Maart 2006

Nieuwsbrief van de vereniging TestNet

TNN

Van de redactie

Door Meile Posthuma
tnn@testnet.org

TestNet Nieuws biedt u deze keer een hoop variëteit. Artikelen over acceptatiecriteria in Erik's Column, ketentesten, monitoring en control op uitbestede werkzaamheden en zelfs een artikel dat software testen geen mensenwerk zou zijn. Verder lopen we een dagje mee met Peter Mourik en beantwoord Riny Nieuwhoff 5 vragen. Maar zeker niet minder interessant voor de testgemeenschap; hoe staat het nu met gestructureerd tes ten? Maar natuurlijk niet de belangrijke TestNet-zaken vergeten, want 5 april hebben we de ALV en het voorjaarsevenement. Kom allen!

In dit nummer

Van de voorzitter

Door Bob van de Burgt
voorzitter@testnet.org

Op 5 april a.s. zal voorafgaand aan het voorjaarsevenement de Algemene Leden Vergadering (ALV) van TestNet gehouden worden. Dit is het moment voor de leden om invloed uit te oefenen op de richting van de vereniging. De vereniging is immers van ons allemaal. Buiten de terugblik op 2005 en de planning voor 2006 zal de mogelijke invoering van een nieuw systeem voor bedrijflidmaatschap op de agenda staan. De laatste maanden bereikt ons steeds meer het verzoek voor bedrijflidmaatschappen met mogelijkheden voor staffelkortingen bij grote aantallen leden. Dit is natuurlijk een onderwerp waar verschillende meningen over bestaan en alleen de ALV over kan beslissen. Het bestuur zal tijdens de ALV hiervoor een voorstel indienen. Jullie mening wordt zeer op prijs gesteld.

Na de ALV zal het voorjaarsevenement beginnen. Het thema van dit evenement is: "Testen van Security". Een aansprekend onderwerp waar we allemaal steeds meer mee te maken gaan krijgen. De ALV en dit evenement zijn dus prima te combineren. Als je je nog niet hebt aangemeld voor het voorjaarevenement, dan kan dat nog door een mail te sturen naar evenementen@testnet.org. Vermeld daarbij je naam, lidnummer en welke trackpresentaties je bij wilt wonen (ter indicatie).

Ik roep jullie op om allemaal op om de ALV te bezoeken. Daarna kunnen we genieten van een spetterend evenement. Laat deze kans niet voorbij gaan!

Evenementen Commissie

Door Michiel Vroon
evenementen@testnet.org

De thema-avonden en evenementen zijn binnen TestNet een zeer bekend verschijnsel en worden daarom dan ook altijd goed bezocht. Ze vormen de gelegenheid voor alle leden om te horen over de laatste ontwikkelingen en ervaringen op het gebied van het vak wat ons allen boeit: Testen. Daarnaast wordt er ook altijd op de avonden en evenementen stevig gewerkt aan de zakelijke (en vooral ook sociale) contacten. Kortom, het is één van de pijlers waarop TestNet zijn succes baseert.

In 2005 zijn we er als Evenementen Commis sie zeer goed in geslaagd een aantrekkelijk en variërend aanbod van verschillende thema-avonden neer te zetten. Verschillende onderwerpen (o.a. Prince II, Common Criteria en Performance Testen) zijn de revue gepasseerd en ook waren de avonden verschillend van opzet (presentaties versus discussies). Ook de evenementen werden zeer goed bezocht en positief gewaardeerd. Absoluut hoogtepunt was natuurlijk dit jaar het najaarsevenement met een recordaantal bezoekers van

bijna 200!

Ook voor dit jaar probeert de Evenementen Commissie weer zo'n gevarieerd en interessant programma aan te bieden aan de leden van TestNet. De afgelopen maanden hebben we niet stilgezeten en is het programma weer samengesteld. We zijn van mening dat we met deze verzameling aan thema-avonden en evenementen weer ingaan op de laatste ontwikkelingen en zo ieder lid van TestNet weer iets kunnen bieden over het gebied wat ons allen boeit: Testen!

Call for papers najaarsevenement 2006

Door Michiel Vroon
evenementen@testnet.org

Op maandag 25 september 2006 organiseert TestNet wederom het najaarsevenement. We gaan ervoor zorgen dat het dit jaar minstens zo bruisend wordt als de voorgaande jaren. Dit jaar willen we met twee keynote presentaties en een flink aantal parallelle track-presentaties de deelnemers weer een interessant programma bieden.

De conferentie zal bestaan uit een middag- en een avondprogramma. Beide programma's starten met een keynote en daarna 4 parallelle tracks met een workshop of 2 opeenvolgende presentaties. Ook dit jaar zullen we (net als vorig jaar) de parallelle tracks herhalen. Zo is de conferentie ook interessant voor mensen die alleen de middag of avond kunnen bijwonen. Mensen die het hele programma volgen krijgen de kans om presentaties die tegelijk worden gehouden toch te bezoeken.

Het thema is: "De ideale teststrategie".

Wij roepen jou op om een voorstel voor een presentatie of een workshop in te zenden. Zorg dat je aansluit op het thema. Daarbij kun je denken aan typen teststrategieën, teststrategieën in de praktijk, of ervaringen maar ook methoden om teststrategieën op te zetten. De presentaties duren 35 minuten plus 10 minuten voor vragen/discussie. Voor een workshop is ruim anderhalf uur beschikbaar. Geef bij je inzending aan of je bereid bent om de presentatie of workshop zowel 's middags als 's avonds te geven.

Geef de kern van je presentatie / workshop weer in maximaal één pagina met daarin de volgende informatie:

- Titel
- Onderwerp van de presentatie
- 3 highlights uit de presentatie
- Korte samenvatting presentatie, circa 1/2 A4
- Beoogd publiek voor de presentatie
- Korte biografie van de spreker (inclusief eerdere presentatie-ervaringen)
- Beschrijving van je praktijkervaring met betrekking tot het onderwerp
- NAW gegevens

Mail je inzending uiterlijk op 15 mei 2006 aan: evenementen@testnet.org. De inzenders krijgen uiterlijk op 1 juli bericht over de acceptatie van hun inzending. De definitieve presentatie moet dan op 15 augustus worden ingeleverd.

Erik's Column

Door Erik van Veenendaal
eve@improveqs.nl

De laatste jaren is testen steeds meer volwassen geworden. Het wordt inmiddels gezien als een serieus vakgebied. Door de International Software Testing Qualifications Board (ISTQB) is zelfs een internationaal erkend testcertificatietraject ontwikkeld. Toch zijn er nog een aantal aspecten binnen het vakgebied testen waar nog veel ontwikkeling dient plaats te vinden, zowel vanuit theoretisch als praktisch perspectief. Acceptatiecriteria is zo'n onderwerp.

Naar mijn mening van de auteur zijn er weinig projecten die met concrete en bruikbare acceptatiecriteria werken. In een testplan lees je vaak "het systeem mag geen fouten bevatten" en "moet volgens specificatie zijn opgeleverd", of er wordt "gewoon" getest totdat de tijd op is en het systeem in productie moet. Tenslotte is er nog de variant waarbij alle eisen worden omgezet in acceptatiecriteria. Al met al volgens mij nauwelijks bruikbaar en hier moet verandering in komen. Het belang van goede acceptatiecriteria wordt nog eens benadrukt doordat gedistribueerd ontwikkelen en outsourcing een enorme vlucht nemen. Indien meerdere (externe) partijen betrokken zijn bij de ontwikkeling van het systeem zal het

TestNet Nieuws

acceptatieproces formeler worden.

Feitelijk zijn er natuurlijk verschillende belanghebbende die allen hun eisen stellen aan het systeem. Het gaat niet alleen om de gebruikersorganisatie of de eindgebruiker, ook de beheerorganisatie evenals de onderhoudsorganisatie dienen te worden betrokken bij het opstellen van acceptatiecriteria. Bij het definiëren van acceptatiecriteria dient niet slechts te worden gekeken naar de gebruikersorganisatie, maar ook vanuit beheerperspectief, daarbij onder andere gebruik makend van de internationale ISO 9126 standaard voor software product kwaliteit. Het plaatst acceptatiecriteria nadrukkelijk in een breder perspectief.

