Stop de hackers in het MKB

Ontwikkeling MKB pentestproduct

Naam: Werner Alsemgeest
Studentnummer: 08022488
Instituut: De Haagse Hogeschool
Opleiding: Information Security Management
Afstudeerstage bedrijf: Deloitte
Begeleider Hogeschool: Ellen Wesselingh
Begeleider Deloitte: Tom Schuurmans

Datum: 18 maart 2012
Versie: 1.4

Versiehistorie

Versienummer	Versiedatum	Controle door:	Wijzigingen
1.0	17-12-2011	Werner Alsemgeest	Concept
1.1	10-02-12	Werner Alsemgeest	Aanpassing aan hand van feedback
1.2	14-02-2012	Werner Alsemgeest	Aanpassing aan hand van feedback
1.3	22-02-2012	Werner Alsemgeest	Aanpassing aan hand van feedback
1.4	07-03-2012	Werner Alsemgeest	Spelling en grammatica controle

Distributielijst

Versienummer	Datum	Naam	Organisatie
1.0	08-02-2012	Ellen Wesselingh	De Haagse Hogeschool
1.2	19-02-2012	Ellen Wesselingh & Arianne Luik-Knoester	De Haagse Hogeschool
1.4	16-03-2012	n.v.t.	De Haagse Hogeschool

Referaat

Afstudeerverslag ontwikkelen penetratietest voor het MKB.

Afstudeerverslag Werner Alsemgeest, Information Security Management, De Haagse hogeschool.

Het project is uitgevoerd voor Deloitte Nederland in de periode 01-11-2011 tot 13-04-2012 in de vorm van een afstudeerstage. In dit rapport wordt de ontwikkeling en uitwerking van de MKB penetratietest beschreven.

Descriptoren:
- Afstudeerstage
- Deloitte
- MKB
- Pentest
- Penetratietest
- Informatiebeveiliging
- Hackers
- Ethisch hacken

Voorwoord

Voor u ligt het afstudeerverslag van Werner Alsemgeest. Dit verslag gaat over mijn afstudeerstage bij Deloitte Nederland te Amstelveen. In dit verslag zijn de werkzaamheden die ik tijdens de afstudeerstage heb uitgevoerd in beeld gebracht. Tevens heb ik in dit verslag mijn afstudeerstage geëvalueerd.

Het onderwerp van mijn afstudeerstage betrof het ontwikkelen van een penetratietestproduct (pentest) voor het midden- en kleinbedrijf. Het pentestproduct bestaat uit een gestandaardiseerde pentest welke voor een vast bedrag, in maximaal vier dagen uitgevoerd kan worden. De klant krijgt aan de hand van de resultaten inzicht in de kwetsbaarheden van zijn informatiesysteem, applicatie of infrastructuur.

Ik wil iedereen bedanken die een bijdrage geleverd heeft aan de totstandkoming van het MKB pentestproduct en mijn afstudeerstage. In het bijzonder wil ik de heren van Deloitte Nederland: Tom Schuurmans, Marko van Zwam, Derk Wieringa, Vojtech Brtnik en Nick Kirtley en de dames Ellen Wesselingh en Arianne Luik-Knoester van De Haagse Hogeschool bedanken voor de bijdrage aan mijn afstudeerstage.

Werner Alsemgeest

Inhoudsopgave

1. Inleiding

Werner Alsemgeest is mijn naam en dit is het laatste document dat ik oplever aan De Haagse Hogeschool te Zoetermeer als student Information Security Management.
Dit document betreft mijn afstudeerstageverslag bij de organisatie Deloitte Nederland te Amstelveen. Deloitte Nederland is een zelfstandige memberfirm van de wereldwijde organisatie Deloitte Touche Tohmatsu.
Dit document heeft als doel de lezer een compleet beeld te geven van de afstudeerstage die ik gelopen heb. Zo wordt onder andere de totstandkoming van de producten beschreven en wordt een evaluatie van de afstudeerstage gegeven.

Deloitte heeft ruimte gezien op het gebied van MKB pentesting[1]. Deze ruimte willen ze graag benutten, maar op dit moment kunnen ze hier nog geen passende dienst voor leveren. Het idee is ontstaan om een product te ontwikkelen (deels geautomatiseerd) waarmee in een korte periode een pentest kan worden uitgevoerd bij een MKB-organisatie. Om het MKB pentestproduct te ontwikkelen is een project gestart in de vorm van een afstudeerstage. De doelstelling van dit project is het ontwikkelen van een pentest "product" voor het MKB.

Dit document is opgedeeld in drie delen. Het eerste deel (Hoofdstuk 2) bestaat uit een korte beschrijving van de organisatie Deloitte. Deel twee (hoofdstuk 3 tot en met 8) bestaat uit een beschrijving van de werkzaamheden van elke fase. In deze hoofdstukken staan onder andere de aanpak, doelstelling en resultaten per fase beschreven. In het derde deel is een evaluatie van de afstudeerstage te vinden. Deze evaluatie bestaat uit drie onderdelen: de productevaluatie, procesevaluatie en de competentie-evaluatie.

Als bijlage zijn alle documenten bijgevoegd die opgeleverd zijn aan Deloitte en/of De Haagse Hogeschool. In de bijlage van dit document is een leeswijzer te vinden van bijgevoegde documenten. Daarnaast is aan het einde van dit document een afbeeldings- en literatuurlijst toegevoegd.

[1] *Pentest is een afkorting van het woord penetratietest. Een penetratietest is een methode om de beveiliging van een informatiesysteem of netwerk te evalueren op beveiliging door het simuleren van aanvallen door kwaadaardige hackers.*

2. De organisatie Deloitte

"Deloitte" is de merknaam waaronder tienduizenden professionals in zelfstandige memberfirms wereldwijd samenwerken. Deze firms maken onderdeel uit van de wereldwijde organisatie Deloitte Touche Tohmatsu Limited (DTTL). Na vele overnames en fusies telt Deloitte Touche Tohmatsu inmiddels 150.000 medewerkers in 150 verschillende landen. Daardoor is DTTL één van de grootste accountant -en adviesbureaus ter wereld.
DTTL heeft een coördinerende functie en is niet actief betrokken bij de dienstverlening. Elke memberfirm is actief in een bepaald gebied en onderworpen aan wetgeving en professionele regelgeving van het land of de landen waarin wordt geopereerd. De structuur van de afzonderlijke DTTL memberfirms verschilt afhankelijk van plaatselijke wet- en regelgeving en andere factoren.

Deloitte Nederland

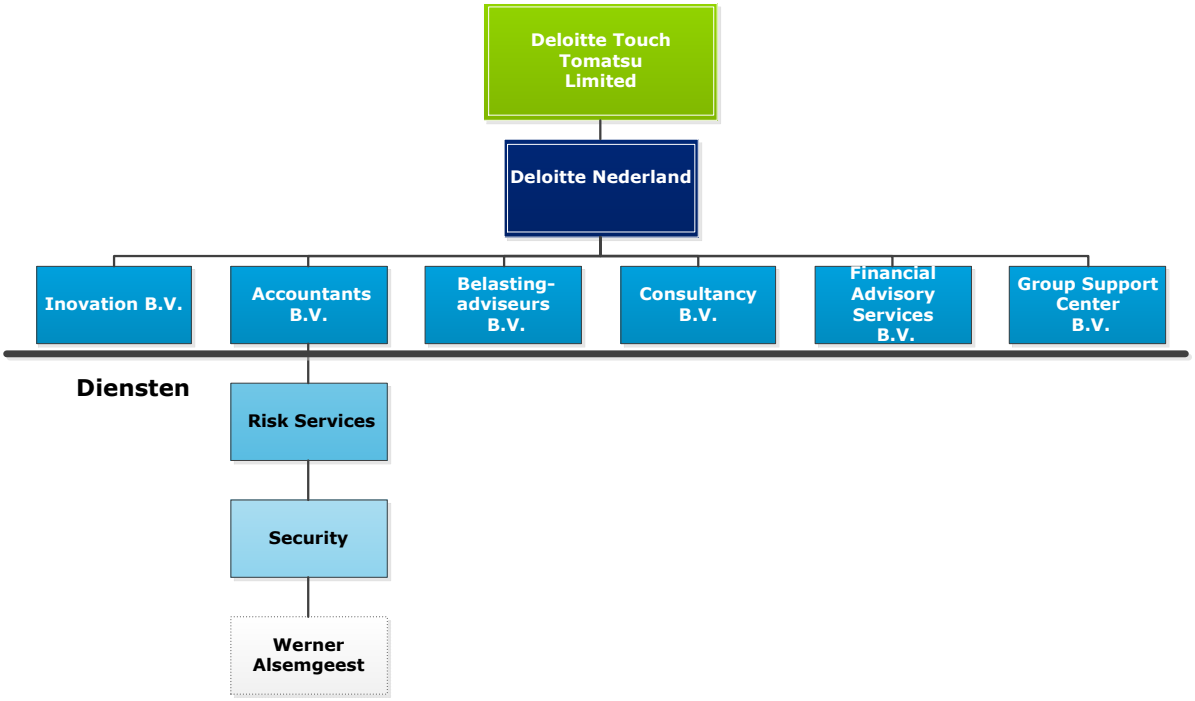
Deloitte Nederland is een zelfstandige memberfirm en heeft op dit moment 18 kantoren verdeeld over vijf regio's. Deloitte Nederland heeft ongeveer 4500 werknemers. In totaal realiseerde Deloitte Nederland in het boekjaar 2010/2011 een omzet van 632 miljoen euro.

Deloitte Nederland gaat uit van een multidisciplinaire aanpak. Vanuit de diensten Accountancy, Belastingen, Consulting en Financial Advisory Services bedient Deloitte de markt.

Figuur 1 – Multidisciplinaire aanpak van Deloitte

Holdingstructuur

Deloitte is in Nederland ingedeeld in een aantal besloten vennootschappen (B.V.). Elke B.V. levert bepaalde diensten. De plek binnen Deloitte waar ik de afstudeerstage gelopen heb is in het onderstaande organogram weergegeven.

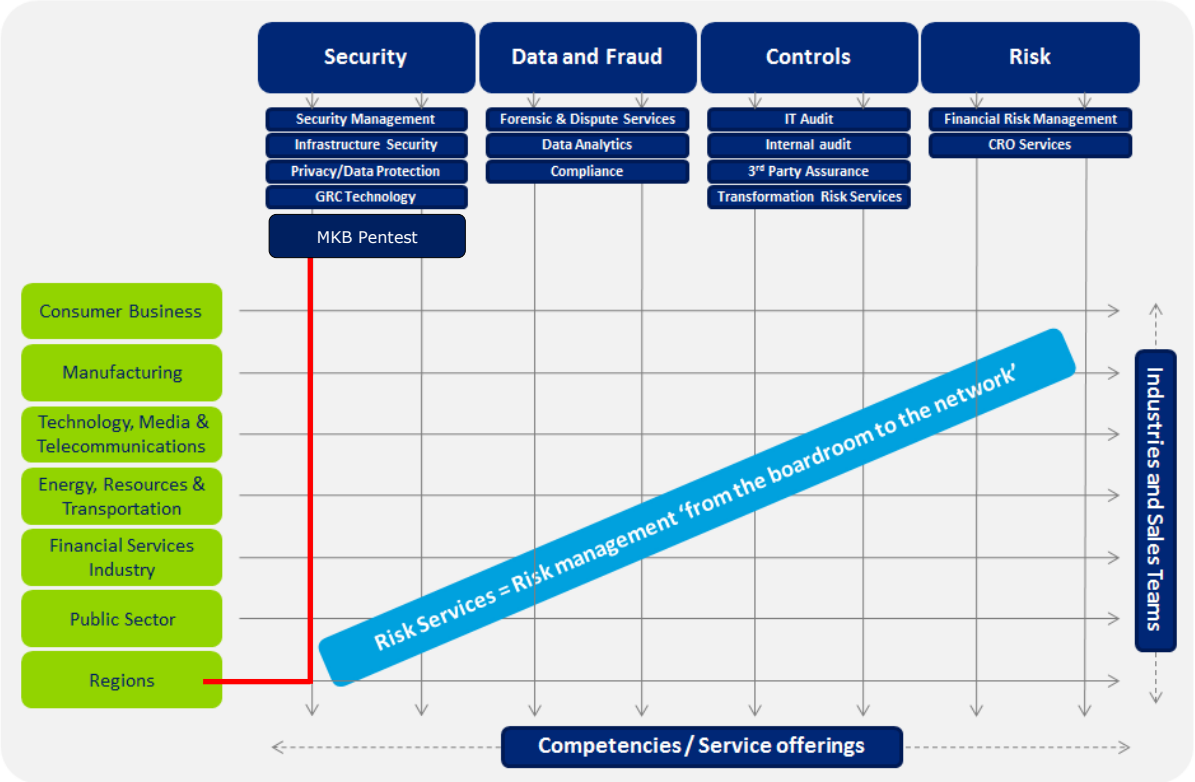


Figuur 2 - Deloitte Holdingstructuur

(Enterprise) Risk Services

De dienst Risk Services (RS) bevat een verscheidenheid aan (informatiebeveiligings-) diensten voor verschillende sectoren (Zie figuur 3). Deze diensten worden aangeboden door de afdelingen: Security, Data en Fraude, Controls en Risk. De dienst Risk Services valt bij Deloitte niet onder consultancy zoals je zou verwachten, omdat sommige diensten binnen Risk Service ondersteuning bieden aan de jaarcontrole (zoals IT audit) valt Risk Services onder accountancy.

De afstudeerstage bevindt zich op de afdeling security. Tijdens de afstudeerstage zal gewerkt worden aan een nieuw product (MKB pentest) die de afdeling Security kan aanbieden aan het marktgebied "regio's" (waarbinnen MKB organisaties vallen). Zie onderstaande afbeelding:



Figuur 3 - Diensten Deloitte Risk Services

3. Plan van Aanpak - Fase 1

Fase 1 bevat de opzet en plan van aanpak van het project. Onder andere wordt de aanleiding, doelstelling, scope en aanpak van het project beschreven. Tot slot zijn mijn uitgevoerde werkzaamheden in fase 1 beschreven. Meer informatie over de opzet van het project is in het bijgevoegde document "Plan van Aanpak" te vinden.

3.1 Aanleiding opdracht

Deloitte levert met de dienst Risk Services een breed pakket aan security en privacy diensten, voornamelijk aan grote organisaties.
Deloitte wil de dienst Risk Services verder uitbreiden door het leveren van diensten aan andere marktsegmenten. Risk Services heeft gezien dat er ruimte is in de markt van het MKB voor het leveren van een pentesting dienst. Deze ruimte willen ze graag benutten, maar op dit moment kunnen ze hier nog geen passende dienst voor leveren. Het idee is ontstaan om een product te ontwikkelen (deels geautomatiseerd) waarmee in een korte periode een pentest kan worden uitgevoerd bij een MKB-organisatie. Dit product moet betaalbaar en waardevol worden voor een MKB-organisatie. Tevens moeten de resultaten van de pentest een goed beeld kunnen geven van de mogelijke kwetsbaarheden van een informatiesysteem, infrastructuur of applicatie. Voor de pentest bij MKB-klanten moet een standaard worden ontwikkeld zodat deze dienst eenvoudig, goedkoop en snel kan worden uitgevoerd. Wel moet in de standaard ruimte worden gehouden voor een stuk maatwerk om de pentest bij de klant aan te laten sluiten. De pentest van Deloitte moet zich onderscheiden van andere pentests door een klantgerichte en begrijpelijke rapportage.

3.2 Doelstelling

De doelstelling van dit project is het ontwikkelen van een pentest "product" voor het MKB. Door middel van dit product krijgt een MKB-organisatie inzicht in de mogelijke kwetsbaarheden van een applicatie, informatiesysteem of infrastructuur. Dit product moet betaalbaar zijn voor een MKB-organisatie en in maximaal vier dagen uitgevoerd kunnen worden. Het resultaat van de pentest moet een klantgerichte en begrijpelijke rapportage worden. De nadruk van het project zal liggen op de pentestontwikkeling en minder op de verkoop/marketing-aspecten van de pentest.

3.3 Scope

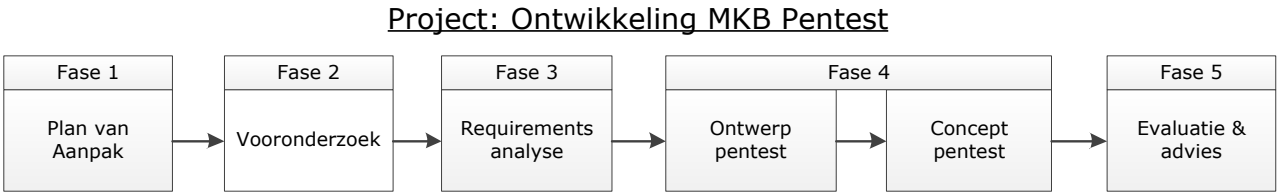
De scope van het onderzoek betreft het ontwikkelen van een pentest voor middelgrote en grote MKB-organisaties binnen Nederland. Onder middelgrote en grote MKB-organisaties vallen organisaties van 50 tot 250 werknemers. Ook worden gemeenten en zorginstellingen meegenomen in de scope van het project. De pentest zal zich richten op organisaties die met vertrouwelijke gegevens werken.

3.4 Aanpak

Het project is uitgevoerd met behulp van een op Prince 2 gebaseerde aanpak. Onderdelen zoals de fasering, indeling van het projectteam, risicobeheersing en kwaliteitsbeheersing zijn gebruikt van Prince 2. Er is gekozen om niet de hele Prince 2-aanpak te gebruiken in verband met de grootte van het project en het projectteam. Het projectteam bestaat namelijk uit vijf personen, maar alle werkzaamheden voer ik uit. De rollen van de andere projectleden zijn begeleider, opdrachtgever of expert.
Voor de projectmethode is Prince 2 gekozen omdat Prince 2 een duidelijke aanpak en structuur biedt voor het beheersen van een project. Tevens heb ik al vaker gewerkt met Prince 2 waardoor al ervaring is met deze methode.

Voor het project zijn de volgende fases gedefinieerd:

Fase	**Beschrijving**
Fase 1	Opstart project
Fase 2	Vooronderzoek (inzicht krijgen in het pentestproces)
Fase 3	Requirements analyse
Fase 4	Ontwerpen, ontwikkeling en testen pentest
Fase 5	Aanbeveling en evaluatie



Figuur 4 - Overzicht van fases

Het indelen van de fases is ontstaan aan de hand van de producten die opgeleverd dienen te worden. Het bepalen van de producten is in overleg gegaan met de opdrachtgever en de begeleider.

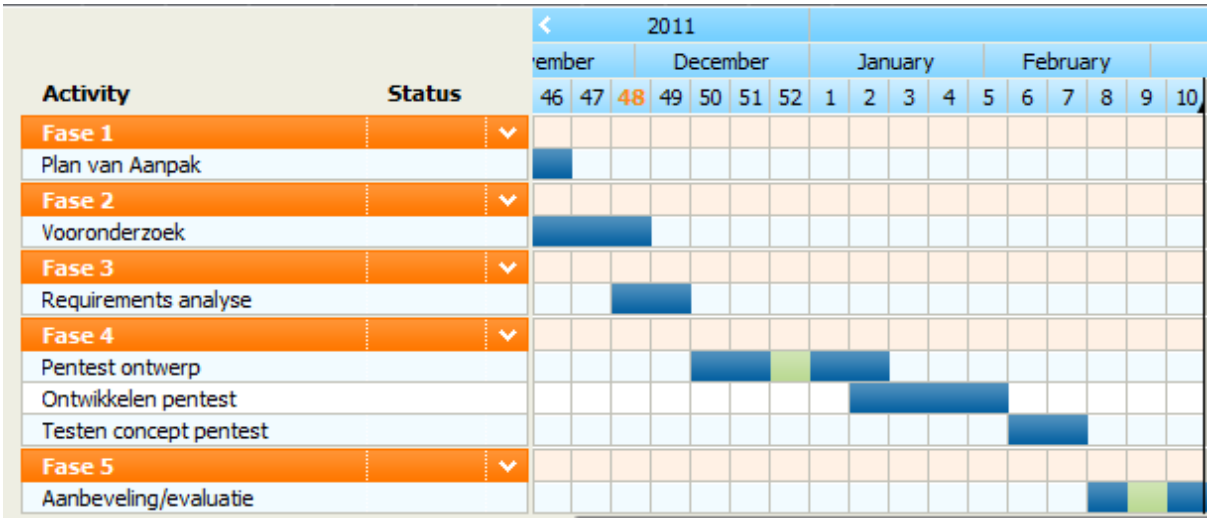
Aan het eind van het project dienen de volgende producten te worden opgeleverd.

Product	**Beschrijving**
Plan van aanpak	In dit document staat beschreven hoe het project aangepakt zal worden. Onder andere staan hier de aanleiding, doelstelling en scope beschreven.
Requirements analyse	In dit document worden de wensen en eisen voor de MKB-pentest in kaart gebracht. Er zal worden gekeken naar de wensen en eisen vanuit Deloitte en vanuit de klant.
Ontwerp pentest	In dit document staat beschreven hoe de pentest ontworpen zal worden. Onder andere staan hier de methode, tools en processtappen beschreven.
Concept pentest	Dit product bevat een concept van de MKB pentest, ontwikkeld aan de hand van het ontwerp pentest. Het concept zal wanneer mogelijk getest worden bij een MKB-organisatie.
Evaluatie & advies	Dit document bevat een evaluatierapport van de pentest die uitgevoerd is bij een MKB-organisatie. Tevens wordt in dit document een advies gegeven aan Deloitte over de vervolgstappen die uitgevoerd dienen te worden voor de ontwikkeling van de MKB pentest.

Om de voortgang, kwaliteit en risico's van het project te waarborgen zijn een aantal beheersingsmechanismen gebruikt. Een uitgebreide beschrijving van de beheersingsmechanismen is te vinden in het "Plan van aanpak".

Planning

Om de projectvoortgang te waarborgen is aan het begin van het project een planning opgesteld. Bij het opstellen van de planning is rekening gehouden met mogelijke vertragingen. Wanneer verwacht wordt dat niet aan de projectplanning gehouden kan worden dient de begeleider op de hoogte te worden gesteld door middel van een "exeption report". In onderling overleg wordt dan de aanleiding, oorzaak en gevolg voor het project besproken. Wanneer de fase binnen de toleranties van de doorlooptijd wordt afgerond, zal er geen exception report worden opgeleverd. De opgestelde toleranties zijn te vinden in het "Plan van aanpak".



Figuur 5 - Project Planning

Kwaliteit

Om de kwaliteit van het project en de documentatie te waarborgen is een wekelijks contactmoment ingepland met de begeleider van Deloitte. Tijdens dit contactmoment zullen de volgende onderwerpen worden besproken: de projectvoortgang, mogelijke problemen, ideeën en documentatie. Ook helpt de begeleider met het nakijken van de documentatie op inhoud en taal gebruik.

Risico's

De projectrisico's zijn aan het begin van het project in kaart gebracht (zie bijlage "Plan van aanpak"). Om de risico's te bepalen is gekeken naar de kans en effect (impact) dat bepaalde zaken kunnen gebeuren. Ook is nagedacht hoe de risico's beperkt kunnen worden met behulp van maatregelen. Een voorbeeld van de risicobeheersing is in onderstaande tabel te vinden:

Bedreiging:	**Tegenmaatregel:**	**Kans**	**Effect**	**Risico**
Tijdnood	Duidelijke planning maken met voldoende speling en wanneer nodig doorwerken in de vakantie	2	4	8
De weersomstandigheden zijn zodanig slecht dat het niet met behulp van (openbaar) vervoer mogelijk is om op kantoor te komen	Thuis werken	3	2	6

3.5 Kennismaking met Deloitte

Het begin van de afstudeerstage bestond uit het kennismaken met de organisatie, diensten en collega's. Kennismaken met de organisatie Deloitte verliep zonder problemen. Deloitte heeft veel ervaring met het inwerken van nieuwe medewerkers omdat per maand +/- 50 nieuwe medewerkers in dienst treden. Elke maand wordt een landelijke introductiedag georganiseerd. Tijdens deze dagen worden verschillende presentaties gegeven om inzicht te krijgen in de organisatie. De dag daarna is een introductie op kantoor en met het team waar de medewerker gaat werken. Omdat het introductieprogramma ook voor stagiaires geldt, heb ik deze ook gevolgd.

Na ongeveer een week, waarin ik veel documentatie van Deloitte heb gelezen en meegekeken heb met een pentestproject, kon een begin gemaakt worden aan het project. Het begin van het project bestond uit kennismaken met de mensen die betrokken zijn bij het project. Er zijn verschillende gesprekken geweest met deze mensen om verder inzicht te krijgen in het project. Aan de hand van alle informatie die vergaard is in de eerste weken kon een opzet gemaakt worden aan het plan van aanpak.

3.6 Ontwikkeling Plan van Aanpak

Zoals in paragraaf 3.4. vermeld staat is het plan van aanpak deels gebaseerd op Prince 2. In het plan van aanpak is niet alleen beschreven hoe het project aangepakt wordt, maar staat ook beschreven hoe de planning, kwaliteit en risico's kunnen worden beheerst. Voor het maken van het plan van aanpak is gebruik gemaakt van een standaard structuur. Hiervoor is gekozen omdat in deze structuur alle benodigde onderdelen zitten, het document overzichtelijk blijft en er goede ervaringen van het gebruik uit het verleden mee zijn (schoolprojecten en vorige stage).

Het concept van het plan van aanpak is voorgelegd aan de begeleider van Deloitte voor controle. Feedback die teruggegeven werd ging over de projectplanning, projectteamstructuur, gebruik van Deloitte logo en over de risico's. Na de aanpassing van de feedback kon er een nieuwe versie opgeleverd worden aan alle leden van het projectteam. Met een aantal leden is het document mondeling doorgenomen tot geen feedback meer terugkwam.

3.7 Resultaten fase 1

Tijdens deze periode zijn onderstaande producten opgeleverd aan Deloitte en De Haagse Hogeschool. Deze documenten zijn als bijlage toegevoegd.

- Verbeterde versie afstudeerplan
  Voordat de afstudeerstage begon, is aan De Haagse Hogeschool een afstudeerplan opgeleverd; maar er is een wijziging gemaakt in de opdrachtgever. De partner van Deloitte Risk Services is enthousiast over het project en neemt de taak van opdrachtgever op zich.
- Plan van Aanpak
  In het Plan van Aanpak staat beschreven hoe het project aangepakt wordt volgens de Prince 2 methode. Hierin staan onder andere het doel, de faseringen, de scope en risico's van het project beschreven.

4. Vooronderzoek – Fase 2

Dit hoofdstuk beschrijft de doelstelling, aanpak, werkzaamheden en resultaten van fase 2; het vooronderzoek. Meer informatie over het vooronderzoek is in het document "Design Pentest" te vinden, welke als bijlage is bijgevoegd.

4.1 Doelstelling vooronderzoek: inzicht in de wereld van het pentesten

Het doel van deze fase is inzicht krijgen in de "wereld" van pentesting. Onder andere is onderzocht uit welke onderdelen een pentest bestaat, hoe een pentest uitgevoerd kan worden, welke methodes en standaarden gebruikt kunnen worden en hoe binnen Deloitte pentests uitgevoerd worden. Het is belangrijk om een goed beeld te krijgen van pentesting omdat een nieuw pentest product ontwikkeld moet worden voor het MKB.

4.2 Onderzoeksmethoden

Het vooronderzoek is aangepakt met behulp van vier verschillende methodes. Door gebruik te maken van triangulatie kan meer informatie gevonden worden en kan de kwaliteit van het vooronderzoek verhoogd worden, omdat de resultaten van de verschillende methodes met elkaar vergeleken kunnen worden.
Voor het vooronderzoek zijn de volgende vier methodes gebruikt:

- **Deskresearch**
  Om algemene informatie te vinden over pentesting is er een literatuuronderzoek uitgevoerd. Hierbij is gezocht naar informatie uit betrouwbare bronnen op het internet zoals instituten, universiteiten en belangrijke organisaties op het gebied van pentesting, tijdschriften en in boeken.
- **Interviews**
  Door middel van interviews is meer informatie verkregen over hoe Deloitte pentests uitvoert, wat voor soorten pentests aangeboden worden en hoe het pentestproces eruit ziet. De interviews zijn in de vorm van open interviews gehouden. Er zijn onder andere interviews gehouden met de pentesters, managers en met de opdrachtgever.
- **Observeren**
  Om meer inzicht te krijgen in hoe binnen Deloitte pentests uitgevoerd worden en hoe een dergelijke pentest er uit ziet heb ik bij een aantal verschillende pentest-projecten meegekeken. Onder andere heb ik meegekeken bij een webapplicatie, infrastructuur en mobiele applicatie pentest.
- **Uitvoeren van "pentest" oefeningen**
  Er zijn erkende organisaties (zoals Certified Secure en OWASP) die gratis trainingen hebben ontwikkeld om inzicht te krijgen in de hacker "mindset" en hoe de beveiliging van bepaalde systemen getest kunnen worden. Hiervoor zijn ook "hack" opdrachten ontwikkeld waar er op een systeem of website ingebroken moet worden om bepaalde informatie te achterhalen. Wanneer je gaat pentesten worden dezelfde methodes gebruikt.

