geheel herziene 4e druk heeft er een harde kaft, een professionele uitstraling en ruim 100 bladzijdes bijgekregen. En dat niet alleen: in de eerste versie was TestFrame 'een praktische handleiding bij het testen van informatie systemen' en nu luidt de ondertitel 'een methode voor gestructureerd testen'. Dat klinkt een stuk volwassener!

Na korte inleidingen in testen en TestFrame leidt het boek de lezer stap voor stap door de TestFrame aanpak: van testclusters via testcondities naar testgevallen en dan door naar test-uitvoering en testautomatisering om tenslotte in hoofdstuk 8 uit te komen bij overdracht en beheer. Het boek is

sterk praktijkgericht en bevat vele voorbeelden die rechtstreeks uit allerlei TestFrame projecten zijn geabstraheerd.

Dat is de kracht en tegelijkertijd de zwakte van het boek. De kracht zit hem in de praktijkgerichtheid en de herkenbaarheid van de voorbeelden. Wie dit boek leest voelt de 15 jaar praktijk die er achter zit; ziet direct hoe je met 'actiewoorden' fysiek testgevallen kunt beschrijven.
De zwakte heeft te maken met de diversiteit. Doordat de gehanteerde voorbeelden geen duidelijke relatie met elkaar hebben, raakt de lezer al snel verdwaald in het actiewoordenbos. De tekst onderwijst 1:n relaties tussen clusterkaarten, testclusters, testcondities en testgevallen. Het zou zo prettig zijn geweest als je die als lezer in de voorbeelden zou hebben kunnen terugvinden.

Maar helaas, consistentie is niet de sterkste kant van dit boek. Ik voel me daarom niet zo aangesproken door de nieuwe subtitel van TestFrame 'een methode voor …'. Wat mij betreft is het nog steeds 'een praktische handleiding bij …'.

Wie behoefte heeft aan inzicht, overzicht en samenhang in het testvak, oftewel wie uitkijkt naar een testmethode, kan beter een ISTQB-cursus gaan volgen.

Wie op zoek is naar een heldere aanpak om fysieke testgevallen eenduidig en herbruikbaar vast te leggen is bij TestFrame aan het goede adres, zeker als deze testgevallen via een testtool moeten worden uitgevoerd.

Succes met de requirements

Door Meile Posthuma

tnn@testnet.org

Uitgeverij:	*Academic Service*
ISBN-nummer:	*978-90-12-12598-7*
Auteur(s):	*Martin Arendsen, Jan Jaap Cannegieter, Arno Grund, Petra Heck, Serge de Klerk, Johan Zandhuis*

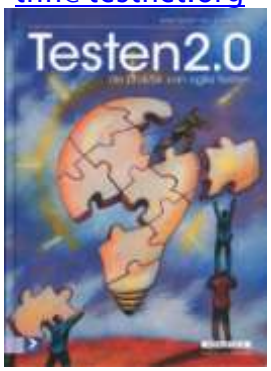
Zes auteurs, drie van SysQA, twee van Logica en één van LaQuSo, zijn erin geslaagd om een toegankelijk boek te schrijven over een toepasbare aanpak van requirement ontwikkeling, requirement validatie, requirement management en requirement levenscyclusbeheer. Op een gestructureerde wijze wordt het gehele proces in kaart gebracht. Natuurlijk worden de verschillende typen requirements uitgelegd, maar vooral wordt er aandacht besteedt aan de verschillende technieken om requirements af te leiden en te beschrijven. Één van de technieken die zeer waardevol is voor de requirement analist is de interactiematrix. Deze matrix zorgt ervoor dat de analist kan zien of er overlap, inconsistenties dan wel conflicten tussen de requirements bestaan. Verder wordt er de nodige aandacht besteedt aan requirement validatie waarbij aandacht wordt besteedt aan de attributen en eisen van requirements. Maar ook de technieken die gebruikt kunnen worden voor

valideren. Requirement management besteedt aandacht aan de manier van vastleggen en natuurlijk aan de traceerbaarheid. Naast deze basiszaken wordt er door de auteurs ook aandacht aan het implementeren van requirements binnen een organisatie besteedt via een implementatiemodel. Voor wie met requirements wil beginnen is dit boek een mooi startpunt.

Testen 2.0

Door Meile Posthuma

tnn@testnet.org



Uitgeverij:	*Academic Service*
ISBN-nummer:	*978-90-12-12580618*
Auteur(s):	*Anko Tijman, Eric Jimmink*

Testen 2.0 is een leuk en interessant boek om te lezen. Zelf ben ik opgegroeid met gestructureerde aanpakken als TMap en TestFrame en dan is het alleen al leuk om de agile vaktaal te lezen. Agile lijkt een dolle beestenboel, want ik ben termen als chicken en pig tegengekomen. Dit zijn natuurlijk metaforen die staan voor teamleden die niet of zijdelings aan het product werken of juist wel aan het product werken. Anko en Eric zijn erin geslaagd om het testen binnen agile projecten goed voor het voetlicht te brengen. Eerst wordt de context van agile beschreven, waarin de verschillende agile methoden de revue passeren als Scrum, eXtreme Programming, RUP en niet te vergeten Lean. Vervolgens wordt er beschreven hoe het testen binnen een agile omgeving plaats vindt, welke normen en waarden er gelden en natuurlijk de principes van testen 2.0. Wat blijkt uit deze principes, dat de klant altijd gelijk heeft, dat testen een teamsport is en dat we vroeg en vaak moeten testen. In het boek wordt uitgebreid in gegaan op de praktijk en de methodische inbedding. Naast de agile valkuilen en de testproblemen binnen een agile team, is er ook aandacht voor het toepassen van agile technieken binnen de traditionele testmethoden als TMap en RRBT en TestFrame, waarbij de laatste twee volgens de auteurs beter geschikt zijn voor een agile aanpak dan de eerste. Ook de rol van de tester komt uitgebreid aan bod. Communicatie met de klant, feedback geven en ontvangen, persoonlijke vaardigheden, attitude en vakkennis komen allemaal aan bod. Achterin het boek staan allerlei bijlagen die je kunnen helpen als je met agile testen aan de slag wilt gaan. Zeker de ‘Definition of Done’is een belangrijke bijlage, want door het gehele boek loopt deze als een rode draad. Hier heb ik zelf ook nog wel wat vragen over, die ik met Anko en Eric zou willen bespreken. Lezen dit boek.

Al onze thema-avonden en voor- en najaarsevenement in 2009 worden gehouden in:

Plaats:	*Gebouw:*	*Informatie:*
Nieuwegein Blokhoeve 1, 3438 LC	NBC	Aanmelden uiterlijk 3 werkdagen van te voren via onze website www.testnet.org of E-mail: evenementen@testnet.org

Thema-avond TestNet
Model Based Testen
maandag
27 april
18:00 – 22:00 uur

Najaarsevenement TestNet
dinsdag
22 september
13:00 – 22:00 uur

EuroSTAR mini-event
donderdag
28 mei
18:00 – 22:00 uur

Thema-avond TestNet
dinsdag
27 oktober
18:00 – 22:00 uur

Thema-avond TestNet
Testen van pakketten
maandag
21 december
18:00 – 22:00 uur

Voorjaarsevenement
maandag
22 juni
13:00 – 22:00 uur

Thema-avond TestNet
dinsdag
24 november
18:00 – 22:00 uur

Evenementen & Thema-avonden E-mail: evenementen@testnet.org
Cees Dulfer
Erik Hendrikx
Jan-Kees Glijnis
Ine Lutterman-Baars
Rik Marselis
Michiel Vroon