Als testexpert, en mede-ontwikkelaar van de Nederlandse teststandaard TMap ben ik natuurlijk geneigd om de oplossing te zoeken in het testvak. Het opstellen van acceptatiecriteria is echter een uitdaging die ook toehoort aan het vakgebied requirements engineering. Het vakgebied dat zich bezig houdt met het afleiden en definiëren van de eisen (requirements) aan een systeem. Daar zou men met de verschillende belanghebbende moeten communiceren en de acceptatiecriteria SMART moeten definiëren. Testen wordt dan eigenlijk slechts uitvoerend; vaststellen of het systeem voldoet aan de van tevoren opstelde acceptatiecriteria. De acceptatiecriteria zorgen dan voor een duidelijke sturing en bepalen de richting van het testproces. Helaas daar zijn we nog (lang) niet.

Oplossingen? Volgens mij zijn de delen 2 en 3 van ISO 9126 goed bruikbaar. Daarnaast is het altijd van belang al na te denken over acceptatiecriteria die iets zeggen over het testproces (feitelijk “hoe betrouwbaar is de uitspraak ten aanzien van product kwaliteit) en over product kwaliteit. Goede acceptatiecriteria zorgen ook voor een gedegen focus van het testproces en iets waartegen die gerapporteerd kan worden. Of het Nederlandse QUINT project, de ontwikkelaars van het extended ISO 9126 model, wellicht een mooie uitdaging voor hen …..

Voor een reactie dan kunt u mailen met Erik van Veenendaal (eve@improveqs.nl)

Ketentesten, zeker en vast!

Door Marcel van Donge
donge@collis.nl

Gegevens van informatiesystemen worden steeds vaker met elkaar uitgewisseld. Vanaf de jaren zeventig worden er al in bepaalde branches ketens ingericht, met name om hier schaalvoordelen mee te behalen. Dit wierp o.a. al in de logistieke sector zijn vruchten af. Tegenwoordig is internet met portals en communities, waarbij allerlei gegevens worden verzameld en op alle mogelijke manieren worden gepresenteerd, een belangrijke trend. Het zogenaamde ketentesten is dus steeds meer aan de orde. Onder ketentesten verstaan we het testen waarbij één of meer bedrijfsprocessen worden doorlopen over een aaneengesloten reeks van systemen en platforms. Het doel van ketentesten is om antwoord te krijgen op de vraag of de processen en systemen op de juiste manier geïntegreerd zijn en of ze een werkend geheel vormen. Hierbij schetsen we onze ervaringen.

Opzet

Voor het opzetten van een ketentest is het belangrijk om een goede doelstelling te bepalen. Binnen deze doelstelling dient de tester te weten wat het belang is van overige organisaties in de keten. Niet alle organisaties willen dat anderen in hun keuken kijken, maar dit hoeft geen onoverkomelijke problemen te veroorzaken. Daarnaast is bij het opzetten van een ketentest veel organisatietalent nodig om de juiste afstemming te krijgen én te houden omtrent de testomgeving. Zo vormen afspraken over interfaceontwerpen een flinke uitdaging, omdat elke wijziging afstemming vereist en de wijzigingsverzoeken conflicterend kunnen zijn. Ook kunnen ogenschijnlijke kleine fouten in het ene systeem grote gevolgen hebben in een ander systeem.

Een belangrijk aandachtspunt voor een ketentest is dat de keten zo sterk is als zijn zwakste schakel. Deze schakels worden met name door de volgende kwaliteitsattributen afgevangen.

- *Security:* beveiliging tijdens de gegevensuitwisseling is zeer belangrijk. In de financiële dienstverlening, bijvoorbeeld, vormt phishing een serieuze bedreiging;
- *Performance:* omdat er in de keten veel overgangen voorkomen die een

bottleneck kunnen vormen wordt het meten van performance belangrijker;
- *Connectiviteit:* bijvoorbeeld, komen gegevens van de ene organisatie naar een andere tijdig en correct binnen? Verloopt de protocolafhandeling correct?;
- *Portabiliteit:* kunnen gegevens die door een operating system (OS) van een organisatie zijn gegenereerd worden verwerkt door een ander OS?

Een praktijkvoorbeeld

We hebben tal van praktijkvoorbeelden, het testen bij de millenniumovergang heeft ons enkele jaren geleden veel bruikbare ervaring opgeleverd. Toen bleek dat een groot deel van de organisaties niet gecharmeerd was van het openbaar maken van allerlei gegevens. Met name het juridische aspect woog nogal zwaar. Er is toen gezocht naar een oplossing in de vorm van een erecode. De erecode was een intentieverklaring waarmee diverse organisaties naar eer en geweten informatie beschikbaar stelden om risico's te beperken. Hieraan waren geen juridische verplichtingen verbonden. Dankzij deze intentieverklaring werd er testdata aangeleverd. Het resultaat van de ketentest met de bestaande systemen was bevredigend; ze vertoonden nauwelijks afwijkingen. Toch bleef de voorspelling voor de situatie na de millenniumovergang onduidelijk. De meeste systemen waren niet goed beschreven en werkten al jaren zonder dat iemand wist waarom. Met betrekking tot het samenstellen van testdata gold dat sommige systemen dusdanig complexe data opleverden dat er een vergroot risico optrad. Uiteindelijk zijn er, op basis van een risicoanalyse, noodscenario's ontwikkeld.

Collis heeft veel ervaring met ketentesten. Mocht u met ons van gedachten willen wisselen over dit onderwerp dan horen wij dat graag.

CMMi Symposium

Door Maurice Siteur
maurice.siteur@capgemini.com

9 februari 2006 – Amstelveen

De schrijver van het nieuwe boek "De Kleine CMMI" hadden in samenwerking met Testnet en Spider een klein symposium georganiseerd rondom de introductie van hun boek.
Beide auteurs, Rini van Solingen en Jan Jaap Cannegieter, gaven een presentatie naast een drietal gastsprekers. De opkomst was met 150 deelnemers groot te noemen.

Ik wil een korte impressie geven van dit evenement, waarin alle mogelijkheid had om mensen tegen te komen die je nog niet kende.

Andrey Heijsteck begon met een statement dat je het model vooral niet te serieus moet nemen. Bedenk dat het model is opgezet met een project als de Joint Strike Fighter. Dus een heel groot project met enorme belangen. Ons gemiddelde project of organisatie voldoet daar niet aan. Met andere woorden: neem de ruimte om dat te nemen wat voor jou van belang is.

Een andere analogie legde hij met de theologie en het schrijven van de bijbel. De schrijver ziet een wereld, heeft daar een beeld van en schrijft dat op; de lezer leest het boek met zijn beeld van de wereld.

Jan Jaap Cannegieter presenteerde een aantal resultaten van een survey uit een niet representatieve groep bedrijven die iets met CMM doen.
Grote bedrijven neigen naar een staged aanpak, terwijl kleinere bedrijven neigen naar de continuous aanpak. Op basis van buitenlandse onderzoeken blijkt dat een ROI van 7 mogelijk is; dat is 7 keer je kosten eruit halen.

Johan Zandhuis belichtte de rol van testen binnen CMMI en kwam niet veel verder dan dat er verificatie en validatie nodig is. Veel meer zegt CMMI er ook niet over. Zijn conclusie is dan ook, dat als een bedrijf bijvoorbeeld TMap® geïmplementeerd heeft, dat zij dan voldoen aan CMMI level 3 voor testen.

Rini van Solingen leidde ons door het boek heen.
Statements van bedrijven dat zijn CMMI level x zijn gecertificeerd, is onmogelijk. Er is geen officieel certificaat.