In overleg met de opdrachtgever en begeleider is besloten om niet alle resultaten van het vooronderzoek uit te werken in een apart document. Dit is besloten omdat de informatie voor hen niet nieuw is, ze hebben al jaren ervaring op het gebied van pentesting. Vooral de pentesters zagen het vooronderzoek niet als meerwaarde voor het project. Toch heb ik besloten om het vooronderzoek uit te voeren om meer inzicht te krijgen op het gebied van pentesting. Een deel van de resultaten van het vooronderzoek is uitgewerkt in het document "design pentest" fase 4. Deze informatie bestaat uit achtergrondinformatie over pentesting. Deze informatie zal gebuikt worden voor het ontwerpen van de MKB pentest.

4.3 Werkzaamheden vooronderzoek

Tijdens het vooronderzoek zijn verschillende activiteiten uitgevoerd om meer inzicht te krijgen op het gebied van pentesting. Deze activiteiten liepen synchroon met elkaar. Voor het literatuuronderzoek is op het internet, in boeken en in Deloitte documentatie gezocht naar relevante informatie op het gebied van pentesting. Ook is documentatie van De Haagse Hogeschool gebruikt, omdat tijdens de opleiding het onderwerp pentesting aan bod is gekomen.

De zoektocht is begonnen met het opzoeken van de definitie van pentesting (penetratietest). Daarna is er gezocht naar organisaties die veel te maken hebben met pentests. Om de kwaliteit van de informatie te waarborgen is vooral gekeken naar betrouwbare organisaties zoals instituten en universiteiten. Ook zijn een aantal organisaties gevonden die standaarden op het gebied van pentesting hebben ontwikkeld zoals OWASP[2] (Open Web Application Security Project), SANS[3] (SysAdmin, Audit, Networking, and Security) en NIST[4] (National Institute of Standards and Technology). Vooral bij de organisatie SANS is er erg veel documentatie gevonden. Deloitte zelf maakt tijdens het pentesten al gebruik van de OWASP standaard.

Een andere activiteit bestond uit het houden van interviews met de pentesters en managers. Ik had ervoor gekozen om open interviews te houden in de vorm van een gesprek. Door op deze manier te werken kon het gesprek alle kanten op zodat ik de verschillende ideeën en meningen kon verkrijgen over het onderwerp pentesting. Het probleem bij open interviews is dat de informatie die gegeven wordt vaak ongestructureerd is. De kans is dan ook aanwezig dat niet de benodigde informatie verkregen wordt. Om dit probleem op te lossen heb ik voor elk interview een doel opgesteld. Wanneer aan het einde van het interview het doel nog niet bereikt was kon ik het interview lichtelijk sturen om toch het doel te kunnen bereiken. Om toch het open karakter van het interview te behouden zijn er geen vragen van tevoren opgesteld.

Om de juistheid en integriteit van de informatie te controleren heb ik hierover gesproken met mijn begeleider. Belangrijke informatie die verkregen is tijdens de interviews is bijvoorbeeld hoe het Deloitte pentestproces eruit ziet, welke soorten pentests Deloitte aanbiedt en wat de (soort) klanten van Deloitte zijn die pentest aanvragen.

Om meer inzicht te krijgen in hoe een pentest wordt uitgevoerd binnen Deloitte heb ik meegelopen met een aantal pentest projecten. Ik heb over de schouder van een pentester mee mogen kijken en heb kunnen waarnemen wat voor stappen worden uitgevoerd. Met die stappen bedoel ik niet alleen het pentesten zelf maar ook de communicatie met de klant, het bijhouden van een logboek en het rapporteren van de resultaten. Om een totaalplaatje te krijgen heb ik mee mogen kijken met verschillende soorten pentests zoals een webapplicatie, infrastructuur en mobiele applicatie pentest.

[2] OWASP is een gezaghebbend open-source project op het gebied van applicatiebeveiliging. OWASP is op gericht door de OWASP foundation en is een non profit organisatie.

[3] De SANS instituut is een Amerikaanse organisatie gespecialiseerd in informatiebeveilingstrainingen en onderzoek. SANS

[4] NIST is een wetenschappelijke instelling die onder de Amerikaanse federale overheid valt. Het NIST zet zich in voor standaardisatie in de wetenschap, zoals het definiëren van eenheden. NIST is binnen de informatiebeveiliging gezaghebbend op het gebied van veilige configuratie standaarden

4.4 Resultaten van het vooronderzoek

Het resultaat van deze fase bestaat uit de informatie die ik verkregen heb op het gebied van pentesting en pentesting binnen Deloitte. Voor deze fase is geen document opgeleverd. Een deel van de resultaten van deze fase is verwerkt in het document "Design pentest" (fase 4) welke als bijlage is bijgevoegd.
Hieronder staan een aantal belangrijke resultaten uit het vooronderzoek weergegeven.

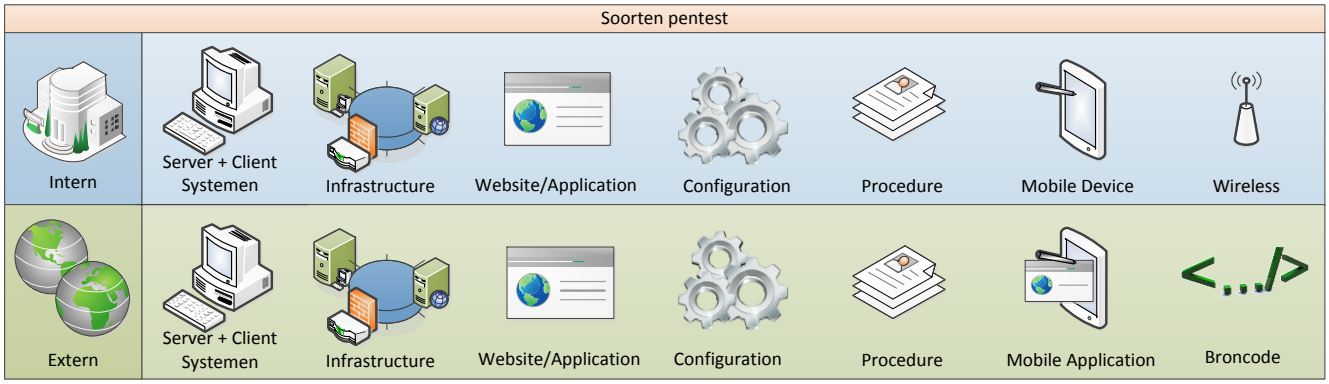
Aanpak pentest

Ik heb de volgende schematisch weergave gemaakt om een algemene aanpak van een pentest weer te geven. Aan de hand van deze aanpak zal ook de MKB pentest ontwikkeld worden.

Figuur 6 - Aanpak pentest

Soorten pentest

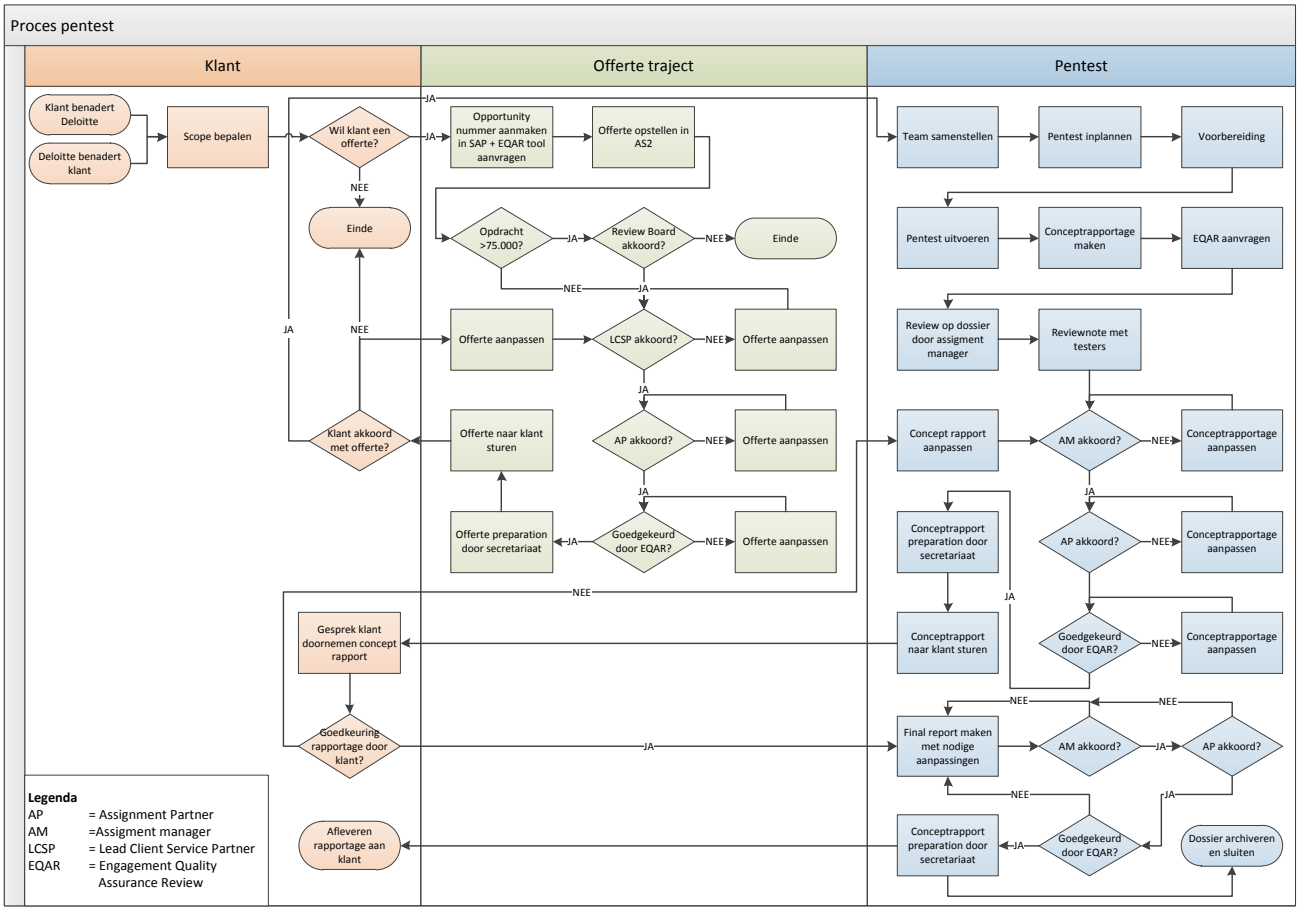
In de door mij uitgewerkte onderstaande afbeelding zijn de verschillende soorten pentests schematisch weergegeven. Deze soorten pentests zijn niet zwart op wit en kunnen ook gelijktijdig worden uitgevoerd. Tevens vallen sommige soorten pentests niet binnen de "officiële" term pentest. Tijdens een pentest wordt geprobeerd in te breken in een systeem, netwerk of applicatie zonder op de hoogte te zijn van de volledige configuratie. Hierdoor vallen de pentests configuratie, broncode en procedure eigenlijk buiten de boot, maar deze soorten vallen wel binnen de pentest term die gebruikt wordt binnen dit project en worden ook verkocht als pentestproduct door Deloitte.



Figuur 7 - Soorten pentest

Deloitte pentestproces

In de volgende schematische weergave heb ik het Deloitte pentestproces uitgewerkt. Een grote versie inclusief beschrijving is te vinden in het document "Design Pentest" (fase 4). Dit proces is samen opgesteld en gecontroleerd door de begeleider van Deloitte. Dit proces zal als basis dienen voor het MKB pentestproces.



Figuur 8 – Deloitte pentestproces

5. Requirements analyse - Fase 3

Om de wensen en eisen van de pentesters (eindgebruikers van de MKB pentest), manager en opdrachtgever in kaart te brengen is er een requirements analyse uitgevoerd in fase 3. In dit hoofdstuk worden de doelstelling, aanpak, werkzaamheden en resultaten van deze fase beschreven. Meer informatie over de requirements analyse is in het document "requirements analyse" te vinden, welke als bijlage is bijgevoegd.

5.1 Doelstelling requirements analyse

De doelstelling van deze fase is het in kaart brengen van de eisen en wensen voor het MKB pentestproduct van de mensen die bij het project betrokken zijn. Deze mensen vervullen de volgende functies: pentesters (dit zijn de mensen die uiteindelijk het pentest product gaan gebruiken), managers en de opdrachtgever.
De eisen en wensen dienen uitgewerkt te worden in een document.

5.2 Aanpak requirements analyse

Om alle wensen en eisen in kaart te brengen voor de MKB pentest zijn verschillende mensen geïnterviewd die bij het project betrokken zijn. Tijdens de interviews is gevraagd hoe de persoon de MKB pentest voor zich ziet en uit welke onderdelen de MKB pentest dient te bestaan. Na de interviews zijn de resultaten samengevoegd en is er een onderverdeling gemaakt tussen de "must have" (eisen) en "nice to have" (wensen). Hierbij is gebruik gemaakt van de MoSCoW[5] methode om de wensen en eisen te prioriteren. Alleen de onderdelen "must have" en "could have" zijn gebruikt van de MoSCoW methode om het project eenvoudig te houden. De "could have" zijn in het project gedefinieerd als "nice to have" om verwarring te voorkomen.
Het concept document "requirements analyse" is naar alle mensen die bij het project betrokken zijn, gestuurd; met de vraag of ze het eens zijn met de requirements. Na het verwerken van de verkregen feedback is een nieuwe versie gemaakt en opgestuurd naar de mensen die betrokken zijn bij het project. Dit proces heeft zich herhaald tot iedereen het eens was met de requirements.

5.3 Totstandkoming wensen en eisen

Voordat ik begon met het houden van de interviews heb ik een opzet gemaakt van de MKB pentest requirements. Niet alleen had ik een aantal must/nice to haves gedefinieerd om de geïnterviewden op weg te helpen met het verzinnen van andere items. Ook heb ik kernwaardes opgesteld. Deze kernwaardes zijn gebaseerd op de hoofdoelen van de MKB pentest, namelijk:

- Korte doorlooptijd
- Lage kosten
- Kwalitatief goed

Deze kernwaardes zijn opgesteld om te controleren of de eisen en wensen meerwaarde leveren aan het doel van de pentest. Ook helpen de kernwaardes bij het bepalen of een item een "must have" of "nice te have" is. Wanneer een item niet bijdraagt aan het doel van de MKB pentest hoeft dit geen "must have" te worden.

[5] De MoSCoW-methode is een wijze van prioriteiten stellen aan de wensen en eisen van een project. MoSCoW definieert vier prioriteiten Must, Should, Could en Won't.

Om ervoor te zorgen dat de interviews binnen de planning van fase 3 bleef heb ik in fase 2 al de interviews ingepland. De meeste interviews konden in een week afgenomen worden. Tijdens de interviews zijn de wensen en eisen die bedacht werden, genotuleerd. Aan het einde van het interview zijn de wensen en eisen herhaald aan de geïnterviewde ter controle. Na alle interviews zijn de resultaten verwerkt en samengevoegd in een conceptversie van het document "requirements analyse". De resultaten zijn per persoon in een gesprek doorgenomen. De teruggekregen feedback van de resultaten is verwerkt in een nieuwe versie.

5.4 Wensen en eisen

De resultaten van deze fase bestaan uit de in kaart gebrachte wensen en eisen van de pentesters, managers en opdrachtgever. De wensen en eisen staan beschreven in het document "Requirements analyse" (fase 3) welke als bijlage is bijgevoegd.
Hieronder staan de requirements beschreven met een korte beschrijving. Meer informatie over de requirements analyse is te vinden in het bijgevoegde document.

De requirements zijn verdeeld in twee categorieën de "must haves" en "nice to haves". De must haves zijn punten die in de MKB pentest dienen te komen. De "nice to haves" zijn punten die handig zijn om te hebben in het product, maar niet benodigd zijn voor het behalen van de doelstellingen van de MKB pentest.

Must have

- **Automatische rapportage**
  Het maken van een pentest rapport kost veel werk, dit kan voor een groot deel geautomatiseerd worden om tijd (en geld) te besparen.
- **Portaal**
  Bij een normale pentest vinden er verschillende gesprekken plaats (bijvoorbeeld een intakegesprek of een presentatie van de rapportage) tussen de klant en Deloitte. Om dit proces te versnellen en kosten te besparen dient het mogelijk te worden om deze stappen digitaal uit te voeren. Klanten dienen in te kunnen loggen op een digitaal portaal om o.a. een aanvraag te doen voor een pentest, pentest rapportages te bekijken, voortgang van informatie beveiliging te monitoren, et cetera.
- **Werkprogramma voor MKB pentest**
  Het huidige werkprogramma voor een pentest kost te veel tijd om volledig uit te voeren in de beperkte tijd die beschikbaar is voor een MKB pentest. Het werkprogramma dient ingekort te worden en te worden toegespitst op MKB organisaties. Afhankelijk van de wensen van de klant wordt een deel van het werkprogramma uitgevoerd (bijvoorbeeld alleen een infrastructuur pentest). Tevens moet de kwaliteit van de pentest gewaarborgd worden met behulp van het werkprogramma.
- **Veilige opslag van rapportages en klantgegevens**
  Wanneer klantgegevens & vertrouwelijke informatie (pentestrapportage) op het online portaal komen te staan dient deze informatie goed beveilig te worden.

Nice to have

- **Bijwerken standaard observaties**
  Door meer gebruik te maken van standaard observaties kan er tijd bespaard worden. Er is in april 2011 een opzet gemaakt voor standaard observaties, deze dienen bijgewerkt te worden. Tevens moeten de standaard observaties naar het Nederlands vertaald worden.
- **De pentest meer automatiseren**
  Er kan nog meer tijd worden bespaard wanneer een deel van de uitvoering van een pentest geautomatiseerd wordt. Dit automatiseren moet zorgvuldig gebeuren omdat de ervaring van Deloitte is dat pentestsoftware nog veel "false positives" vindt.
- **Aanpassen rapportage**
  De pentest rapportage dient krachtiger, bondiger en minder technisch te worden voor MKB organisaties. Er kan bijvoorbeeld op één pagina een bondige samenvatting met "heatmap"[6] worden gemaakt. Ook dient er te worden uitgezocht of een (Word)document de beste manier is om de resultaten te presenteren.
- **Benchmark database**
  Met een benchmark database kunnen de pentest resultaten van verschillende klanten vergeleken worden. De resultaten kunnen bijvoorbeeld per branche worden ingedeeld zodat de klant kan zien hoe hij scoort ten opzichte van andere organisaties.

Aan de hand van de requirements zal de MKB pentest ontworpen worden. De prioriteit van dit project zal liggen op de "must haves".

[6] Een heatmap is een grafische weergave van gegevens waarbij de afzonderlijke waarden in een matrix worden weergegeven met behulp van verschillende kleuren. In de pentestrapportage kunnen alle bevindingen in een heatmap worden geplaats, waarbij hoge risico's in het rode gebied en lage risico's in het gele gebied geplaatst kunnen worden.

6. Ontwerp MKB pentest – Fase 4

Fase 4 betreft de belangrijkste en grootste fase van het project. Fase 4 bestaat uit drie onderdelen: het design van de pentest, het concept pentest en het testen van de pentest. In dit hoofdstuk wordt het ontwerp van de MKB pentest beschreven. Meer informatie over het ontwerp pentest is in het document "design pentest" te vinden welke als bijlage is bijgevoegd.

6.1 Doelstelling fase 4

Het doel van fase 4 is het ontwikkelen van een concept MKB pentest. Het concept MKB pentest zal worden ontwikkeld aan de hand van het vooronderzoek (fase 2) en de requirements (fase 3). Naast het ontwikkelen zal het concept van de MKB pentest ook getest worden.

6.2 Aanpak

De ontwikkeling van de pentest bestaat uit drie onderdelen. Het eerste gedeelte bestaat uit het maken van een ontwerp van de MKB pentest. Dit ontwerp is gebaseerd op het vooronderzoek, de wensen en eisen uit de requirements analyse en op de ICT trends voor 2012. Dit ontwerp is uitgewerkt in een document. Ook is aan de belanghebbenden van het project een presentatie gegeven. In deze presentatie is het ontwerp gepresenteerd en is er gediscussieerd over de uitwerking van de MKB pentest. Na goedkeuring kan de MKB pentest ontwikkeld worden aan de hand van het ontwerp. Wanneer een concept MKB pentest is ontwikkeld kan deze uitvoerig getest worden. Een evaluatie van deze test wordt gedaan in fase 5.

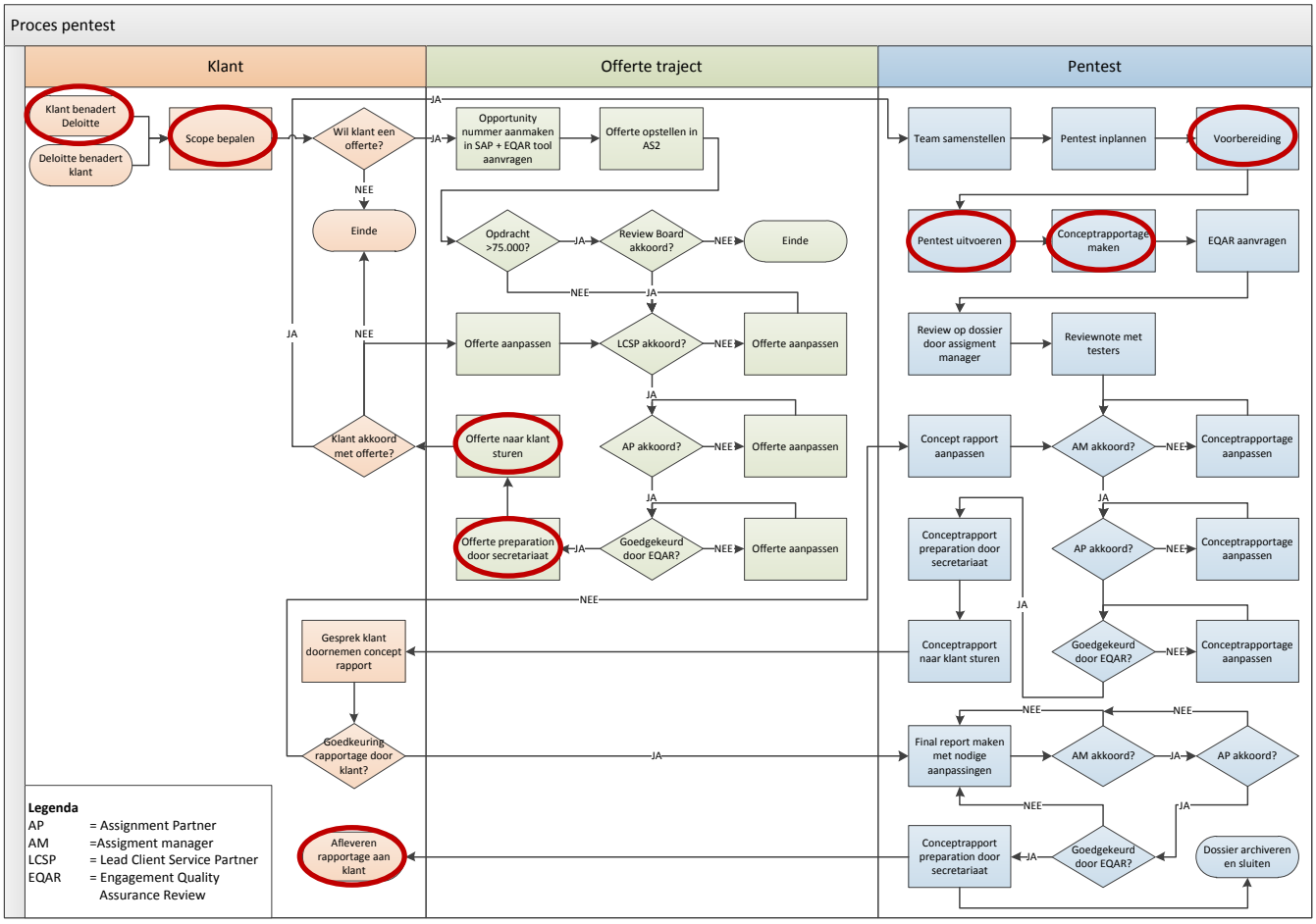
6.3 Design MKB pentest

Het ontwikkelen van de MKB pentest begon met het maken van het ontwerp. Voor het ontwerp is gebruik gemaakt van de gegevens uit het vooronderzoek. Hierdoor zijn een deel van de resultaten uit het vooronderzoek terug te vinden in het document "ontwerp MKB pentest". De informatie uit het vooronderzoek geeft achtergrondinformatie op het gebied van pentesting en geeft een kader uit welke onderdelen de MKB pentest moet bestaan. Het ontwerp is opgebouwd aan de hand van de requirements uit fase 3. De "must haves " zijn dan ook terug te vinden in het ontwerp. Naast het vooronderzoek en de requirements is er ook gekeken naar de ICT trends binnen het MKB. Deze trends kunnen worden gebruikt om de MKB pentest goed aan te laten sluiten op de markt.
De trend "analyse" is uitgevoerd door middel van een deskresearch. De trends zijn niet uitgebreid onderzocht omdat hier de focus niet op lag.
Om de MKB pentest goed aan te laten sluiten op MKB organisaties zijn er verschillende interviews gehouden met mensen die erg betrokken zijn in de MKB wereld. Zo is o.a. besproken waar het MKB behoefte aan heeft en wat voor aandachtspunten het MKB heeft met betrekking tot de pentest.
Voor de verdere uitwerking van het ontwerp zijn verschillende gesprekken gevoerd met pentesters, managers en andere mensen die kunnen helpen bij het ontwikkelen van de pentest. Zo is bijvoorbeeld een gesprek gevoerd met iemand binnen Deloitte die een portaal heeft ontwikkeld voor MKB organisaties. Door gebruik te maken van dit portaal hoeft het wiel niet opnieuw uitgevonden te worden.

Het MKB pentestproces zal voor een groot deel gebaseerd zijn op het normale pentestproces van Deloitte. Hiervoor is gekozen omdat dit proces al jaren gebruikt wordt en alle controle (kwaliteit) stappen bevat. Wel kunnen een aantal processtappen verbeterd/aangepast worden voor de MKB pentest. De volgende processtappen heb ik gedefinieerd die verbeterd/aangepast dienen te worden voor de MKB pentest:

- Klant benadert Deloitte
- Scope bepalen (intake)
- Offerte
- Voorbereiding
- Pentest
- Concept rapport
- Presentatie

Deze stappen zijn op de volgende plekken terug te vinden in het pentestproces (rode cirkels). Een grote variant van deze afbeelding is in de bijlage te vinden.



Figuur 9 - Verbeterpunten MKB pentestproces

Wat per stap verbeterd kan worden en hoe deze stappen uitgewerkt worden voor de MKB pentest, staat beschreven in het document "design pentest" welke als bijlage is bijgevoegd.

Toen het ontwerp af was heb ik het document samen met de begeleider van Deloitte doorgenomen. Met behulp van zijn feedback kon het document verder aangescherpt worden zodat een presentatie van het ontwerp gegeven kon worden aan de belanghebbenden. Deze presentatie was het idee van de begeleider van Deloitte. Het doel van de presentatie was om de mensen die betrokken zijn bij het project op één lijn krijgen voordat de MKB pentest ontwikkeld werd. Omdat ik me kon vinden in het idee heb ik de organisatie van de presentatie op me genomen (geschikt moment voor de presentatie zoeken, mensen uitnodigen, ruimte huren, presentatie maken enz.). Aan deze presentatie deden onder andere managers, pentesters en de opdrachtgever mee.

Ik presenteerde het ontwerp gebaseerd op het document MKB pentest ontwerp. Na de presentatie was er ruimte ingepland om te discussiëren over mijn ideeën. Van deze mogelijkheid werd goed gebruik gemaakt zodat het ontwerp goed aansluit op de wensen en eisen van de gebruikers en opdrachtgever. Ook verhoogt een dergelijke sessie de kwaliteit van de producten, omdat de feedback verwerkt kan worden voordat de MKB pentest is ontwikkeld in plaats van achteraf als de MKB pentest al af is.

