Juni 2006

Nieuwsbrief van de vereniging TestNet

TNN

TestNet Nieuws

Van de redactie

Door Meile Posthuma
tnn@testnet.org

We komen er niet onderuit, maar veiligheid wordt steeds belangrijker voor onze applicaties. Of het nu interne applicaties zijn of applicaties die we als bedrijf via het Internet aan onze klanten ter beschikking stellen. Ons voorjaarsevenement stond al in het teken van Security-testen en nu ook deze TNN. Verscheidene sprekers van het voorjaarsevenement hebben voor deze TNN een artikel ingestuurd, maar ook andere TestNet-leden. Onze vaste columnist neemt ons mee naar Amerika en geeft ons een indruk van STAREast. Verder vindt u verslagen van een thema-avond over Agile-testen en een verslag van de ALV. De redactie wenst u veel leesplezier. Na alle security-artikelen geeft Ernst van den Bos volledig openheid van zaken in de 5 vragen aan..

In dit nummer

Van de voorzitter

Door Bob van de Burgt
voorzitter@testnet.org

Security testen

Het voorjaarevenement met als thema "Het testen van security" is door velen van u met enthousiasme ontvangen. Het onderwerp is kennelijk "hot". Toch zijn er nog maar weinig testers met dit onderwerp bezig. De security-discipline is bij veel bedrijven vanuit de infrastructuur afdeling ontstaan. In het verleden werden aanvallen dan ook vaak op netwerkniveau of autorisatieniveau gepleegd. De meeste testers houden zich nog nauwelijks met security-testen bezig. Als het al gebeurd is het vaak beperkt tot het functioneel testen van de autorisatiemodules van de systemen. Op het voorjaarevenement werd onder andere maar weer eens duidelijk dat de praktijk van vandaag de dag laat zien dat steeds meer aanvallen via applicaties worden uitgevoerd. Dit is primair niet het gebied waar de afdeling infrastructuur zich mee bezig houdt, maar veel meer de testers. Er zou veel meer gezocht moeten worden naar aanpakken vanuit beide disciplines in een intensieve samenwerking. Dan zullen de beste resultaten bereikt kunnen worden. Er ligt dus wéér een mooie uitdaging op ons te wachten!

Blijft nog over de security-aspecten rond "social engineering", het toegang verkrijgen middels het informatie ontfutselen en/of misleiden van mensen. Tja, dat is ook een vak apart ;-)

De Algemene LedenVergade-ring 2006

Door Hans van Loenhoud
secretaris@testnet.org

4 April jongstleden werd, voorafgaand aan het drukbezochte voorjaarsevenement 'Testen van Security', de jaarlijkse algemene ledenvergadering van TestNet gehouden. Naast het bestuur waren 18 leden aanwezig om mee te praten over het afgelopen jaar 2005 en het beleid voor 2006. Voorzitter Bob van de Burgt stelde in zijn opening met genoegen vast dat ieder jaar een trouwe kern van leden de moeite nemen om de ALV bij te wonen.

In het jaarverslag 2005 legde het bestuur verantwoording af over het gevoerde beleid. In het algemeen kan worden gezegd dat het bestuur het jaarplan 2005 nauwgezet heeft gevolgd. Ook de financiële kant is door penningmeester Han Toan Lim goed verzorgd, wat formeel werd vastgesteld door de kascommissie, Rob Baarda en Rik Marselis. De vergadering verleende dan ook unaniem decharge aan het bestuur voor het in 2005 gevoerde beleid.

Bij de bespreking van het jaarplan 2006 meldde secretaris Hans van Loenhoud een voorspoedige groei van TestNet. Bij de start van 2006 stond de teller op bijna 440 leden en ten tijde van de ALV was de 500 al gepasseerd.

Namens, de wegens vakantie verhinderde, Michiel Vroon schetste Bob van de Burgt de geplande evenementen van 2006. Naast een aantal interessante thema-avonden en het aansluitend aan de ALV gehouden voorjaarsevenement belooft het najaarsevenement over teststrategie weer een echte klapper te worden.
Bestuurslid Meile Posthuma kondigde op zijn beurt een geheel vernieuwde versie van de website aan. De werkgroepen hebben in 2005, wegens onderbezetting in het bestuur, niet veel aandacht gekregen. Desondanks zijn er afgelopen jaar 4 werkgroepen actief geweest, waarvan de in samenwerking met ITB opgezette werkgroep over Outsourcing is afgerond met de oplevering van een white paper; de overige werkgroepen zullen in 2006 met resultaten komen. Om in 2006 een actiever beleid ten aanzien van de werkgroepen te kunnen voeren is Bart Watertor aangetrokken als nieuw bestuurslid. De aanwezige leden stemden unaniem in met zijn kandidatuur, zodat vanaf nu het bestuur weer op volle sterkte is.
De begroting voor 2006 laat een beperkt tekort zien, dat waarschijnlijk grotendeels kan worden opgevangen door de verwachte ledengroei en anderzijds probleemloos kan worden afgedekt vanuit de, in de afgelopen jaren opgebouwde, reserves. De leden hadden daar geen moeite mee en keurden het jaarplan 2006 volmondig goed.

Het bestuur legde twee punten ter besluitvorming voor aan de vergadering.
Het eerste punt betrof het voeren van een stringenter toelatingsbeleid voor niet-leden op thema-avonden. Uitgangspunt is dat niet-leden die incidenteel een thema-avond willen bezoeken daarvoor voortaan een kostendekkende bijdrage betalen. Voor 2006 is deze vastgesteld op € 35. Dit voorstel werd door de vergadering aangenomen.
Daarnaast stelde het bestuur een kortingsstaffel voor, waardoor bedrijven korting krijgen naarmate zij meer medewerkers als lid aanmelden. Dit voorstel is geïnitieerd door een, in de afgelopen maanden, duidelijk toegenomen belangstelling voor het bedrijfslidmaatschap. De leden echter betwijfelden nut en noodzaak van deze regeling en vonden daarnaast de financiële onzekerheid te groot. Het voorstel werd dan ook met een grote meerderheid van stemmen verworpen.

Door de leden werden ook enkele punten ter bespreking aangedragen. Zo werd onder andere bezorgdheid geuit over het gebrekkig functioneren van de aanmeldfunctionaliteit op de website. Bestuurslid Meile Posthuma gaf aan dat deze problemen na de introductie van de nieuwe site tot het verleden zullen behoren.
Verder werden suggesties gedaan voor het opzetten van extra commissies voor speciale evenementen, bijvoorbeeld een lustrumcommissie voor het tienjarig bestaan van TestNet in 2007. Het bestuur zegde toe daar te zijner tijd een oproep voor te zullen doen.

Aan het eind van deze in goede sfeer verlopen vergadering dankte de voorzitter de aanwezigen voor hun actieve inbreng. Hierna liet iedereen zich het gereedstaande buffet smaken, waarna het voorjaarsevenement ruimschoots tegemoet kwam aan hun intellectuele behoeften.

Even voorstellen...

Door Bart Watertor
werkgroepen@testnet.org

Mijn naam is Bart Watertor en ik in april toegetreden tot het bestuur van onze vereniging en verantwoordelijk voor de portefeuille Marktverkenning & Werkgroepen. Ik ben 37 jaar, woon in Almere met vrouw en 2 zoons en ben al ruim 10 jaar actief op het vakgebied testen, waarvan de laatste jaren als Testmanager.
Sinds ik een paar jaar terug in mijn werk werd geconfronteerd met het fenomeen outsourcing is bij mij het besef gegroeid dat professionalisering van ons vakgebied van steeds groter belang wordt. Toen ik vorig jaar samen met Hans van Loenhoud deelnam in een werkgroep m.b.t. outsourcing, zag ik ook in dat innovatie van ons vakgebied noodzaak aan het worden is. We moeten immers toegevoegde waarde kunnen bieden voor onze werk-/opdrachtgevers als we 'in business' willen blijven.
Met Testnet als vereniging hebben we een geweldig platform om niet alleen kennis te delen en te vergroten, maar ook om de benodigde professionalisering en innovatie te realiseren. Ik wil hier graag mijn steentje aan bijdrage.

Dat brengt mij gelijk bij het volgende……

Oproep

We hebben op dit moment een aantal actieve werkgroepen, waarvan jullie later dit jaar nog meer gaan horen. Juist deze werkgroepen dragen actief bij

aan de professionalisering en innovatie van ons vakgebied, dus je begrijpt dat we deze successen graag willen voortzetten en liefst nog uitbreiden. Om dit te realiseren hebben we jullie creatieve geesten nodig. Dus, laat me weten welk onderwerp jij vindt dat nadere bestudering of uitwerking in de vorm van een werkgroep verdient op werkgroepen@testnet.org.
Als we werkgroeponderwerpen hebben maar geen testnet leden die hier invulling aan kunnen geven, komen we natuurlijk ook geen stap verder, dus geef ook aan of jullie een actieve bijdrage aan de invulling van deze werkgroep willen leveren. Het is dé kans om richting te geven aan je eigen toekomst (én het staat ook goed op je CV, trouwens).
Ik zie jullie ideeën en aanmeldingen met veel plezier tegemoet!