Hans Aerts vertelde over hoe CMMI binnen Philips Semiconductor is ingevoerd. De redenen waarom ze voor CMMI gekozen hadden en niet gewoon bij CMM gebleven waren zijn mij het meeste bijgebleven. CMMI is meer op de bedrijfsprocessen gericht. Voor CMM hadden ze een grote hoeveelheid interpretatieregels en die waren bij CMMI veel minder nodig.

CMMI is duidelijker in wat het model vraagt, maar is ook uitgebreider; voor een bedrijf als Philips is dat laatste alleen maar prettig.

Voor informatie over het boekje, kijk op www.kleinecmmi.nl.

ISTQB / ISEB nieuws

Het meeste nieuws komt momenteel vanuit de International Software Testing Qualification Board. Per 1 april zal het niet meer mogelijk zijn om cursussen te volgen en examens te doen op basis van de "oude" ISEB syllabus. De nieuwe internationaal breed erkende ISTQB syllabus wordt m.i.v. 1 april operationeel. Uiteraard betekent dit dat de cursussen en ook de examens zijn aangepast. Alle cursussen bij Improve Quality Services van na 1 april zijn daarom op basis van de nieuwe syllabus. Let wel, alle in het verleden behaalde ISEB certificaten blijven volledig geldig en worden als Foundation certificaat erkend door de ISTQB.
De belangrijkste verschillen:

- een nieuwe terminologie standaard (ISTQB glossary);
- minder testtechnieken, maar wel diepgaander;
- nieuw: use cases en exploratory testing;
- meer over test management (risk-based testing en bevindingen rapportage);
- uitgebreider aandacht voor alternatieve ontwikkelmodellen en onderhoudstesten.

De nieuwe glossary evenals de nieuwe syllabus kunt u aanvragen via de verschillende course providers in Nederland en België.
Deze beide kunt u ook downloaden op de site van de Dutch Testing Qualifications Board (www.istqb.nl)

5 vragen aan Riny Nieuwhoff

Door Riny Nieuwhoff van Polteq IT Services

Ik vind testen een leuk vak want....

Het belang van een goed testproces is erg groot. Ik haal veel motivatie en plezier uit het kunnen meebouwen aan een goed testproces en het hiermee verbeteren van de kwaliteit van de producten.

Het grootste misverstand over testen is...

Dat testen zich richt op programma's, applicaties, systemen…..
Ja, daar richt testen zich OOK op. Maar het beschouwinggebied van testen is veel groter dan alleen de geautomatiseerde processen. Bij het testen hoort ook de aansluiting van de geautomatiseerde processen op de handmatige processen, het beoordelen van handleidingen, werkinstructies, etc.
En het testen begint al voordat er maar een regel code is geschreven, bijvoorbeeld bij het reviewen van het ontwerp.

Over 5 jaar zie ik mijzelf in de functie van...

Lastige vraag….ik heb net de overstap gemaakt naar Polteq IR Services. Het bedrijf en mijn rol als testconsultant bevallen zeer goed. Dus laat ik antwoorden: als testconsultant maar dan met een accentverschuiving richting coachen, om mijn kennis en ervaring over te kunnen brengen aan collega's binnen het testvakgebied.

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

Goed te kunnen communiceren. Om het testen heen hangt vaak een bepaalde sfeer. Planningen die onder druk staan, bouwers die bevindingen van testers zien als een afkeuring van hun product, (te) hoge verwachtingen van het testproces, etc.
Het gaat er dus vaak niet om WAT je zegt, maar HOE je de boodschap brengt. En communiceren houdt niet op bij het roepen van dingen, controleer ook of de boodschap juist is overgekomen en of de ontvanger van de boodschap het gewenste verdrag vertoont.

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

Dat testen een volwaardige fase binnen een ontwikkeltraject wordt.
Nu wordt al wel vaak 'rekening' gehouden met het testtraject; er wordt aan het einde van het traject een aantal weken ingepland voor het uitvoeren van tests. Maar om een volwaardig testproces te krijgen is meer nodig.
Testen is ook net als projectmanagement, java-ontwikkelaar of dba'er een vakgebied, waarbij kennis en vaardigheden erg belangrijk zijn.
En wat misschien wel belangrijker is; testen is niet het proces dat alleen maar een waardeoordeel uitspreekt over producten (van een bouwer). Nee, het project moet zo zijn

ingericht dat alle disciplines er samen voor zorgen dat uiteindelijk een goed product wordt opgeleverd.

Ik geef de vraag door aan..., omdat...

Ernst van den Bos van KZA. Ik werk samen met Ernst aan het optimaliseren van het testtraject (systeemtest en assemblagetest). Ernst is een zeer prettige collega.

Monitoring & control op uitbestede testwerkzaam-heden

Door: Kees Blokland
testconsultant bij Polteq
kees.blokland@polteq.com

Veel bedrijven besteden de bouw van hun informatiesystemen uit. De controle of de applicatie correct functioneert (de functionele- of acceptatietest) is normaal gesproken een activiteit die nog wel binnen eigen geledingen wordt uitgevoerd. Stel nu dat er wordt besloten om ook de functionele test uit te besteden en wel aan de leverancier die het ook heeft gebouwd? Dat betekent nogal wat voor de bij het realisatietraject betrokken partijen:

1. voor de leverancier betekent het dat er een informatiesysteem wordt geleverd waarvan door de leverancier zelf vóór oplevering door middel van testen is vastgesteld dat het aan de gestelde eisen voldoet;
2. de opdrachtgever (in de rol van functioneel beheerder) hoeft niet meer langdurig functioneel te testen en kan zich richten op andere belangrijke werkzaamheden;
3. de opdrachtgever mist daardoor wel een mogelijkheid om uitgebreid te bekijken of de leverancier wel goed gebouwd en getest heeft.

Dit zijn belangrijke aandachtspunten voor het implementeren van testuitbesteding. Punt één heeft bijvoorbeeld als consequentie dat de leverancier een gestructureerd testproces moet inrichten. Het tweede punt verandert de werkinhoud van functioneel beheerders wat zorgvuldig begeleid moet worden. Het derde punt vergt een andere kijk van de opdrachtgever op testen. In plaats van zelf veel functionele tests uit te voeren moet er op een andere manier beoordeeld worden of er goed gebouwd en getest is.

Door het uitoefenen van een goede monitoring & control op de uitbestede testwerkzaamheden kan die beoordeling worden gerealiseerd. De leverancier moet diverse ‘bewijzen van goed testen’ opleveren aan de hand waarvan de opdrachtgever het vertrouwen in de goede afloop stap voor stap kan opbouwen. Monitoring & control heeft twee belangrijke effecten. Ten eerste tap je als opdrachtgever informatie af uit het realisatietraject en komt zo vroeg te weten hoe het met de voortgang en de kwaliteit van het op te leveren informatiesysteem gaat en ten tweede leg je zo een druk op de leverancier om het serieus te (blijven) nemen met het volgen van een gestructureerd testproces.

Het namens de opdrachtgever uitvoeren van de monitoring & control vergt de nodige kennis en ervaring in testen en moet bij voorkeur worden uitgevoerd door een testcoördinator of testmanager. Omdat die persoon niet echt het testen zelf aanstuurt wordt die functie hier testregisseur genoemd. Als lid van de opdrachtgeverorganisatie adviseert de testregisseur de projectleiders en rapporteert (en escaleert indien nodig) de testregisseur naar senior management. Relevante opmerkingen van de testregisseur over het testproces moeten door de leverancier ter harte worden genomen.

Het moet voor de leverancier duidelijk zijn wat er verwacht wordt van een gestructureerd testproces. Dit kan worden vastgelegd in een Generiek Master Test Plan, een SLA voor testen. Ook de monitoring & control functie moet daarin duidelijk zijn omschreven, zodat de taken en bevoegdheden van de testregisseur helder zijn.