Onder andere zijn de volgende punten besloten die afwijken van mijn ontwerp:

- Er komen drie MKB pentestproducten (Mobile, (web)applicatie en infrastructuur). In mijn ontwerp waren dit er twee. Ik had de pentest infrastructuur samengevoegd met de (web)applicatie pentest. De verwachting is dat sommige MKB organisaties alleen een infrastructuur pentest willen.
- Het werkprogramma zal alleen bestaan uit de meest voorkomende kwetsbaarheden in de vorm van een top x. In mijn ontwerp lag de focus op de meest voorkomende kwetsbaarheden, maar ook minder belangrijke onderdelen werden behandeld in het werkprogramma. Om nog meer tijd te besparen worden alleen de meest voorkomende kwetsbaarheden getest.

6.4 Resultaten ontwerp MKB pentest

De resultaten van deze fase bestaan uit het ontwerp van de MKB pentest en een conceptversie van de MKB pentest. Voor deze fase is het document "design pentest" opgeleverd. Hieronder staan een aantal belangrijke resultaten weergegeven uit het ontwerp.

Trends in de ICT

De MKB pentest dient goed aan te sluiten op de vraag van MKB organisaties. Om de verwachte vraag in kaart te brengen is gekeken naar de (MKB) ICT trends voor 2012. Trendonderzoekbureaus hebben verschillende inzichten over de (MKB) ICT trends voor 2012. Maar er zijn ook overeenkomsten welke in de volgende opsomming worden gegeven:

- Mobiele apparaten
- Mobiele applicaties
- Cloud computing
- Groei van (gevoelige) data
- MKB gaat meer online doen

Deze punten kunnen gebruikt worden voor de ontwikkeling van de MKB pentest. De trends voorspellen bijvoorbeeld veel gebruik van mobiele apparaten en applicaties. De MKB pentest dient zo ontwikkeld te worden dat mobiele apparaten en applicaties getest kunnen worden op kwetsbaarheden.

Focus MKB pentest op meest gevraagde producten

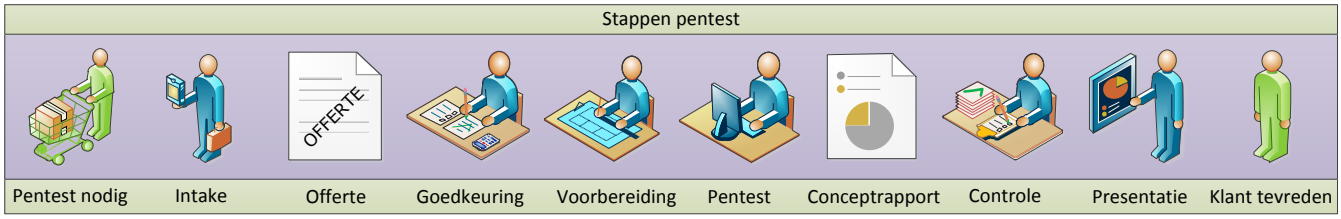
Om het MKB pentest aanbod eenvoudig en overzichtelijk te houden voor de klanten zal de focus van de MKB pentest liggen op drie producten. De verwachting is dat deze drie producten het meest aangevraagd zullen worden. Deze verwachting is gebaseerd op de ervaring van de pentesters, managers en de (2012) ICT trends. De samenstelling van de producten is ontstaan door het samenvoegen van een aantal soorten pentests. Deze producten zullen een vaste prijs krijgen.

Website	Mobile	Infra
		
• Kwetsbaarhedenscan website • Kwetsbaarhedenscan webserver	• Kwetsbaarhedenscan mobiele applicatie • Kwetsbaarhedenscan mobiel apparaat	• Kwetsbaarhedenscan infrastructuur

Figuur 10 - MKB pentestproducten

MKB pentestproces

In het onderstaande model is een schematisch weergave gemaakt van het MKB pentestproces. De manier waarop een processtap wordt uitgevoerd (bijvoorbeeld digitaal, telefonisch of mondeling) is niet gedefinieerd. Een uitgebreidere beschrijving van het pentestproces is te vinden in het document "Design pentest" welke als bijlage is toegevoegd.



Figuur 11 - MKB pentestproces

MKB aandachtspunten

MKB organisaties ondernemen op een andere manier dan grote organisaties. Om de pentest goed aan te laten sluiten op het MKB moet rekening worden gehouden met de manier van werken binnen het MKB. Aan de volgende punten moet aandacht worden besteed voor de MKB pentest:

- Externe partijen
- Afwezigheid van pre-productie
- Maakt gebruik van kant-en-klare oplossingen

Deze punten zijn opgesteld aan de hand van mijn eigen analyse met behulp van informatie uit het vooronderzoek. Het is interessant om te zien dat deze punten niet aangegeven waren door de pentesters/opdrachtgever tijdens de requirements analyse. Dit benadrukt het belang van het vooronderzoek, welke als overbodig werd gezien door de pentesters.

Meer dan pentest alleen

De nadruk van de MKB pentest ligt op het uitvoeren van de pentest en het leveren van de rapportage aan de klant. Wanneer blijkt dat er veel vraag is naar de MKB pentest kan de dienst voor het MKB worden uitgebreid. Hierbij kan worden gedacht aan verschillende mogelijkheden:

- Periodieke pentest
- Problemen oplossen
- Adviespartner
- Informatiebeveiliging incidenten
- Andere diensten op het gebied van informatiebeveiliging binnen het MKB

7. Ontwikkeling concept MKB pentest – Fase 4

Na afronding en goedkeuring van het MKB pentest ontwerp kan begonnen worden aan de ontwikkeling van de MKB pentest. In dit hoofdstuk staat het ontwikkeltraject en de uitwerking van het concept MKB pentest beschreven. Het concept MKB kon niet in zijn geheel worden bijgevoegd als bijlage omdat niet alle onderdelen tastbaar zijn. Wel wordt de uitwerking van alle onderdelen in dit hoofdstuk beschreven.

7.1 Ontwikkeltraject MKB pentest

De ontwikkeling van de MKB pentest is aangepakt aan de hand van het ontwerp MKB pentest. Het doel van deze fase was het uitwerken van de pentest onderdelen die beschreven staan in het ontwerp, die gebaseerd zijn op de requirements. Voor het uitwerken van deze onderdelen zijn meerdere gesprekken gevoerd met experts. Voor het ctrl portal zijn bijvoorbeeld gesprekken gevoerd met de manager die het portal heeft opgezet en voor het uitwerken van het pentest werkprogramma is samengewerkt met een pentester.
Er is doorgewerkt aan het concept van de MKB pentest tot de geplande einddatum (zie planning). Dit concept is getest in de volgende sub-fase. Welke methode is gebruikt om de MKB pentest te testen en wat de resultaten zijn van deze test is te lezen in het volgende hoofdstuk (8.2).

7.2 Waar bestaat het concept uit

Het concept MKB pentest bestaat uit een aantal uitgewerkte onderdelen welke in deze paragraaf beschreven worden. Alle onderdelen heb ik zelf uitgewerkt met hulp van experts.

- **Ctrl Portal**
  Het ctrl portal is een portaal ontwikkeld door de afdeling controls van Deloitte. Via het portaal krijgen MKB klanten de gelegenheid om online samen te werken met hun Deloitte adviseur, kunnen ze gebruik maken van online diensten en toegang krijgen tot informatie die relevant is voor hun onderneming. Klanten kunnen via het portaal ook nieuwe diensten aanvragen (in de vorm van een "app store"). De MKB pentest zal in deze "app store" worden toegevoegd zodat mensen de dienst kunnen aanvragen. Een voorbeeld van hoe deze pagina eruit komt te zien is te vinden in de bijlage. Dit document is door mij gemaakt en gebruikt als opzet voor het ctrl portal. Dit document is ook besproken tijdens de gesprekken met de manager van het ctrl portal.

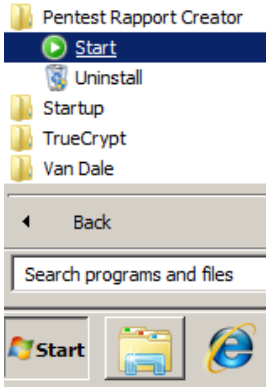
Bij het aanvragen van de MKB pentest via het portal dient de klant een aantal gegevens in te voeren welke gebruikt kunnen worden voor het maken van de offerte (zij bijlage "tekst voor ctrl portal").

- **Offerte**
  De nieuw ontwikkelde offerte is gebaseerd op de normale pentest offerte met het verschil dat de MKB pentest offerte nog bondiger en meer gestandaardiseerd is. De offerte is opgebouwd aan de hand van de verschillende soorten pentest (web, mobile en infra) en de vaste kosten die deze pentest hebben (zie het document ontwerp MKB pentest). Wanneer een klant een pentest aanvraagt via het ctrl portal kan heel snel een offerte worden gemaakt met behulp van de door de klant ingevulde gegevens.

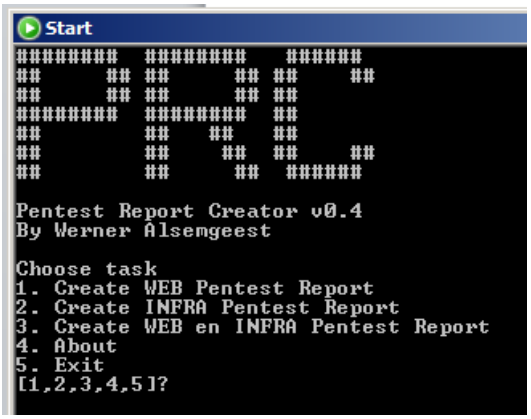
- **Pentest**
  De uitvoering van de pentest bestaat uit het volgen van een werkprogramma door een pentester. Deze methode wordt ook bij de normale pentest van Deloitte gebruikt. Het werkprogramma van de MKB pentest is deels gebaseerd op het normale werkprogramma. Het verschil tussen deze twee is dat de MKB pentest zich alleen richt op kwetsbaarheden met een hoog risico. Het uitvoeren van het volledige normale werkprogramma zou te veel tijd in beslag nemen en daardoor te duur worden voor een MKB organisatie.
  Voor de website pentest werkprogramma is bijvoorbeeld een top 7 opgesteld van kwetsbaarheden met een hoog risico. Deze top 7 is gebaseerd op de OWASP top 10[7] en ervaringen van de pentesters. Een voorbeeld van een werkprogramma is bijgevoegd als bijlage. Om de kwaliteit van het werkprogramma te waarborgen is deze gecontroleerd door de begeleider van Deloitte en is het werkprogramma getest (zie hoofdstuk 8.2).

- **Rapportage** (tooling)
  Het onderdeel rapportage bestaat uit een tool die ontwikkeld is door mij om pentest rapportages te genereren. De tool heet 'Pentest Report Creator' en maakt gebruik van een database met standaard bevindingen die in de rapportage verwerkt worden. Een voorbeeld van een standaardbevinding is bijvoorbeeld dat de gebruikte software verouderd is. Bij een dergelijke bevinding staat ook de kans dat de kwetsbaarheid misbruikt wordt, de impact op het systeem wanneer de kwetsbaarheid misbruikt wordt en hoe de kwetsbaarheid opgelost kan worden. De tool maakt gebruikt van batchscripts, een database, templates en macro's.

  De tooling kon niet als bijlage worden bijgevoegd. Om toch een beeld te kunnen geven van de tooling zijn hieronder een aantal screenshots bijgevoegd en is in de bijlage een procestekening bijgevoegd.



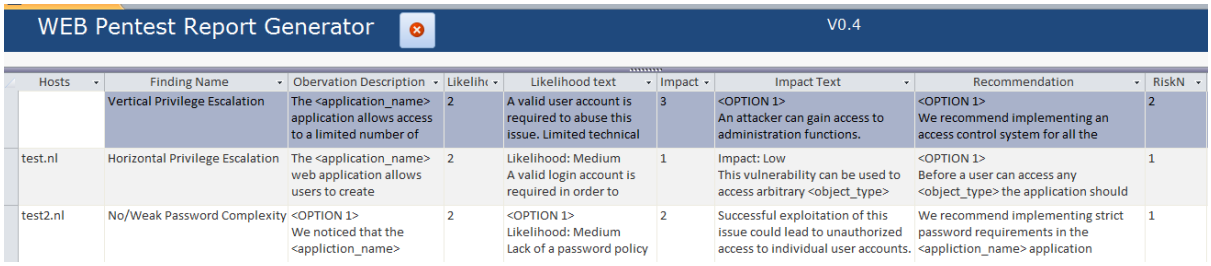
← 1) het starten van de 'Pentest Rapport Creator'



2) Het kiezen van het soort pentestrapport →

[7] OWASP top 10 - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

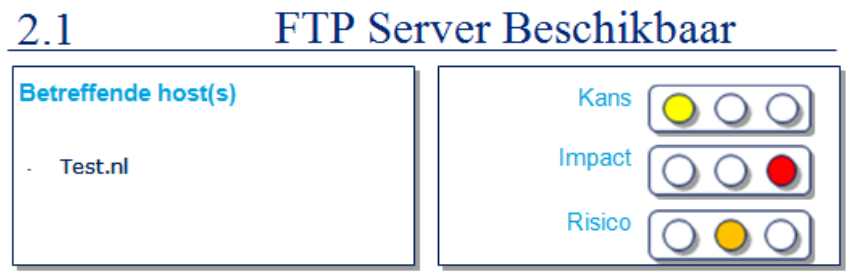
3) Automatisch na het kiezen van de soort pentestrapportage wordt een database geopend waar de pentester kan kiezen welke standaard bevindingen in de rapportage moeten komen (door middel van een 'checkbox'). Ook kan de pentester aangeven voor welk object de bevinding geldt en is er een mogelijkheid om eigen bevindingen bij te voegen.



WEB Pentest Report Generator V0.4

Hosts	Finding Name	Obervation Description	Likelih	Likelihood text	Impact	Impact Text	Recommendation	RiskN
	Vertical Privilege Escalation	The <application_name> application allows access to a limited number of	2	A valid user account is required to abuse this issue. Limited technical	3	<OPTION 1> An attacker can gain access to administration functions.	<OPTION 1> We recommend implementing an access control system for all the	2
test.nl	Horizontal Privilege Escalation	The <application_name> web application allows users to create	2	Likelihood: Medium A valid login account is required in order to	1	Impact: Low This vulnerability can be used to access arbitrary <object_type>	<OPTION 1> Before a user can access any <object_type> the application should	1
test2.nl	No/Weak Password Complexity	<OPTION 1> We noticed that the <appliction_name>	2	<OPTION 1> Likelihood: Medium Lack of a password policy	2	Successful exploitation of this issue could lead to unauthorized access to individual user accounts.	We recommend implementing strict password requirements in the <appliction_name> application	1

4) Na het kiezen van de bevindingen kan het rapport worden gegenereerd. Het rapport bestaat uit een aantal onderdelen zoals het management samenvatting, hoe de pentest is aangepakt, de bevindingen enz. De tooling genereert het hele rapport maar richt zich voornamelijk op de bevindingen. Hieronder is een voorbeeld van een bevinding weergegeven.



2.1 FTP Server Beschikbaar

Betreffende host(s)

- Test.nl

Kans

Impact

Risico

Observatie

We hebben vastgesteld dat een FTP server actief is op <server>. FTP is een „plaintext" protocol, hierdoor worden gegevens niet versleuteld wanneer deze over het netwerk worden verstuurd. Connecties kunnen worden onderschept waardoor gebruikersnamen en wachtwoorden kunnen worden bemachtigd.

Kans

Om FTP te onderscheppen moet een aanvaller zich in het netwerkpad bevinden tussen de gebruiker en de server. Het onderscheppen van FTP verkeer vereist geavanceerde technische kennis.

Impact

Het succesvol onderscheppen van FTP verkeer kan ertoe leiden dat een aanvaller de gebruikersnaam en wachtwoord combinatie van gebruikers van de betreffende FTP server kan bemachtigen.

De pentester dient nog wel de bevinding klant specifiek te maken en waar nodig te kiezen tussen een aantal opties. De tooling is niet bedoeld om het werk van de pentesters te vervangen, maar om te ondersteunen. Er kan veel tijd worden bespaard door het automatisch generen van het pentest rapportage.

8. Afsluiting project en advies - Fase 5

Dit is de afsluitende fase van het project "ontwikkelen van de MKB pentest". Fase 5 bestaat uit twee onderdelen: een evaluatie van de test, die uitgevoerd is om de pentest te testen en een advies aan Deloitte over welke vervolgstappen ze moeten ondernemen voor de verdere ontwikkeling van de MKB pentest.

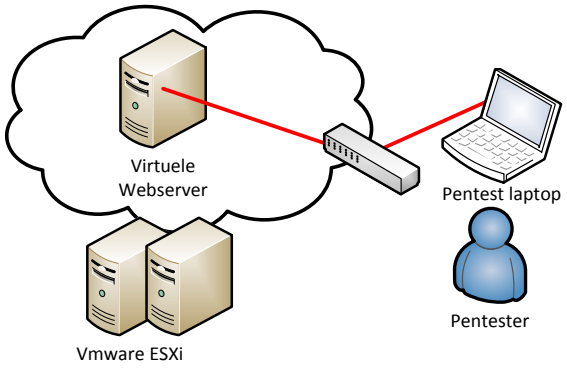
8.1 Doelstelling fase 5

De doelstelling van deze fase is het controleren van de werking en kwaliteit van de ontwikkelde MKB pentest. Omdat deze fase de afsluitende fase is van het project zal Deloitte worden geadviseerd over de verdere uitwerking van de MKB pentest.

8.2 Test concept pentest

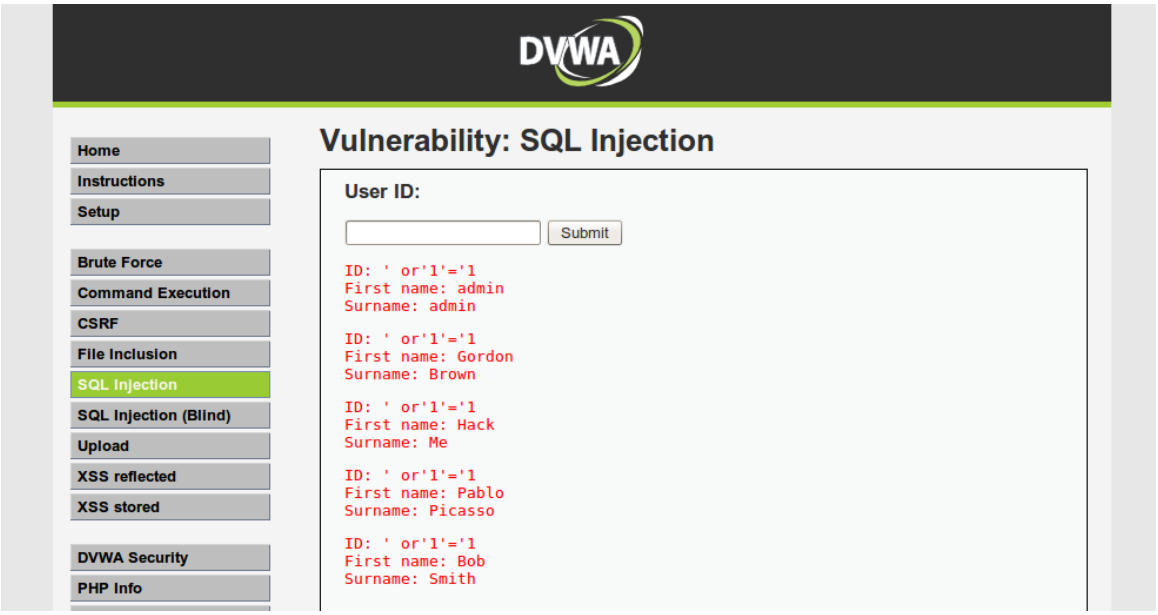
Het concept van de MKB pentest is door mij getest om te controleren of de pentest uitgewerkt is zoals bedacht was in het ontwerp. Wanneer fouten gevonden worden in de pentest kunnen deze opgepakt worden voordat de pentest aan klanten wordt verkocht. Tevens kan met behulp van de test de kwaliteit van de pentest gecontroleerd worden. Tijdens de test is niet gekeken hoe snel een MKB pentest uitgevoerd kan worden. Hiervoor was geen tijd beschikbaar.
De test is uitgevoerd met behulp van twee methodes. Er zijn twee methodes gebruikt om verschillende aspecten van de pentest te testen.

- De eerste methode bestond uit het testen van de werking van de pentest. Met deze test kan worden gecontroleerd of alle onderdelen van het ontwerp goed zijn ontwikkeld. Om deze test uit te voeren heb ik een testsysteem opgezet in een afgeschermde omgeving, waarop ik een deel van de MKB pentest heb uitgevoerd. In verband met de tijd die beschikbaar was in fase 5 heb ik alleen de website en infrastructuur pentest kunnen testen. In het kort beschrijf ik de stappen die ik uitgevoerd zijn:
    - **Opzetten testomgeving**
      De testomgeving is op een eenvoudige manier opgezet bestaande uit een webserver en een laptop waar vandaan de test worden uitgevoerd. Er is gebruik gemaakt van software die ook binnen MKB organisatie gebruikt wordt. In de test is gebruikt gemaakt van het besturingssysteem Windows server 2008 R2 en van de hostingssoftware Parallels Pleks 10.4. Voor het opzetten van de testomgeving is de virtualisatiesoftware Vmware ESXi gebruikt. In de volgende afbeelding is een schematische weergave te vinden van de testomgeving.



Figuur 12 - Opzet testomgeving MKB pentest

- **Kiezen webapplicatie**
  Omdat er een website/webapplicatie getest wordt tijdens de pentest dient er een website geplaatst te worden op de webserver. Om tijd te besparen is een standaard website geïnstalleerd die bekende kwetsbaarheden bevatten. Organisaties maken dergelijke website voor test-doeleinden[8]. De keuze is gevallen op de website: 'Damn Vulnerable Web Application"[9] (DVWA). Er is gekozen voor deze website omdat deze gebruikt maakt van PHP en MySQL. Dit zijn website talen die erg veel gebruikt worden door websites.
- **Uitvoeren concept MKB pentest**
  Na het installeren van de website kon de MKB pentest worden uitgevoerd. De test is uitgevoerd aan de hand van de website en infrastructuur werkprogramma. Hierbij zijn alle stappen gevolgd en alle programma's uitgevoerd. (voor een voorbeeld zie het 'web pentest werkprogramma' welke als bijlage is bijgevoegd.)



Figuur 13 - Voorbeeld gevonden kwetsbaarheid door de MKB pentest

- **Resultaten**
  De resultaten van de pentest zelf zijn niet zo belangrijk. Het was van te voren al bekend welke kwetsbaarheden in de website zitten en dat de gebruikte tooling de kwetsbaarheden zou vinden. Er zal dan ook niet op de pentestresultaten worden ingegaan.
  Wat interessant is, is of de werking van het pentestproces klopt. Het resultaat is dat het werkprogramma goed doorlopen kan worden, de stappen goed worden beschreven en de juiste resultaten behaald worden. Ook kwam uit het resultaat naar voren dat sommige stappen in het werkprogramma nog wat aangescherpt kunnen worden om verwarring te voorkomen. Deze aanpassing is gelijk doorgevoerd in het werkprogramma.

[8] Voorbeeldlijst van kwetsbare websites http://securitythoughts.wordpress.com/2010/03/22/vulnerable-web-applications-for-learning/
[9] Website van DVWA: http://dvwa.co.uk

- De tweede methode bestond uit het controleren van de kwaliteit van de pentest. Met behulp van deze test konden de resultaten van de MKB pentest vergeleken worden met de resultaten van een normale pentest. Het vergelijken van de resultaten is gedaan met pentest rapportages die al uitgevoerd waren. Ik heb samen met een pentester gecontroleerd of dezelfde bevindingen waren gevonden als het MKB pentest werkprogramma gevolgd was. Uit de resultaten van deze test kwam naar voren dat er een verschil zit in de resultaten van de MKB pentest en de normale pentest. Dit verschil is te verklaren door het aantal kwetsbaarheden dat getest worden per werkprogramma. Bij het werkprogramma van de MKB pentest worden alleen de kwetsbaarheden met een hoog risico getest.
  De volgende vraag is dan of het erg is dat de MKB pentest bepaalde kwetsbaarheden niet vindt. De kwetsbaarheden die niet gevonden werden waren kwetsbaarheden met een laag risico (zoals verkeerd gebruik van "cookie flags[10]"). Omdat de MKB pentest goedkoop moet zijn kan niet naar alle kwetsbaarheden gezocht worden. De MKB pentest geeft ook geen garantie (Assurance) dat de website/systeem niet gehackt kan worden. De resultaten van de test kon niet worden bijgevoegd in verband met gevoelige (klant-) informatie.

[10] http://en.wikipedia.org/wiki/HTTP_cookie

8.3 Vervolgstappen MKB pentest

Na afronden van het project MKB pentest houdt de ontwikkeling van de MKB pentest niet op. Deloitte zal verder moeten gaan met de verdere ontwikkeling en het in de markt zetten van de MKB pentest. In deze paragraaf wordt het advies beschreven dat ik aan Deloitte gegeven heb voor de verdere ontwikkeling van de MKB pentest. De vervolgstappen zijn per onderdeel beschreven.

Offerte

Het ontwikkeltraject van de offerte heeft geen vervolgstappen nodig.

Pentest

De volgende stap is het uitvoeren en evalueren van de pentest bij een klant. Tijdens het afstuderen was hier helaas geen tijd voor. Deze test zal waarschijnlijk na het inleveren van het afstudeerdossier worden uitgevoerd.

Rapportage

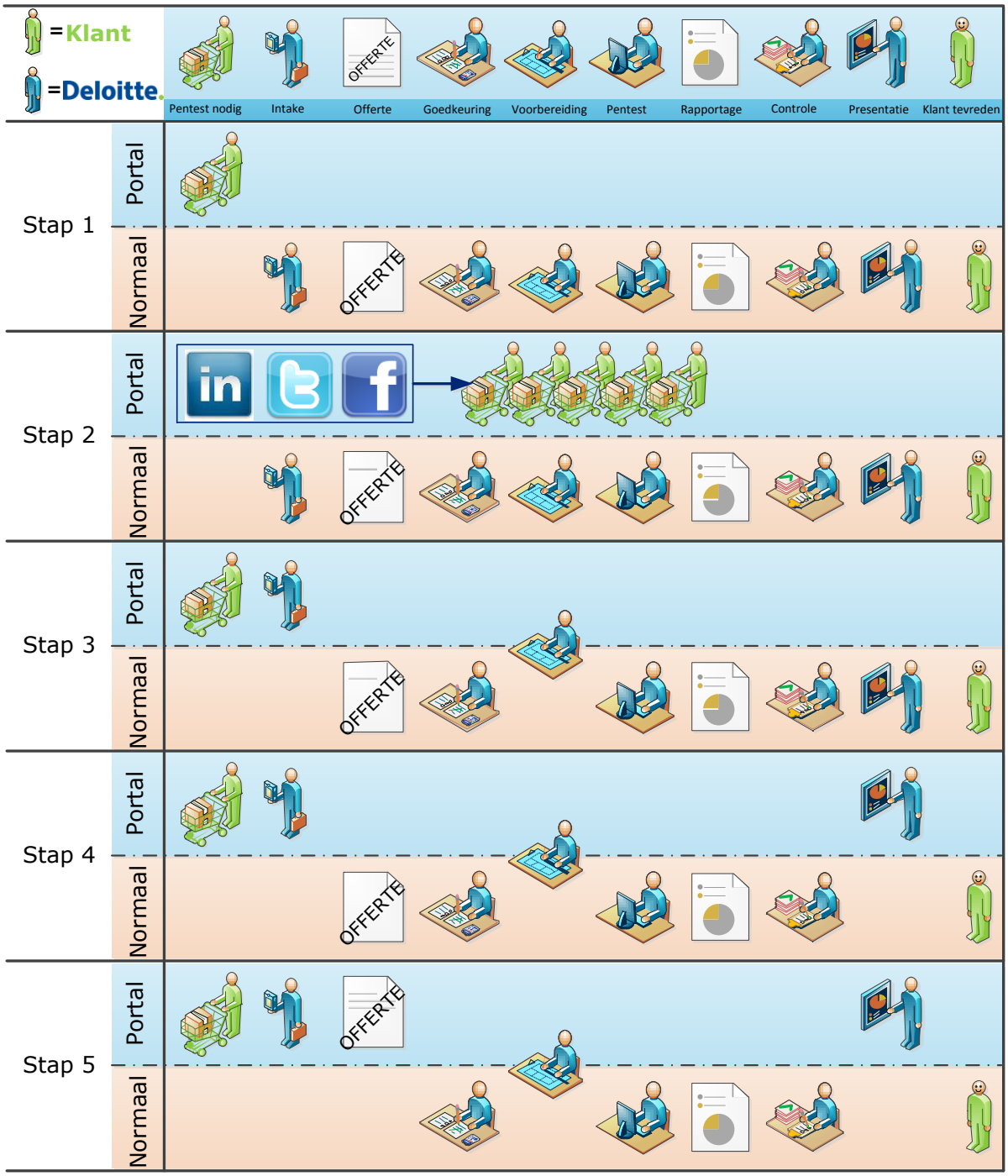
De template voor de pentestrapportage is goedgekeurd en de tooling om de rapportages te genereren werkt. De volgende stap is het verder automatiseren van de rapportage en het automatisch laten genereren van de "heat map". Deze vervolgstappen zijn onderdeel van de "nice to have" uit de requirements analyse.