Erik's Column

Door Erik van Veenendaal
eve@improveqs.nl

Testen in Amerika

Lekker weer, mensen in korte broeken, veel vrouwen …. Vakantie aan de Middellandse zee? Nee hoor een testconferentie in Amerika: STAREast. Het Amerikaanse familielid van EuroSTAR. Vele malen groter dan EuroSTAR, zoals alles in Amerika groter is. Opvallend is de veel meer ontspannen sfeer, daar waar op EuroSTAR iedereen in pak rondloopt, kan je hier bijna geen pak ontdekken. Vind je een lezing niet leuk, dan loop je toch gewoon halverwege de zaal uit. Dit gedrag wordt zelfs gestimuleerd door de organisatie!! Tijdens STAR waren er drie Nederlandse sprekers, de drie auteurs c.q. ontwikkelaars van onze Nederlandse teststandaard TMap. Martin Pol en Ruud Teunissen deden een tutorial over respectievelijk TPI en TPA en ondergetekende was uitgenodigd door de organisatie voor een keynote met als onderwerp "Practical Risk Based Testing".

De inhoud van de conferentie was zeker interessant. Opvallend was dat er in Amerika duidelijke twee stromingen zijn. De proces georiënteerde testers die spreken over testen in de context van CMMi, of over het toepassen van gestructureerde testtechnieken en testcertificatie in de context van ISTQB (dat inmiddels een flinke aanhang heeft in de States). Opvallend was ook de ruime bekendheid van onze TMap methode. Daarnaast is er de groep die behoort tot de agile stroming waarin exploratory testen, SCRUM e.d. veel wordt besproken. Iedereen behoort tot één van de twee groepen. Je bent voor of je bent tegen! Het Nederlandse poldermodel en balanceren is duidelijk nog niet de oceaan over gestoken. Opnieuw viel mij op dat alle agile verhalen bijna allemaal een context hebben die duidelijk niet afkomstig is van echte grote (multidisciplinaire) systemen met een aanzienlijk risicogehalte. Ook een keynote van Jon Bach (jawel, de broer van …) viel mij tegen, weinig echte nieuwe zaken.

Voor mij sprongen er twee lezingen boven uit, die echt toegevoegde waarde hadden. Een lezing door Isabel Evans van over toepassen van de "balanced score card" op het testen met als doel het verbeteren van test awareness en een rapportagestructuur te creëren die ook het management aanspreekt. Heel langzaam wordt testen volwassen en gaan we praten in de taal van de business. Nog veel te veel rapporteren wij in een technische taal en zijn we verbaasd dat niet naar ons wordt geluisterd.

De andere lezing die mij vooral aansprak had CTM als onderwerp. Via ISEB Practitioner ben ik een aantal jaren geleden in contact gekomen met de testontwerp techniek Classification Tree Method (CTM). Inmiddels hebben wij (Improve) deze techniek bij veel bedrijven kunnen implementeren en het blijkt een uitermate gedegen techniek te zijn, niet in het minst door de ondersteunende tools die beschikbaar zijn. Tijdens de presentatie werden praktijkervaring met CTM besproken en werd de techniek nogmaals uitgebreid gedoceerd. Een tip voor de tester die deze techniek nog niet kent, ga je hier eens in verdiepen.

Is men verder met testen dan in Europa? Wat mij betreft niet, echte nieuwsfeiten heb ik niet gehoord, hoewel het gemiddelde niveau van de presentatie hoger ligt dan tijdens EuroSTAR. Al met al een plezierige week in een prettige omgeving: Happy Testing !!
Voor vragen of een reactie kunt u mailen met Erik van Veenendaal.

TestNet Site

Door Meile Posthuma
webmaster@testnet.org

Als u dit artikel leest, dan kan het u niet ontgaan zijn dat onze TestNet-site compleet vernieuwd is. Op 1 mei zijn we life gegaan. De site biedt nu meer mogelijkheden om zaken online af te handelen. Het aanmeldingsformulier werkt nu beter en tevens is er de mogelijkheid om de eigen gegevens online te wijzigen. Ook bestaat er nu de mogelijkheid om je online aan te melden voor een TestNet-evenement. TestNet gaat ervan uit dat de nieuwe site bijdraagt aan een betere dienstverlening voor nieuwe en bestaande leden. Hebt u op- en / of aanmerkingen op de inhoud of de werking van de nieuwe site, laat het dan even weten via het ons emailadres webmaster@testnet.org.

Thema-avond "Agile testen"

Door Rick de Jong - R.de.Jong@cimsolutions.nl

Donderdag 16 maart jl. organiseerde TestNet een thema-avond rondom het thema "Agile testen". De bijeenkomst vond (zoals vaker) plaats in het NBC te Nieuwegein en werd deze keer inhoudelijk verzorgd door Marc Evers en Anko Tijman.

Presentatie "Agile testen – Kwaliteit onder controle"

Tijdens hun presentatie zijn Marc en Anko ingegaan op de rol van testen binnen agile processen. Wat betekent agile testen? Hoe vindt de kwaliteitsborging plaats in agile projecten? Daarbij hebben ze diverse aanknopingspunten aangereikt waarmee testers aan de slag kunnen. Normen en waarden, kwaliteitsprincipes en technieken van een agile testproces staan centraal. Ook zijn begrippen als Test Driven Development, Quality Assurance en enkele eenvoudige toepasbare testtechnieken vanuit een agile context besproken.

Agile… ???

… is niet de zoveelste methodiek of wondermiddel: het is een manier van denken en een houding. Agile processen zijn zeer klant- en kwaliteitsgericht. De focus ligt primair op het resultaat (vaak een product), minder op methoden en procedures. In de praktijk blijkt steeds vaker dat met een agile manier van denken en werken softwareprojecten succesvol opgeleverd kunnen worden, met efficiënt gebruik van middelen.

Projecten die gebruik maken van Agile systeemontwikkeling worden over het algemeen gekenmerkt door een 5-tal karakteristieken. Ze zijn iteratief, wat feitelijk betekent dat (deel)processen zo vaak als noodzakelijk herhaald. Er wordt gewerkt aan een vaste, vooraf bepaalde, hoeveelheid functionaliteit, een zogenaamd "increment". Iteraties zijn kort cyclisch, ca. 2 tot 4 weken, waarbij optimalisatie van de hele cyclus plaatsvindt (loop) en niet slechts een deel. Er wordt continue bekeken wat de meeste waarde heeft, ofwel het stellen van prioriteiten en ten slotte: "Eenvoud eerst". Het gebruik van deze karakteristieken betekent niet dat er per definitie Agile wordt ontwikkeld, het is echter wel een startpunt. Een startpunt dat invulling geeft aan de betekenis van Agile: flexibel, wendbaar.

Agile is voor een groot deel ontstaan uit bestaande en bewezen werkwijzen (Min. van Defensie VS.) en vindt zijn oorsprong in o.a. de "lean" productie, het JIT-principe en het Toyota Productie Systeem (lees hierover o.a. het boek "The Toyota Way"). De nadruk ligt enerzijds op het systeemdenken, maar tegelijkertijd is er aandacht voor de rol van de mens en teamdynamiek. Een project waarbij meer fouten worden ontdekt zodra het koffiezetapparaat wordt weggehaald, is één van de mooie voorbeelden die worden aangehaald tijdens de presentatie. Bottom line: "Het systeem is uiteindelijk meer dan de som der delen".

Op de vraag of er voor Agile-projecten een grens is aan het aantal projectleden, weet Anko te vertellen dat er geen absoluut maximum is, maar dat een projectteam van 4 tot 8 personen wel vaker regel, dan uitzondering is. Overigens is het lastig om van tevoren een goede schatting te geven van het aantal benodigde FTE's voor een project. Hoeveel testers zijn er bijvoorbeeld nodig? In een van de huidige projecten werd in het begin een standaardverhouding van één tester op elke 3 ontwikkelaars gehanteerd, echter na een aantal iteraties wordt hier vanuit de ervaring van het project(verloop) wel op gestuurd.

Zoals eerder genoemd is Agile erg resultaatgericht, met de nadruk op een duurzaam resultaat! Het opleveren van waardevolle software. Dit betekent tevens dat elke iteratie

in principe een oplevering (van software) kent die gereleased zou moeten kunnen worden. Werkende software wordt dan ook beschouwd als beter/ belangrijker dan documentatie. Ook is er duidelijk aandacht voor de “mensen” en het “proces” binnen een project. Mensen (de klant, eindgebruikers, ontwikkelaars, testers, …) worden niet als vanzelfsprekend beschouwd, maar gezien als een grote meerwaarde tijdens het ontwikkeltraject.

Agile is grotendeels een denkwijze en houding waarbij continue gestuurd wordt op basis van feedback. Een van de aanwezigen vraagt zich af of de feedback van (bijv.) gebruikers ook een gevaar kan vormen, bijvoorbeeld m.b.t. wijziging in de releasesamenstelling en uiteindelijk de planning en doorlooptijd van het project. De keerzijde is echter dat de wensen van de gebruiker te laat of niet gehoord worden. Een mechanisme om toch enige rust in het team te behouden, is het vasthouden aan de taken die afgesproken zijn voor een iteratie. Voor elke nieuwe iteratie krijgen de wensen vanuit stakeholders een prioriteit en worden afhankelijk daarvan meegenomen bij de ontwikkeling. Samenwerken met “de klant” werkt ook meer op vertrouwensbasis dan aan de hand van een contract.

Er is geen plaats voor de zogenaamde “hokjes gedachte”. Niet de tester of bouwer doet iets, … maar het team doet iets. Daarbij komt dat het proces continue wordt aangepast aan de veranderende omgeving. Dit alles met het doel om op een effectieve en efficiënte wijze goede software op te leveren. Verbeteringen vinden plaats in kleine stappen en communicatie speelt een belangrijke (zo niet de belangrijkste!) rol.