<u>De drie-eenheid van monitoring & control</u>

Het bewijs van goed testen wordt in deze praktische aanpak op drie manieren door de leverancier geleverd en door de opdrachtgever beoordeeld:

1. de testproducten die als onderdeel van het gestructureerde testproces bij de leverancier ontstaan worden beoordeeld door de opdrachtgever;
2. bepaalde testmetrics worden door de leverancier gerapporteerd aan de opdrachtgever;
3. de opdrachtgever voert health checks uit op het testproces bij de leverancier.

1. Het beoordelen van de

testproducten

De belangrijkste testproducten in dit verband zijn het testplan, de testgevallen en het testrapport/ vrijgave-advies. Het testplan wordt beoordeeld op compleetheid en vooral op de teststrategie. Het is van het allergrootste belang dat de leverancier zich een goed beeld heeft gevormd van de productrisico's en die in voldoende mate in de testaanpak heeft verwerkt. De teststrategie wordt doorvertaald naar de testgevallen. Van de testgevallen wordt door de testregisseur de testdekking en de testdiepgang beoordeeld. De testdekking is de mate waarin alle onderdelen van de testbasis zijn afgedekt met testgevallen. De testdiepgang is de mate waarin er voor gebieden met een hoger risico iets extra's wordt gedaan, bijvoorbeeld door het toepassen van een formelere en/of zwaardere testspecificatietechniek. Dit doet de testregisseur steekproefsgewijs, want alle testgevallen in detail beoordelen is niet praktisch en zou te hoge kosten met zich meebrengen. In het testrapport geeft de leverancier het vrijgaveadvies af en licht dit advies uitgebreid toe door aan te geven wat er daadwerkelijk getest is en wat de resultaten daarvan zijn. Belangrijke aspecten zijn daarbij het vermelden van eventuele resterende risico's en bijbehorende vervolgacties. De testregisseur beoordeelt het testrapport en controleert dit zorgvuldig op volledigheid.

2. Testmetrics

Tijdens het testtraject wordt er door de leverancier kwantitatieve informatie opgeleverd over het testproces. Door de testregisseur worden hieruit nuttige metrics afgeleid die informatie geven over de kwaliteit van het testobject en de voortgang van het testen. Daarnaast kunnen er aan de hand van de metrics projecten met elkaar worden vergeleken. Het is belangrijk dat de testregisseur uit de metrics signalen afleidt over mogelijke risico's. De volgende metrics moeten minimaal worden bijgehouden:

- het aantal testgevallen gepland/uitgevoerd/ok/niet ok,
- het aantal bevindingen per status en ernstcategorie en
- het aantal geplande en actuele uren.

Een voorbeeld van een 'signaal' is bijvoorbeeld een te laag percentage uitgevoerde testgevallen 'ok', wat er op duidt dat de leverancier te vroeg is gestart met deze testronde (dan wel dat bouw een te lage kwaliteit heeft opgeleverd). Aan het eind van het testtraject kunnen nog meer metrics worden afgeleid, zoals het aantal uur testen per gevonden bevinding. Bij grote afwijkingen van dit soort gegevens van vergelijkbare projecten kan de testregisseur daar kritische vragen over stellen aan de leverancier.

3. Health checks

De beoordelingen en de metrics geven al een aardig beeld van het testen. De testregisseur zal wanneer daar aanleiding toe is een nader gesprek aangaan met testcoördinator van de leverancier. Aanleidingen kunnen zijn: de tests zijn pas net uitbesteed aan de leverancier, er is een nieuwe testcoördinator of er zijn veel vragen rond de beoordeling van een testproduct. Dit wordt een health check genoemd en gebeurt bij voorkeur op locatie van de leverancier (als dat dichtbij genoeg is, hoewel een snoepreis je naar Bangalore…). De agenda van een health check kan heel breed zijn (het hele testproces) of heel beperkt (bijvoorbeeld nader overleg over de beoordeling van de testgevallen).

<u>Acceptatie</u>

De monitoring & control heeft als doel om druk te leggen op de leverancier zodat er een fatsoenlijk gestructureerd testproces wordt gevolgd, maar ook om als opdrachtgever tijdig zicht te krijgen op het verloop van de testwerkzaamheden en de kwaliteit van het informatiesysteem dat in ontwikkeling is. De acceptant, vaak een functioneel beheerder, zal dit meenemen in zijn of haar overweging om het informatiesysteem functioneel te accepteren. Naast het bewijs van goed testen dat de leverancier heeft opgeleverd aan de testregisseur zal de acceptant ook altijd een (als het goed is beperkte) functionele acceptatietest uitvoeren voordat het akkoord gegeven kan worden. Deze finale acceptatie kan uiteraard niet uitbesteed worden!

<u>Ervaringen</u>

Monitoring&control is een boeiend proces: doordat de testregisseur optreedt namens de opdrachtgever 'moet' de leverancier wel luisteren. Dat is in een interne organisatie wel eens anders! Als het proces eenmaal goed loopt en het routine is geworden kunnen de teugels wel wat gevierd worden. Dit kan bijvoorbeeld door bij kleinere projecten met minder risico niet alle of helemaal geen testproducten te beoordelen.
Bij de tijdsbesteding voor monitoring & control moet

men denken aan tussen de 4 en 10% van de totale urentestbegroting van de leverancier. 4% bij soepel verlopende testtrajecten en 10% bij problematische trajecten die veel extra aandacht vragen.

Conclusie
Met monitoring & control kun je effectief afdwingen dat de leverancier een gestructureerd testproces volgt. Daarnaast geeft het goed zicht op de projectvoortgang en kwaliteit van het informatiesysteem. Het is geen garantie dat de door de leverancier opgeleverde software aan alle wensen voldoet, maar helpt wel een heel stuk in de goede richting!

Software testen is geen mensenwerk

Door Gerjon de Vries
Senior Consultant bij de Software Improvement Group
www.sig.nl

Bij onze klanten signaleren we vaak dat het testen van software een aparte taak is, die zoveel mogelijk apart van het bouwtraject wordt gehouden. Software ontwikkelaars moet je niet hun eigen software laten testen en het testen van software vereist andere kwaliteiten dan die van ontwikkelaars verwacht mogen worden, is de algemene opvatting.
Het resultaat is dat softwaretesten als aparte activiteit pas vlak voor het in productie nemen van software gebeurt, en dat het testen van software een dure activiteit is waaraan veel mankracht wordt besteed.

Veranderbaarheid van Software

Softwaretesten wordt zo een activiteit die de veranderbaarheid van software in de weg zit: het opnieuw testen na wijzigingen kost veel tijd en geld, waardoor wijzigingen ofwel achterwege gelaten worden omdat ze te duur zijn, of slecht getest worden, wat een risico is voor de kwaliteit van het product.

Dit is om een aantal redenen jammer:

Hoe eerder je begint met testen, en daarmee dus problemen signaleert, hoe minder kosten er verbonden zijn aan het oplossen van die problemen.

Testen is, na het opstellen van een testplan, een repetitieve taak. Een deel van de testtaak is bijvoorbeeld het handmatig starten van de applicatie, openen van schermen, velden invullen en de resultaten controleren tegen vooraf vastgestelde verwachte waarden. Bij uitstek een taak waar computers goed in zijn.

Daarbij geldt dat je de tests zo vaak mogelijk wilt herhalen. Elke wijziging, hoe klein ook, in software, kan onverwachte problemen veroorzaken in andere onderdelen van een systeem. Herhaling van acties is iets waar computers goed in zijn. Een testteam vraag je niet alle tests opnieuw uit te voeren bij een last-minute aanpassing, er is dan simpelweg niet genoeg tijd.

Programmeurs moeten veel meer betrokken worden bij testen. Het blijkt in de praktijk dat programmeurs die hun eigen unit-tests schrijven beter testbare en minder complexe software produceren. De opvatting dat, wanneer de tester en programmeur dezelfde persoon zijn, de kwaliteit afneemt omdat alleen het testresultaat nog telt blijkt in de praktijk onzin.