Ctrl portal

De vervolgstappen voor de ontwikkeling van het ctrl portal zijn weergegeven in de schematische weergave op de volgende pagina. De ontwikkeling is opgedeeld in stappen omdat het teveel tijd kost om het hele traject in één keer te implementeren. Met behulp van deze aanpak kunnen klanten al in de eerste stap beginnen met het aanvragen van de MKB pentest.

- **Stap 1**
  De eerste stap is het plaatsen van het product in de "app store" van het ctrl portal. Een concept hiervan is te vinden in de bijlage "Tekst voor ctrl portal". Het is vanaf deze stap mogelijk voor klanten om het product aan te vragen.
- **Stap 2**
  In deze stap wordt het product actief gepromoot met behulp van social media, nieuwsartikelen op het ctrl portal en een nieuwsbrief. Het resultaat hiervan is dat meer klanten het product zullen aanvragen.
- **Stap 3**
  De intake zal via het ctrl portal plaatsvinden. Tijdens de intake kan de klant via het portaal gegevens over de pentest scope invullen. Meer informatie over het intakeproces zie het document "design pentest. Wanneer deze gegevens online in het portaal komen te staan heeft de processtap "voorbereiding van de pentest" hier ook profijt van.
- **Stap 4**
  In stap 4 zal een "E-dossier" omgeving worden opgezet voor de klant. In het "E-dossier" worden documenten geplaats die de klant online kan bekijken. Onder andere kan de offerte en het pentestrapport online worden geplaatst.

- **Stap 5**
  In de laatste stap zal het gehele offerte gedeelte online worden gezet. De klant vraagt online het product aan, krijgt automatisch de offerte toegestuurd en kan hem via het ctrl portaal digitaal ondertekenen zodat gelijk aan de pentest begonnen kan worden.



Figuur 14 - Schematische weergave van de vervolgstappen voor het ctrl portal

9. Evaluatie

Dit hoofdstuk bevat de evaluatie van mijn afstudeerstage. De evaluatie bestaat uit drie delen: de productevaluatie, procesevaluatie en de evaluatie van mijn competentie-ontwikkeling. Aan het einde van dit hoofdstuk wordt de afstudeerstage in het "algemeen" geëvalueerd.

9.1 Productevaluatie

In dit hoofdstuk worden de producten die opgeleverd zijn aan Deloitte, geëvalueerd.

Plan van Aanpak

In het plan wordt duidelijk gemaakt wat de aanleiding en doelstelling van het project is, hoe het project aangepakt zal worden en hoe de kwaliteit, planning en risico's gewaarborgd worden. Voor het maken van het plan van aanpak kon een standaard design worden gebruikt wat tijd heeft bespaard. Ik heb geen negatieve feedback gekregen op het plan van aanpak. De feedback die ik kreeg ging over kleine aanpassingen in de planning, projectteamstructuur en risico's. Het enige dat ik jammer vind is dat de Deloitte logo's niet gebruikt mogen worden voor de documentatie. Wanneer het Deloitte logo op een document staat betekent dit dat Deloitte achter de ideeën en plannen staat en dat kan (nog) niet gewaarborgd worden voor de documenten die ik oplever (vandaar dat in dit document geen Deloitte logo te vinden is). Over het plan van aanpak kan ik tevreden zijn.

Vooronderzoek

Voor het vooronderzoek is geen apart product (document) opgeleverd. Deze productevaluatie gaat over het eerste deel van het document "design pentest" (fase 4). In het eerste gedeelte staat onder andere achtergrondinformatie over pentesting beschreven, hoe een pentest aangepakt kan worden, wat voor soorten pentests er zijn en hoe Deloitte pentests uitvoert. Deze informatie is gebaseerd op het vooronderzoek. Ik ben van mening dat de eerste hoofdstukken een duidelijk kader scheppen over het onderwerp pentesting. Om de informatie eenvoudig en overzichtelijk te houden heb ik een deel van de informatie gevisualiseerd met behulp van schematische tekeningen. Ik heb een mondelinge positieve reactie gehad op mijn visuele uitwerking van het Deloitte pentestproces door de opdrachtgever. Hij wil dat het pentestproces schema vergroot, uitgeprint en ophangen wordt op de afdeling.

Requirements analyse

Dit document is het resultaat van fase 3. Ik ben tevreden over dit document omdat de wensen en eisen voor de MKB pentest op een bondige en overzichtelijke manier zijn uitgewerkt. Er was eerst twijfel over de meerwaarde van de in het document beschreven kernwaarden maar na enig overleg en een aanpassing in de beschrijving kon de twijfel weg worden genomen. Dit document zal als basis dienen voor het ontwerp van de MKB pentest (fase 4).

Ontwerp MKB pentest

In het ontwerp MKB pentest staat beschreven hoe de MKB pentest eruit komt te zien na de ontwikkeling. Ook staat beschreven waarom voor dit ontwerp is gekozen. De keuzes worden onderbouwd aan de hand van het vooronderzoek, informatie van de experts en de (MKB) ICT trends. Ik ben van mening dat het ontwerp goed onderbouwd is. Ik heb geprobeerd zoveel mogelijk gebruik te maken van informatie van de bestaande pentest,

om het wiel niet opnieuw uit te vinden en de kwaliteit te waarborgen. Wel heb ik een aantal nieuwe onderdelen aangepast aan de markt van het MKB.
Het document beschrijft in chronologische volgorde het tot stand komen van de MKB pentest (achtergrondinformatie, hoe voert Deloitte de pentest uit, noodzaak voor pentesting binnen MKB, trends in ICT, soorten MKB pentest, aanpak MKB pentest, MKB pentestproces, aandachtspunten MKB en de uitgewerkte onderdelen). Met behulp van dit document kan de MKB pentest op een gestructureerde en goedgekeurde manier ontwikkeld worden.

Concept MKB pentest
Het concept pentest is moeilijk te evalueren omdat de pentest uit meerdere onderdelen bestaat. Deze onderdelen zijn ontwikkeld aan de hand van het MKB pentest ontwerp. Ik zal elk onderdeel in het kort behandelen:

- (ctrl) Portal
  Voor het portaal zijn een aantal goede gesprekken gevoerd met een andere afdeling die het ctrl portal ontwikkeld heeft. Tijdens deze gesprekken hebben ze een aantal goede ideeën en punten waar we rekening mee moeten houden aangedragen. Zoals het op de markt zetten van het product en het gebruik van Social Media. Het is alleen niet gelukt om de MKB pentest op het crtl portal te zetten tijdens de afstudeerstage. Het traject om een product op het portaal te krijgen kost veel tijd. Mede omdat de afdeling die het crtl portal beheert het erg druk heeft met een andere opdracht. De belangrijkste stappen zijn wel gemaakt. We weten hoe het product op de pagina moet staan, de tekst voor het portaal is gemaakt en het proces is uitgewerkt.
- Offerte
  De offerte voor de MKB pentest is gemaakt aan de hand van een offerte die een keer naar een MKB klant gestuurd is. De klantgegevens zijn uit de offerte gehaald en vervangen door algemene tekst zoals: <klantnaam>. Deze velden kunnen worden ingevuld met behulp van de door de klant ingevoerde gegevens in het ctrl portal tijdens het aanvragen van de MKB pentest. Verder is de tekst in de offerte aangepast aan het MKB pentest product en generiek gemaakt, zodat de offerte naar verschillende klanten kan worden gestuurd zonder veel aanpassingen.
- Pentest
  De pentest bestaat uit een werkprogramma. Het werkprogramma richt zich alleen op de kwetsbaarheden met een hoog risico. Dit product kon eenvoudig in elkaar worden gezet met behulp van het normale pentest werkprogramma. Ik heb gebruik gemaakt van de OWASP top 10 en kennis van de pentester om in het pentest werkprogramma alleen de kwetsbaarheden met hoog risico te testen.
- Rapportage
  Toen de eis ontstaan was om automatisch een rapportage te genereren in de requirements analyse dacht ik dat dit me nooit zou lukken om een dergelijk tool te ontwikkelen. Een pentester vertelde me dat het met behulp van macro’s zou moeten lukken, alleen had ik daar nog nooit mee gewerkt. Gelukkig zijn macro’s niet moeilijk om te leren en is er veel over dit onderwerp op het internet te vinden. Ik kreeg het daardoor snel voor elkaar om een testversie te ontwikkelen. Tijdens het verder ontwikkelen van de tool liep ik nog tegen een aantal kleine problemen op zoals de template, de beveiligingsrechten waar de macro’s tegen aan lopen enz. Maar ik ga het niet te veel over deze problemen hebben. Uiteindelijk heb ik een werkende versie opgeleverd waar ik best trots op kan zijn. De tooling doet wat hij moet doen, namelijk het automatisch generen van een rapportage; en hij is gebruiksvriendelijk.

9.2 Procesevaluatie

In deze paragraaf wordt het proces per fase geëvalueerd. Per fase wordt behandeld wat goed ging en wat verbeterd kan/moet worden.

Fase 1 – opzet project

Fase 1 bevat de start van de afstudeerstage en de start van het project. De start en inwerking bij Deloitte zijn erg goed bevallen. Ik was eerder begonnen met de afstudeerstage dan de datum die door De Haagse Hogeschool werd voorgesteld zodat ik kon deelnemen aan het maandelijkse introductieprogramma. De introductie vond plaats in het hoofgebouw van Deloitte, de Maastoren in Rotterdam. Tijdens de introductiedag heb ik kennis gemaakt met andere nieuwe Deloitte medewerkers en heb ik inzicht gekregen in de organisatie aan de hand van een aantal presentaties.

Deze dag heb ik als heel positief ervaren; er hing een gezellige en informele sfeer. Je voelt je gelijk welkom en betrokken bij de organisatie. De introductie op het kantoor in Amstelveen en de kennismaking met het security team verliepen ook vloeiend. Op de eerste dag kreeg ik een laptop en kon er gelijk aan de slag worden gegaan omdat alles al goed stond ingesteld. Deze vloeiende manier van inwerken heb ik weleens anders gezien bij organisaties, duim omhoog voor Deloitte dus. Ook al zorgde de goede introductie voor een comfortabel begin, ik liep de eerste dag gelijk tegen een probleem op. Een deel van de mensen waarmee ik samen zou werken tijdens mijn afstudeerstage spreken geen Nederlands en de kennismaking met deze mensen verliep daardoor niet erg vloeiend. Ik was niet gewend om samen te werken met mensen uit Tsjechië, Engeland, Oekraïne, Amerika enz. Dit was een omschakeling naar Engels als voertaal die ik niet verwacht had, maar na een paar gesprekken merk je dat alle woorden en zinnen weer terugkomen zodat je veel zelfverzekerder een gesprek aangaat.

Het werken aan het plan van aanpak verliep erg vlot. De mensen die bij het project betrokken waren zijn erg behulpzaam en geïnteresseerd in het project. De meeste tijd zat in het op één lijn te krijgen van iedereen betreft de aanpak van het project. Sommige mensen waren bijvoorbeeld niet geïnteresseerd in het vooronderzoek maar wilden gelijk beginnen aan de uitwerking van de MKB pentest.
Na nog een aantal gesprekken waarin het concept plan van aanpak werd besproken, was iedereen tevreden over de aanpak en kon een begin worden gemaakt aan de volgende fase.

Fase 2 - vooronderzoek

Normaal is vooronderzoek niet erg spannend. Ook tijdens deze afstudeerstage moest een hoop gelezen worden, maar deze keer was het een stuk interessanter. Het vooronderzoek is interessant geworden omdat het onderwerp pentesten veel overlap heeft met het onderwerp hacking en hacken is spannend. Wanneer je naar informatie op gebied van hacking zoekt kom je op de duistere kant van het internet terecht. Er zijn bijvoorbeeld communities te vinden die ideeën, gevonden kwetsbaarheden en tooling uitwisselen. Uiteraard kan het vooronderzoek niet gebaseerd worden op deze informatie, dus ik heb me gericht op instanties die zich richten op pentesting en het bescherming van het internet zoals OWASP en SANS. Bij deze partijen is erg veel informatie te vinden over hoe een pentest aangepakt kan worden en wat voor standaarden daarvoor gebruikt kunnen worden.

Een heel leerzame ervaring tijdens fase 2 was het meelopen met pentesters bij het uitvoeren van pentestopdrachten. Niet alleen heb ik een hoop nieuwe dingen geleerd op gebied van pentesting, ook heb ik tijdens de pentests inzicht gekregen in betrouwbare informatie van klanten. Door het meekijken was ik bijvoorbeeld op de hoogte van de kwetsbaarheden die de website van een klant betrof. Het was erg interessant om een echte hacker aan het werk te zien. Zelf mocht ik ook aan de slag als ethische hacker door het uitvoeren van "hackers"/pentesters traingen. Zo heb ik bijvoorbeeld bij een bepaalde training inloggegevens achterhaald van een website.

Ik denk dat ik tijdens het vooronderzoek voldoende relevante informatie heb gevonden voor de rest van het project. Tijdens het vooronderzoek heb ik inzicht gekregen in hoe een (Deloitte) pentest uitgevoerd wordt, uit welke onderdelen een pentest bestaat en hoe het Deloitte pentestproces eruitziet. Ook heb ik aan mijn eigen vaardigheden gewerkt op het gebied van pentesting door het uitwerken van "hack" oefeningen. Tijdens deze "hack" oefeningen worden kwetsbaarheden misbruikt die je ook tijdens een pentest tegen komt zoals XSS.[11]

Fase 3 – requirements analyse
Fase 3 bestaat uit vier onderdelen: interviews voorbereiden, interviews afnemen, resultaten uitwerken en feedback verwerken. Het voorbereiden van de interviews is erg goed verlopen. Ik was op tijd begonnen met het inplannen van de interviews (al in fase 2). Hierdoor kon ik in één week bijna iedereen interviewen. Iedereen behalve de opdrachtgever omdat hij het erg druk had die week. Ik heb van hem de feedback later gekregen via de mail. Het was zelfs zoveel later dat de feedback van iedereen al verwerkt was. Samen met mijn begeleider is gekeken of de wensen en ideeën meerwaarde leverde voor het project en of deze overeen kwamen met de andere ideeën. Omdat dit het geval was, is er een nieuwe versie gemaakt van het document waar ook zijn feedback in verwerkt is.
Het afnemen van de interviews is (mede door de goede voorbereiding) zonder problemen verlopen. Het uitwerken van de feedback was ook geen probleem. De begeleider van Deloitte heeft hier ook een belangrijke rol in gespeeld omdat we samen hebben bepaald of het in dit project haalbaar was om de wensen en eisen uit te voeren. Ik ben tevreden over deze fase omdat er een lijst met duidelijke "must haves" en "nice to haves" is opgesteld. Met deze lijst kan het ontwerpen van het MKB pentest beginnen en weet ik waar de prioriteiten liggen (bij de must haves).

Fase 4 – ontwikkeling pentest
Het ontwikkelproces van de MKB pentest is goed verlopen. Ik kon de meeste onderdelen zelfstandig uitvoeren en wanneer ik hulp nodig had werd ik goed geholpen door collega's. De enige problemen waar ik deze fase tegenaan liep waren planningsproblemen, welke hieronder worden beschreven.

Het idee was om in week 3 een presentatie te houden over het MKB pentestontwerp aan belanghebbenden zoals de opdrachtgever, begeleider, aantal managers en een aantal

[11] Cross-site scripting (XSS) is de naam van een fout in de beveiliging van een webapplicatie. Het probleem wordt veroorzaakt doordat de invoer die de webapplicatie ontvangt (zoals cookie, url, request parameters) niet afdoende wordt gevalideerd en hierdoor in de uitvoer terecht komt naar de eindgebruiker. Via deze bug in de website kan er kwaadaardige code (JavaScript, VBScript, ActiveX, HTML, Flash, etc) geïnjecteerd worden

pentesters. Tijdens deze presentatie wilde ik duidelijk maken hoe de MKB pentest uitgevoerd zal worden en uit welke onderdelen de pentest zal bestaan. Aan het einde van de presentatie was er ruimte voor feedback en discussie over het ontwerp. Deze feedback is gebruikt voor de ontwikkeling van de MKB pentest.
Ondanks het tijdig aanvragen en inplannen (in week 52) van de presentatie was het niet haalbaar voor iedereen om tijd vrij te maken in de agenda en is daarom de presentatie verplaatst naar week 5.
Er is besproken met de begeleider van Deloitte of er al begonnen kon worden aan het volgende onderdeel van fase 4 (de ontwikkeling) voordat ik de presentatie gegeven had. Om de kwaliteit, doelstelling en te tevredenheid van de opdrachtgever te waarborgen werd de feedback (op het pentest ontwerp) van de begeleider gebruikt. De feedback die de mensen tijdens de presentatie geven zal alleen worden verwerkt als dit geen gevolgen heeft voor de totale planning van het project.
De presentatie verliep goed en er ontstond een goede discussie over het ontwerp. Alle deelnemers van de presentatie konden zich vinden in het ontwerp, alleen zouden ze graag nog enkele aanpassingen zien. Zo is bijvoorbeeld besloten om in plaats van twee MKB pentestproducten drie producten uit te brengen. Dit is besloten aan de hand van de verwachte vraag naar de MKB pentest.

Nu iedereen het ontwerp van de MKB pentest had goedgekeurd kon worden begonnen aan de ontwikkeling. De ontwikkeling van de MKB pentest gebeurt aan de hand van het ontwerp. Omdat het ontwerp goed is uitgewerkt was het voor mij erg duidelijk wat precies gemaakt moest worden en wat de wensen en eisen waren. Het ontwikkelen van de pentest verliep zonder grote problemen.
Alleen liep ik wel tegen een ander probleem op en dat was de planning. Doordat de ontwerpfase uitgelopen was en extra werkzaamheden uitgevoerd moesten worden (na feedback van de MKB pentest ontwerp presentatie) liep ik uit op de planning. Deze "exception" (onderdeel uit prince 2 methodiek) heb ik besproken met mijn begeleider. Ik heb een aangepaste planning gemaakt waarbij het project een week langer duurt en de vakantie in februari komt te vervallen. Voordat het project begon was al rekening gehouden met de mogelijkheid dat het project uit kon lopen, hiervoor waren ook maatregelen uitgewerkt om deze risico's op te lossen (zie document "Plan van Aanpak").

Figuur 15 - Nieuwe planning na exception

Fase 5
Deze fase is de afsluitende fase van het project. Er was voor deze fase weinig tijd overgebleven. Dit kwam door het uitlopen van fase 4 en door de werkzaamheden die aan dit afstudeerverslag moesten plaatsvinden. Door het tijdgebrek moest er hard gewerkt worden om de doelstelling uit het plan van aanpak te behalen. De doelstelling was het evalueren van de test die gedaan is met het concept MKB pentest (uit fase 4) en een aanbeveling voor Deloitte over de vervolgstappen van de MKB pentest.
Het was jammer dat de pentest niet getest kon worden bij een MKB klant in verband met de beperkte tijd die beschikbaar was. Om ervoor te zorgen dat de MKB pentest toch getest kon worden is besloten (in overleg met de pentesters en de begeleider) om de MKB pentest intern te testen. Voor de aanpak van de test zie hoofdstuk 8.2.
De tests zijn met succes afgerond en ik kan tevreden zijn over het resultaat, want het resultaat is dat het MKB pentestproces werkt en de belangrijkste kwetsbaarheden gevonden kunnen worden. Het is nog wel de bedoeling dat ik samen met een pentester de MKB pentest ga testen bij een klant van Deloitte.

Het tweede gedeelte van fase 5 was het adviseren van de vervolgstappen van de MKB pentest aan Deloitte. In eerste instantie heb ik gecontroleerd welke wensen en eisen uit de requirements analyse (fase 3) behaald zijn. Van de eisen (must haves) is het niet gelukt om het portaal te realiseren. Alle andere punten zijn wel voltooid. De werkzaamheden om het portaal te realiseren zijn wel uitgevoerd, maar de ontwikkeling van het portaal heb ik niet in de hand. De ontwikkeling van het portaal wordt namelijk gedaan door een andere afdeling van Deloitte. De vervolgstappen die nog uitgevoerd dienen te worden voor het portaal heb ik beschreven en geadviseerd aan Deloitte. Zie hoofdstuk 8.3). Ook heb ik een begin kunnen maken aan de wensen (nice to haves). Zo heeft het (MKB) pentestrapportage een nieuw design en indeling gekregen (zie bijlage MKB pentest rapport sjabloon). Deze nieuwe rapportage kan ook al door mijn ontwikkelde rapportage generator (zie hoofdstuk 7.2) gemaakt worden.

Dankzij deze werkzaamheden ben ik van mening dat de beoogde doelstellingen behaald zijn ondanks de beperkte tijd die beschikbaar was. Ook kan Deloitte verder met het op de markt brengen van de MKB pentest aan de hand van de vervolgstappen (zie hoofdstuk 8.3).

9.3 Competentie evaluatie

De competenties die tijdens de afstudeerstage behaald dienen te worden staan beschreven in het afstudeerplan welke, voor de afstudeerstage begon, ingeleverd is bij De Haagse Hogeschool. In dit hoofdstuk worden de competenties geëvalueerd en staat beschreven of deze behaald zijn.

ISM-VC-9

Op een gestructureerde wijze (en methodisch onderbouwde methode) een analyse kan uitvoeren om de afhankelijkheden en kwetsbaarheden van de informatievoorziening in een organisatie vast te kunnen stellen en op basis van het resultaat een advies kan opstellen over de te nemen maatregelen.

Ik heb deze competentie behaald door het uitvoeren van een pentest op een informatiesysteem. Het doel van de pentest is het in kaart brengen van kwetsbaarheden van het informatiesysteem. De pentest is op een gestructureerde wijze uitgevoerd met behulp van een (door Deloitte goedgekeurd) werkprogramma. De klant wordt door middel van een rapportage op de hoogte gebracht van de kwetsbaarheden, ook is de klant geadviseerd hoe deze kwetsbaarheden opgelost kunnen worden. Ik heb zelf niet aan de rapportage gewerkt omdat de klantenrelatie op het spel kan komen te staan als de rapportage door een stagiair is opgebouwd. Wel heb ik samen met een pentester de resultaten van de pentest geanalyseerd.

ISM-VC-10

Zowel technische als organisatorische maatregelen kan implementeren waarmee de betrouwbaarheid van informatie, binnen zekere grenzen, kan worden gegarandeerd, alsmede het beheren en exploiteren van de processen en de systemen die hiervoor nodig zijn.

De betrouwbaarheid van informatie kan alleen worden gegarandeerd als het systeem waarop de informatie is opgeslagen ook betrouwbaar is. Door middel van een pentest kan een deel van deze betrouwbaarheid getest worden. Wanneer bijvoorbeeld een informatiesysteem kwetsbaarheden bevat kan de beschikbaarheid, integriteit en vertrouwelijkheid van de opgeslagen informatie in gevaar komen. Aan de hand van de resultaten van de pentest kunnen maatregelen worden getroffen om de betrouwbaarheid van informatie te waarborgen. Doordat ik de MKB pentest heb ontwikkeld en geïmplementeerd heb, heb ik deze competentie kunnen behalen.

ISM-VC-14

Controles kan opstellen en uitvoeren waarmee de kwaliteit van de informatiebeveiliging kan worden vastgesteld en op basis van de uitkomst een advies over verbetering van de kwaliteit van de informatiebeveiliging kunnen opstellen.

Door middel van een pentest kan een informatiesysteem, infrastructuur of applicatie getest worden op de kwaliteit van de informatiebeveiliging. Deze competentie heb ik kunnen behalen door het ontwikkelen van een pentest voor het MKB. Onder andere heb ik een werkprogramma opgesteld die een web-applicatie kan testen op kwetsbaarheden. Dit werkprogramma is ook uitgevoerd en getest op de werking. Op basis van de resultaten van de pentest kan een advies worden gegeven aan de klant. In dit advies staat ook beschreven hoe de klant de kwaliteit van de informatiebeveiliging kan verbeteren door het oplossen van de gevonden kwetsbaarheden.

ISM-VC-15
Een stelsel van preventieve maatregelen kan ontwerpen, ontwikkelen en inrichten om in geval van calamiteiten de betrouwbaarheid van de informatievoorziening zeker te stellen.
Voor de MKB pentest is een database ontwikkeld waarin standaardbevindingen in beschreven staan. Deze standaardbevindingen zijn gebaseerd op de meest voorkomende kwetsbaarheden tijdens een pentest. Met behulp van deze standaardbevindingen kan er snel een rapport worden gegenereerd. Een standaardbevinding bestaat uit een beschrijving van de kwetsbaarheid, wat de kans is dat de kwetsbaarheid misbruikt wordt, wat voor impact de kwetsbaarheid op het systeem heeft wanneer het misbruikt wordt en hoe de kwetsbaarheid opgelost kan worden. Voor de oplossingen worden ook preventiemaatregelen geadviseerd om de kwetsbaarheid in de toekomst te voorkomen. Hierbij kan bijvoorbeeld worden gedacht aan het inrichten van een password management proces.

ISM-AC-2
Binnen een projectteam, ongeacht de diversiteit ervan (internationaal, multicultureel, virtueel), kan samenwerken, de daarvoor geëigende vaardigheden inzet en het vereiste gedrag vertoont om de gestelde projectdoelstellingen te behalen.
Het projectteam dat samengesteld was voor het project bestond uit een diversiteit van Deloitte medewerkers. Zo kwam er bijvoorbeeld één uit Tsjechië en een ander uit Engeland. Het gevolg hiervan was dat tijdens een aantal overleggen de voertaal Engels was. Ook moest de voorbereiding van de gesprekken aangepast worden, omdat documentatie in het Engels uitgewerkt diende te worden.

9.4 Ter afsluiting
Met dit laatste stukje tekst komt mijn afstudeerverslag tot een einde. Met behulp van dit afstudeerverslag beëindig ik ook mijn afstudeerstage bij Deloitte. Het was een afstudeerstage waarin de tijd vloog voor mijn gevoel. Ik heb een hoop werk weten te verzetten in de afgelopen periode en dat is terug te zien aan het resultaat. Namelijk een werkende MKB pentest die aan de eisen van het afstudeerplan en Deloitte voldoet. De opdrachtgever, begeleider en pentesters hebben aangegeven tevreden te zijn over de samenwerking en resultaten.
Er vanuit gaande dat De Haagse Hogeschool mijn afstudeerstage met een voldoende beoordeelt rond ik ook de opleiding Information Security Management af. Het enige wat ik niet afrond zijn mijn werkzaamheden bij Deloitte, want Deloitte heeft me een baan aangeboden als consultant Risk Services welke ik met grote dankbaarheid aanneem.

Nu kan ik hard aan de slag gaan om de (digitale) wereld een stukje veiliger te maken!

Afbeeldinglijst

Literatuurlijst

Dit is een lijst van gebruikte bronnen die gebruikt zijn tijdens dit project

De gebruikte bronnen staan als volgt genoteerd:
[Bron nummer] Achternaam auteur, voorletter(s) of Titel van het document / de website. *Organisatie*. [Bron soort] Publicatiejaar of update. [Geopend op.] URL van website.

Fase 1

1. SME Definition. *European Commission.* [Online] 1 Januari 2005. [Citaat van: 15 November 2011.] http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm.
2. Nederlands mkb nog steeds slecht beveiligd. *Webwereld.* [Online] 11 mei 2009. [Citaat van: 18 November 2011.] http://webwereld.nl/nieuws/58056/nederlands-mkb-nog-steeds-slecht-beveiligd.html.
3. Nederlands MKB is slecht beveiligd. *Computable.* [Online] 13 Februari 2008. [Citaat van: 18 November 2011.] http://www.computable.nl/artikel/ict_topics/security/2346125/1276896/nederlands-mkb-is-slecht-beveiligd.html.