Agile en testen

Agile softwareontwikkeling is een beweging die de afgelopen jaren sterk in opkomst is. Agile processen lijken voor een buitenstaander op het eerste gezicht ongestructureerd, chaotisch en onvoorspelbaar. Vaak word gedacht dat testers hierin geen rol kunnen spelen, bij gebrek aan structuur.

DSDM en RUP zijn voorbeelden van Agile systeemontwikkeling waarin een duidelijke rol voor testers is weggelegd. Een uitdaging voor testers is de verwachting van “snelle feedback”. Dit kan betekenen dat de tester zich in eerste instantie zal moeten richten op de eenvoud, d.w.z. de simpele onderdelen van het systeem. Ook op het gebied van communicatie ligt er een uitdaging voor testers, het is niet langer mogelijk om met de deur dicht te werken of bij wijze van spreken “aan de andere kant van de muur”. Het draait om teamwork, waarbij communicatie het middel is om elkaar constant te informeren. Dit is van essentieel belang, aangezien voor Agile projecten min of meer geldt: “vandaag is de waarheid!” Hoe achterhaal je de waarheid? Juist, door te communiceren. De collega naast je (een willekeurige stakeholder) is in dit geval je “Orakel” cq. “Testbasis”. Cem Kaner, James Bach en Bret Pettichord hebben o.a. deze pragmatische aanpak beschreven in het boek “Context driven testing”, volgens Marc en Anko een echte aanrader.

Testen is binnen Agile systeemontwikkeling geen aparte fase, maar een ingebedde (essentiële) activiteit. Alle betrokkenen moeten overigens testen kunnen begrijpen, of in ieder geval het resultaat kunnen interpreteren en analyseren. Testen wordt gezien als de basis voor kwaliteit- en risicomanagement, de basis om projecten te sturen. Kort gezegd betekent “Niet-testen”, geen feedback en dus geen informatie.

Test Driven Development

Het ontwikkelen van software, waarbij eerst de test wordt uitgewerkt en vervolgens pas de (te testen) functionaliteit wordt Test Driven Development (TDD) genoemd. TDD verloopt incrementeel (niet alle testen tegelijk, maar stap voor stap), zorgt voor snelle en regelmatige feedback over de kwaliteit van het product, en is toepasbaar op verschillende niveaus en aspecten: technisch ontwerp/ coderen, functionaliteit, performance & schaalbaarheid (zgn. non-functionals). TDD heeft als een van de voordelen dat het software “simpel” houdt, d.w.z. het is gericht op de oplossing (wat moet het component doen?) en voorkomt daardoor veel overbodige code. In projecten waar geen TDD wordt toegepast is soms zelfs sprake van 50% niet-gebruikte code. De geautomatiseerde unit-tests die geschreven worden door de programmeurs vormen een (groeiend) vangnet van tests, een regressieset die continue en snel feedback geeft over (de impact van) wijzigingen in de code.

In TDD is niet alleen plaats

voor unit-tests. Ook systeem- en acceptatietesten (d.w.z. functionele tests) worden geautomatiseerd. Dit gebeurt op basis van bijv. use cases of “stories’. Tests worden aan het begin van elke iteratie gedefinieerd en vormen de specificatie van functionaliteit en acceptatiecriteria. Het voorkomen van regressie, herhaalbaarheid en snelheid, en het direct inzicht kunnen bieden in de voortgang zijn positieve eigenschappen van functionele tests bij TDD. Werken volgens TDD heeft overigens wel vaak een extra onderhoudsinspanning tot gevolg en vereist ook een ‘iets’ andere houding t.a.v. testen dan menig techneut gewend is.

Agile testtechnieken

Traditionele testtechnieken gaan vaak uit van een watervalsysteemontwikkeling, (veel) documentatie als testbasis, een aparte specificatiefase voor testgevallen en testen worden uitgevoerd door de tester. Agile testtechnieken worden gekenmerkt door eenvoud, (snel) toepasbaarheid, snelle feedback en zijn er “voor en door” teamleden. Ondanks dat bij traditionele systeemontwikkeling beslissingstabellen als testtechniek beschikbaar zijn, haken veel mensen (testers) af in het gebruik van deze techniek, of gebruiken hem slechts gedeeltelijk. In een Agile omgeving krijgt/ heeft de tester daarnaast geen tijd om 3 dagen lang testspecificaties uit te werken. KISS (Keep It Simple Stupid) is een van de toverwoorden bij de toepassing van Agile testtechnieken. Een voorbeeld hiervan is een “1-page-reference-card”.

Veel gebruikte technieken zijn equivalentieklassen/grenswaard enanalyse, Exploratory Testing, Pair Testing, Heuristic Evaluation (met o.a. 10 grondregels van Jacob Nielsen) en het alternatief voor de beslissingstabel bij Agile testen, Beslissingsanalyse.

Achtergrond van de sprekers

Marc Evers (marc.evers@systemsthinking.net) helpt softwareontwikkelaars, klanten en projectmanagers in het gezamenlijk opleveren van waardevolle projecten, als softwareontwikkelaar, trainer en coach. Hij organiseert tevens workshops en conferenties (zoals XP Day Benelux en Agile Open) op het gebied van Extreme Programming, agile softwareontwikkeling en systeemdenken. Op dit moment is Marc werkzaam als softwareontwikkelaar voor de Koninklijke Nederlandse Academie van Wetenschappen en verzorgt daarnaast trainingen en workshops via zijn eigen bedrijf Piecemeal Growth.

Anko Tijman (anko.tijman@ordina.nl) heeft acht jaar ervaring in professioneel software testen. Hij is ISEB Practitioner gecertificeerd tester en heeft de waarde van agile werkwijzen ervaren in diverse soorten projecten. Hij verzorgt regelmatig opleidingen op het gebied van software testen en heeft in 2005 een training over agile testen voor testers en niet-testers ontwikkeld. Hij heeft presentaties over dit onderwerp gegeven bij de conferenties Agile 2005, EuroSTAR 2003 en XP Day Benelux 2005. Sinds 2001 is hij een actief lid binnen de Nederlandse Extreme Programming interessegroep.

Tot slot…

Naast de hoge mate van interactiviteit met de aanwezigen, was het vooral de dynamiek tussen beide sprekers die mij erg is opgevallen tijdens deze TestNet bijeenkomst. Marc en Anko wisselden elkaar vrijwel continue af en vulden elkaars verhaal aan met voorbeelden uit hun eigen praktijkervaring. Naar mijn mening hebben zij met hun presentatie een helder beeld gegeven over de huidige stand van zaken rondom Agile systeemontwikkeling en “Agile testen” in het bijzonder.

Het inhoudelijke deel van de avond is afgesloten met een discussie, waarbij nog een aantal interessante vragen de revue passeerden, zoals: “Zou je in een vliegtuig stappen waarvan de software m.b.v. Agile systeemontwikkeling is gebouwd?” Anko reageerde door het stellen van een wedervraag: “Stap je in een vliegtuig dat op een 'traditionele’ manier is ontwikkeld? Een manier waarbij in ca. de helft van de tijd projecten uitlopen”. Als pleit voor “Agile” wordt ook wel eens gezegd: “Kleine stappen, klein probleem… Grote stappen, groot probleem!” Hiermee enigszins doelend op de (over het algemeen) kort cyclische werkwijze, die het mogelijk maakt om vroegtijdig te anticiperen op problemen en waar mogelijk bij te sturen!

Op de vraag hoe je het vertrouwen in “Agile” systeemontwikkeling bij stakeholders van het project kunt opbouwen, kwam als voorstel om deze stakeholders

regelmatig een kijkje in de keuken te laten geven. In ieder geval op alle belangrijke momenten, maar in principe zo vroeg mogelijk.

Een van de aanwezigen vraagt zich ook af in hoeverre je een risicostrategie kunt voeren bij "Agile" systeemontwikkeling, ofwel "hoe kun je succesvol en in een vroeg stadium gebruik maken van risico analyse, temeer omdat in de beginfase van een project lang niet altijd duidelijk is waar de prioriteiten van de stakeholders liggen?" Anko en Marc geven aan dat risico analyse in een "Agile"-project 'minder' voorspellend zal zijn. Het is echter maar de vraag in hoeverre het mogelijk is om bij traditionele systeemontwikkeling alle eisen direct vast te leggen. Waarschijnlijk is het verstandig om per functionaliteit een risicogebied te bepalen en deze vervolgens van een prioriteit te voorzien (dit zal ook onderdeel zijn van je teststrategie). Elke iteratie zul je vervolgens de risicostrategie bekijken en waar nodig bijsturen, gestuurd door de kritische succesfactoren en indicatoren die vanuit de stakeholders worden aangegeven. Deze succesfactoren en indicatoren zullen minder worden bepaald door de regels, maar meer door het product (het doel/resultaat).

Of Non-functionele eisen aan een product ook voldoende aandacht krijgen bij "Agile" systeemontwikkeling is afhankelijk van input hierover vanuit de stakeholders. Is een goede performance bijvoorbeeld een 'hot item' dan is het verstandig om een dergelijke eis naar voren te halen en hier vanaf de eerste iteraties aandacht aan te besteden. Hetzelfde geldt voor usability, schaalbaarheid, etc.