Deze teststrategie focust voornamelijk op het eindproduct als geheel. Er is weinig aandacht voor unit-testen. Terwijl juist unit-tests eenvoudig te automatiseren zijn, en de kwaliteit van deze tests heel goed objectief te meten is. Unit-tests zijn daarnaast vanaf de eerste minuut dat er code ontwikkeld wordt in te zetten.

Automatiseren van testen kost minder

Er is tegenwoordig veel standaard tooling beschikbaar voor het maken, onderhouden en beoordelen van automatische unit-tests, user interface tests en regressie tests. Het toepassen van deze tooling waarborgt de kwaliteit van de applicatie met de spreekwoordelijke druk op de knop. Dit betekent niet dat er geen testers meer nodig zijn. Maar de mankracht wordt ingezet voor het bepalen van de teststrategie en om bijvoorbeeld de usability aspecten van software te testen. Taken die niet of moeilijk geautomatiseerd kunnen worden. De aanwezigheid van automatische unit-tests zorgt ervoor dat de testinspanning voor een acceptatie test veel minder hoeft te zijn.
Daarbij geldt dat ontwikkelaars de programma units die zij ontwikkelen toch al moeten testen. Het herhaalbaar maken van zulke tests door ze te programmeren kost weinig extra, maar levert wel op dat de tests altijd uit te voeren zijn. Ook het automatiseren van user interface tests hoeft niet veel te kosten, als er tijdens het

ontwerp en de bouw rekening mee wordt gehouden.
Door een grotere nadruk te leggen op het in vroeg stadium beginnen met testen van kleine units en onderdelen van een systeem, en het automatiseren van een belangrijk deel van de testinspanning, kan software sneller, doeltreffender en goedkoper aangepast worden.

Automatische tests zorgen voor veranderbare software

Kortom, om ervoor te zorgen dat software veranderbaar blijft, moet de teststrategie aangepast worden. Er moet meer nadruk komen op automatiseerbare tests, die eenvoudig te herhalen zijn en waarvan de kwaliteit objectief is vast te stellen. Dit betekent dat tests vaker uitgevoerd kunnen worden, problemen eerder gesignaleerd worden, de software beter onderhoudbaar en sneller aanpasbaar is, de test- en ontwikkelkosten afnemen en last-but-not-least er simpelweg betere software wordt gemaakt.

TMap® survey 2006 - Testbasis doorslaggevend

Door Theo van der Kooi
theo.vander.kooi@sogeti.nl

Zonder een goede testbasis loopt een ontwikkeltraject met de helft uit. Weliswaar werkt een detailintake op de testbasis kwaliteitsverhogend, maar nog niet de helft van de testprojecten voert deze uit. Met TMap® als testmethodiek wordt het inzetten van de detailintake verdubbeld.

TMap® survey

In de afgelopen maanden hebben ruim 200 testprofessionals de moeite genomen om de survey in te vullen. De leden van de TMap®/ TPI-nieuwsbrief en de bezoekers aan www.tmap.net die de 55 vragen invulden willen we hartelijk bedanken. Met deze informatie konden we analyseren wat de effecten van de verschillende testonderdelen zijn op het ontwikkeltraject.

Uit meer dan 20 verschillende landen is, vooral door testmanagers en testers, meer dan 1300 jaar testervaring gedeeld. Dik de helft hiervan zijn gecertificeerde professionals, die werken bij de wat grotere organisaties (tussen de 100 en 10.000 medewerkers). Een derde is werkzaam bij financiële dienstverleners, maar ook vanuit branches als de auto-industrie en medische systemen is gereageerd.

Testbasis

Met een goede testbasis loopt de uitloop op de planning van het ontwikkeltraject terug naar 20 procent. Bij een slechtere testbasis is dit 50 procent. In de industriële sector wordt de testbasis vaker als goed beoordeeld. Factoren die de kwaliteit van de testbasis positief beïnvloeden zijn een iteratieve ontwikkelmethode en de detailintake. Helaas wordt de detailintake nog niet vaak genoeg ingezet. Iteratief ontwikkelen lijkt haaks te staan op een goede testbasis, vaak schort het bij iteratief ontwikkelen aan documentatie en dus aan testbasis. Maar blijkbaar wordt wat er is, juist als goed beoordeeld. De doelstelling van iteratief ontwikkelen, om nauw op de behoeften van de gebruiker aan te sluiten, lijkt geen slechte gedachte.

Bij een goede testbasis wordt vaker een mastertestplan en een business driven teststrategie gehanteerd. Er wordt dan in ieder geval meer gestructureerd getest, bijvoorbeeld door meer gebruik te maken van TestPuntAnalyse en testontwerptechnieken.

Omgeving

Service oriented architecture is een ware ontdekking. Al een kwart van de ondervraagden werkt met dergelijke architecturen. Het zijn vooral de kleinere organisaties die hiermee werken. Meestal echter worden webapplicaties en client-server systemen ontwikkeld, voornamelijk om primaire bedrijfsprocessen te faciliteren.

Testmethodiek

Van de respondenten werkt 70 procent met TMap® of een methodiek gebaseerd op TMap®. Met TMap® geïnteresseerden als respondenten is dat geen verrassing. De methodiek is gemiddeld vier jaar in gebruik. De belangrijkste kwaliteitsattributen die met TMap® getest worden zijn functionaliteit, performance, gebruiksvriendelijkheid, connectiviteit en beveiliging. Andere kwaliteitsattributen worden in minder dan de helft van de gevallen getest.

TMap®-gebruikers schrijven vaker een mastertestplan. Ook hebben ze meer invloed op de duur van het testtraject. Niet TMap®'ers zoeken oplossingen eerder in het gebruik van testtools en in het uitvoeren van een pretest.
Ondanks het grote aantal TMap®-gebruikers, werkt slechts 40 procent aan de hand van een op TMap® gebaseerde teststrategie (risk based of business driven). En dat terwijl het gebruik van een strategie een sterker positief effect heeft

dan alleen het gebruik van TMap® als testmethodiek.

Wanneer sprake is van een TMap®-teststrategie volgt vaker ook een gebruikersacceptatietest, een detailintake en het hergebruik van testware. Het gebruik van een TMap®-teststrategie leidt tot een eerdere oplevering van de testbasis en het testobject. En uiteindelijk tot 10 procent minder uitloop van de ontwikkeltrajecten van de respondenten.

Het mastertestplan wordt in driekwart van de testtrajecten opgesteld, een hoog percentage! Alleen in de sector telecommunicatie stelt slechts de helft dit plan op. En dat terwijl een MTP een belangrijke bijdrage levert aan de structurering van het testproces.
Bij een MTP is er meer aandacht voor planning & beheer en afronding. Het testplan en de voortgangsrapportage zijn uitgebreider, de detailintake wordt weer vaker uitgevoerd en testen wordt meer betrokken bij wijzigingen. Vooral bij de black-box testsoorten lukt het om veel beter volgens planning te werken. Ook het testobject is na oplevering sneller geschikt om te testen.

Nederland vs. de rest

Exclusief voor de TNN is een dwarsdoorsnede van Nederlanders (137 respondenten) gemaakt. Hieruit blijkt dat de Nederlandse respondenten meer dan anderen actief zijn in de financiële sector. Ze (maar voor het Oranjegevoel hanteer ik hier verder de “we”-term) hebben wat minder ervaring dan de buitenlandse testprofessionals en zijn dan ook eerder terug te vinden in functies als tester en consultant dan als testmanager. Wat we aan ervaring missen maken we goed met certificering en het gebruik van TMap®.