Fase 3

1. MoSCoW Method. *Wikipedia.* [Online] 17 Januari 2012. [Citaat van: 14 Februari 2012.] http://en.wikipedia.org/wiki/MoSCoW_Method

Fase 4

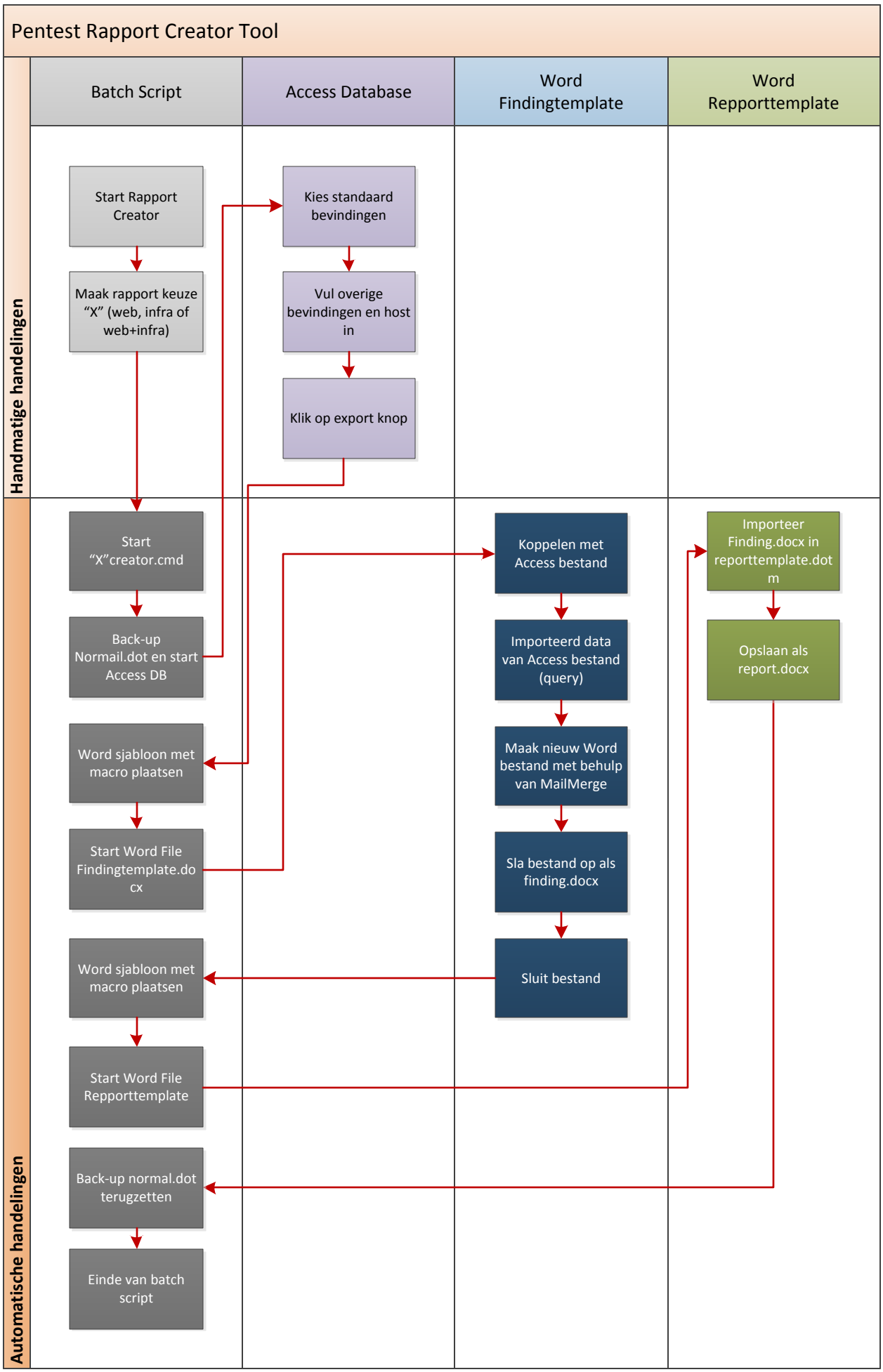
1. **Wikipedia.** Penetration test. *Wikipedia.* [Online] 15 December 2011. [Citaat van: 16 December 2011.] http://en.wikipedia.org/wiki/Penetration_test.
2. **Jonathan Gershater, Puneet Mehta.** What is Penetration Testing? *SecPoint.* [Online] [Citaat van: 16 December 2011.] http://www.secpoint.com/what-is-penetration-testing.html.
3. Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010. *GovCERT.* [Online] GovCERT, November 2010. http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/trendrapporten/trendrapport-2010.html.
4. **ISIS.** ISIS - MKB ICT Onderzoek 2009. *consultancy.nl.* [Online] ISIS, September 2009. http://www.consultancy.nl/rapporten/deloitte/mkb-ict-onderzoek-2009.
5. **Young, Ernst &.** ICT Barometer over. *ICT barometer.* [Online] Ernst & Young, 2011. http://www.ict-barometer.nl/_files-cms/File/Rapport%20onderzoeksresultaten%20ICT%20Barometer%20over%20cybercrime%202011.pdf.
6. **Symantec.** Symantec 2010 SMB Information Protection Survey. *Symantec.* [Online] Symantec, November 2010. http://www.symantec.com/content/en/us/about/media/pdfs/SMB_ProtectionSurvey_2010.pdf.
7. **Metro.** Kleine bedrijven dupe cybercrime. *Metro.* [Online] Metro, 16 November 2010. http://www.metronieuws.nl/nieuws/kleine-bedrijven-dupe-cybercrime/SrZjkp!OqunuyNweMAbo/.

8. Informatiebeveiliging. *Wikipedia.* [Online] 30 December 2011. http://nl.wikipedia.org/wiki/Informatiebeveiliging.
9. **Infosecurity.** Mkb stuwt wereldwijde vraag naar security. *Infosecurity.* [Online] 22 December 2011. http://www.infosecurity.net/Nieuws/77952/Mkb-stuwt-wereldwijde-vraag-naar-security.
10. **EMC.** EMC GEEFT DE 10 IT-TRENDS AAN VOOR 2012. *Binnenlands Bestuur.* [Online] 3 Januari 2012. http://www.binnenlandsbestuur.nl/digitaal-besturen/partners/emc/emc-geeft-de-10-it-trends-aan-voor-2012.3427400.lynkx.
11. **Gartner.** Gartner's Top Predictions for IT Organizations and Users, 2012 and Beyond: Control Slips Away. *Gartner.* [Online] Gartner, 2012. http://www.gartner.com/technology/innovation/it-predictions-2012.jsp?prm=TW_CHINNV.
12. **Group, SMB.** 2012 Top 10 SMB Technology Market Predictions. *SMB Group.* [Online] 2012.
13. **Bueters, Philip.** De IT trends van 2012. *Management Team.* [Online] 30 December 2011. http://www.mt.nl/95/54709/ict/de-it-trends-van-2012.html.
14. **Week, Information.** 4 Tech Trends For SMBs In 2012. *Information Week.* [Online] 14 December 2012. http://www.informationweek.com/news/smb/ebusiness/232300521.
15. **Young, Ernst &.** ICT Barometer over . *ict-barometer.nl.* [Online] Ernst & Young, Februari 2011. http://www.ict-barometer.nl/_files-cms/File/ICT%20Barometer%20-%20Business%20Process%20Outsourcing.pdf.
16. **Security.nl.** 4.000 gehackte WordPress blogs vergiftigen Google. *Security.nl.* [Online] Augustus 2011. http://www.security.nl/artikel/38043/4.000_gehackte_WordPress_blogs_vergiftigen_Google.html.
17. **Stansberry, Glen.** Top 10 Most Usable Content Management Systems. *Glen Stansberry.* [Online] Net Tuts, Augustus 2009. http://net.tutsplus.com/articles/web-roundups/top-10-most-usable-content-management-systems/.
18. **Lazaris, Bryan.** 10 best Ecommerce dominant shopping cart applications. *Webgranth.* [Online] September 2011. http://www.webgranth.com/10-best-ecommerce-dominant-shopping-cart-applications.
19. **Mosher, Barb.** SharePoint Portal Alternatives - A Credible List. *cmswire.* [Online] cmswire, Maart 2010. http://www.cmswire.com/cms/enterprise-cms/sharepoint-portal-alternatives-a-credible-list-005080.php.
20. Trendstudie MKB en . *Ondernemerschap.* [Online] ondernemerschap, Maart 2011. http://www.ondernemerschap.nl/sys/cftags/assetnow/design/widgets/site/ctm_getFile.cfm?file=A201103.pdf&perId=596.

Bijlagen

De bijlagen bestaan uit een aantal losse documenten die tegelijk met dit document zijn opgeleverd. In onderstaande opsomming staat een lijst van de bijgevoegde documenten. Tevens wordt elk document in het kort beschreven. Alle bijgevoegde documenten zijn door mij gemaakt.

- **Plan van aanpak (fase 1)**
  In dit document staat beschreven hoe het project aangepakt is. Onder andere staan hier de aanleiding, doelstelling en scope van het project beschreven.
- **Requirements analyse (Fase 3)**
  In dit document zijn de wensen en eisen voor de MKB pentest in kaart gebracht. Er is gekeken naar de wensen en eisen van de opdrachtgever, manager en de pentesters.
- **Design pentest (Fase 4)**
  In dit document staat beschreven hoe de pentest ontworpen wordt. Onder andere staat hier de methode, tools en processtappen beschreven.
- **Presentatie ontwerp MKB pentest (Fase 4)**
  Dit is de originele presentatie die tijdens fase 4 gegeven is aan het projectteam ter goedkeuring van het MKB pentest ontwerp. De verkregen feedback is niet verwerkt in deze presentatie.
- **Diagram Pentest Rapport Creator Tool (Fase 4)**
  In dit diagram zijn de processtappen weergegeven van de (door mij ontwikkelde) Pentest Rapport Creator tool.
- **Concept WEB werkprogramma MKB pentest (Fase 4)**
  Dit document is een concept van het WEB MKB pentest werkprogramma.
- **Tekst voor ctrl portal (Fase 4)**
  Dit document is een demo pagina voor het ctrl portal waar klanten de MKB pentest kunnen aanvragen
- **MKB pentest rapport sjabloon (Fase 4)**
  Dit is het sjabloon dat gegenereerd wordt door de "MKB pentest rapport creator" tool.
- **School documenten**
  De schooldocumenten bestaat uit een set documenten die vereist zijn door De Haagse Hogeschool. Namelijk het afstudeerplan, voortgangsverslag en het tussentijdsassessment.


Pentest Rapport Creator Tool
Batch Script
Access Database
Word Findingtemplate
Word Repporttemplate
Handmatige handelingen
Automatische handelingen
Start Rapport Creator
Maak rapport keuze "X" (web, infra of web+infra)
Kies standaard bevindingen
Vul overige bevindingen en host in
Klik op export knop
Start "X"creator.cmd
Back-up Normail.dot en start Access DB
Word sjabloon met macro plaatsen
Start Word File Findingtemplate.docx
Koppelen met Access bestand
Importeerd data van Access bestand (query)
Maak nieuw Word bestand met behulp van MailMerge
Sla bestand op als finding.docx
Sluit bestand
Word sjabloon met macro plaatsen
Start Word File Repporttemplate
Importeer Finding.docx in reporttemplate.dotm
Opslaan als report.docx
Back-up normal.dot terugzetten
Einde van batch script

Afstudeerplan

Informatie afstudeerder en gastbedrijf

Afstudeerblok: 2011-2.2
Startdatum uitvoering afstudeeropdracht: 7 november 201
Inleverdatum afstudeerdossier volgens jaarrooster: 19 maart 2012

Studentnummer: 08022488
Achternaam: dhr Alsemgeest
Voorletters: W.M.
Roepnaam: Werner
Adres: Oudlaan 109
Postcode: 2672AP
Woonplaats: Naaldwijk
Telefoonnummer:0618559359
Mobiel nummer: 0618559359
Privé emailadres: Werneralsemgeest@gmail.com

Opleiding: Information Security Management
Locatie: Zoetermeer
Variant: voltijd

Naam studieloopbaanbegeleider: Leo van Koppen
Naam begeleidend examinator: Ellen Wesselingh
Naam tweede examinator: Arianne Luik-Knoester

Naam bedrijf: Deloitte
Afdeling bedrijf: Enterprise Risk Services
Bezoekadres bedrijf: Laan van Kronenburg 2
Postcode bezoekadres: 1183 AS
Postbusnummer:
Postcode postbusnummer:
Plaats: Amstelveen
Telefoon bedrijf: +31 (0)88 2882 888
Fax bedrijf: +31 (0)882889709
Internetsite bedrijf: www.deloitte.com

Achternaam opdrachtgever: dhr. Van Zwam
Voorletters opdrachtgever*:* M.
Titulatuur opdrachtgever: drs.
Functie opdrachtgever: Partner
Doorkiesnummer opdrachtgever: +31 088 288 08 90
Email opdrachtgever: MvanZwam@deloitte.nl

Achternaam bedrijfsmentor: dhr. Tom Schuurmans
Voorletters bedrijfsmentor: T.
Titulatuur bedrijfsmentor:
Functie bedrijfsmentor: Consultant
Doorkiesnummer bedrijfsmentor: +31 (0)88 2881 591
Email bedrijfsmentor: tschuurmans@deloitte.nl

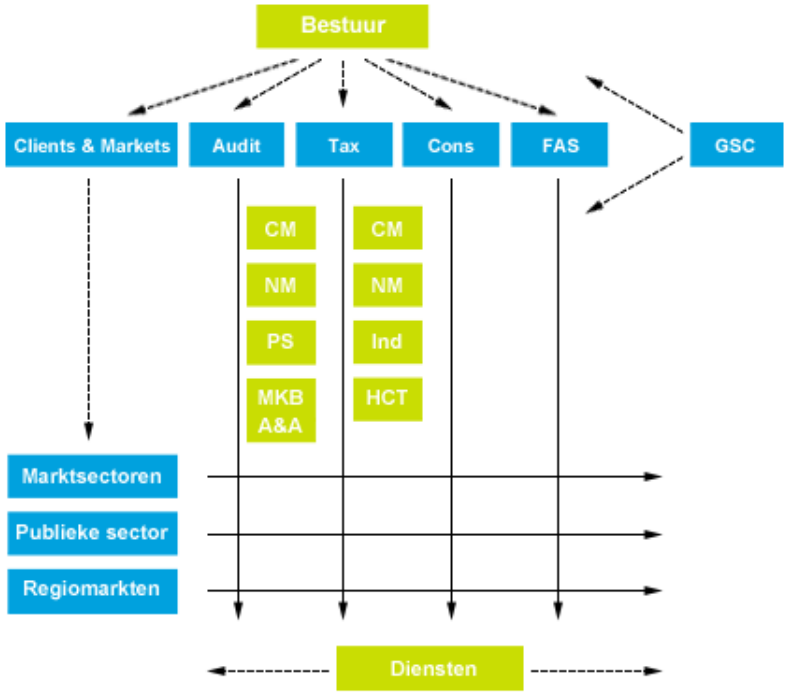
Doorkiesnummer afstudeerder*:* +31 (0)88 2888 882
Functie afstudeerder (deeltijd/duaal): Voltijd

Titel afstudeeropdracht:
Opzetten pentesting product gericht op het MKB bij Deloitte

Opdrachtomschrijving

1. **Bedrijf**
   Deloitte Nederland is een zelfstandige memberfirm van de wereldwijde organisatie Deloitte Touche Tohmatsu. De oorsprong van deze organisatie ligt in Londen waar in 1845 William Welch Deloitte zijn eigen accountantskantoor opende. Na vele overnames en fusies telt Deloitte Touche Tohmatsu (DTTL) inmiddels 150.000 medewerkers in 150 verschillende landen. DTTL heeft een coördinerende functie en is niet actief betrokken bij de dienstverlening. In totaal realiseerde Deloitte in het boekjaar 2010/2011 een omzet van 632 miljoen euro. Daarmee is Deloitte een van de grootste accountant -en adviesbureaus ter wereld.
   Deloitte Nederland gaat uit van een multidisciplinaire aanpak. Vanuit de diensten Accountancy, Belastingen, Consulting en Financial Advisory Services bedient Deloitte de markt.
   De afstudeerstage zal worden uitgevoerd op de afdeling Enterprise Risk Services op het kantoor in Amstelveen.

   In het onderstaande schema is de organisatiestructuur van Deloitte weergegeven.



Bestuur: Raad van Bestuur
MKB A&A: MKB Accountancy & Advies
FAS: Financial Advisory Services
Cons: Consulting
GSC: Group Support Center
CM: Corporate markt
NM: Nationale markt
PS: Publieke Sector
Ind: Indirect tax
HCT: Human capital tax

2. Probleemstelling

Deloitte richt zich voornamelijk op grote organisaties met een breed pakket aan diensten. Deloitte Risk Services heeft gezien dat er meer ruimte in de markt van het MKB is voor pentesting. Deze ruimte willen ze graag benutten, maar op dit moment kunnen ze hier nog geen passende dienst voor leveren. Het idee is ontstaan om een product te ontwikkelen (deels geautomatiseerd) waarmee in een korte periode een pentest kan worden uitgevoerd bij een MKB organisatie. Dit product moet betaalbaar en interessant worden voor de klant. Tevens moet de resultaten van de pentest een goed beeld kunnen geven van het huidige niveau van informatiebeveiliging binnen een MKB-organisatie. Voor de pentest bij MKB-klanten moet er een standaard worden ontwikkeld zodat deze dienst makkelijk, goedkoop en snel kan worden uitgevoerd. Wel moet er ruimte gehouden worden in de standaard voor een stuk maatwerk om de pentest bij de klant aan te laten sluiten. De pentest van Deloitte moet zich onderscheiden van andere pentests door een klantgerichte en begrijpbare rapportage.

3. Doelstelling van de afstudeeropdracht

Ontwikkelen van een pentest “product” voor het MKB. Door middel van dit product krijgt een MKB organisatie inzicht in het huidige niveau van informatiebeveiliging en de mogelijke kwetsbaarheden. Dit product moet betaalbaar zijn en in maximaal vier dagen uitgevoerd kunnen worden. De resultaat van de pentest moet een klantgerichte en begrijpbare rapportage worden. De nadruk van het project zal liggen op de product ontwikkeling en minder op de verkoop/marketing aspecten.

4. Resultaat

Wanneer het project naar behoren wordt uitgevoerd dan is het resultaat een pentestproduct voor MKB klanten van Deloitte. Met dit product kan de klant inzicht krijgen in de huidige stand van informatiebeveiliging binnen de organisatie en de mogelijke kwetsbaarheden. Ook krijgt de klant advies hoe er een hoger niveau van informatiebeveiliging kan worden behaald. De pentest zal waarschijnlijk bestaan uit verschillende modules. Een website wordt namelijk anders op kwetsbaarheden getest dan een netwerk of een server, ook kan een pentest intern of extern worden uitgevoerd.

Uit te voeren werkzaamheden, inclusief een globale fasering, mijlpalen en bijbehorende activiteiten
In het begin van het project zal er een plan van aanpak worden opgesteld. In dit document staat onder andere de doelstelling, probleemstelling en de aanpak van het project beschreven. Het plan zal worden gemaakt in de opstartfase van het project (fase 1). De informatie die nodig is voor fase 1 zal worden vergaard door middel van gesprekken/interviews met de opdrachtgever en collega's binnen Deloitte.

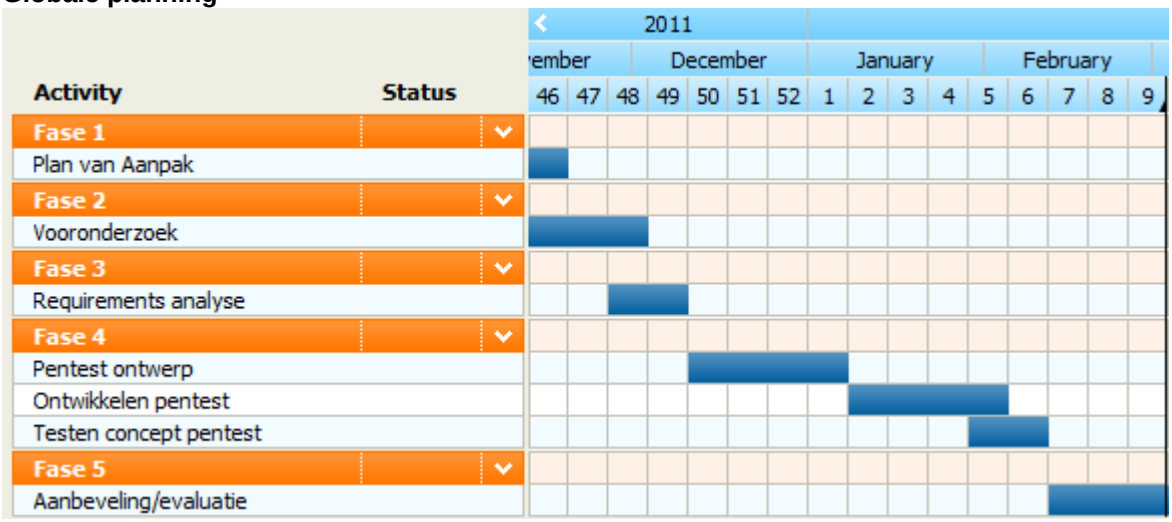
Vervolgens zal er een vooronderzoek worden uitgevoerd (fase 2). In dit vooronderzoek zal er gekeken worden hoe Deloitte pentests uitvoert, uit welke onderdelen een pentest bestaat, hoeveel tijd een pentest in beslag neemt en of er standaarden bestaan die voor de pentest gebruikt kunnen worden. Dit vooronderzoek zal worden uitgevoerd door het meelopen met een aantal pentesters van Deloitte.

In fase drie worden de "requirements" opgesteld. De eisen en wensen zullen worden verzameld van collega's binnen de securityafdeling en van MKB klanten van Deloitte. De wensen en eisen zullen in kaart worden gebracht door middel van interviews. Er zijn al een aantal personen aangewezen binnen Deloitte die me met de juiste mensen in contact kunnen brengen.

Wanneer alle eisen en wensen in kaart zijn gebracht en er genoeg informatie is verzameld over de werking en onderdelen van een pentest zal er begonnen worden met de ontwikkeling (fase 4). Het volledige product zal ontwikkeld worden inclusief het voortraject. De ontwikkeling bestaat uit drie delen het ontwerp, de uitwerking en een test. Voordat er aan de uitwerking zal worden begonnen zal het ontwerp moeten worden goedgekeurd door de opdrachtgever.
Wanneer er een concept pentest is ontwikkeld zal deze worden getest bij een MKB klant van Deloitte. Of dit mogelijk is hangt af van de "opportunity's" op dat moment, maar de verwachting is dat dit mogelijk is.

Tot slot zal er een advies worden gegeven aan Deloitte. In dit advies zal onder andere de vervolgstappen worden geadviseerd en een advies over het marktsegment waar dit product zich op moet gaan richten (fase 5).

Globale planning



5. Op te leveren (tussen)producten
De volgende producten zullen worden opgeleverd aan Deloitte:

- Plan van aanpak
- Requirements analyse
- Ontwerp pentest
- Concept Pentest
- Advies

6. Te demonstreren competenties en wijze waarop

Tijdens de afstudeer stage zal er aan de volgende competenties gewerkt worden.

Competentie	Hoe te behalen
ISM-VC-9 op een gestructureerde wijze (en methodisch onderbouwde methode) een analyse kan uitvoeren om de afhankelijkheden en kwetsbaarheden van de informatievoorziening in een organisatie vast te kunnen stellen en op basis van het resultaat een advies kan opstellen over de te nemen maatregelen	Dit project draait om pentesting. Met deze pentests worden de afhankelijkheden en kwetsbaarheden van de informatievoorzieningen in een organisatie vastgesteld. Deze pentests worden met behulp van een onderbouwde methode uitgevoerd. Nadat een pentest is uitgevoerd zal er een klantgericht en begrijpelijk advies worden gegeven aan de klant.
ISM-VC-10 zowel technische als organisatorische maatregelen kan implementeren waarmee de betrouwbaarheid van informatie, binnen zekere grenzen, kan worden gegarandeerd, alsmede het beheren en exploiteren van de processen en de systemen die hiervoor nodig zijn	Nadat er een pentest is uitgevoerd zijn de kwetsbaarheden in kaart gebracht. De volgende logische stap is het oplossen van de gevonden kwetsbaarheden. Hiervoor zullen er technische en organisatorische maatregelen moeten worden geïmplementeerd.
ISM-VC-14 controles kan opstellen en uitvoeren waarmee de kwaliteit van de informatiebeveiliging kan worden vastgesteld en op basis van de uitkomst een advies over verbetering van de kwaliteit van de informatiebeveiliging kunnen opstellen	De pentest die ontwikkeld gaat worden tijdens het project is voor klanten een controlemechanisme om de kwaliteit en effectiviteit van de informatiebeveiliging te controleren. Het resultaat van de pentest is een overzicht van de gevonden kwetsbaarheden en een advies over hoe de informatiebeveiliging verbeterd kan worden.
ISM-VC-15 een stelsel van preventieve maatregelen kan ontwerpen, ontwikkelen en inrichten om in geval van calamiteiten de betrouwbaarheid van de informatievoorziening zeker te stellen	Het uitvoeren van een pentest is een preventiemaatregel, omdat de klant inzicht krijgt in de kwetsbaarheden voordat deze misbruikt kunnen worden. De klant kan deze kwetsbaarheden dichten voordat bijvoorbeeld de nieuwe website online wordt gezet. Door het controleren op kwetsbaarheden kan de betrouwbaarheid van informatievoorzieningen verbeterd worden.
ISM-AC-2 binnen een projectteam, ongeacht de diversiteit ervan (internationaal, multicultureel, virtueel), kan samenwerken, de daarvoor geëigende vaardigheden inzet en het vereiste gedrag vertoont om de gestelde projectdoelstellingen te behalen	Tijdens dit project zal er veel worden samengewerkt met een diversiteit van personen. De opdrachtgever komt bijvoorbeeld uit Tsjechië en spreekt geen Nederlands. Dit betekend een grote aanpassing in de communicatie omdat de voertaal Engels wordt. Ook zal er worden gesproken met collega's van andere afdelingen en met klanten van Deloitte.

Plan van Aanpak

Ontwikkeling MKB pentestproduct

Naam: Werner Alsemgeest
Studentnummer: 08022488
Instituut: De Haagse Hogeschool
Opleiding: Information Security Management
Afstudeerstage bedrijf: Deloitte
Begeleider Hogeschool: Ellen Wesselingh
Begeleider Deloitte: Tom Schuurmans

Datum: 20 januari 2012
Versie: 0.2

Versiehistorie

Versienummer	Versiedatum	Controle door:	Wijzigingen
0.1 (Concept)	10-11-2011	Werner Alsemgeest	Opzet concept
0.2	28-11-2011	Werner Alsemgeest	Aanpassing na feedback Tom Schuurmans

Distributielijst

Versienummer	Datum	Naam	Organisatie
0.1	18-11-2011	Tom Schuurmans	Deloitte
0.1	18-11-2011	Nick Kirtley	Deloitte
0.1	18-11-2011	Vojtech Brtnik	Deloitte

Inhoud

1. Inleiding en achtergrond project

Dit document bevat het Plan van Aanpak voor het project "ontwikkeling MKB pentestproduct". Onder de term MKB vallen kleinen en middelgrote organisaties die gevestigd zijn in Nederland. Dit document heeft als doel de lezer een compleet beeld te geven van het project dat uitgevoerd gaat worden binnen Deloitte. Het project zal worden uitgevoerd door stagiair Werner Alsemgeest in opdracht van Deloitte Nederland afdeling Risk Services, team Security en Privacy services te Amstelveen. Het project zal door de stagiaire uitgevoerd worden in het kader van een afstudeerstage.

De aanleiding tot het project is ontstaan vanuit een observatie van Deloitte Risk Services, waarbij ruimte op de markt is gezien van pentesting voor MKB-organisaties. Het idee is om een product te ontwikkelen (deels geautomatiseerd) waarmee in een korte periode een pentest kan worden uitgevoerd bij een MKB-organisatie. Dit product moet betaalbaar en waardevol worden voor MKB-organisaties. Tevens moet de resultaten van de pentest een goed beeld kunnen geven van het huidige niveau van informatiebeveiliging van een informatiesysteem.