Heb je de thema-avond gemist en ben je toch geïnteresseerd in de presentatie van Marc en Anko, dan is een kopie van de presentatie evenals een boeklijst m.b.t. "Agile testen", enkele voorbeelden van TDD en een overzicht van de "Agile"-werkwijze bij Planon te downloaden van de (vernieuwde!) TestNet-website (www.testnet.org).

Definitie

De definitie van security testing of beveiligingstesten zoals de Nederlanders zeggen en natuurlijk volgens de glossary van ISTQB:

Testen om de beveiliging van een softwareproduct te bepalen.

Legal hack

Door Jeroen van Dongen
jeroen@lbvd.nl

Een legal hack wordt ook wel een penetratietest genoemd. En daarmee zitten we in het domein van deze nieuwsbrief: testen. Behalve functionele eisen worden aan de meeste informatiesystemen ook veiligheidseisen gesteld. Bijvoorbeeld dat alleen geautoriseerde gebruikers toegang mogen krijgen tot het systeem. Of dat de scheiding tussen verschillende functieniveaus gehandhaafd moet worden (gewone gebruikers mogen geen admin-rechten kunnen verkrijgen). Middels een 'legal hack' kan nagegaan worden of het systeem voldoende weerstand kan bieden aan diverse aanvalsscenario's.

De definitie van "voldoende" en de waarschijnlijke aanvalsscenario's vloeien doorgaans voort uit het karakter van het informatiesysteem. Hieruit kan ook worden afgeleid of een legal hack zinnig is. Vast omlijnde criteria zijn hiervoor helaas niet te geven. Zodra er sprake is van mogelijke invloed op geldstromen, mogelijke serieuze aantasting van het imago van de organisatie of van mogelijke aantasting van de privacy en/of invloed op de persoonlijke levenssfeer van personen is een grondige test op het gebied van beveiliging doorgaans zeer wenselijk. Bedenk ook dat een ketting zo sterk is als zijn zwakste schakel: één kwetsbaar systeem kan een hele infrastructuur onderuit halen. Uiteindelijk is het uiteraard aan de systeemeigenaar/ eindverantwoordelijke of hij de kosten van een legal hack vindt opwegen tegen de mogelijke risico's van het niet testen van het systeem.

Overigens, hoe nuttig een legal hack ook kan zijn, voorkomen is beter dan genezen. Helaas is het nog teveel zo dat er ten tijde van een ontwikkeltraject weinig tot geen aandacht wordt besteedt aan beveiliging van het systeem. Ja, natuurlijk wordt er in de functionele specificaties opgenomen dat een gebruiker moet inloggen. En dat wordt ook braaf geïmplementeerd. Echter men kijkt nog te weinig naar de kwaliteit van de implementatie. Zaken als bijvoorbeeld OWASP *(Zie www.owasp.org)* zijn nog grotendeels onbekend bij ontwikkelaars. En kennis over bijvoorbeeld de toepasbaarheid en toepassing van encryptie-algoritmen

ontbreekt even zo vaak. Men gebruikt in veel gevallen eenvoudig weg wat voorhanden is, zonder na te gaan of dit toereikend is. Maar dat terzijde …

Naast “digitale” aanvalsscenario´s kan ook gezocht worden naar kwetsbaarheden op het fysieke of menselijke vlak. Immers, waarom zou je moeite doen om in te breken in een database als je de benodigde informatie met een goede smoes gewoon kan opvragen bij een relevante medewerker … Er wordt dan gesproken over onder meer “social engineering”*(Het boek “The Art of Deception” van Kevin Mitnick is in dit licht wel aardig)*. Dit artikel beperkt zich echter tot de digitale varianten van de “legal hack”.

In grote lijnen komt het er op neer dat één of meerdere ter zake deskundigen de opdracht van een systeemeigenaar krijgen om gedurende een bepaalde tijd en binnen een vooraf gesteld kader te trachten oneigenlijk gebruik te maken van een bepaald systeem. Uit deze korte omschrijving blijkt ook al het verschil met een “illegal hack”: er is sprake van een opdracht van de eigenaar van het systeem en de hack vindt onder gecontroleerde omstandigheden plaats. Een ander belangrijk verschil is tevens dat daar waar een “echte hacker” kan volstaan met het blootleggen van één enkele kwetsbaarheid, van de “legal hacker” zal worden verwacht dat hij (afhankelijk van de afspraken) een zo compleet mogelijke test uitvoert.

Er zijn verschillende vormen en gradaties van een “legal hack” te onderscheiden als ook verschillende testdoeleinden. Daarom zal als eerste een overzicht gegeven worden van de verschillende vormen en gradaties. Hierbij is het goed om op te merken dat indeling en naamgeving kan verschillen van organisatie tot organisatie.

Doorgaans worden een drietal gradaties onderscheidden. In de “lichtste” variant is er alleen sprake van het identificeren van potentiële kwetsbaarheden zonder te trachten deze daadwerkelijk uit te buiten. Dit wordt doorgaans een kwetsbaarheidsscan genoemd. Het is echter discutabel of dit onder de noemer “legal hack” mag vallen. Een stap verder gaat het als de potentiële kwetsbaarheden ook worden geverifieerd – met andere woorden als de potentiële van de werkelijke kwetsbaarheden worden gescheiden. Afhankelijk van de vorm van de test kan dit gebeuren met of zonder medewerking van de opdrachtgever. In de zwaarste variant worden gevonden kwetsbaarheden zover mogelijk uitgebuit om maximaal door te kunnen dringen in de informatiesystemen van de opdrachtgever. In dat scenario gebeurt dit doorgaans geheel zonder (bewuste) medewerking van de opdrachtgever.

Qua testvorm zijn er ruwweg drie vormen te onderscheiden (wederom is de naamgeving niet altijd consistent):

- Blackbox: minimale voorinformatie, geen hulp van de opdrachtgever (behoudens het faciliteren van het testteam in de vorm van een werkplek, voorzover de opdracht dit toelaat/vereist), niet meer toegang tot het te testen object dan “het grote publiek”.
- Graybox: vergelijkbaar met blackbox, maar in dit geval wordt de onderzoeker voorzien van dezelfde informatie en toegang als een reguliere gebruiker. Het doel is in dit geval niet zozeer toegang, maar meer toegang - het verhogen van rechten. Een dergelijke test is nuttig indien de potentiële dreiging vooral/ ook van de gebruikers van het systeem komt, in plaats van alleen van buitenaf.
- Crystalbox: volledige openheid, toegang tot broncode, intensieve samenwerking met de opdrachtgever, enzovoorts.

De scope van een test kan variëren van één specifiek systeem, of zelfs een onderdeel van een systeem, tot een complete infrastructuur. Ook de plaats van uitvoering kan variëren, zoals bijvoorbeeld Internet of het lokale netwerk van de opdrachtgever – wederom afhankelijk van het doel dat de opdrachtgever voor ogen heeft.

Kijkende naar de feitelijke uitvoering van een legal hack kan gesteld worden dat hiervoor een tweetal zaken nodig is:

- Brede én diepgaande kennis op het gebied van ICT-systemen in het algemeen, en de voor het doelobject gebruikte technieken in het bijzonder;
- Een structuur c.q. procedure om tot een heldere, eenduidige en herhaalbare uitvoering en verantwoording van de legal hack te komen.

Het eerste punt zal vrijwel in geheel geleverd moeten worden door het testteam, in zekere

mate aangevuld met kennis van derden welke is gematerialiseerd in diverse ondersteunende tools. Het tweede punt kan worden ontleend aan de ervaring middels een methodiek zoals bijvoorbeeld de OSSTMM *(Zie http://www.osstmm.org)*. In grote lijnen is de structuur als volgt:

- Voorbereiding, verkrijgen van toestemming en vrijwaring
- In kaart brengen doelobject, afhankelijk van testvorm i.s.m. opdrachtgever
- Aftasten doelobject (hoe werkt e.e.a. onder normale omstandigheden)
- Identificeren kwetsbaarheden
- Verifiëren en eventueel uitbuiten kwetsbaarheden
- Rapporteren en presenteren resultaten
- Ondersteunen opdrachtgever bij het opstellen en uitvoeren van een verbeterplan

Het soort kwetsbaarheden waar tijdens een legal hack naar gezocht wordt is zeer divers en ieder type kwetsbaarheid zou een artikel op zich kunnen zijn. Een aantal veel voorkomende kwetsbaarheden in informatiesystemen zijn hieronder weergegeven.

Met stip op 1: gebrekkige controle op invoer en uitvoer. Alle invoer die een gebruiker (= potentiële hacker) kan beïnvloeden is per definitie onveilig en moet als zodanig behandeld worden totdat is gecontroleerd of de invoer is wat het zou moeten zijn. En “invoer die een gebruiker kan beïnvloeden” is feitelijk alle data die het systeem niet zelf heeft gegenereerd. Ook invoer uit “verborgen velden” of gegenereerd door een front-end applicatie in een 2-tier systeem is door een gebruiker te beïnvloeden! Een veel voorkomende categorie (vooral bij web based applicaties) is zgn. SQL injectie(Zie o.a. http://en.wikipedia.org/wiki/SQL_injection voor een korte introductie of http://www.securiteam.com/securityreviews/5DP0N1P76E.html voor een hands-on walk-through). Een ander voorbeeld is de zgn. bufferoverflow (http://en.wikipedia.org/wiki/Buffer_overflow).

Configuratiefouten zijn ook een rijke bron van kwetsbaarheden: o.a. veel te zwakke, default of zelfs geen wachtwoorden, “security by obscurity” - het verbergen van features zonder ze daadwerkelijk af te schermen of informatie vrijgeven die de aanvaller verder kan helpen.