Toch leggen de Nederlandse testprofessionals het af tegen de buitenlandse.
De niet-Nederlanders identificeren in driekwart van de testprocessen expliciet een unit- en systeemtest, terwijl wij dat maar in iets meer dan de helft doen. Ook testen wij slechts tegen een derde van de bekende kwaliteitsattributen. De rest van de wereld dekt nagenoeg de helft van alle kwaliteitsattributen. Over het algemeen testen we meer gestructureerd, bijvoorbeeld in het maken van een mastertestplan en de inzet van testontwerptechnieken. Maar onze buitenlandse collega’s richten zich meer op managementaspecten als begroting en rapportage. Daarnaast richten ze zich ook meer op de business door bijvoorbeeld testgevallen af te leiden van een business case en requirements.

De bottom-line? Voor het gehele ontwikkeltraject is er maar een klein verschil in de uitloop van de planning tussen de verschillende nationaliteiten. Maar vooral bij de specificatie- en ontwerpfase van een ontwikkeltraject en bij de acceptatietest slagen de andere nationaliteiten er veel beter in de overschrijding van de geplande inspanning te beperken. Toch wil ik (Nederlanders zijn slechte verliezers) nog een kanttekening maken bij deze vergelijking: gestructureerd testen is in Nederland al vele jaren bekend bij de meeste testers, in het buitenland zijn het (nog) slechts de ervarener test(manag)ers die er vanaf weten. Dit heeft ongetwijfeld de resultaten wat gekleurd.

De volledige survey is te vinden op www.tmap.net, onder TMap/downloads/TMap survey 2006. Als je nog een specifieke vraag hebt, waar de survey-resultaten een antwoord op kunnen geven, dan hoor ik deze graag.

Een dag van Peter Mourik, testmanager bij KZA

Door Peter van Mourik

Huidig project: Vernieuwing Keten Schade bij Nationale-Nederlanden.

’s Ochtends om half zeven gaat de wekker en omdat we gisterenavond salsa-les hebben gehad en pas na twaalven in bed lagen, gaat het opstaan vandaag niet van harte. Toch moet ik er meteen uit, want met morgen een bruiloft op het programma moet er op deze donderdag nog een hoop gebeuren om deze 4-daagse werkweek tot een goed einde te brengen.

Douchen, aankleden, ontbijt met koffie in de auto. Omdat het voorjaarsvakantie is, staat er gelukkig slechts zeer beperkte file van Gouda naar Den Haag. Om 8 uur loop ik de afdeling op en ben toch nog een van de laatste. Het is momenteel een redelijk drukke en spannende periode. De afgelopen weken heeft het testteam enorm overgewerkt om de Systeemtest af te ronden en op tijd met de Ketentest te kunnen starten. Deze

krachtsinspanning heeft ertoe geleid dat wij er nu wel klaar voor zijn, maar een aantal omgevingspartijen echter nog niet. Dit heeft geleid tot het uitstellen van de implementatiedatum en een nieuwe integrale planning.

Om negen uur is er een conference call met projectleiders van de eerder genoemde projecten om deze planning te bewaken. Omdat mijn projectmanager er deze week niet is, vervang ik hem bij deze conference call. Na een dik uur telefoneren verlaat ik de call met wat actiepunten die ik vandaag wil afhebben.

10.00 uur. Mail doorlopen en wat bellen met een collega testmanager over een tester die ik kan missen en die hij goed kan gebruiken voor zijn project. Afgesproken dat zij maandag meteen bij hem begint. Prettig om te merken dat door veel (ook informeel) te communiceren, zulke zaken snel kunnen worden geregeld.

Er is gebak! In mijn testteam is het traditie dat bij elke honderdste bevinding degene die hem heeft gevonden trakteert. Dit is al de achtste keer dat er gebak is en bijna iedere tester is nu aan de beurt geweest. Bij de 1000ste bevinding zal ik zelf maar eens trakteren.

Het is al bijna elf uur en dan is het tijd voor het projectleidersoverleg dat twee keer per week plaatsvindt. In dit overleg wordt met de projectleider van onze leverancier, de implementatiemanager en de projectleider de issue- en de risklog besproken. Deze keer houden we het kort, omdat er helaas weinig is veranderd sinds het vorige overleg. Dit komt mij goed uit omdat ik nog genoeg te doen heb.

Na de lunch heb ik een afspraak met mijn manager van KZA. We bespreken mijn opdracht en de consequenties van mijn verlenging. Verder komt mijn POP ter sprake en bespreken we welke opleidingen ik het komende jaar ga doen. Het grootste onderdeel daarvan zal bestaan uit een management development programma waaraan ik mee mag doen. Iets waar ik erg veel van verwacht.

Na deze afspraak bel ik een andere collega testmanager. Zijn opdracht is het opleveren van een geautomatiseerde regressietest voor het project waar ik mee bezig ben. Onze uitloop heeft ook gevolgen voor zijn project. We bespreken de mogelijkheid om zijn project aan mijn testteam te laten opleveren in plaats van aan de Service management organisatie. Op deze manier hoeft hij zijn projectteam niet extra lang vast te houden en kunnen wij de regressietest in de rest van de periode gebruiken en onderhouden. Na dit gesprek bel ik de programmamanager en leg hem dit idee voor. Ik krijg een in principe akkoord en spreek af dat ik na het weekend met een uitgewerkt voorstel kom.

Na wat mailen en bellen is het al heel snel bijna zes uur en dat betekent dat ik weg moet om te gaan trainen. Ik voetbal in het eerste elftal van sv Gouda en dat brengt verplichtingen met zich mee. Op de terugweg is het drukker dan heen. Ik heb net genoeg tijd om mijn pak te verruilen voor iets casuals en vertrek met mijn tas naar het veld. Vanwege de sneeuwval verwacht ik dat de wedstrijd van zondag niet door zal gaan. De trainer denkt dit geloof ik ook, want we doen nogal rustig aan. Na een warme douche is het tijd voor een welverdiend biertje in de kantine. En omdat ik morgen vrij ben kan dat best een latertje worden…

"Testen van beveiliging volgens Common Criteria"

Door Ine Lutterman
i.lutterman@interpay.nl

Testnet Thema avond 15 december 2005.
Donderdag 15 december heeft TestNet een avond rondom het thema "Testen van beveiliging volgens Common Criteria" georganiseerd. Met een volle zaal, de nodige interactie en nog boeiende discussies na afloop aan de bar, blijkbaar een thema wat leeft. Common Criteria kent haar oorsprong in de wereld van de beveiliging van softwaresystemen. Het betreft in feite het testen van beveiliging (vooral van software). Inmiddels wordt Common Criteria ook veel toegepast bij het testen van beveiliging in hardware als smartcards en PEDs (PIN Entry Devices). In Nederland zijn zo'n 45 certificaten uitgegeven, wereldwijd al een paar honderd.

De spreekster

Ellen Wesselingh is meer dan acht jaar werkzaam in de beveiliging van IT-systemen. In de eerste jaren betrof het vooral de beveiliging van netwerken bij IBM en KPN. In 2000 is Ellen overgestapt naar TNO-ITSEF om zich daar bezig te houden met het

beoordelen van de IT-beveiliging van producten. De laatste jaren heeft ze zich gespecialiseerd op de evaluatie van hardware security devices, waaronder smartcards.

Inhoud van de presentatie

Opkomende regelgeving en een steeds grotere dreiging van hackers noodzaken het bedrijfsleven om de beveiliging van steeds meer IT-systemen op orde te brengen. De wereld wordt steeds kleiner; er komen steeds meer geïntegreerde systemen en alles hangt met elkaar samen. databases, webservers, Smartcards, PED's, Printers, … - alles hangt aan netwerken en is dus te hacken; de controller is de poort naar binnen/ buiten. Niemand kan garanderen dat het vertrouwelijke printje niet door onbevoegden onderschept is. Om informatiebeveiliging in te bouwen in plaats van aan te bouwen zal het onderwerp ook geïntegreerd moeten zijn in het proces van creatie, in het beheerproces en het gebruik van het informatiesysteem. Beveiliging is nog steeds vaak een sluitpost bij het ontwerpen en bouwen van een IT-systeem, Functionele eisen als eenvoudig beheer, gebruikersvriendelijke interfaces en schaalbaarheid worden standaard meegenomen, maar pas ná de bouw gaan bedrijven nadenken over security. We moeten toe naar een situatie waarin beveiliging een integraal onderdeel wordt van het systeemontwerp. Dit vereist een voorafgaande grondige risicoanalyse en het meenemen van security in acceptatietesten.