In hoofdstuk twee staat de project definitie beschreven. In het hoofdstuk daarna wordt de Business Case van het project beschreven. De organisatiestructuur van de projectgroep is te vinden in hoofdstuk vier. In hoofdstuk vijf wordt de planning, randvoorwaarden en productdecompositie beschreven. De beheersingsmechanismen voor het project worden beschreven in hoofdstuk zes. Tot slot worden in het laatste hoofdstuk de projectrisico's beschreven. Als bijlage is een bronnenlijst toegevoegd, hierin staan de gebruikte bronnen van dit document.

2. Projectdefinitie

2.1 Doelstellingen

De doelstelling van dit project is het ontwikkelen van een pentest "product" voor het MKB. Door middel van dit product krijgt een MKB-organisatie inzicht in de mogelijke kwetsbaarheden van een informatiesysteem of infrastructuur. Dit product moet betaalbaar zijn voor een MKB-organisatie en in maximaal vier dagen uitgevoerd kunnen worden. Het resultaat van de pentest moet een klantgericht en begrijpelijke rapportage worden. De nadruk van het project zal liggen op de pentestontwikkeling en minder op de verkoop/marketing aspecten van de pentest.

2.2 Aanpak en faseringen

Het project wordt aangepakt met behulp van een op Prince 2 gebaseerde aanpak. Voor het project zijn de volgende fases gedefinieerd:

Fase	Beschrijving
Fase 1	Opstart project
Fase 2	Vooronderzoek (inzicht krijgen in het pentestproces)
Fase 3	Requirements analyse
Fase 4	Ontwikkeling en testen pentest
Fase 5	Aanbeveling en evaluatie

Tabel 1: fases

2.3 Resultaten

Aan het eind van het project zullen de volgende producten opgeleverd zijn.

- Plan van Aanpak
- Requirements analyse
- Pentestproduct ontwerp
- Concept pentestproduct
- Evaluatie van de uitgevoerde conceptpentest
- Advies van vervolgstappen

2.4 Scope

De scope van het onderzoek betreft het ontwikkelen van een pentest voor middelgrote en grote MKB-organisaties binnen Nederland. Onder middelgrote en grote MKB-organisaties vallen organisaties van 50 tot 250 werknemers (1). Ook worden gemeenten en zorginstellingen meegenomen in de scope van het project. De pentest zal zich richten op organisaties die met vertrouwelijke gegevens werken.

Het project zal zich voornamelijk focussen op de ontwikkeling van de pentestproduct en minder op marketing aspecten zoals het op de markt brengen van het product.

2.5 Randvoorwaarden en beperkingen

Om het project succesvol af te ronden zijn enkele randvoorwaarden en beperkingen opgesteld:

- Tijdige besluitvorming (door opdrachtgevers en belanghebbenden).
- Ruimte en middelen (laptop, telefoon) dienen beschikbaar worden gesteld door Deloitte om aan het project te kunnen werken.
- Mensen die bij het project betrokken zijn dienen tijd vrij te maken voor bijvoorbeeld overleg, interviews, feedback etc.
- Informatie en kennis over pentesting die binnen Deloitte aanwezig is dient beschikbaar te worden gesteld aan de projectuitvoerder.
- Begeleiding vanuit De Haagse Hogeschool

2.6 Relaties met andere projecten

Er zijn zo ver bekend geen relaties met andere projecten aanwezig.

3. Initiële Business Case

3.1 Redenen

Deloitte richt zich met een breed pakket aan security en privacy diensten voornamelijk op grote organisaties. Deloitte Risk Services heeft gezien dat er meer ruimte is in de markt van het MKB voor pentesting. Deze ruimte willen ze graag benutten, maar op dit moment kunnen ze hier nog geen passende dienst voor leveren. Het idee is ontstaan om een product te ontwikkelen (deels geautomatiseerd) waarmee in een korte periode een pentest kan worden uitgevoerd bij een MKB-organisatie. Dit product moet betaalbaar en waardevol worden voor een MKB-organisatie. Tevens moet de resultaten van de pentest een goed beeld kunnen geven van de mogelijke kwetsbaarheden van een informatiesysteem of infrastructuur. Voor de pentest bij MKB-klanten moet een standaard worden ontwikkeld zodat deze dienst makkelijk, goedkoop en snel kan worden uitgevoerd. Wel moet er ruimte gehouden worden in de standaard voor een stuk maatwerk om de pentest bij de klant aan te laten sluiten. De pentest van Deloitte moet zich onderscheiden van andere pentests door een klantgerichte en begrijpbare rapportage.

3.2 Aannames

Ten behoeve van de Business Case zijn de volgende aannames gedaan:

- Het uitvoeren van een pentest en het uitwerken van de rapportage voor een MKB organisatie kan binnen vier dagen uitgevoerd worden.
- De ontwikkeling van de MKB pentest kan voor een deel gebaseerd worden op de bestaande Deloitte pentest aanpak.

3.3 Kosten

De kosten voor het uitvoeren van dit project bestaat uit tijd van de mensen die bij het project betrokken zijn. Er is geen budget voor dit project opgesteld.

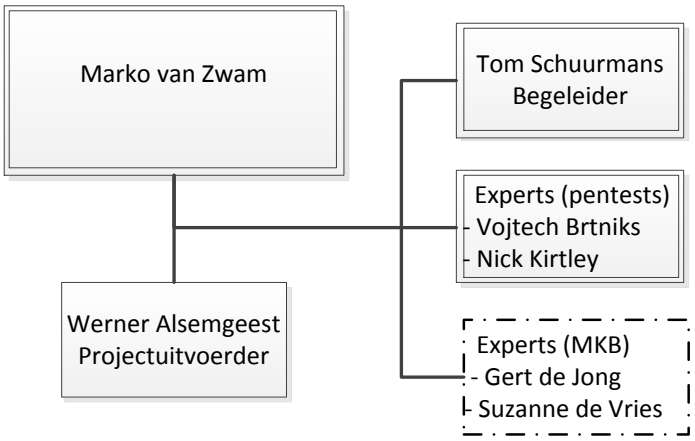
3.4 Baten

Wanneer het project afgerond is, heeft Deloitte een nieuw product die ze kunnen verkopen aan MKB-organisaties binnen Nederland. Het verkopen van dit product zal extra inkomsten genereren voor Deloitte. Daarnaast krijgt Deloitte een groter marktaandeel in het MKB waardoor cross selling van andere Deloitte diensten mogelijk wordt.

Ook draagt Deloitte met dit product bij aan de bescherming tegen cybercriminaliteit. MKB-organisaties kunnen hulp bij het verbeteren van informatiebeveiliging nog steeds goed gebruiken, dit blijkt uit verschillende onderzoeken (2) (3).
Met behulp van de pentest krijgen MKB-organisaties beter inzicht in de mogelijke kwetsbaarheden van informatiesystemen en/of infrastructuren en kunnen met behulp van aanbevelingen adequate beveiligingsmaatregelen treffen om gevonden kwetsbaarheden te reduceren.

4. Projectteam structuur

Voor de duur van het project wordt een projectteam opgezet:



Corporate management	
Na(a)m(en)	**Rol**
Marko van Zwam / Derk Wieringa	Team leaders Deloitte Risk Services – Security en Privacy team

Corporate management is verantwoordelijk voor de optimale inpassing van het project in het programma en aansluiting bij de bedrijfsdoelstellingen.

Project Board	
Na(a)m(en)	**Rol**
Tom Schuurmans	Begeleider
Nick Kirtley / Vojtech Brtnik	Expert (Pentesting)
	Expert (MKB)

Het project board is eindverantwoordelijk voor het "overall" eindresultaat van het project en voor het ter beschikking stellen van mensen en middelen. De project board komt formeel alleen bij elkaar voor het bespreken van faseplanningen en uitzonderings-rapportages.

Projectmanager en uitvoerder	
Na(a)m(en)	**Rol**
Werner Alsemgeest	Projectmanager en uitvoerder

De projectmanager krijgt van het project board de verantwoordelijkheid en bevoegdheid voor de dagelijkse gang van zaken in het project. De projectmanager kan beslissingen nemen binnen de grenzen zoals aangegeven door het project board. De belangrijkste verantwoordelijkheid van de Projectmanager is het zekerstellen dat het project de gewenste producten oplevert, binnen tijd, binnen budget en volgens de afgesproken kwaliteit. De projectmanager rapporteert aan het project board.

5. Initiële Projectplanning

De projectplanning geeft aan welke acties wanneer worden ondernomen.

5.1 Randvoorwaarden

Om de onderstaande planning te kunnen halen dient aan de randvoorwaarden te worden voldaan die in hoofdstuk 2.5 beschreven staan.

5.2 Externe afhankelijkheden

Het project is afhankelijk van de volgende externe afhankelijkheden om de onderstaande planning te kunnen halen.

- Medewerking van MKB-organisaties wanneer deze bij het project betrokken worden. Bijvoorbeeld bij het uitvoeren van interviews of een concept pentest.

5.3 Productdecompositie

Hier staan alle op te leveren producten met een korte beschrijving. Ook is onder de tabel een schematische weergave te vinden die de relatie tussen de producten weergeeft.

Product	Beschrijving
Plan van aanpak	In dit document staat beschreven hoe het project aangepakt gaat worden. Onder andere staat hier de aanleiding, doelstelling en scope beschreven.
Requirements analyse	In dit document worden de wensen en eisen voor de MKB pentest in kaart gebracht. Er zal worden gekeken naar de wensen en eisen vanuit Deloitte en vanuit de klant.
Ontwerp pentest	In dit document staat beschreven hoe de pentest ontworpen gaat worden. Onder andere staat hier de methode, tools en processtappen beschreven.
Concept pentest	Dit product bevat een concept van de MKB pentest, ontwikkeld aan de hand van het ontwerp pentest. Het concept zal wanneer mogelijk getest worden bij een MKB-organisatie.
Evaluatie & advies	Dit document bevat een evaluatierapport van de pentest die uitgevoerd is bij een MKB-organisatie. Tevens wordt in dit document een advies gegeven aan Deloitte over de vervolgstappen die uitgevoerd dienen te worden voor de ontwikkeling van de MKB pentest.

Tabel 2: Productcompositie

5.4 Planning aannames

Er zijn nog geen planning aannames gedaan.

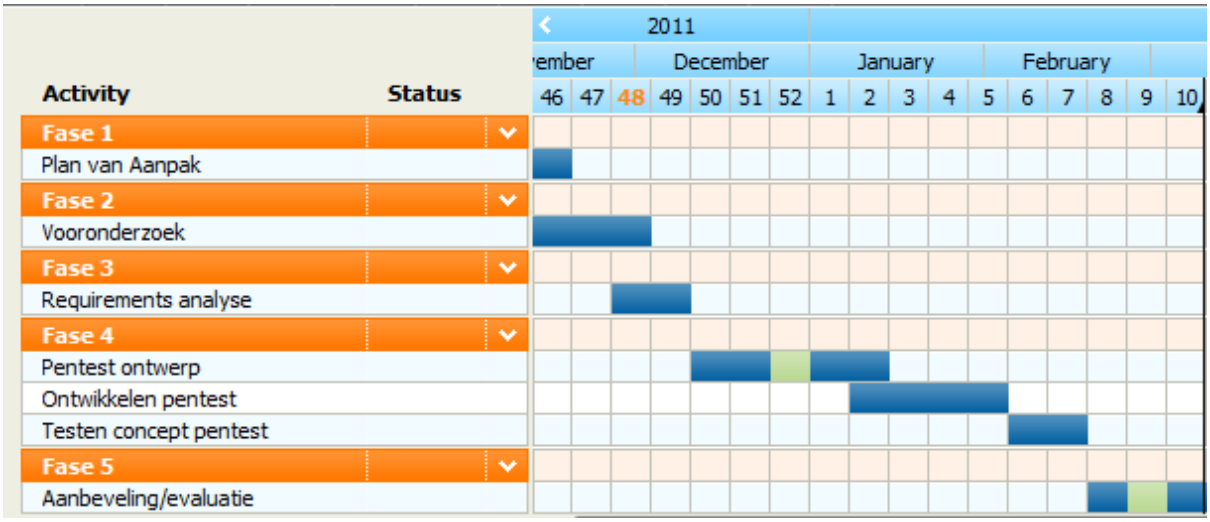
5.5 Projectplanning

De planning is ingedeeld in fases. Elke fase heeft zijn eigen deadline.
Tijdens de uitvoering van het project zijn er twee schoolvakanties, aan de hand van de voortgang van het project zal worden besloten of binnen de vakanties doorgewerkt zal worden. Onder de tabel is de planning grafisch weergegeven.

Fase	Geplande Startdata	Geplande Einddata	Geplande Uren	Doorlooptijd cumulatief
Fase 1	14-11-2011	18-11-2011	20 uur	5 dagen
Fase 2	14-11-2011	02-12-2011	80 uur	15 dagen
Fase 3	28-11-2011	09-12-2011	60 uur	10 dagen
Fase 4	12-12-2011	10-02-2011	400 uur	50 dagen
Fase 5	13-02-2011	02-03-2010	120 uur	15 dagen
		TOTAAL:	**680 uur**	**90 dagen**

Tabel 3: projectplanning

Planning grafisch weergegeven



Schoolvakanties

De onderstaande data zijn de schoolvakanties gedefinieerd door De Haagse hogeschool:
Maandag 26 december 2011 t/m vrijdag 6 januari 2012
Maandag 27 februari 2012 t/m vrijdag 2 maart 2012
Deze vakanties zijn groen gekleurd in de bovenstaande grafische planning.

6. Beheersingsmechanismen

6.1 Toleranties

Per fase is de tolerantie in de doorlooptijd aangegeven. Wanneer de fase binnen de toleranties van de doorlooptijd wordt afgerond dan zal er geen exception report worden opgeleverd.

Fase	Doorlooptijd in %
Fase 1	Doorlooptijd plus of min 05%
Fase 2	Doorlooptijd plus of min 05%
Fase 3	Doorlooptijd plus of min 10%
Fase 4	Doorlooptijd plus of min 10%
Fase 5	Doorlooptijd plus of min 10%

Tabel 5: toleranties

6.2 Voortgangsrapportage

Tijdens dit project zullen er twee soorten voortgangsrapportages worden gebruikt:

Rapport	Beschrijving	In te leveren bij
Highlight Report	Wekelijkse voortgangsrapportage, kwalitatief en kwantitatief in de vorm van een mondeling gesprek.	Begeleider
Exception Report	Rapportage indien de tolerantiegrenzen van het project of de fase in tijd dreigen te worden overschreden. In de rapportage staat de fase die uitloopt, de reden van uitloop en de gevolgen op het project beschreven. In overleg met de Project Board zal worden besloten welke acties de projectuitvoerder dient te ondernemen om het project succesvol af te kunnen ronden.	Project Board

Tabel 6: voortgangsrapportage

6.3 Uitzonderingsprocedure

De uitzonderingsprocedure treedt in werking wanneer van een fase of het project verwacht wordt dat het niet binnen de afgesproken tolerantiegrenzen ten aanzien van tijd wordt afgerond. Zodra de Projectmanager dit verwacht, meldt de Projectmanager dit in een Exception Report aan de project board. In onderling overleg wordt de aanleiding, oorzaak en gevolg voor het project besproken.

7. Projectrisico's

Door middel van risicomanagement wordt er gestreefd om het effect van de risico's te minimaliseren. De kans van optreden en de mate van negatief effect op het project wordt aangeven op een schaal van 1 t/m 5. De laatste kolom geeft het risico aan (kans*effect=risico). Op deze wijze kan goed worden afgewogen welke bedreigingen de meeste aandacht of hulpbronnen vereisen.

Bedreiging:	**Tegenmaatregel:**	**Kans**	**Effect**	**Risico**
Onvoldoende kennis in huis voor het uitvoeren van het onderzoek	Hulp inschakelen van experts binnen Deloitte	2	5	10
Tijdnood	Duidelijke planning maken met voldoende speling	2	4	8
De weersomstandigheden zijn zodanig slecht dat het niet met behulp van (openbaar)vervoer mogelijk is om op kantoor te komen	Thuis werken	3	2	6
Product voldoet niet aan verwachting	Tussentijdse feedback op product vragen door begeleider	2	3	6
Projectlid wordt langdurig ziek	Scope bijstellen	1	5	5
Gegevensverlies	Het projectmanagement is zelf verantwoordelijk voor de opslag en back-up van de gegevens	1	4	4
De opdrachtgever is verhinderd (ziekte, geen vervoer enz.) om aan het project mee te werken	Iemand uit de project board zal de taak van opdrachtgever op zich nemen	1	4	4
Scope verbreding	Vasthouden aan oorspronkelijk gestelde kaders in het plan van aanpak	1	3	3

Tabel 7: risicoanalyse

Bronnenlijst

Dit is een lijst van gebruikte bronnen in dit document:

De gebruikte bronnen staan als volgt genoteerd:
[Bron nummer] Achternaam auteur, voorletter(s) of Titel van het document / de website. *Organisatie*. [Bron soort] Publicatiejaar of update. [Geopend op.] URL van website.

1. SME Definition. *European Commission.* [Online] 1 Januari 2005. [Citaat van: 15 November 2011.] http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm.
2. Nederlands mkb nog steeds slecht beveiligd. *Webwereld.* [Online] 11 mei 2009. [Citaat van: 18 November 2011.] http://webwereld.nl/nieuws/58056/nederlands-mkb-nog-steeds-slecht-beveiligd.html.
3. Nederlands MKB is slecht beveiligd. *Computable.* [Online] 13 Februari 2008. [Citaat van: 18 November 2011.] http://www.computable.nl/artikel/ict_topics/security/2346125/1276896/nederlands-mkb-is-slecht-beveiligd.html.

Design pentest

Ontwikkeling MKB pentestproduct

Naam: Werner Alsemgeest
Studentnummer: 08022488
Instituut: De Haagse Hogeschool
Opleiding: Information Security Management
Afstudeerstage bedrijf: Deloitte
Begeleider Hogeschool: Ellen Wesselingh
Begeleider Deloitte: Tom Schuurmans

Datum: 12 maart 2012
Versie: 1.1

Versiehistorie

Versienummer	Versiedatum	Controle door:	Wijzigingen
0.1 (Concept)	14-12-2011	Werner Alsemgeest	Opzet concept
0.2	11-01-2012	Werner Alsemgeest	Wijziging na Feedback Tom Schuurmans + toevoeging samenvatting
0.3	23-01-2012	Werner Alsemgeest	Wijziging na Feedback Tom Schuurmans
1.0	14-02-2012	Werner Alsemgeest	Wijziging na Feedback Tom Schuurmans
1.1	22-02-2012	Werner Alsemgeest	Wijziging na feedback Ellen Wesselingh

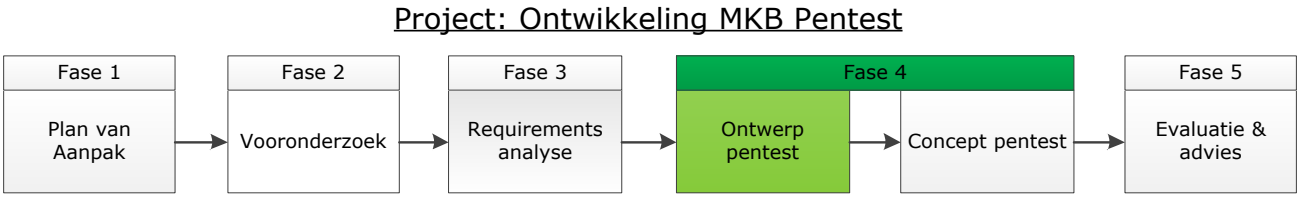
Distributielijst

Versienummer	Datum	Naam	Organisatie
0.1	11-01-2012	Tom Schuurmans	Deloitte
0.3	23-01-2012	Tom Schuurmans	Deloitte
1.0	19-02-2012	Ellen Wesselingh	De Haagse Hogeschool

Inhoud

1. Inleiding

Dit document is een onderdeel van het project "Ontwikkeling MKB pentest" in opdracht van Deloitte Nederland te Amstelveen. Dit document bevat het resultaat van fase 4 van het project. In de onderstaande schematische weergave is de plek van dit document (groen gekleurd) in de projectfases weergegeven. Voor meer informatie over het project zie het document "Plan van Aanpak".



In dit document staat het ontwerp beschreven dat gebruikt zal worden voor het ontwikkelen van de MKB pentest. Het ontwerp voor de MKB pentest is gebaseerd op de wensen en eisen die in kaart zijn gebracht tijdens de requirements analyse. Wanneer het ontwerp wordt goedgekeurd kan er een concept MKB pentest worden ontwikkeld aan de hand van dit ontwerp.

In het eerste volgende hoofdstuk wordt achtergrondinformatie gegeven over het gebied van pentesting. Onder andere staat beschreven wat een pentest is en hoe een pentest uitgevoerd kan worden. In het derde hoofdstuk staat beschreven hoe op het moment een pentest wordt uitgevoerd binnen Deloitte en hoe dat proces eruit ziet. Waarom het MKB een pentest nodig heeft staat beschreven in hoofdstuk 4. In het hoofdstuk daarna (hoofdstuk vijf) staat beschreven hoe de pentest voor het MKB eruit komt te zien. Wat de onderdelen zijn van de MKB pentest staat beschreven in hoofdstuk zes. In het hoofdstuk daarna worden de standaarden beschreven die gebruikt kunnen worden voor de pentest. Tot slot is aan het einde van dit document een samenvatting te vinden.

Bijlagen en een bronnenlijst zijn bijgevoegd aan het einde van dit document.

2. Achtergrondinformatie pentest

Dit hoofdstuk bevat achtergrondinformatie over het onderwerp pentest. In dit hoofdstuk staat onder andere beschreven wat een pentest is, hoe een pentest aangepakt kan worden en wat voor soorten pentests er zijn.

2.1 Wat is een pentest

Pentest is een afkorting van het woord penetratietest. Een penetratietest is een methode om de beveiliging van een informatiesysteem of netwerk te evalueren op beveiliging, door het simuleren van aanvallen door kwaadaardige hackers (1). Met een penetratietest worden de mogelijke kwetsbaarheden van het systeem/software/netwerk in kaart gebracht. Tegen deze kwetsbaarheden kunnen gerichte maatregelen worden getroffen om het niveau van informatiebeveiliging te verhogen.
Kwetsbaarheden in een systeem/software/netwerk kunnen ontstaan door een verkeerde configuratie, fouten in de hardware/software, menselijke onopzettelijke fouten of door operationele tekortkomingen in een proces.

Pentests worden uitgevoerd na toestemming van de eigenaar van het informatiesysteem/netwerk door zogenaamde ethische hackers. Kwetsbaarheden die ontdekt zijn door middel van een pentest worden gepresenteerd aan de opdrachtgever van de pentest. Vaak wordt ook het risico (kans x impact) van de kwetsbaarheden in kaart gebracht en worden maatregelen geadviseerd om de gevonden kwetsbaarheden op te lossen. Pentests kunnen los als worden project uitgevoerd of in combinatie met bijvoorbeeld een audit.

2.2 Aanpak pentest

Er zijn verschillende manieren om een pentest uit te voeren. Van binnen of buiten het bedrijf(snetwerk) en met veel of weining voorkennis. De keuze van de aanpak wordt in overleg met de opdrachtgever afgesproken.

Intern of Extern

Een pentest kan vanbinnen de organisatie worden uitgevoerd of van buitenaf. Als een pentest vanuit intern wordt uitgevoerd wordt de pentest op het zelfde lokale bedrijfsnetwerk uitgevoerd als de systemen die getest moet worden. Bij een externe pentest wordt de aanval vanuit een andere locatie (vaak via het internet) uitgevoerd.

White Box, Grey Box & Black Box

De voorkennis bepaalt de hoeveelheid informatie die de pentesters van te voren krijgen van de eigenaar van het te testen systeem. Als de pentesters meer informatie hebben, kan de pentest gerichter en efficiënter worden uitgevoerd. De pentester hoeft dan namelijk geen tijd te besteden aan het vergaren van karakteristieken van het systemen en heeft dan meer tijd voor het vinden van kwetsbaarheden.

- **White box**
  Tijdens een white box pentest krijgen de pentesters volledige kennis van de infrastructuur en systemen (soms zelfs met diagrammen, broncode, ip adressen, enz.) Een white box pentest simuleert wat kan gebeuren tijdens een ontslag van een medewerker of na een "lek" van gevoelige informatie, waar de aanvaller toegang heeft tot de broncode, netwerk lay-outs en misschien zelfs wachtwoorden.
- **Black box**
  Black box testen simuleert een aanval van iemand die niet bekend is met het systeem. De pentesters moeten de karakteristieken van de systemen eerst bepalen voordat ze op zoek kunnen gaan naar kwetsbaarheden.
- **Grey box**
  Ook zijn verschillende variaties mogelijk die tussen de white en de black box in liggen. Deze variaties vallen in een grijs gebied (grey box). Tijdens een grey box wordt een gedeelte van de informatie aan de pentesters gegeven. Hierbij wordt er een aanval gesimuleerd waarin een hacker zich deels inzicht heeft weten te verschaffen in de organisatie. Vaak wordt voor deze middenweg gekozen om tijd te besparen. Een volledige black box kan erg veel tijd kosten.

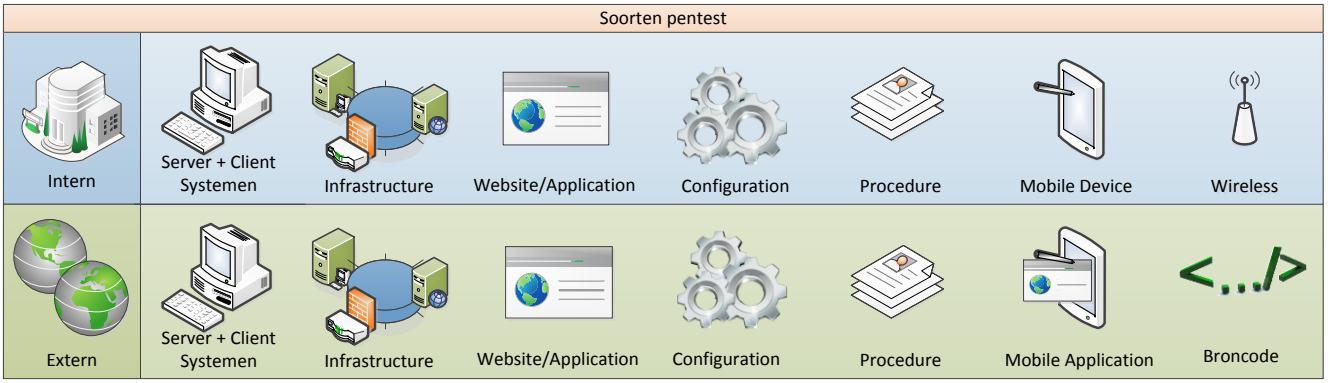
2.3 Werkwijze van een pentester

In de volgende schematische werkwijze is een algemene aanpak weergegeven van een pentest. (2)

- **Informatie verzamelen scope**
  Afhankelijk van de aanpak van de test (white v.s. black box) moet eerst informatie over de scope verzameld worden. Zoals: welke systemen zijn er, welke applicaties zijn er, welke IP-adressen zijn er enz. Tijdens deze stap kan er ook informatie worden gezocht op google, de site van de organisatie en sociale netwerken.
- **Informatie verzamelen systemen**
  Tijdens de tweede stap wordt zo veel mogelijk informatie verzameld van de specifieke systemen die zich in de scope bevinden. Zoals: welk besturingssysteem wordt er gebruikt, software versie, welke systemen zijn "live" enz.
- **Kwetsbaarheden identificeren**
  De volgende stap is het in kaart brengen van de kwetsbaarheden. De kwetsbaarheden kunnen in kaart gebracht worden met behulp van tooling en het handmatig hacken van de site.
- **Exploiteren/Aanvallen**
  Aan de hand van de gevonden kwetsbaarheden kan (wanneer gewenst) misbruik worden gemaakt van het systeem door het systeem aan te vallen en de kwetsbaarheden te exploiteren door middel van tooling of handmatige handelingen. Dit kan worden gedaan om de gevolgen in kaart te brengen die een hacker zou kunnen aanrichten.
- **Rapporteren**
  Tot slot worden alle bevindingen gerapporteerd en aan de opdrachtgever opgeleverd.