Er zijn nog vele pagina's te vullen over de verschillende aspecten van (legal) hacking, maar het aantal beschikbare pagina's is ruimschoots gevuld. Het mag duidelijk zijn dat een legal hack een tamelijk complexe en diverse aangelegenheid is. Zowel het plannen van een legal hack als het uitvoeren vereist diepgaande kennis op het gebied van informatiebeveiliging in het algemeen, en computer beveiliging in het bijzonder. Het is dan ook zeer aan te raden om zo vroeg mogelijk in een ontwikkel en test traject een beveiligingsspecialist “bij te schakelen”.

Smart Card Security Testen

Door Marc Witteman technisch directeur bij Riscure.
info@riscure.com .

In tegenstelling tot veel functioneel georiënteerde testuitvoerders is de beveiligingstester nauwelijks geïnteresseerd in normale gebruiksituaties. De beveiligingstester richt zich primair op ongebruikelijk of foutief gedrag, en probeert hiermee inzicht te krijgen in sterkte van een systeem tegen kwaadwillende aanvallers. Smart cards zijn kleine apparaten met een centrale beveilingsfunctie. Ze zijn vaak uitgevoerd in een plastic kaart (zoals de chipknip of SIM), maar kunnen ook geïntegreerd worden in bijv. een autosleutel of paspoort. In de verpakking zit een chip met meerdere functies zoals een CPU, geheugen (permanent, herschrijfbaar en vluchtig), en communicatie interface.

Figuur 1: smart card voorbancaire toepassing

Een smart card wordt geacht “tamper proof” te zijn, wat betekent dat haar beveiliging ‘onbreekbaar’ is. Door deze eigenschap kan de smart card een centrale rol spelen in veel gevoelige processen, zoals bijv. betaling (chipknip), telefonie (SIM), identificatie (paspoort), transport (OV Chipkaart), vermaak (betaaltelevisie). De belangrijkste beveiligingsfuncties van de

smart card worden uitgevoerd met cryptografie: informatie kan vertrouwelijk worden uitgewisseld door vercijfering; toegang kan worden verleend door authenticatie; en echtheid kan worden gecontroleerd met elektronische handtekeningen. Het spreekt vanzelf dat als de beveiliging van de smart card gebroken wordt dat de hiervan afhankelijke processen ernstig ontregeld of zelfs onmogelijk raken. Om die reden is er bijzondere aandacht voor de kwaliteit van de uitgevoerde beveiliging. Smart card beveiligingstesten concentreren zich op de cryptografie, omdat het geheim van de sleutel haar achilleshiel is. De volgende dreigingen worden onderscheiden:

- **Brute force**: is het mogelijk de sleutel met brute kracht uit te rekenen?
- **Crypt analyse**: is het cryptografisch algoritme middels wiskundige herleidingen te kraken?
- **Protocol misbruik**: is het beschermde berichtenverkeer te misleiden?
- **Vulnerabilities**: zijn er fouten of zwakheden in hard- of software die misbruikt kunnen worden?
- **Side channel**: lekt er onbedoeld geheime informatie (bijv. door straling)?

Elk van deze dreigingen is realistisch, getuige de volgende praktijkvoorbeelden.

SIM kloon probleem
In de GSM wereld is ooit een authenticatie algorithm (COMP128) onder geheimhouding afgesproken. In 1998 raakte dit algoritme toch publiek bekend en werd middels crypt-analyse een zwakheid gevonden. In 2002 kwam een "SIM copy" programma beschikbaar op het internet. Door gebruikmaking van de zwakheid in het algoritme kon binnen enkele uren een zogenaamde kloon van de SIM kaart gemaakt worden, waarmee kwaadwillenden mogelijk konden frauderen. Meerdere GSM operators merkten dubbele identiteiten op hun netwerk en zagen zich genoodzaakt nieuwe SIM kaarten uit te geven.

DES algoritme verouderd
DES is het meest gebruikte symmetrische cryptografie algoritme. Sinds haar geboorte in de jaren '60 van de vorige eeuw is computerkracht echter enorm toegenomen waardoor de 56 bits sleutel niet meer voldoende was. Enkele jaren geleden werd aangetoond dat het zowel met een netwerk van computers als met een speciaal ontworpen machine het mogelijk was in korte tijd de sleutel met brute kracht te herleiden. Veel financiële instellingen hebben sindsdien hun bankkaarten omgeschakeld naar nieuwere algoritmes, zoals het veel sterkere 3DES.

Betaaltelevisie gratis
Aanbieders van betaaltelevisie gebruiken decoders met een smart card om middels een abonnement de betaling voor hun diensten te verzekeren. Al geruime tijd lijden zij verliezen doordat valse kaarten in omloop komen waarmee televisiekanalen zonder abonnement gedecodeerd kunnen worden. De originele kaarten blijken vaak middels een 'side channel' gemanipuleerd en gekopieerd te worden. Een populaire aanval wordt uitgevoerd met een zogenaamde 'unlooper', een kastje waarmee de voedingsspanning van de kaart dusdanig gemanipuleerd wordt zodat een foutieve authenticatie geaccepteerd wordt. De aanbieders zien zich genoodzaakt tot versnelde investeringen in nieuwere technologie om de piraten de pas af te snijden.

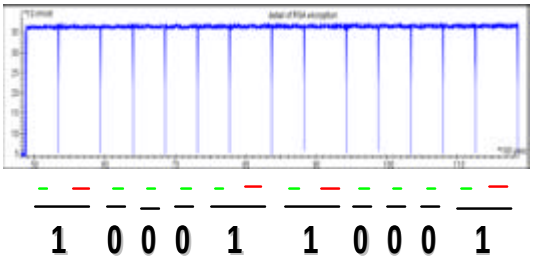
Het vervangen van smart cards is vaak een dure en lastige exercitie. Ook de imagoschade ten gevolge van een beveilingsprobleem is vaak aanzienlijk. Fabrikanten en beheerders van smart card gebaseerde systemen laten daarom zeer diepgaande tests uitvoeren om het vertrouwen te winnen dat hun product voor langere periode voldoende veilig is.

Riscure is een security test lab dat zich tot doel stelt haar klanten te helpen praktijkproblemen met hun smart cards en embedded devices te voorkomen. Zij doet dit door gedegen advies en geavanceerde test technieken. Deze testen omvatten meerdere activiteiten, zoals:

- Systeem en code reviews
  probeer zwakheden in het systeemontwerp in een vroegtijdig stadium te identificeren en beveiligingsfouten in source code te detecteren.
- Logisch penetratie testen
  test de robuustheid van het systeem over alle beschikbare interfaces
- Hardware testen
  test de bescherming van de hardware door de chip te openen en tot transistor niveau te onderzoeken
- Side channel testen
  test de mate waarin het apparaat informatie lekt, of gevoelig is voor

manipulatie van omgevingsfactoren zoals bijv. voedingsspanning of straling

Bovenstaande activiteiten zijn zeer divers en vereisen dan ook een breed scala aan deskundigheid op het gebied van informatica, elektronica, cryptologie, natuurkunde, scheikunde en wiskunde.



Figuur 2: Het energieverbruik van een smart card gemeten met een oscilloscoop verraad soms de cryptografische sleutel

Beveilingstesten zijn meer risico- dan functie gebaseerd. Dit kan leiden tot een gefragmenteerde en niet structurele aanpak. De grote uitdaging is dan ook om een systematische aanpak te vinden met veel aandacht voor een gebalanceerde test dekking. Ook de automatisering van beveiligingstesten blijft een bijzondere uitdaging om een maximale reproduceerbaarheid en efficiency te bereiken.

Veiliger met Intelligente camera systemen?

Door Stephanie Moro-Ellenberg
Stephanie.moro@tno.nl

De verwachtingen rond intelligente camera's als bijdrage aan de veiligheid op straat, bij een evenement of op een station zijn groot. Hollywood laat de mooiste voorbeelden zien van hoe met camera's personen door drukke straten gevolgd kunnen worden of hoe een tas met explosieven achtergelaten bij de afvalbak in een druk bezocht parkje feilloos gevonden wordt, etc. Helaas blijkt het in de praktijk minder makkelijk en soepel te gaan. Er moet aan behoorlijk wat randvoorwaarden voldaan worden om intelligente camera's hun intelligentie te kunnen laten benutten.
De behoefte aan technische middelen voor beveiliging is groot. De maatschappij is complexer geworden. Er heerst anonimiteit en mensen voelen zich onveiliger. De inzet van meer politie of bewaking biedt vaak geen oplossing omdat dit financieel en logistiek op grenzen stuit. Camerabewaking kan een nuttig hulpmiddel zijn om de surveillanten die er zijn met betere informatie te voorzien. Het ophangen van camera's alleen is maar een deel van de oplossing. Door de overvloed aan camerabeelden is het voor surveillanten of bewakingspersoneel onmogelijk om elke onveilige situatie op tijd te ontdekken. Camera's hebben pas toegevoegde waarde als ze zelf in staat zijn onveilige situaties te herkennen en de surveillant erop kunnen attenderen. Met het beeldmateriaal kan een onveilige situatie door de surveillance beoordeeld worden en kunnen snel gepaste maatregelen genomen worden en zelfs erger voorkomen worden.