Als een leverancier van een product een wanprestatie levert kun je in Nederland na een mislukte onderhandeling altijd nog naar de rechter stappen. Voor IT producten geldt dit niet. Er bestaat een End users agreement die grofweg inhoudt dat je rechten hebt voor het medium waarop het product verkocht wordt, maar verder niets. Hierdoor is de vraag naar een onafhankelijke evaluatie van software door een partij als TNO sterk toegenomen. Waar ontwikkelaars graag aantonen dat iets werkt, hanteren zij de negatieve/ kritische insteek; doet het niet ook iets wat het niet hoort te doen? Als onafhankelijke 3e partij is TNO certificeringsbevoegd, maar wat zegt een certificaat wanneer er niet op vermeld is wat, hoe, tegen welke standaards, waarop en door wie getest is.
Er zijn teveel instanties die als 3e partij optreden om ze allen te kennen, dus je moet weten waar je een bonafide testclub aan kunt herkennen. Bovendien hangt het van je situatie en de garantie die je wilt over de kundigheid van de testers af voor welke partij je zult kiezen: een overheidsinstantie, interne audit-afdeling, familie, …
Hoeveel bevestiging wil je hebben dat iets echt goed is? Dit zal afhangen van het soort product en de omgeving, dus de waarde die je wilt beschermen.
Zekerheid zonder kader is niet definieerbaar en 100% zekerheid zal nooit verkregen worden.

Common Criteria richt zich op de secure claim van een fabrikant of klant over wat een product doet. Safety en security hangen nauw samen maar er is géén directe link tussen beide standaards!
Het certificaat is gebaseerd op de claim en algemene richtlijnen die bepalen of de claim zinvol is.
Een certificaat wordt verleend voor 1 configuratie / versie van het product.
Een test tegen Common Criteria zoekt antwoord op de WAT, HOE en WIE vragen:

- WAT doet het product; is het product ook echt dat wat beschreven wordt, is het veilig te installeren en veilig te beheren, hoe is de aflevering?
  hiertoe wordt alle documentatie en de sourcecode gelezen, installatie handleidingen en instructies getoetst en de aflevering beoordeeld
- HOE is het product beoordeeld / getest?
  hiertoe wordt een rapport opgesteld waarin vermeld staat tegen welke criteria het product getoetst is en welke methode hiervoor gebruikt is
- WIE heeft het product beoordeeld / getest?
  wanneer een certificeringbevoegde instantie het certificaat afgeeft geeft dit meer zekerheid dan wanneer een certificaat via internet gekocht wordt

Het is van belang een certificeringbevoegde instantie zo vroeg mogelijk bij het product te betrekken – de evaluatie kan de ontwikkelaar laten zien wat hij moet doen, er wordt getoetst aan een lijst van criteria. Bij de evaluatie wordt aangegeven wát beveiligingtechnisch gezien niet handig gedaan is, maar niet hóe het dan wel moet omdat daarmee de kans bestaat dat informatie over hoe concurrenten het opgelost hebben verklapt wordt. Een onafhankelijke

certificeringbevoegde instantie mag deze informatie niet geven.
Ontwikkelaars gaan uit van een positieve situatie of technische problemen waarin ze keuzes moeten maken. Dit kan een verkeerde keuze worden doordat een ideaal eindbeeld in het hoofd bestaat en security gerelateerde zaken in de zijlijn staan. Neem bijvoorbeeld de PIN-controle;
Voor het bijhouden van het aantal fout PIN-pogingen bestaan meerdere mogelijkheden:

a) trek eerst 1 van de teller af, controleer de PIN en bij goede PIN tel er weer 1 bij de teller op
b) controleer de PIN en bij foute PIN, trek 1 van de teller af

Het resultaat is in beide gevallen hetzelfde, maar vanuit security oogpunt is B niet aan te raden omdat dan de teller te manipuleren is wanneer na een PIN ingave de kaart direct weggetrokken wordt voordat de teller verminderd is.

In het oerwoud van certificeringen, dat ontstond doordat ieder land zijn eigen specificaties gebruikte, is met de ISO-standaardisatie voor Common Criteria duidelijkheid geschapen.

De verschillende specificaties zijn onder ISO 15408 opgenomen.

Je kunt het zo idioot niet verzinnen of er zit tegenwoordig wel een IT-component in.
Alle IT-componenten vallen onder Common Criteria.
Common Criteria is gedefinieerd met het oog op softwareontwikkeling. Dit geeft soms problemen in samenhang met de hardware (bedenk bijvoorbeeld dat élke chip anders is). Common Criteria lost specifieke problemen op in specifieke beschrijvingen bij de oorspronkelijke definitie. Voor hardware is er methodologie bijgeschreven, m.n. voor smartcards. Dit geldt nog niet voor alle hardware, maar dit is nog groeiende!
Een ander voorbeeld is Differential Power Analysis: een IC geeft energie af bij operaties. Door dit te meten en de resultaten te analyseren kun je te weten komen wat de IC doet en zelfs sleutels bemachtigen. Een hardware fabrikant kan dit nooit tegengaan, dus moet het softwarematig voorkomen worden, bijvoorbeeld door elke operatie een willekeurige tijdsduur te geven.

Marketingmensen zijn goed in het verhullen van het wat, maar beveiliging zit in alle aspecten van het product. Doelgroepen van Common Criteria zijn klanten (kunnen we het gebruiken?), ontwikkelaars (kunnen we het maken?) en testers (kunnen we het testen?).
De probleembeschrijving gebeurt a.d.h.v. dreigingen waartegen het product beschermd moet worden. Deze dreigingen kunnen worden weggenomen door het product zelf, door aanpassingen in de omgeving of door een combinatie van beide.
Bij de dreiging worden bijbehorende policy's vermeld (een password is minimaal 10 karakters lang en bevat zowel hoofd- als kleine letters en cijfers) en de gedane aannames vastgelegd (secured room, enige verbinding, gescreend personeel, …)
Deze vormen de uitgangspunten bij de ontwikkeling.

Common Criteria biedt geen vaststaande set van functionele requirements, maar een set van ca 150 requirements waaruit je kunt kiezen. Wanneer je vindt dat deze niet voldoende zijn voor jouw product, kun je eigen requirements toe laten voegen. Deze moeten echter door het evaluation board beoordeeld worden en dit kost dus extra tijd. Ervan uitgaande dat producenten zo snel mogelijk de markt op willen met hun gecertificeerd product, gebeurt dit dus niet vaak.
Per blok van requirements worden de afhankelijkheden onderkend (bv: identificatie/ authenticatie is gekoppeld aan een tijdsaspect).
Common Criteria is niet perfect of uitputtend – het doel is een set requirements te geven die ondubbelzinnig, consistent en zo compleet mogelijk is. Dit lukt nog niet overal, maar de internationale interpretatiecommissie blijft het geheel aanscherpen en verbeteren.
In de nieuwste versie van Common Criteria (V3.0) verdwijnen de functiebeschrijvingen; testen tegen zowel requirements als security-functionaliteit heeft geen toegevoegde waarde – je zou twee maal hetzelfde aan het testen zijn.