2.3 Soorten pentest

Zoals te lezen is in hoofdstuk 2.1 kan een pentest op verschillende soorten producten uitgevoerd worden. In de onderstaande opsomming worden de verschillende soorten pentests beschreven die binnen Deloitte uitgevoerd kunnen worden.
Deze soorten pentests zijn niet zwart op wit en kunnen ook gelijktijdig worden uitgevoerd. Tevens vallen sommige soorten pentests niet binnen de "officiële" term pentest. Tijdens een pentest wordt er geprobeerd in te breken op een systeem, netwerk of applicatie zonder op de hoogte te zijn van de volledige configuratie. Hierdoor vallen de pentest configuratie, broncode en procedure eigenlijk buiten de boot, maar deze soorten vallen wel binnen de pentest term die gebruikt wordt binnen dit project en worden ook verkocht als pentestproduct.



- **Infrastructuur**
  Een pentest op de infrastructuur richt zich op het vinden van kwetsbaarheden in het netwerk, VPN verbindingen en de verbinding met het internet. Er wordt bijvoorbeeld gecontroleerd welke kwetsbaarheden er zijn wanneer systemen vanaf het internet benaderd worden.
- **Systemen (server + Client)**
  Doormiddel van een pentest op systemen kunnen mogelijke kwetsbaarheden in kaart worden gebracht. Deze kwetsbaarheden kunnen bijvoorbeeld ontstaan door oude software of een slechte soft/hardware matige beveiliging.
- **Website**
  Tijdens een pentest op een website wordt er gezocht naar kwetsbaarheden op de website. Door kwetsbaarheden in de website zouden vertrouwelijke gegevens achterhaald kunnen worden of misbruik kunnen worden gemaakt van de webserver.
- **Applicatie**
  Met een applicatiepentest wordt er gezocht naar kwetsbaarheden op de software laag. Deze pentest komt veel overeen met de website pentest. Applicaties draaien meestal in het interne netwerk van een bedrijf of lokaal op een computer.
- **Configuratie**
  Tijdens een configuratiepentest worden de instellingen gecontroleerd van bijvoorbeeld een server of een router op kwetsbaarheden. De configuratiepentest lijkt erg op een systeempentest, het verschil zit hem in de informatie die beschikbaar word gesteld. Tijdens een configuratiepentest wordt er documentatie van alle instellingen beschikbaar gesteld. Bij een systeempentest moet de pentester deze informatie zien te achterhalen.

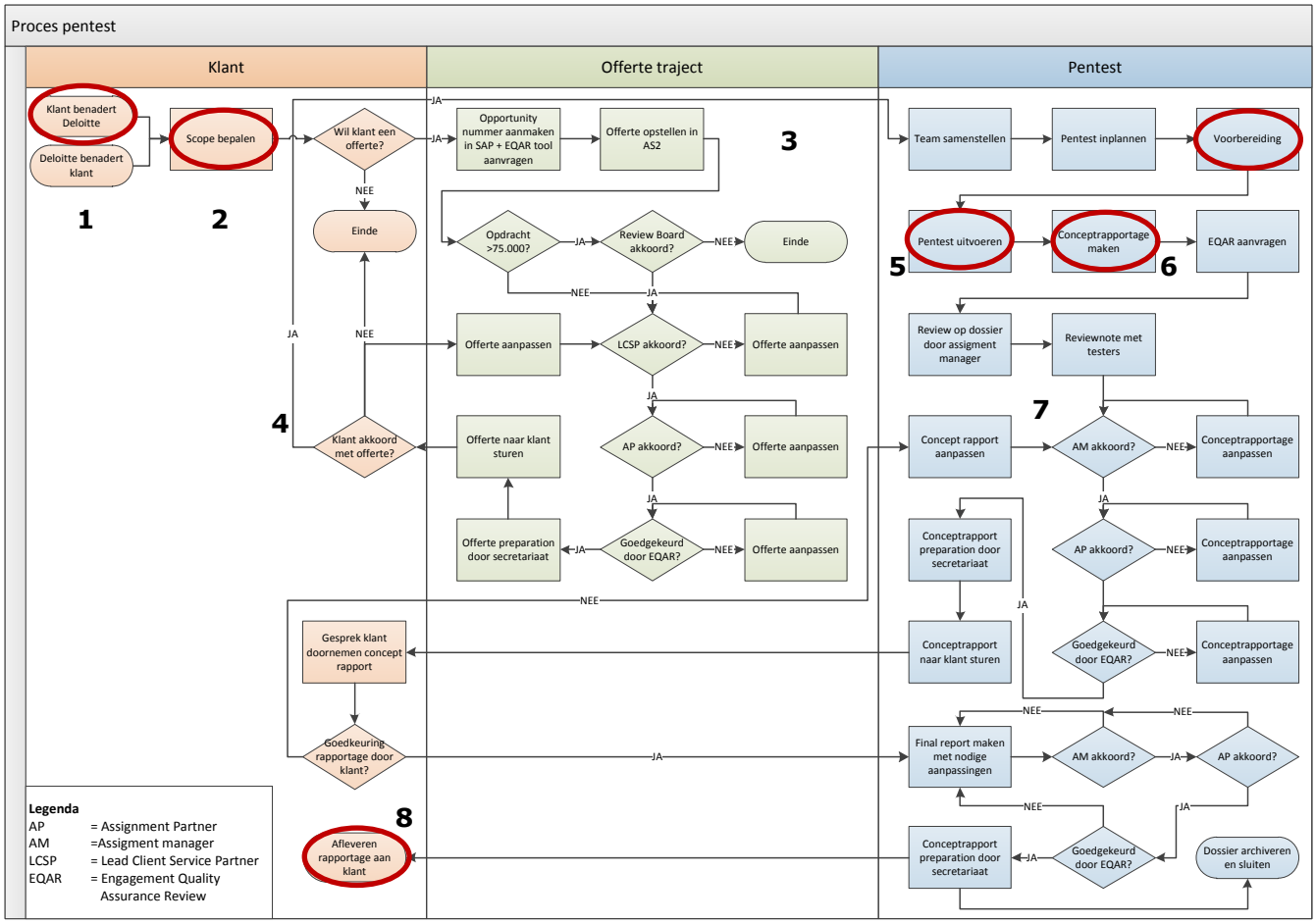
- **Broncode (review)**
  Bij een broncode pentest wordt de code (HTML, PHP, ASP) van bijvoorbeeld een applicatie nagekeken op kwetsbaarheden die de code kan veroorzaken. Significante codefouten zouden kunnen resulteren in een volledig compromis van de server waarop de applicatie draait.
- **Mobiele apparaten**
  Er worden steeds meer mobiele apparaten gebruikt in het bedrijfsleven zoals smartphones en tablets. Deze apparaten hebben vaak volledige toegang tot het bedrijfsnetwerk en de bedrijfsdata. Met een pentest kunnen mogelijke kwetsbaarheden van mobiele apparaten in kaart worden gebracht. Aan de hand van de resultaten kunnen er maatregelen worden getroffen om de informatie op de apparaten beter te beschermen.
- **Mobiele applicaties/websites**
  Mede door de toename aan mobiele apparaten is er ook een toename aan mobiele applicaties te zien. De pentest voor mobiele applicaties verschilt niet veel van een pentest voor websites of applicaties. Aandachtspunten voor een mobiele applicatie pentest kunnen bijvoorbeeld het downloaden van de applicatie via een "appstore", de rechten van de applicatie op het mobiele apparaat en de installatie van de applicatie zijn.
- **Draadloos**
  De beveiliging van een draadloos netwerk kan worden getest door een pentest. Tijdens deze pentest kan bijvoorbeeld de encryptie of de manier van authenticatie worden getest. In de scope van een draadloze pentest zou ook de authenticatieserver meegenomen kunnen worden.
- **Procedures**
  Zelfs wanneer de technische beveiliging van een systeem op orde is kunnen er nog kwetsbaarheden optreden. Er kunnen bijvoorbeeld procedurele handelingen zijn waar niemand goed over nagedacht heeft. Bijvoorbeeld bij het resetten van het wachtwoord door een gebruiker waarbij niet om het oude wachtwoord is gevraagd of het nieuwe wachtwoord in "plain text" via een onbeveiligde verbinding op de website komt te staan.

3. Deloitte pentest

Binnen Deloitte worden al een aantal jaar pentests uitgevoerd voor diverse organisaties. In deze jaren is veel ervaring opgedaan op het gebied van pentests en zijn procedures en standaarden ontwikkeld. Deze ervaring zal worden gebruikt bij de ontwikkeling van de MKB pentest. In dit hoofdstuk zal in het kort worden ingegaan hoe op het moment binnen Deloitte een pentest wordt uitgevoerd.

3.1 Huidig pentestproces

In de onderstaande flowchart staat het pentest proces beschreven, op de volgende pagina zijn de stappen die tijdens een pentest worden uitgevoerd in het kort beschreven. Een grote versie van de flowchart is te vinden in bijlage A.



Met de rode cirkels is aangegeven op welke plekken binnen het proces een aanpassing gemaakt kan worden voor de MKB pentest. Deze plekken zijn bepaald aan de hand van het vooronderzoek en de requirements analyse voor de MKB pentest. In hoofdstuk 5 zal worden ingegaan op deze punten.

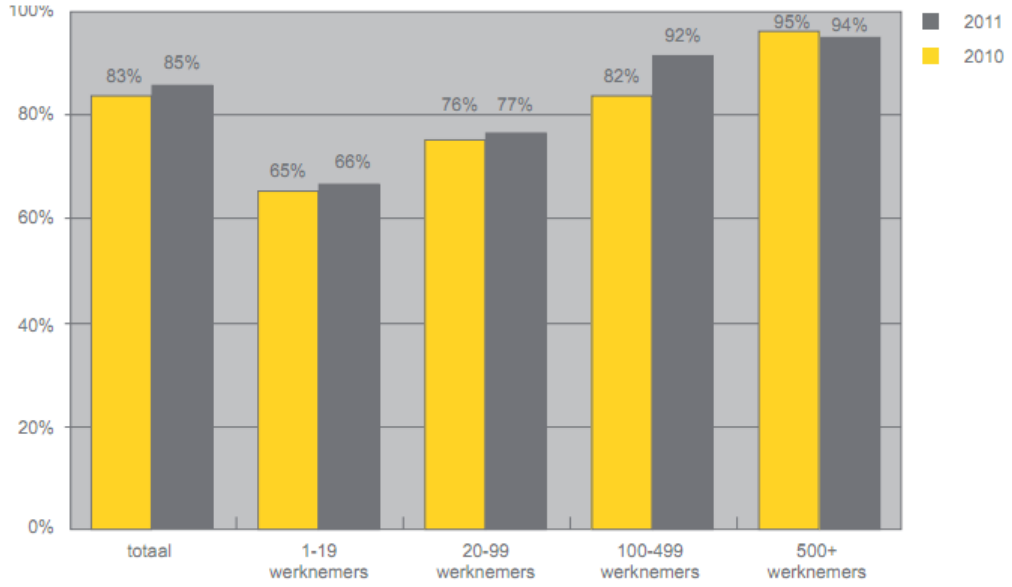
Het pentest proces is een uitgebreid proces met veel controleslagen die door verschillende afdelingen binnen Deloitte loopt. In het kort worden de onderstaande hoofdstappen uitgevoerd voor een pentestproject. Deze stappen zijn met een nummer aangegeven in de flowchart op de vorige pagina.

1) **Klant**
   De klant (van Deloitte) heeft behoefte aan een pentest en is opzoek naar een partij die een pentest kan uitvoeren. Wanneer de klant voor Deloitte kiest zal er een intakegesprek plaatsvinden.
2) **Intake**
   Tijdens het intakegesprek probeert Deloitte onder andere de volgende punten duidelijk te krijgen:
   - Waarom wil de klant een pentest?
   - Wat is de scope van de pentest?
   - Wat voor soort pentest wil de klant? (Zie hoofdstuk 2.3)
   - Wat wordt de aanpak van de pentest? (Zie hoofdstuk 2.2)
   - Is de pentest op een Productie / pre-productie systeem?
   - Zijn er derde partijen bij betrokken?
   - Welke mensen worden op de hoogte gesteld van de pentest?
   - Wat wordt de planning voor de pentest?
3) **Offerte**
   Wanneer Deloitte voldoende inzicht heeft gekregen in de wensen en eisen van de pentest wordt er een offerte opgesteld. In de worden ook specifieke pentest voorwaarden toegevoegd zodat Deloitte bevoegd is om de pentest uit te voeren. Tijdens het offerte traject wordt een aantal controles en goedkeuringen uitgevoerd.
4) **Goedkeuring door de klanr**
   Pas als Deloitte een getekende offerte teruggekregen heeft en toestemming heeft van de klant om de pentest uit te voeren, kan worden begonnen met de pentest.
5) **Pentest**
   Er zal een pentest worden uitgevoerd binnen de vastgestelde tijdsduur, op de afgesproken scope zoals beschreven staat in de offerte. Tijdens de pentest zal er een dossier worden bijgehouden met de uitgevoerde tests en bewijs (bijvoorbeeld screenshots).
6) **Conceptrapport**
   Het testteam dat de pentest heeft uitgevoerd schrijven de bevindingen op en verwerken dit in een conceptrapport.
7) **Controle**
   Het conceptrapport wordt gecontroleerd op spelling, opmaak, zinsopbouw en inhoud door verschillende personen. Wanneer goedgekeurd wordt de rapportage opgeleverd aan de klant.
8) **Presentatie**
   Wanneer de rapportage is goedgekeurd door de klant wordt er een presentatie gegeven door Deloitte aan de opdrachtgever. De presentatie kan in verschillende vormen plaatsvinden (zoals digitaal, mondeling, document enz.).

4. Noodzaak voor pentesting binnen het MKB

Omdat organisaties en burgers niet meer zonder ICT kunnen, groei ook de vraag naar informatiebeveiliging (3). Hoe belangrijk de ICT voor MKB organisaties is, is onderzocht door verschillende partijen. Ernst & Young heeft aan ongeveer 600 directeuren/managers gevraagd hoe belangrijk de ICT voor de organisaties is. Deze resultaten zijn in percentage uitgedrukt.

Onderzoek Ernst & Young: Hoe belangrijk is ICT voor de organisatie (5)



Financiële instellingen en grote internationale organisaties zijn zich bewust dat ze goede informatiebeveiliging moeten hebben. Dit komt mede omdat zware eisen vanuit wet- en regelgeving en klanten worden gesteld aan de informatiebeveiliging van organisaties. In dit hoofdstuk wordt gekeken naar de noodzaak van informatiebeveiliging binnen het MKB.

Wet- en regelgeving
Elke organisatie moet voldoen aan bepaalde wet- en regelgeving. De volgende wet- en regelgeving met betrekking tot informatiebeveiliging kan voor het MKB van belang zijn. Het is afhankelijk van de organisatie aan welk van de onderstaande wet- en regelgeving voldaan dient te worden.

- BW deel II titel 9 (informatiebeveiliging in het kader van de jaarrekeningcontrole)
- Telecommunicatiewet
- Wet Bescherming Persoonsgegevens
- Wet Toezicht Verzekeringswezen
- Archiefwet
- GBA-vereisten bij gemeente
- Wetboek van Strafrecht / Wet Computer Criminaliteit
- Bescherming van intellectuele eigendomsrechten (IPR) in Auteurswet, Octrooiwet

MKB organisaties zouden zich dus bewust moeten zijn dat ze aan bepaalde wet- en regelgeving zouden moeten doen die betrekking hebben tot informatiebeveiliging.

Cyberaanvallen
Cyberaanvallen vormen een zeer grote bedreiging voor het MKB. Volgens het 2010 Global SMB Information Protection Survey (uitgevoerd door Symantec) rapport was 73% procent van de ondervraagden in het afgelopen jaar het slachtoffer van cyberaanvallen. Dertig procent van deze aanvallen werd als enigszins/zeer succesvol beschouwd. Honderd procent van deze MKB-organisaties leed daardoor schade, zoals kostbare computerstoringen en verlies van belangrijke bedrijfsgegevens en persoonlijke gegevens van klanten en werknemers. Dit bracht bij alle ondervraagden directe kosten met zich mee, onder meer door het verlies van productiviteit, inkomsten en vertrouwen van de klant. (6) Dit concludeert ook Metro in een artikel. (7)

Verlies van gegevens
Het verlies van essentiële zakelijke gegevens vormt een andere belangrijke bedreiging voor het MKB. 74% procent van de ondervraagde MKB-organisaties van het 2010 Global SMB Information Protection Survey is enigszins/zeer bezorgd over het verlies van digitale gegevens. 42% procent is in het verleden zelf vertrouwelijke of geheime informatie kwijtgeraakt. Honderd procent van de organisaties die zijn gegevens kwijtgeraakt is, heeft daardoor directe schade geleden, bijvoorbeeld door winstderving of directe financiële kosten.

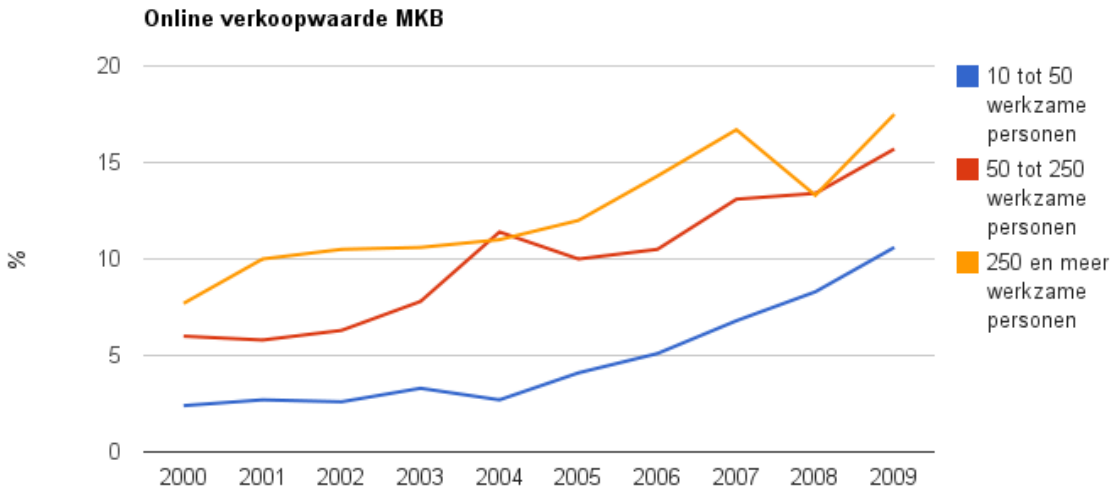
Verlies van apparatuur
Een ander probleem voor MKB-organisaties is het verlies van apparatuur. Bijna twee derde van de organisaties is in het afgelopen jaar laptops, smartphones, iPads of andere apparaten kwijtgeraakt. 100% van de MKB organisaties die meegedaan hebben aan het 2010 Global SMB Information Protection Survey maakt gebruik van apparaten die niet zijn beveiligd met een wachtwoord en waarvan de gegevens niet op afstand kunnen worden gewist om in het geval van verlies vertrouwelijke en zakelijke informatie te beschermen.

Eisen vanuit klanten

Klanten die diensten afnemen bij een MKB organisatie kunnen eisen stellen aan de informatiebeveiliging. Een grote organisatie die aan ISO27001 moet voldoen zal bijvoorbeeld alleen hosting afnemen bij een MKB organisatie die ook aan de ISO norm kan voldoen.

Meer digitale handel

Een trend is dat MKB organisaties in de afgelopen jaren steeds meer verdienen met online handel zoals hosting, webshops en online ticketverkoop. Deze stijging is weergegeven in de onderstaande grafiek. Bij deze manier van handelen is meer informatiebeveiliging nodig, omdat de communicatie, gegevensverwerking en opslag via openbare kanalen (het internet) verloopt.



4.1 Pentesting als onderdeel van de informatiebeveiliging

Er kan geconcludeerd worden dat voor het MKB zeker een noodzaak is om aan informatiebeveiliging te doen. De punten die informatiebeveiliging noodzakelijk maken staan hieronder samengevat.

- Wet- en regelgeving
- Eisen vanuit klanten
- Cyberaanvallen
- Verlies van gegevens
- Verlies van apparatuur
- Meer digitale handel

Het uitvoeren van een pentest zal niet alle informatiebeveiligingsproblemen binnen een MKB organisatie oplossen. Informatiebeveiliging is een proces en dient goed verankerd te zijn in de gehele organisatie.

Definitie informatiebeveiliging:
"Informatiebeveiliging is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie binnen een organisatie of een maatschappij garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken." (8)

Een pentest is een onderdeel van het informatiebeveiligingsproces. Waar grote organisaties meestal een totaal securitybeleid voeren, ziet het MKB zichzelf niet als doel voor hackers. Hierdoor investeren de meeste MKB organisaties niet volledig in het informatiebeveiligingsproces, voornamelijk wordt gekeken naar bescherming tegen online bedreigingen op basisniveau (9). Mede hierdoor is een pentest een goed middel om belangrijk informatiesystemen binnen een MKB organisatie te controleren op mogelijke kwetsbaarheden.

4.2 Trends in de ICT

Om de pentest goed aan te laten sluiten op de gebruikte en toekomstige ICT middelen binnen het MKB is het handig om naar de ICT trends te kijken. In de onderstaande tabel staan de ICT trends van 2012 volgens een aantal organisaties (in een top 10). De trend die gebruikt zijn in de tabel geciteerd uit de onderzoeken

	ALgemeen	**Algemeen**	**MKB gericht**	**MKB gericht**	**MKB gericht**
	EMC (10)	**Gartner** (11)	**SMB Group** (12)	**Management Team** (13)	**InformationWeek** (14)
1	Eenvoud is nieuwe 'killer-app'	Mobiele apparaten	Economische angst verlaagt MKB omzet verwachting en verkleint ICT budget	Big Data	De opkomst van de "Progressieve" MKB.
2	Mobiel eerst	Mobiele applicaties	Progressieve MKB wint terrein	Bring Your own Device	Cloud wordt "Business As Usual"
3	Meer vraag naar Data Scientists	Sociale en contextuele gebruikerservaringen	De sociale media kloof wordt groter	Apps, Apps, Apps	De mobiele markt wordt volwassen
4	Toenemende concurrentie tussen it-afdeling en externe leveranciers	Applicatie markten	Cloud computing wordt normaal	De muis is dood	De sociale kloof verbreedt.
5	Groei van het digitale business model	Het Internet als centraal middelpunt	Het gebruik van mobiele toepassingen groeit	Social Media	
6	Andere benadering IT-beveiliging	Volgende generatie analytics	Meer behoefte aan Business Intelligence en analytics aangewakkerd door Social Media, mobiele apparaten en cloud computing	Energieverbuik	
7	Groei gespecialiseerde IT service providers	Enorme hoeveelheid datastromen	Managed Service ontmoet mobiele platform	Cloud computing	
8	Kosten dalen - consumptie neemt toe	In-memory computing	Meer behoefte aan ICT oplossingen voor ZZP'ers		
9	Vraag naar nieuwe 'cloud-vaardigheden'	Extreme energie-arme servers	Verhoogde acceptie van integrale communicatie en samenwerk diensten		
10	Big data als kans	Cloud computing	Door Social Media, Cloud en mobiel verandert de vraag en aanbod van ICT "kanalen"		

Er zijn verschillende inzichten naar ICT trends voor 2012, maar er zijn ook overeenkomsten die interessant zijn voor MKB pentesting. Dat zijn de volgende onderwerpen:

- Mobiele apparaten
- Mobiele Applicaties
- Cloud computing
- Veel (gevoelige) data
- MKB gaat meer online doen

Deze punten kunnen gebruikt worden voor de ontwikkeling van de MKB pentest. De trends voorspellen bijvoorbeeld veel gebruik van mobiele apparaten en applicaties. De MKB pentest dient zo ontwikkelt te worden dat mobiele apparaten en applicaties getest kunnen worden op kwetsbaarheden.

5. MKB pentest

In dit hoofdstuk staat op een hoog niveau beschreven uit welke onderdelen de MKB pentest zal bestaan, welke soorten pentests aangeboden kunnen worden voor het MKB en op welke manier de MKB pentest uitgevoerd kan worden.

5.1 Soorten MKB pentest

Een MKB pentest kan bestaan uit een aantal verschillende soorten tests. Niet alle soorten pentests zoals die beschreven staan in hoofdstuk 2.3. zijn meegenomen. Bij de keuze is rekening gehouden met de tijd die benodigd is voor het uitvoeren van de pentest, de ideeën van ervaren pentesters, managers en de (2012) ICT trends voor het MKB. Om deze reden is bijvoorbeeld de broncode pentest niet meegenomen omdat een broncodereview te veel tijd in beslag neemt.
Om het MKB pentest aanbod eenvoudig en overzichtelijk te houden voor de klanten zal de focus van de MKB pentest liggen op drie producten. De verwachting is dat deze drie producten het meest aangevraagd zullen worden. De samenstelling van de producten is ontstaan door het samenvoegen van een aantal soorten pentests. Deze producten zullen een vaste prijs krijgen (zie hoofdstuk 6.1).

Website	Mobile	Infra
		
• Kwetsbaarhedenscan website • Kwetsbaarhedenscan webserver	• Kwetsbaarhedenscan mobiele-applicatie • Kwetsbaarhedenscan mobiel-apparaat	• Kwetsbaarhedenscan infrastructuur
Trend: Cloud en gevoelige data	**Trend:** Meer mobiele apparaten en applicaties	**Trend:** MKB doet meer online

5.2 Aanpak MKB pentest

Zoals te lezen is in hoofdstuk 2.2 zijn er verschillende methodes om een pentest aan te pakken. Bij een normale pentest kunnen alle methodes gebruikt worden. Omdat voor een MKB pentest de tijd en kosten beperkt moeten blijven zullen de pentests aangepakt worden vanuit een "white" of "grey" box, waar al een deel van de informatie beschikbaar wordt gesteld door de klant. Hierbij kan worden gedacht aan onder andere ip gegevens, inlog gegevens, softwareversie en infrastructuur gegevens. Deze informatie zal tijdens de intake worden gegeven (zie hoofdstuk 6.1).
De MKB pentest kan intern en extern worden uitgevoerd. De nadruk zal liggen op externe pentest, omdat een externe pentest meestal sneller uitgevoerd kan worden en minder manuren kost dan een interne pentest.

5.3 MKB pentestproces

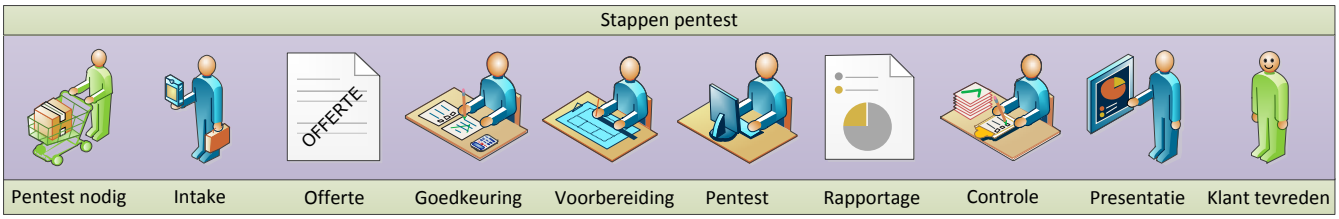
Het pentestproces voor het MKB moet eenvoudig zijn en in een korte tijd uitgevoerd kunnen worden. Het MKB pentestproces is gebaseerd op het normale pentestproces welke beschreven staat in hoofdstuk 3.1. Het MKB pentestproces is gebaseerd op het normale pentestproces omdat dit proces al heeft bewezen goed te werken en er zitten verplichte (controle)processtappen in die uitgevoerd dienen te worden binnen Deloitte.

De volgende processtappen voor de MKB pentest zullen verschillen van de normale pentest:

- Klant benadert Deloitte
- Intake
- Voorbereiding
- Pentest uitvoeren
- Conceptrapport maken
- Afleveren rapportage aan klant

Waar deze procestappen uit bestaan staat beschreven in hoofdstuk 3.1.

In het onderstaande model is een schematisch weergave gemaakt van het MKB pentestproces. De manier waarop een processtap wordt uitgevoerd (bijvoorbeeld digitaal, telefonisch of mondeling) is niet gedefinieerd. Onder het model is een korte beschrijving te vinden van het proces. Een uitgebreidere beschrijving van het pentestproces is te vinden in hoofdstuk 3.1.