Intelligente camera's worden voor de volgende taken gewenst:

- Bewegingsdetectie
- Detectie van afwijkende situaties
- Druktemeting of tellen van personen
- Gedragsherkenning
- Identificatie op afstand

De verschillende taken representeren verschillende moeilijkheidsgraden voor intelligente camera systemen (ICS). Op het laagste niveau wordt alleen naar beweging gekeken. Als beweging optreedt wordt een melding gegenereerd.
Op het volgende niveau wordt de beweging geanalyseerd en kan informatie over bijvoorbeeld objectgrootte en bewegingsrichting bepaald worden. Systemen zijn in staat om oninteressante beweging van bijvoorbeeld bomen in de wind of golven op een wateroppervlak te negeren.
Het derde niveau ICS omvat functionaliteiten als objectclassificatie (meestal beperkt tot personenauto, vrachtwagen, fiets of motor en persoon) en volgen (tracking en tracing) van objecten. Systemen kunnen omgaan met korttijdige occlusie (verdwijnen achter andere objecten) van het te volgen object. Ook wordt rekening gehouden met het perspectief in beeld (objecten op de achtergrond zijn immers kleiner dan op de voorgrond).
Op het vierde niveau wordt het gedrag van objecten herkend. Bijvoorbeeld "een personenauto rijdt slingerend over de weg" of "een persoon loopt rechtstreeks naar de uitgang toe". Het gedrag moet zich vooral door grove bewegingen (verplaatsing van het object) kenmerken. Subtiel gedrag (dreigende houding, wapen trekken, zakkenrollerei)

is vooralsnog niet uit videobeelden te achterhalen.

ICS van het eerste niveau zijn volop commercieel verkrijgbaar en worden vaak in combinatie met video registratie apparatuur aangeboden. De systemen zijn vooral geschikt voor het bewaken van gebieden waar juist geen beweging verwacht wordt (bijvoorbeeld industrieterrein bij nacht). Systemen van niveau 2 en 3 worden commercieel aangeboden maar zijn in de praktijk minder vaak ingezet dan de folders van leveranciers ons doen geloven. Er lopen tal van proeven, ook in Nederland, maar de resultaten tot nu toe zijn tamelijk teleurstellend. De systemen blijken zeer gevoelig voor de omgeving waar zij ingezet worden en moeten op elke situatie individueel afgesteld worden. Hiervoor is veel kennis van het systeem zelf nodig.
Op niveau 4 wordt vooral onderzoek verricht. Enkele bedrijven claimen oplossingen voor specifieke applicaties te hebben, maar in die gevallen gaat het vaak om slimme interpretatie van de gegevens die met systemen van niveau 2 of 3 verkregen worden. Echte gedragsanalyse is nog in het stadium van universitair onderzoek.

Om de betrouwbaarheid van een ICS te beoordelen is het nodig om een systeem voor een langere periode in de gewenste applicatie te testen. Omdat de huidige oplossingen nog niet generiek genoeg zijn treden in elke nieuwe applicatie vaak toch weer nieuwe struikelblokken op.

Enkele bekende struikelblokken voor ICS zijn:

Weersomstandigheden: als een ICS in buitenomstandigheden moet opereren moet het om kunnen gaan met verschillende weersomstandigheden. Vaak gebeurt dat intern door de achtergrond op basis van enkele seconden opname te schatten. Dit werkt goed in situaties van langzame verandering zoals veranderde belichting i.v.m. de loop van de zon. Minder goed werkt het voor de in Nederland vaak voorkomende situatie dat laag hangende bewolking door de wind snel door de lucht gedreven wordt. Hierdoor kan de schaduw van een wolk heel snel door het beeld lopen en door het ICS als een object gezien worden .

Drukte: als in een drukke omgeving informatie over individuen bepaald moet worden falen de huidige ICS. De systemen zijn niet in staat om in een drukke omgeving, als het object vaak maar gedeeltelijk in beeld is of soms ook korte tijd helemaal achter een ander object verdwijnt, het object vast te houden en een track weer op te pakken.

Camerapositie: voor de vele verschillende taken die men graag met ICS op wil lossen geldt vaak dat een aangepaste camerapositie nodig is. Als men met één camerapositie meerdere taken wil bedienen kan dat tot conflicterende eisen aan de positie leiden.

Omdat de huidige ICS (van niveau 2 en hoger) nog in hun kinderschoenen staan is het nodig om tijdens een pilotfase het systeem grondig te testen. Tijdens een praktijktest kan het beste bepaald worden hoe een systeem op de specifieke locatie en de te detecteren incidenten reageert. Het kost vaak enkele dagen om het systeem goed af te stellen. Er zijn veel parameters die aangepast kunnen worden. Soms zijn parameters afhankelijk van elkaar en betekent het draaien aan een knop dat een ander onderdeel van het systeem ook beïnvloed wordt.
Het is verleidelijk om bij het instellen van het systeem alleen op de valse meldingen (false positives) te focussen omdat deze gegevens direct beschikbaar zijn. Maar een systeem heeft pas echt nut als het in balans is en dus weinig valse meldingen geeft maar ook geen of nauwelijks incidenten mist (false negatives). Bij elke verandering van de parameters hoort eigenlijk ook een check of het systeem nog wel op de gewenste situaties reageert. Het is daarom aan te bevelen om in de periode van inregeling van het systeem verschillende incidenten op locatie na te spelen om ook informatie over de ten onrechte gemiste incidenten te verzamelen.

Een hinderlijk misverstand rond ICS (en ook andere technologieën) is de opvatting dat ICS beter zou kunnen zijn dan de mens en een mens kan vervangen. Dit is niet het geval. ICS kan wel een zeer nuttige rol vervullen als filter van een enorme stroom aan informatie. In deze datastroom zitten maar enkele relevante incidenten waarop actie ondernomen moet worden. ICS kan de datastroom reduceren tot een voor een mens beheersbare hoeveelheid data waarin de kans op een incident ook nog vele malen

hoger is als in de oorspronkelijke datastroom. Op deze manier blijft het werk voor surveillanten en bewakingspersoneel interessanter omdat hun vaardigheden (namelijk het snel inschatten van een situatie en passende maatregelen nemen) efficiënter ingezet kunnen worden. ICS is in eerste plaats een hulpmiddel en geen oplossing op zich. Het succes van ICS is afhankelijk van de inbedding in het hele beveiligingsproces. Juist het samenspel van mens en ICS bepaald de meerwaarde van de technologie.

Software security testen voor de testprofessional

Door Bas van Vossen (bas.van.vossen@logicacmg.com) met dank aan Gabriël Felten, Berry Kersten, Jos van Rooyen en John de Goei.

Het vakgebied security testen staat vooral in Amerika in hoog aanzien en dit komt vooral door de gespecialiseerde universitaire studies; de (afgestudeerde) studenten zijn voortreffelijke security testers. Security vormt een onderdeel van testen en het is een vak apart. Het is in Nederland helaas nog een ondergeschoven kindje. Dat security testen steeds belangrijker wordt is vooral merkbaar aan de vele dagelijkse nieuwsberichten over beveilingslekken in applicaties, systemen en andere IT componenten. De impact van inbraken in systemen, aanvallen op websites, netwerken en computers, creditcard fraude, identiteitsfraude, virussen en gebrekkige software is enorm. Deze voorbeelden geven al aan dat security testen een vrij uitgebreid vakgebied is. De doelgroep van dit artikel zijn softwaretesters, daarom ligt focus op de security van software. Doelstelling is het uitleggen dat software security testen voor de professionele softwaretester heel uitdagend, interessant, leuk en leerzaam kan zijn.

Wat houdt security testen eigenlijk in? Volgens kwaliteitsattribuut Beveiliging (ISO9126) gaat beveiliging over de mate waarin opzettelijke of abusievelijk ongeoorloofde toegang wordt voorkomen. Security testen is dan ook heel wat anders dan functioneel testen in de vorm van het toetsen van de ontwikkelde software ten opzichte van de requirements en specificaties. Een groot verschil bij software security testen is dat vooral de aandacht wordt gericht op het vinden van fouten, die niet zouden mogen verschijnen, maar toch doen. Immers, van de oorspronkelijke verwachte functionaliteit wordt een gedeelte ook werkelijk gerealiseerd conform de specificaties, maar een bepaald gedeelte niet en daarin zitten nu juist de onverwachte fouten volgens het bollenmodel van Security Innovation [12]; “While most functional bugs are the result of missing functionality, most security bugs are the result of extra functionality”. Testen van software security vereist dan ook dan een andere manier van denken en werken; niet meer van “werkt het volgens de specificaties?” maar leef je in als hacker: hoe kan je bepaalde functionaliteit omzeilen door te anticiperen wat de ontwikkelaar niet had voorzien of niet had verwacht en op die manier je meer uit de applicatie weet te halen dan eigenlijk is toegelaten (volgens Erwin Geirnaert, Security Innovation [13]). Daardoor kan men ongeoorloofde toegang krijgen tot bijvoorbeeld databases, systemen en mogelijke beheertransacties.

Is software security testen dan saai? Welnee! Het omvat een zeer gevarieerd gebied, want nog meer dan bij functioneel testen kom je in aanraking met internationale (informatiebeveiligings-) standaards (ISO 17799, Basel-2 en Sarbanes-Oxley), andere testtechnieken (threat modelling [9 en 10], code reviews en data mutation) en voor web applicatie security tester gelden diverse aspecten van web en internetplatformen; netwerk- en webserver architecturen, webservices security, firewalls/intrusion detection, Apache, IIS, PHP, Java/J2EE en databases (SQL, autorisaties). Als software security tester dien je naast het signaleren van security bugs ook advies uit te kunnen uitbrengen over verbetermaatregelen. Door een totaalpakket aan diensten aan te bieden aan de opdrachtgever kun je als software security-tester een veelzijdige job hebben. Doordat je in aanraking komt met diverse applicaties, platformen, programmeertalen etc. kun je jezelf continue blijven bijscholen. Dat is vrijwel noodzaak om de snelle groei bij te benen.