De certificeringbevoegde testlabs behouden hun onafhankelijkheid doordat zij alleen het evaluatierapport opstellen. Het werkelijke certificaat wordt na beoordeling van dit rapport uitgegeven door een aparte "certification body", welke meestal een overheidsinstantie is.
De CB's reviewen elkaar en

controleren alle evaluatieresultaten.
De testlabs moeten ISO 17025 gecertificeerd zijn en worden jaarlijks aan een audit onderworpen. Daarnaast moeten de medewerkers aantonen dat zij de Common Criteria kennen.
Elk land kan als CB aantreden na behalen van het vereiste examenresultaat.
Cultuurverschillen leiden soms tot verschillende interpretaties tussen de diverse landen, maar de gezamenlijke CB's vormen de interpretatiecommissie die de criteria bewaken, verbeteren en misinterpretaties afwijzen.
De testlab's testen op functionaliteit, kwaliteit van de procedures, lifecyclemanagement, development security (on side controles), development documentatie (worden de security-functies correct beschreven) en een availability analyse (functionele testen & penetratietesten).
Common Criteria gaat uit van de goedwillende ontwikkelaar onder de aanname dat lang consequent liegen erg moeilijk vol te houden is.

Common Criteria kent 7 "Evaluation Assurance Levels", gepredefinieerde sets waar verschillende IT-systemen aan zouden moeten voldoen.
Op niveau 1 bevinden zich hele grote systemen en systemen die niet voor beveiliging bedoeld zijn - alle requirements worden een beetje getest. Op niveau 4-5 bevinden zich de smartcards Op niveau 7 bevinden zich zeer kleine producten als datadiodes en zeer kritische (deel-)systemen – alle requirements worden helemaal getest.
Er bestaat geen enkele relatie tussen de EAL's en levels zoals die binnen CMM onderkend worden, hoewel de CMM levels wel meewerken om een hoger EAL te kunnen bereiken.

Frank Brunnekreeft

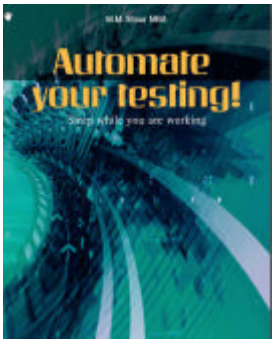
Hierbij wil het bestuur Frank Brunnekreeft bedanken voor zijn jarenlange inzet binnen de kascommissie. Frank heeft vorig jaar afscheid genomen nadat hij sinds de oprichting van TestNet in de kascommissie een belangrijke rol heeft gespeeld.
Frank bedankt voor je inzet.

Publicaties door leden

Automate your testing! Sleep while you are working
Auteur: Maurice Siteur
ISBN 90395 24424

Tijdens EuroSTAR in Kopenhagen is het tweede boek van Maurice Siteur gepresenteerd. Het eerste exemplaar werd aan Martin Pol overhandigd, de Chairman van EuroSTAR.

Voor wie zijn eerste boek (testen en testtools - slapend werken) al kent zal merken dat het behalve in het Engels ook sterk veranderd is. De helft van het boek heeft een totaal andere inhoud gekregen en de bestaande onderdelen zijn aangepast aan de zienswijze van het heden. De buitenkant is niet een standaard formaat uit een reeks, maar een eigenzinnige weergave van het boek. Het straalt snelheid uit.



Als Maurice spreekt over test tooling, dan komt de term "testtoolstrategie" regelmatig uit zijn mond. Hij is er van overtuigd dat elke bedrijf er één zou moeten maken om een juiste afweging te maken van de testactiviteiten die er zijn en de mogelijkheid om die te automatiseren of te ondersteunen. In het boek is er een apart hoofdstuk aan gewijd. Meer informatie is te vinden op:
http://home.casema.nl/msiteur

Evenementen

Voorjaarsevenement "Testen van security" en ALV

Plaats	Nieuwegein
Gebouw	: NBC
Datum	5 april
Tijd	ALV vanaf 16.00 uur Evenement vanaf 18.00 uur

Belangrijk :
Aanmelden uiterlijk 1 april
Beschrijving:
"Security" staat op alle fronten en vanuit verschillende perspectieven in de belangstelling. Maar wat betekent dit voor het testen van systemen? Verschillende sprekers zullen hierover vanuit verschillende invalshoeken hier een boekje over open doen:
Peter Cornelisse van KPMG geeft een keynotepresentatie over de securityrisico's in hedendaagse systemen.
Daarna zijn er drie parallelpresentaties:

- Edwin van Vliet (Yacht) : Hack Me, Test Me - Websecuritytest
- Ruud van Munster (TNO) : Biometrie en Intelligente Camerasystemen
- Marc Witteman (Riscure) : Security en smartcards

De avond wordt afgesloten met een keynotepresentatie van Ruud Goudriaan van de ING over digitale handtekeningen.
E-mail: evenementen@testnet.org
Fax: 055 - 5415715

Thema-avond "Testinfrastructuur"

Plaats	Nieuwegein
Gebouw	: NBC
Datum	17 mei
Tijd	18:00 - 22:00

Belangrijk :
Aanmelden uiterlijk 1 maart
Hoe zet je een infrastructuur op voor testen en hoe beheer je deze. Denk aan testdata, omgevingen, tools e.d. Andere aspecten zijn ketentesten, synchronisatie van testdata, hoe om te gaan met wetten en regelgeving.
E-mail: evenementen@testnet.org
Fax: 055 - 5415715

Thema-avond "Model Based Testing"

Plaats	Nieuwegein
Gebouw	: NBC
Datum	8 juni
Tijd	18:00 - 22:00

Belangrijk :
Aanmelden uiterlijk 1 maart
E-mail: evenementen@testnet.org
Fax: 055 - 5415715

Najaarsevenement

Plaats	Nieuwegein
Gebouw	: NBC
Datum	25 september
Tijd	-

Belangrijk :
Aanmelden uiterlijk 1 maart
E-mail: evenementen@testnet.org
Fax: 055 - 5415715

Thema-avond "Testen van chips (in de financiële wereld"

Plaats	Nieuwegein
Gebouw	: NBC
Datum	24 oktober
Tijd	18:00 - 22:00

Belangrijk :
Aanmelden uiterlijk 1 maart
E-mail: evenementen@testnet.org
Fax: 055 - 5415715

Thema-avond "Testen van pakketten (ervaringsverhalen)"

Plaats	Nieuwegein
Gebouw	: NBC
Datum	13 december
Tijd	18:00 - 22:00

Belangrijk :
Aanmelden uiterlijk 1 maart
E-mail: evenementen@testnet.org
Fax: 055 - 5415715

Colofon

TestNet Bestuur

Bob van de Burgt	Voorzitter
Hans van Loenhoud	Vice-voorzitter & 2e penningmeester & Marktverkenning
Han Toan Lim	Penningmeester
Hans van Loenhoud	Secretaris & Ledenadministratie
Meile Posthuma	Informatievoorziening en beheer
Hans van Loenhoud a.i.	Marktverkenning Informatievoorziening & Beheer
Michiel Vroon	Evenementen & Thema-avonden

TestNet Marktverkenning, Informatievoorziening en Beheer

Hans van Loenhoud a.i. (T)

TestNet Web

Meile Posthuma (T)
Bob van de Burgt

TestNet Nieuws

Meile Posthuma (T)
Milo van der Kruis
Hein Baan
Johan Vink
E-mail: tnn@testnet.org

TestNet Evenement & Thema

Michiel Vroon (T)
Rik Marselis
Cees Dulfer
Ine Lutterman-Baars
Bart Knaack,
Guido Dulos
E-mail: cie-ce@testnet.org (algemeen)
E-mail: evenementen@testnet.org (aanmelden)

TestNet Lid worden

U kunt lid worden door een e-mail te sturen naar de ledenadministratie of door op onze Internet site het on-line registratieformulier in te vullen.
Internet site: www.testnet.org

TestNet Ledenadministratie

Hans van Loenhoud
E-mail: ledenadministratie@testnet.org

TestNet Nieuws©

TestNet Nieuws verschijnt eenmaal per kwartaal. Kopij aanleveren per e-mail aan de redactie
Het is niet toegestaan om de nieuwsbrief of delen eruit zonder bronvermelding over te nemen.

Legenda: (T) = Trekker aandachtsgebied