Welke eisen worden er aan een software security tester gesteld? Belangrijk is dat het testen van software security gericht is op de onverwachte situaties, waarvoor geen specificaties zijn; dit vereist ervaring en feeling met de

materie. Als je je wilt gaan specialiseren in web security, dan moet je niet alleen weten hoe een web applicatie werkt, maar ook weten hoe de onderliggende architectuur en database (Oracle, DB2 etc.) in elkaar zit, hoe de autorisaties werken en hoe je gegevens kunt opvragen of zelf manipuleren (SQL voor gevorderden!) en welke (web)services gebruikt worden.

Hoe zit het met (inter)nationale erkenning en certificering? Voor software security testen is er nog geen mogelijkheid, wel voor ICT security testen in het algemeen; als je minimaal 4 jaar relevante security ervaring hebt, dan kun je je certificeren tot Certified Information Systems Security Professional (CISSP) [8]. Deze titel wordt verstrekt door de Amerikaanse organisatie International Information Systems Security Certification Consortium $(ISC)^2$, die zich ten doel stelt het vakgebied Security Management te professionaliseren en bij te dragen aan standaardisering. Het is een intensieve, praktijkgerichte masterclass waarbij je diepgaande kennis van belangrijke thema's krijgt. Dus CISSP kan een belangrijke specialisatie zijn voor ISEB Foundation voor softwaretesten.

Is het moeilijk om een security tester te worden? Nou dat valt wel mee, want je hoeft technisch expert te zijn. Met behulp van bijvoorbeeld technieken als threat modelling [9 en 10] worden al bijna 50% van de security bugs gevonden volgens Microsoft's Michael Howard [11]. Threat modelling is een methode om bedreigingen systematisch te identificeren en te inventariseren, en te rangschikken volgens ernst bij het ontwerpen van een nieuwe applicatie.
Het probleem is wel dat er geen eenduidige standaard trainingen of bijv. master classes zijn. Het komt er op aan vooral ervaring op te doen, trainingen volgen en te leren van experts en collega's. Er is wel heel veel materiaal beschikbaar in de vorm van zeer praktijkgerichte boeken van Amerikaanse experts [1, 2, 3 en 4] en websites als die van OSSTMM (The Open Source Security Testing Methodology Manual, [7]) en OWASP (Open Web Application Security Project, [5]). OSSTMM is de eerste en meest wijdverspreide open standaard voor het opstellen, evalueren en meten van informatiebeveiliging. OWASP is een wereldwijde non-profit organisatie, die zich richt op preventie en kennisuitwisseling over web application security. Van OWASP bestaat ook een Nederlandse tak [6].

Waar moet ik beginnen, als ik me wil gaan verdiepen in software security testen? Door de enorme hoeveelheid beschikbare boeken en websites zie je al gauw de bomen door het bos niet meer. Heel logisch, maar er is hoop, want het meest interessant voor softwaretesters is OWASP. Immers, het merendeel van ons testwerk heeft betrekking op webapplicaties en bijna iedereen heeft wel ervaring met webtesten. De OWASP website biedt met haar eigen leeromgeving (WebGoat) en beschikbare documentatie een prima basis om de grondbeginselen van web security testen te leren. Als je een achtergrond hebt als (web)ontwikkelaar of webtester biedt dat zeker voordelen. Daarnaast heeft OWAPS een top 10 van security problemen. Voor elk onderdeel is beschreven wat het security issue is, hoe je het kunt testen en welke verbetermaatregelen er zijn. Het is heel nuttig om deze top 10 eens door te nemen, want zo krijg je een goed beeld van wat web software security testen inhoudt. Als je de smaak en drive te pakken hebt, dan zijn er specifiek trainingsfaciliteiten op het web met betrekking tot allerlei aspecten van hacken, Hack This Site [14] en Hacker games [15].

Hoe past software security testen in de teststrategie? Als het security aspect al binnen een testproject een plek heeft, dan is dat meestal achteraan; de penetratietest wordt en kan pas worden uitgevoerd als de applicatie klaar staat voor productie. Pas dan zijn alle infra- en architectuur zaken geïmplementeerd. Het netwerk en de systemen, zoals firewalls, webservers en mail servers, van een organisatie worden dan aangevallen op een manier zoals een hacker dat ook zou doen. Een penetratie test bestaat globaal gezien uit twee delen: een quick scan en een uitgebreide test met diepgang. Tijdens de quick scan wordt met diverse automatische tools gezocht naar bekende kwetsbaarheden. Eenvoudig te vinden en te gebruiken exploits voor gevonden kwetsbaarheden worden uitgevoerd. Er is geen twijfel over het nut en de plaats van penetratietest, maar veel security fouten zijn dan nog aanwezig, terwijl die al in een veel vroeger stadium ontdekt hadden kunnen worden.

Immers, de systeem- en functionele testers hebben dan al langere tijd met de applicatie gewerkt en kennen deze van binnen en buiten. Door het toepassen van een aantal specifieke testtechnieken kunnen al heel wat security fouten worden gevonden. Hoe later deze worden gevonden, hoe duurder het is om ze te repareren. Kortom, de penetratietest blijft noodzakelijk, maar security moet al vanaf het begin van het software ontwikkeltraject deel uitmaken van het testproject.

Meer informatie is te vinden in de onderstaande lijst met boeken en websites:

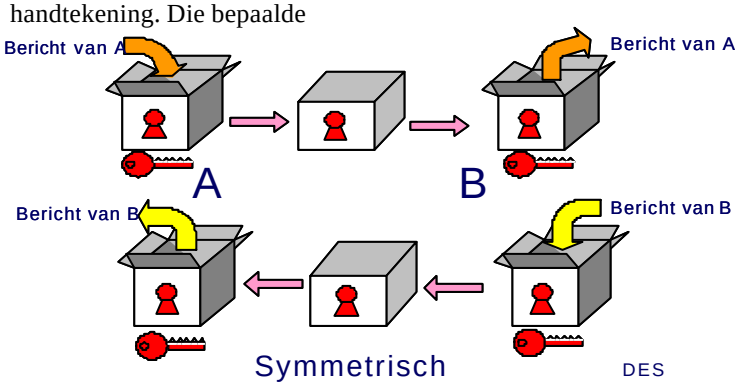
1. “How to break Software Security”; James A. Whitakker en Herbert h. Thompson, 2004, ISBN0-321-19433-0 (praktijkgericht boek over software security in het algemeen)
2. “How to break Web Software”; Mike Andrews en James A. Whitakker, 2005, ISBN 0-321-36944-0 (praktijkgericht boek over web software security)
3. “19 Deadly Sins of Software Security”; Michael Howard, David LeBlanc en John Viega, 2005, ISBN 0072260858
4. http://www.howtobreaksoftware.com/
5. http://www.owasp.org
6. http://www.owasp.org/index.php/Netherlands
7. http://www.isecom.org/osstmm/
8. http:/www.cissp.nl
9. http://www.microsoft.com/mspress/books/6892.asp (boek over threat modelling)
10. http://blogs.msdn.com/ptorr/archive/2005/02/22/GuerillaThreatModelling.aspx (website over threat modelling)
11. http://www.cigital.com/ssw/presentations/howard.ppt (presentatie “Pragmatic Trustworthy Computing” van Michael Howard)
12. http://www.sisecure.com/chart.htm (bollenmodel van Security Innovation)
13. http://www.ti.kviv.be/Ittelecom/IC-SOFT-Presentaties.html (presentatie Erwin Geirnaert, Security Innovation - Security Testen van (web) applicaties)
14. http://www.hackthissite.org/ (trainingssite hacken)
15. http://www.hackergames.net (trainingssite hacken)

Digitale Handtekening – Praktische problemen bij toepassingen

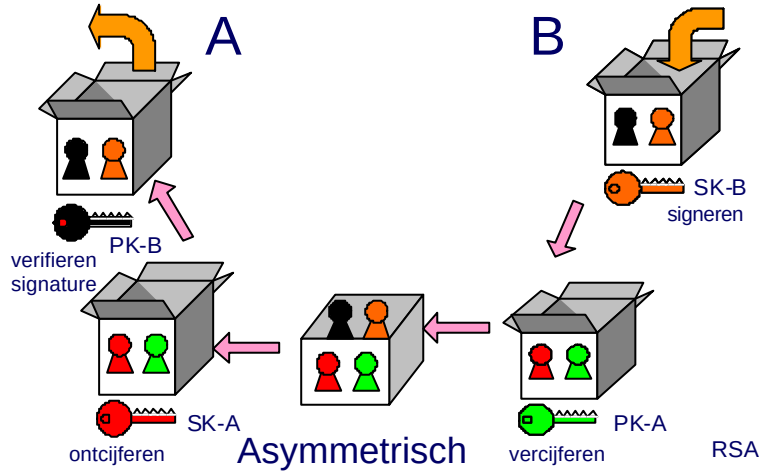
Door Ruud Goudriaan
ruud.goudriaan@mail.ing.nl

Digitale handtekeningen worden steeds belangrijker. In de Europese Unie is tussen de lidstaten afgesproken dat een 'elektronische handtekening' die aan bepaalde minimum eisen voldoet juridisch dezelfde rechtsgeldige betekenis moet krijgen als een fysiek gezette handtekening. Die bepaalde eisen komen erop neer dat alleen 'digitale handtekeningen', gebaseerd op een Public Key Infrastructuur (PKI), kunnen worden goedgekeurd. De wetgeving op dit gebied in alle lidstaten is al enkele jaren ingevoerd, maar de uitvoering stuit op een aantal problemen.
In dit artikel zullen praktische aspecten van digitale handtekeningen worden toegelicht, vooral van de eerste handtekeninguitwisseling tussen zender en ontvanger. Als kapstok voor de uitleg wordt de opzet en het gebruik van een 'secure mail' uitwisseling gebruikt.

Met 'secure mail' wordt bedoeld de uitwisseling tussen twee partijen van vertrouwelijke e-mail die 'elektronisch getekend' en vercijferd zijn, inclusief de attachments. Dit gebeurt met behulp van een 'onkraakbare' wiskundige formule (algoritme) en een lange wiskundige bit string (sleutel) voor het vercijferen en ontcijferen.
Als je daarvoor een symmetrisch algoritme zou nemen, dan hebben de zender en de ontvanger allebei dezelfde sleutel en dan zou de ontvanger als het ware dezelfde handtekening kunnen zetten als de zender: zie plaatje 'Symmetrisch'.



Daarom moet voor een unieke handtekening van de zender een asymmetrisch algoritme gebruikt worden. Daarbij hebben de zender en de ontvanger allebei een 'sleutelpaar' bestaande uit een geheime 'private key' en een openbare 'public key'.
In het plaatje 'Asymmetrisch' heeft zender B het bericht eerst vercijferd met de publieke sleutel PK-A van ontvanger A en vervolgens getekend met zijn eigen geheime en unieke sleutel SK-B. Ontvanger A kan het bericht ontcijferen en verifiëren dat het van B is, maar nooit een bericht 'tekenen' alsof het van A komt. Dit heet een Digitale Handtekening op basis van PKI.



Er zijn verschillende soorten 'Secure mail' relaties:
- End-to-end relaties, waarbij de vercijfering toegepast wordt van het werkstation van de zender tot het werkstation van de ontvanger en vice versa.
- Point-to-point relaties, waarbij de vercijfering werkt van de mail server van de zender tot de mail server van de ontvanger, maar er geen vercijfering is van het werkstation van de zender naar de mail server van de zender en ook niet van de mail server van de ontvanger naar het werkstation van de ontvanger.
- Werkstation-naar-mail server relatie, waarbij de zender vanaf het werkstation een vercijferd en getekend bericht stuurt, maar de ontvanger een centrale gateway server heeft die een end-to-end ontvang-relatie simuleert, maar het bericht via het eigen netwerk naar de ontvanger stuurt. Als de ontvanger zelf een bericht stuurt, simuleert de gateway server een end-to-end zend-relatie.

Bij de end-to-end relatie moeten de eindgebruikers 'Public Key Certificaten' bilateraal uitwisselen en expliciet van elkaar accepteren. Een Public Key Certificaat is een soort 'elektronische echtheidsverklaring' dat PK-A echt de publieke sleutel van A is. Certificaten worden gegarandeerd door een 'trusted CA' ofwel een vertrouwde Certification Authority. In Nederland kennen als erkende 'trusted CA' bijvoorbeeld Diginotar en Pink-Roccade. In het buitenland is 'Verisign' een dominante CA.

Bij de point-to-point relatie worden de Public Key Certificaten uitgewisseld tussen de mail servers. De eindgebruikers merken hier niets van.
Bij werkstation-naar-mail server relatie worden alle certificaten van de zenders door de ontvangende mail server opgeslagen om bij de end-to-end simulatie gebruikt te worden. De zender hoeft alleen het mail server-certificaat op te slaan en te accepteren.

In de praktijk werkt secure mail alleen als iedereen hetzelfde systeem gebruikt. Een heel goede kandidaat voor een secure mail wereldstandaard is 'S/MIME' dat zowel door Microsoft Outlook als door verschillende andere leveranciers (Lotus Notes) ondersteund wordt. In MS Outlook zijn alle handelingen voor het uitwisselen van 'S/MIME' certificaten en voor het vercijferen en tekenen van e-mail berichten al opgenomen. Maar zelfs als beide eindgebruikers dezelfde standaard gebruiken moet een aantal dingen kloppen:
- Is het certificaat van de juiste afzender?
- Is het certificaat te vertrouwen (trusted CA)?
- Is het certificaat van voldoende kwaliteit (algoritme)?
- Accepteert de mail server of eindgebruiker het certificaat?
- Is het certificaat opgeslagen in de lijst 'contactpersonen' (of Global Address List)?
- Ondersteunt een eventueel gebruikte chipkaart het protocol?

De conclusie is dat het realiseren van bij wet erkende elektronische handtekeningen

door de Europese wetgeving steeds urgenter wordt en dat het op basis van bovengenoemde standaard heel goed mogelijk is om vercijferde en van een digitale handtekening voorziene e-mail berichten uit te wisselen. Een goede website om verder op het toekomstig gebruik van digitale handtekeningen in te gaan is: www.ecp.nl .

Links

Voor iedereen nog even de links uit deze nieuwsbrief op een rijtje:

- http://en.wikipedia.org/wiki/SQL_injection
- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- (http://en.wikipedia.org/wiki/Buffer_overflow).
- http://www.howtobreaksoftware.com/
- http://www.owasp.org
- http://www.owasp.org/index.php/Netherlands
- http://www.isecom.org/osstmm/
- http:/www.cissp.nl
- http://www.microsoft.com/mspress/books/6892.asp
- http://blogs.msdn.com/ptorr/archive/2005/02/22/GuerillaThreatModelling.aspx
- http://www.cigital.com/ssw/presentations/howard.ppt
- http://www.sisecure.com/chart.htm
- http://www.ti.kviv.be/Ittelecom/IC-SOFT-Presentaties.html
- http://www.hackthissite.org
- http://www.hackergames.net
- www.ecp.nl

5 vragen aan Ernst van den Bos

Door Ernst van den Bos,
testmanager van KZA

Ik vind testen een leuk vak want...

Het is nooit saai, omdat géén dag hetzelfde is. Dit komt mede door de interactie met de klant en natuurlijk met andere ICT medewerkers. Je bent samen met hen bezig een goed product op te leveren, zodat het bedrijfsproces van de klant in de dagelijkse praktijk optimaal ondersteund wordt door dat product.

Het grootste misverstand over testen is...

Ik kom in mijn dagelijkse praktijk twee misverstanden tegen.
De eerste is een opmerking die ik vaak te horen krijg: “Ach, we testen de kwaliteit er wel in.“
Dat is natuurlijk niet zo, testen vergelijk ik altijd met het geweten van de ICT. Testers constateren afwijkingen en rapporteren daarover. Het is aan de ontwikkelaars om ervoor te zorgen dat er een basis kwaliteitsniveau wordt neergezet.
Het tweede misverstand is dat testen begint als het product gebouwd is. Ook dit is niet waar, testen begint mijns inziens al bij de start van een project. Wat is het doel dat de klant nastreeft, en hoe wordt dit veroorzaakt. Als je dat begrijpt, dan ga je samen met de klant naar oplossingen zoeken. Vervolgens wordt de omzetting gemaakt naar requirements en dan kan het selectie of ontwikkelingsproces naar ICT producten beginnen. Dus testen is in de ideale situatie gedurende het gehele traject aanwezig.

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

Testconsultant of kwaliteitsconsultant, om ervoor te zorgen dat het ondersteunen van het bedrijfsproces van de klant op een hoger platform gebracht wordt. Dit in plaats van het kiezen van een ICT product wat in de markt het meest ingezet wordt.

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

Kritisch te zijn en zich niet te laten afschepen als lastig. Daarnaast zijn eigenschappen als standvastig en stressbestendig géén overbodige luxe. Ook communicatieve vaardigheden zijn enorm belangrijk.
Ontwikkeltrajecten staan altijd onder tijdsdruk. Vaak doordat vooraf niet volledig SMART is gemaakt wat er ontwikkeld moet worden, waardoor er gedurende het ontwikkeltraject constant wijzigingen nodig zijn om bij te sturen. Deze wijzigingen gaan altijd ten kosten van de testtijd, omdat testen achteraan in het ontwikkelproces uitgevoerd wordt. Door bij het opstellen van de requirements al kritisch te zijn op het SMART maken kan een hoop ellende worden voorkomen.
In de toekomst hoop ik dat binnen het test vakgebied ... is veranderd, omdat...
De klantbetrokkenheid voorop staat.
Door met de klant in discussie te gaan en de requirements SMART te maken zorg je ervoor dat er duidelijkheid ontstaat over wat er ontwikkeld moet worden. Door vervolgens tijdens het testtraject kritisch te blijven op de klant specificaties in combinatie met de ICT

specificaties kan de bandbreedte die tussen beide ontstaat beter worden geoptimaliseerd.

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

Pepijn van de Vorst, omdat ik hem bij de belastingdienst heb leren kennen als een kundige collega met wie ik altijd van gedachten kon wisselen en sparren over testvragen. Pepijn aan jou de eer.

Evenementen

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

TestNet Nieuws

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