De klant heeft behoefte aan een pentest en neemt contact op met Deloitte. Deloitte zal met de klant een intake uitvoeren. Wanneer Deloitte voldoende inzicht heeft gekregen in de wensen en eisen van de pentest wordt er een offerte opgesteld. De offerte gaat door een aantal interne controles en na goedkeuring kan de pentest uitgevoerd worden. Tijdens de pentest worden de bevindingen in een conceptrapport verwerkt. Voordat het pentestrapport naar de klant gaat vinden er een aantal controles op het rapport plaats. Wanneer het rapport is gecontroleerd (en waar nodig aangepast) wordt het rapport aan de klant gepresenteerd. Als het proces goed is uitgevoerd zal de klant tevreden zijn.

= Klant

= Deloitte.

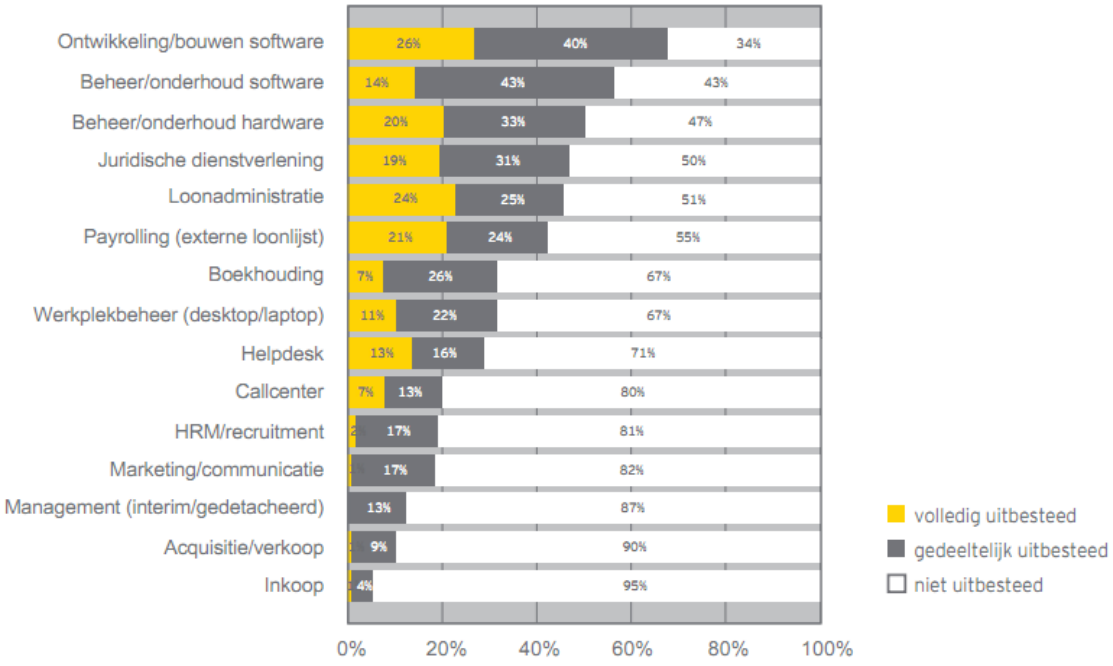
5.4 MKB pentest aandachtspunten

MKB organisaties ondernemen op een andere manier dan grote organisaties. Om de pentest goed aan te laten sluiten op het MKB moet er rekening worden gehouden met de manier van werken binnen het MKB. In dit subhoofdstuk staan een aantal aandachtspunten beschreven die veel bij het MKB voorkomen en invloed hebben op de uitvoering van een pentest.

Externe partijen

In het MKB worden veel activiteiten uitbesteed zodat de organisatie zich kan richten op hun eigen product/dienst. Ook de IT wordt veel uitbesteed (zoals te zien is in de onderstaande afbeelding). Uitbesteding heeft gevolgen voor het afnemen van een pentest.

Onderzoek Ernst & Young, 2011: welke activiteiten worden uitbesteed (15)



Wanneer een pentest op een informatiesysteem binnen de organisatie van de klant wordt uitgevoerd is de klant eigenaar van dat systeem. Wanneer ICT systemen/diensten worden uitbesteed heeft de klant geen volledige zeggenschap over de systemen/software. Om een pentest uit te mogen voeren op een uitbesteed informatiesysteem is er toestemming nodig van de partij waar het informatiesysteem staat.

Ook dient een pentest op een uitbesteed informatiesysteem met extra zorgvuldigheid worden uitgevoerd. Wanneer dit niet gebeurd kan het zijn dat andere klanten die ook hun informatiesysteem aan die partij hebben uitbesteedt hinder ondervinden of (financiële)schade op lopen.

Afwezigheid van pre-productiesysteem
Pentest die op het moment worden uitgevoerd bij grote organisaties worden vaak uitgevoerd op een systeem die nog niet beschikbaar is voor het publiek (pre-productie). Het voordeel van een pentest op pre-productie systeem is dat er uitgebreider gepentest kan worden, omdat het minder erg is als het systemen plat gaat of er (gebruikers)gegevens veranderd worden. Bij MKB pentesten zal het vaker voorkomen dat er geen pre-productie systemen aanwezig zijn, hier kan bijvoorbeeld voor gekozen zijn uit het oogpunt van kostenbesparing. Om te vermijden dat er gegevens op het systeem veranderd worden, het systeem plat gaat of andere gebruikers op het systeem last hebben van de pentest, zal het pentesten zorgvuldig moeten gebeuren.

Maakt meer gebruik van kant en klare oplossingen
De verwachting is dat het MKB minder gebruikt maakt van maatwerk en meer gebruik maakt van kant en klare oplossingen. Onder kant en klare oplossingen vallen bij voorbeeld webshop applicaties, CMS applicaties, portals, Cloud diensten, applicaties voor mobiele apparaten enz. Het voordeel van deze kant en klare pakketten is (omdat het door veel mensen gebruikt wordt) er goed naar de beveiliging is gekeken en wanneer er een kwetsbaarheid wordt gevonden het bedrijf van de applicatie het probleem (snel) kan oplossen. Het nadeel van deze pakketten is omdat veel mensen het gebruiken, het ook interessanter is voor mensen om in de applicatie kwetsbaarheden te vinden. Wanneer een dergelijk lek gevonden wordt is dit nieuws meestal snel op internet te vinden (16). Dan is het ook nog de vraag hoe snel de gebruiker de applicaties bijwerkt naar een nieuwe versie.

Voorbeelden van kant en klare applicaties:

CMS (17)	**Webshop** (18)	**Portal/Intranet** (19)	**Andere voorbeelden**
Wordpress	KonaKart	Sharepoint	Online boekhouding
Drupal	Zen Cart	Box.net	CRM applicaties
Joomla	OsCommerce	Glasscubes	HRM applicaties
ExpressionEngine	Magento	HyperOffice	Online offertes
TextPattern	Apache OFBiz	Google Site/Docs	Online back-up
Radiant CMS	PrestaShop		
Cushy CMS	Jentla		
SilverStripe	DashCommerce		
Alfresco	OpenCart		
TYPOlight	Batavi		

5.5 Meer dan pentest alleen

De nadruk van de MKB pentest ligt op het uitvoeren van de pentest en het leveren van de rapportage aan de klant. Wanneer blijkt dat er veel vraag is naar de MKB pentest kan de dienst voor het MKB worden uitgebreid. Hierbij kan worden gedacht aan verschillende mogelijkheden:

- **Periodieke pentest**
  De ontwikkeling in de ICT zit niet stil. Mede door de nieuwe ontwikkelingen worden er ook nieuwe kwetsbaarheden ontdekt. Een klant doet er dan ook goed aan om periodiek het informatiesysteem te controleren op kwetsbaarheden.
- **Problemen oplossen**
  Wanneer de pentest afgerond is krijgt de klant een lijst met kwetsbaarheden en een kort en bondig advies om het probleem om te lossen. Niet alle MKB organisaties hebben de expertise in huis om de problemen op te lossen. Deloitte zou de klant kunnen ondersteunen bij het oplossen van de problemen om de informatiebeveiliging te verbeteren.
- **Adviespartner**
  Zoals vermeldt wordt in hoofdstuk 4.1. is een pentest niet de oplossing voor alle informatiebeveiligingsproblemen. Deloitte zou voor het MKB een adviespartner kunnen worden op het gebied van informatiebeveiliging.
- **Informatiebeveiliging incidenten**
  Wanneer een MKB organisatie te maken krijgt met een (ernstig) informatiebeveiligingsincident is er niet altijd voldoende kennis in huis om het incident op te lossen. Toch moet het incident snelt opgelost worden omdat de organisatie veel (financiële)schade kan oplopen. Deloitte zou de klant kunnen ondersteunen om het incident onder controle te krijgen en op te lossen.
- **Andere diensten op het gebied van informatie beveiliging**
  Naast pentesting zou Deloitte ook andere diensten kunnen aanbieden die betrekking hebben met informatiebeveiliging zoals awareness trainingen, identity en acces management, business continuity management enz.

6. Onderdelen MKB pentest

In dit hoofdstuk wordt er inhoudelijk ingegaan op de onderdelen waaruit de MKB pentest zal bestaan. Deze onderdelen komen overeen met de MKB pentest processtappen die beschreven staan in hoofdstuk 5.3.

6.1 Onderdelen

Intake/portal

Het idee is om het intake proces digitaal te laten verlopen. Het voordeel hiervan is dat er tijd bespaard kan worden omdat niemand van Deloitte naar de klant hoeft voor een gesprek. De klant kan de pentest 24/7 aanvragen wanneer het voor hem uitkomt. Er zal nog wel een telefonisch contactmoment met de klant zijn tijdens de intake.

De digitale intake zou kunnen gebeuren via een portal. Om het moment heeft Deloitte al een portal ontwikkeld voor het MKB genaamd crtl.
Via de ctrl portal van Deloitte krijgen MKB klanten de gelegenheid om online samen te werken met hun Deloitte adviseur, kunnen ze gebruik maken van online diensten en toegang krijgen tot informatie die relevant is voor hun onderneming. Klanten kunnen via de portal ook nieuwe diensten aanvragen (in de vorm van een appstore).

De MKB pentest producten zou op deze pagina geplaatst kunnen worden zodat klanten een pentest kunnen aanvragen. Tijdens het aanvragen zal de klant gevraagd om een aantal gegevens in te vullen. Deze informatie kan worden gebruikt om de prijs te bepalen voor de pentest en meer inzicht te krijgen in wat voor soort pentest de klant precies wil.

De volgende gegevens zouden gevraagd kunnen worden voor de MKB pentest:

- Bedrijfsnaam
- Naam
- Emailadres
- Telefoonnummer
- Soort pentest product (Website, Mobile, etc)
- Aantal systemen die getest moeten worden
- Naam website (wanneer van toepassing)
- Productie/pre-productie
- Opmerkingen

Offerte/contract

Wanneer de klant via het ctrl portal een MKB pentest heeft aangevraagd dient deze aanvraag snel verwerkt te kunnen worden. Deze snelle verwerking is belangrijk om de doorlooptijd van het proces kort te houden en de prijs voor de MKB pentest laag te houden. Deze sneller verwerking kan alleen als de inhoud/scope van de pentest opdracht duidelijk is en er een standaard offerte/contract kan worden opgesteld.

Het bepalen van de inhoud/scope van het project kan voor een groot deel gebeuren via de intake. Wanneer er onduidelijkheden zijn kan er nog een (telefonisch) contact moment zijn met de klant. Als alle benodigde informatie binnen is kan er een offerte worden opgesteld. Voor de offerte zal een standaard template worden gemaakt die voldoet aan de Deloitte standaarden (zie hoofdstuk 7). Voor het bepalen van de prijs en benodigde uren voor de pentest zou een modulair schema gebruikt kunnen worden met vaste prijzen.

Een voorbeeld van een dergelijk schema is hieronder weergegeven. Aan de hand van het aantal te pentesten objecten en het soort pentest zou een vaste prijs bepaald kunnen worden. Een object kan een systeem/website/IP zijn. Omdat niet elke soort pentest even snel is uitgevoerd is er een verschil in uren en prijs aangegeven door middel van een kleur. Wanneer een klant meerdere soorten pentest wil kunnen de uren en bedragen opgeteld worden.

	MKB pentest producten (focus)			**Overige pentest producten**	
Aantal objecten/Soort MKB pentest	**Website**	**Mobile**	**Infra**	**configuratie**	**draadloos**
1 object	Uren: XX Prijs: €XXX	Uren: XX Prijs: €XXX	Uren: XX Prijs: €XXX	Uren: XX Prijs: €XXX	Uren: XX Prijs: €XXX
2 objecten	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX
3 objecten	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX
4 objecten	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX
5 objecten	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX
6 objecten	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX
7 objecten	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX	Uren: XX Prijs: €XXXX

Wanneer vaste prijzen worden gebruikt zou de offerte automatisch gegeneerd kunnen worden aan de hand van de klant en pentest gegevens. De offerte zal naar de klant worden gestuurd welke (digitaal) ondertekend kan worden.

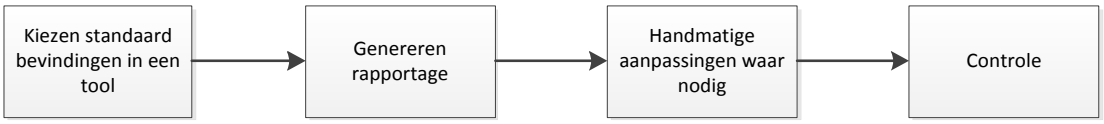
Een ander voordeel van het gebruik maken van standaard pentests en prijzen is dat de controle op de aanvraag voor de pentest sneller verwerkt kan worden omdat het minder maatwerk is.

Pentest
De pentest zal door een om meer pentesters worden uitgevoerd binnen de aangegeven scope en periode aan de hand van werkprogramma's. Voor elke soort pentest zal een ander werkprogramma beschikbaar zijn. De werkprogramma's voor de MKB pentest zullen gebaseerd worden op de normale pentest. Er zullen aanpassingen worden gemaakt aan de werkprogramma's om de pentest in een kortere tijd uit te kunnen voeren en irrelevante onderdelen voor het MKB zullen er uit gehaald worden.
De werkprogramma's worden opgebouwd aan de hand van standaarden (zie hoofdstuk 7).

Rapportage
De rapportage van de MKB pentest gebaseerd worden op de normale pentest rapportage. Aanpassingen zullen o.a. gemaakt worden in het design van de rapportage, de rapportage zal meer gebaseerd worden op standaard bevindingen en er zal een andere vorm van management samenvatting komen.
De wens is om de management samenvatting bondiger en minder technisch te maken, ook dienen de resultaten van de pentest grafisch weergegeven te worden in één duidelijk schema.

De verwachting is dat het MKB veel gebruikt maakt van kant en klare software (zie hoofdstuk 5.2). Het voordeel hiervan is wanneer versie x.x applicatie bij de ene klant gebruikt wordt, dezelfde kwetsbaarheden ook bij andere klanten zijn die zelfde versie applicatie gebruiken. Voor deze kwetsbaarheden kunnen deels standaard bevindingen worden gemaakt om tijd te besparen.

In het maken van een pentest rapportage gaat veel tijd zitten, tijd die er niet is tijdens een MKB pentest. Een groot deel van het maken van de pentest zal geautomatiseerd kunnen worden, waardoor een hoop tijd bespaard kan worden. Het generen van de rapportage zal kunnen gebeuren door het zelf ontwikkelen van een tool. Onder andere kunnen de bevindingen, het risico van de bevinding, de kans dat de kwetsbaarheden misbruikt worden, hoe de kwetsbaarheden opgelost kunnen worden en het bevindingenschema voor de managementsamenvatting automatisch gegenereerd worden.



Presentatie
Om ook tijdens de laatste stap van het pentestproces tijd te besparen zou de presentatie digitaal gegeven kunnen worden aan de klant in de vorm van een webinar (online seminar). Ook kan de rapportage en presentatie aangeboden worden op het cntrl portal in een beschermde omgeving. Hier zou de klant (wanneer hij periodiek een pentest uit laat voeren) de informatiebeveiliging in de gaten kunnen houden op een dashboard. Voordat deze gegevens op internet komen te staan zal er onderzocht moeten worden of de bescherming van deze gegevens gewaarborgd kan worden omdat het om gevoelige informatie gaat. Wanneer deze gegevens op straat belanden weten de "hackers" precies waar de kwetsbaarheden zitten en hoe deze misbruikt kunnen worden.

6.2 Tooling

Het makkelijkst zou zijn als er een tool bestond die de pentest geheel geautomatiseerd kan uitvoeren. Alleen een dergelijk alles omvattende tool bestaat niet, er zijn wel tools die beweren een volledige pentest uit te kunnen voeren alleen deze rapporteren veel false postivives (een bevinding die niet bestaat). Als Deloitte alleen tooling zou draaien tijdens een pentest zal er geen meerwaarde worden geleverd dan wanneer de klant zelf de tool zou draaien. Juist door handmatig te pentesten, te denken als een echte "hacker" en met de klant mee te denken kan er een kwalitatief goede pentest worden uitgevoerd. Mede hierdoor onderscheid Deloitte zich van andere pentest organisaties.
Ook voor de MKB pentest dient deze kwaliteit gewaarborgd te worden omdat het image van Deloitte anders in geding komt. Veel handmatig werk kost alleen veel tijd. Om toch tijd te besparen tijdens de MKB pentest kunnen sommige tools helpen bij het vinden van kwetsbaarheden. Deze kwetsbaarheden zullen wel handmatig geverifieerd worden.

Hieronder is een lijst beschreven van tooling die gebruikt kan worden tijdens de MKB pentest. Per tool is ook beschreven wat het doel is van het programma. Het merendeel van de tooling wordt al gebruikt in de normale pentest.

- **Nessus**
  Nessus is een uitgebreide geautomatiseerde scanner die zoekt naar kwetsbaarheden. Nessus kijkt onder andere naar open porten op systemen, software versies en exploit mogelijkheden. Aan het einde van een scan kan nessus een uitgebreid rapport genereren.
- **Nmap**
  Nmap is een snelle gratis port scanner. Ook heeft de scanner de mogelijkheid om de versie van de gebruikte software te detecteren.
- **Wireshark**
  Wireshark is gratis software die network pakketten kan loggen en analyseren. Deze software kan ook worden gebruikt om een log van de pentest bij te houden.
- **Secunia**
  Secunia is er op gericht om te controleren of de gebruikte software op een systeem bijgewerkt is tot de laatste versie.
- **Nikto**
  Nikto is een open source webserverscanner. Nikto kan onder andere zoeken naar kwetsbare bestanden op de webserver, detecteren van de gebruikte software en kan zoeken naar mappen die gebruikt worden op de webserver.
- **Burp**
  Burp is een software proxy waarmee je tussen de browser en de webserver kan zitten (man-in-the-middle). Door deze mogelijkheid kan communicatie tussen de browser en de webserver worden onderschept en waar nodig aangepast worden.
- **W3AF**
  w3af is een Web Application Aanval en Audit Framework. Met deze software kunnen kwetsbaarheden op een website worden gevonden.
- **WPscan**
  Software gericht om kwetsbaarheden in het CMS WordPress en WordPress plugins te vinden. Kan ook gebruikersnamen opzoeken.
- **Joomscan**
  Software gericht om kwetsbaarheden in het CMS Joomla en Joomla plugins te vinden. Kan ook gebruikersnamen opzoeken.

7. Standaarden

De pentest kan niet "uit de losse pols" ontwikkeld worden. Alle diensten/producten binnen Deloitte moeten voldoen aan een aantal standaarden. Ook kunnen externe standaarden gebruikt worden voor de ontwikkeling van de pentest. Deze standaarden dragen bij aan de kwaliteit van de pentest en het wiel wordt niet opnieuw uitgevonden. Ook kan een pentest die gebaseerd is op stadaarden sneller uitgevoerd worden dan een pentest die "ad-hoc" uitgevoerd wordt, omdat de standaarden "best practices" bevatten.

Interne standaarden

Een interne standaard die gebruikt kan worden voor de MKB pentest is de Deloitte Policy Manual. In dit document staat beschreven waar bepaalde documenten aan moeten voldoen.
Documenten die gebruik gaan worden voor de MKB pentest en moeten voldoen aan deze standaard zijn:

- Standaard templates
- Standaard offerte
- Pentest werkprogramma's
- Rapportages

Externe Standaarden

Er zijn een aantal externe partijen die standaarden hebben opgezet op het gebied van pentesting. Deze standaarden kunnen gebruikt worden voor de ontwikkeling van de pentest en zullen bijvoorbeeld verwerkt worden in het werkprogramma.

OWASP

De Open Web Application Security Project (OWASP) is een non-profit organisatie die zich richt op het verbeteren van de beveiliging van applicatiesoftware. OWASP houdt ook een top 10 bij van meest voorkomende kwetsbaarheden op het gebied van webapplicaties.
Website: https://www.owasp.org

W3C

Het World Wide Web Consortium (W3C) is een organisatie die de webstandaarden voor het World Wide Web ontwerpt, zoals HTML, XHTML, XML en CSS. W3C stelt ok standaarden op voor het beveiligen van een web site/applicatie.
Website: http://www.w3.org/

OVAL

OVAL is een openbare informatiebeveiliging community die zich inspant om het rapporteren van kwetsbaarheden te standaardiseren. OVAL behoort tot de organisatie MITRE die ook de kwetsbaarheden standaard taal CVE heeft ontwikkeld.
Website: http://oval.mitre.org

NIST
Het National Institute of Standards and Technology (NIST) is een wetenschappelijke instelling die onder de Amerikaanse federale overheid valt. Het NIST zet zich in voor standaardisatie in de wetenschap, zoals het definiëren van eenheden. Het NIST houdt ook een database bij van kwetsbaarheden op het gebied van informatiebeveiliging.
Website: http://nvd.nist.gov/

SANS
Het SANS instituut werd opgericht in 1989 als een gezamenlijk onderzoeks en educatie organisatie. SANS bestaat uit vele security experts over de hele wereld, ze werken samen om de wereld van informatiebeveiliging te helpen en te verbeteren.
Website: http://pen-testing.sans.org/

8. Uitbesteding

Bij het uitvoeren van een pentest gaan de meeste kosten zitten in de uren van de pentesters. Een deel van de uren wordt besteed aan het starten van tooling en het rapporteren van de resultaten. Voor de tooling gelden bij elke pentest dezelfde instellingen. Deze werkzaamheden zou uitbesteed kunnen worden aan Deloitte India. De werknemers daar kunnen via werkprogramma's hetzelfde werk uitvoeren en rapporteren aan de pentester in Nederland. Door de uitbesteding kunnen kosten bespaard worden, wat de MKB pentest goedkoper maakt.

De uitbesteding wordt niet in de uitwerking van de pentest meegenomen omdat dit buiten de scope van het project valt.

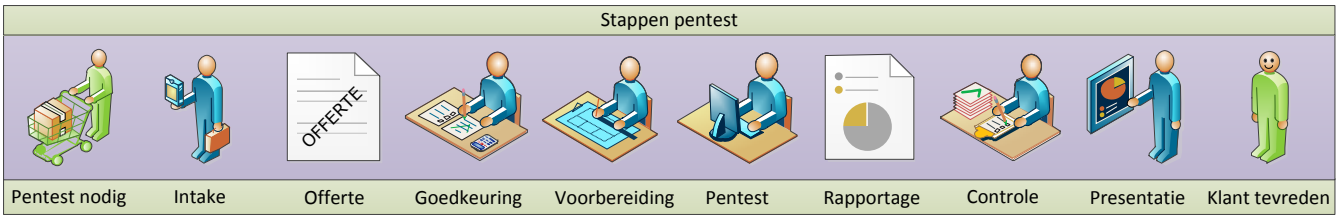
9. Samenvatting

Uit het vooronderzoek blijkt dat MKB organisaties behoefte hebben aan een pentest. Ook is duidelijk geworden dat de bestaande pentest niet goed aansluit aan de behoefte van MKB organisaties. Het ontwerp voor de MKB pentest is gebaseerd op de wensen en eisen die in kaart zijn gebracht tijdens de requirements analyse en op de bevindingen van het vooronderzoek. Het ontwerp van de MKB pentest is deels gebaseerd op de huidige pentest van Deloitte. Op de volgende punten verschilt de MKB pentest zich van de normale pentest:

- **Soorten pentest**
  Er zijn verschillende soorten pentest die uitgevoerd kunnen worden, alleen niet alle soorten pentests sluiten aan op MKB organisaties. De focus zal liggen op de volgende pentest producten:

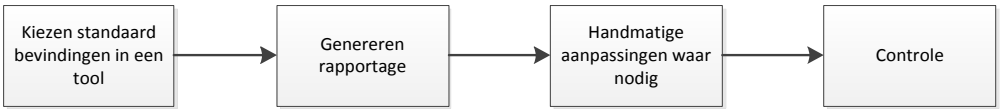
Website	Mobile	Infra
		
• Kwetsbaarhedenscan website • Kwetsbaarhedenscan webserver	• Kwetsbaarhedenscan mobiele-applicatie • Kwetsbaarhedenscan mobiel-apparaat	• Kwetsbaarhedenscan infrastructuur

- **Aanpak**
  Omdat voor een MKB pentest de tijd en kosten beperkt moeten blijven zullen de pentests aangepakt worden vanuit een "white" of "grey" box, waar al een deel van de informatie beschikbaar wordt gesteld door de klant. Hierbij kan worden gedacht aan onder andere ip gegevens, inlog gegevens, softwareversie en infrastructuur gegevens. Deze gegevens worden tijdens de intakefase aangeleverd.
- **MKB Pentest processtappen**
  Het MKB pentestproces is in het onderstaande schema versimpeld weergegeven.



- **Intake**
  Het idee is om het intake proces digitaal te laten verlopen. Het voordeel hiervan is dat er tijd bespaard kan worden omdat niemand van Deloitte naar de klant hoeft voor een gesprek. De digitale intake zou kunnen gebeuren via de Deloitte voor MKB ontwikkelde ctrl portal.
- **Offerte**
  Voor het bepalen van de prijs en benodigde uren voor de pentest zal een modulair schema gebruikt gaan worden met vaste prijzen.

- **Pentest**
  De werkprogramma's voor de MKB pentest zullen gebaseerd worden op de normale pentest. Er zullen aanpassingen worden gemaakt aan de werkprogramma's om de pentest in een kortere tijd uit te kunnen voeren en irrelevante onderdelen voor het MKB zullen er uit gehaald worden.
- **Rapportage**
  In het maken van een pentest rapportage gaat veel tijd zitten, tijd die er niet is tijdens een MKB pentest. Een groot deel van het maken van de pentest zal geautomatiseerd kunnen worden, waardoor een hoop tijd bespaard kan worden. Het generen van de rapportage zal kunnen gebeuren door het zelf ontwikkelen van een tool.



- **Presentatie**
  Om ook tijdens de laatste stap van het pentestproces tijd te besparen zou de presentatie digitaal gegeven kunnen worden aan de klant in de vorm van een webinar (online seminar). Ook kan de rapportage en presentatie aangeboden worden op het cntrl portal in een beschermde omgeving.
- **Tooling**
  Voor de MKB pentest zal merendeels dezelfde tooling gebruikt gaan worden als de normale pentest. Er zal extra tooling gebruikt gaan worden voor veel voorkomende systemen in het MKB (zoals CMS systemen).
- **Uitbesteding**
  Een deel van de MKB pentest bestaat uit het uitvoeren van tooling en het rapporteren van de resultaten. Deze stap zou uitbesteed kunnen worden aan Deloitte India om kosten te besparen.
- **Meer dan pentest alleen**
  Wanneer blijkt dat er veel vraag is naar de MKB pentest kan de dienst voor het MKB worden uitgebreid onder andere met periodieke pentests, hulp bij oplossen van incidenten, Deloitte als adviespartner)

Aandachtspunten MKB

Om de pentest goed aan te laten sluiten op het MKB moet er rekening worden gehouden met de manier van werken binnen het MKB.

- **Externe partijen**
  In het MKB worden veel activiteiten uitbesteed zodat de organisatie zich kan richten op hun eigen product/dienst. Uitbesteding heeft gevolgen voor het afnemen van een pentest.
- **Afwezigheid van pre-productiesysteem**
  Bij MKB pentesten zal het vaker voorkomen dat er geen pre-productie systemen aanwezig zijn. Om te vermijden dat er gegevens op het systeem veranderd worden, het systeem plat gaat of andere gebruikers op het systeem last hebben van de pentest, zal het pentesten zorgvuldig moeten gebeuren.
- **Maakt meer gebruik van kant en klare oplossingen**
  De verwachting is dat het MKB minder gebruikt maakt van maatwerk en meer gebruik maakt van kant en klare oplossingen. Onder kant en klare oplossingen vallen bij voorbeeld webshop applicaties, CMS applicaties, portals, Cloud diensten, applicaties voor mobiele apparaten enz.

10. Bronnenlijst:

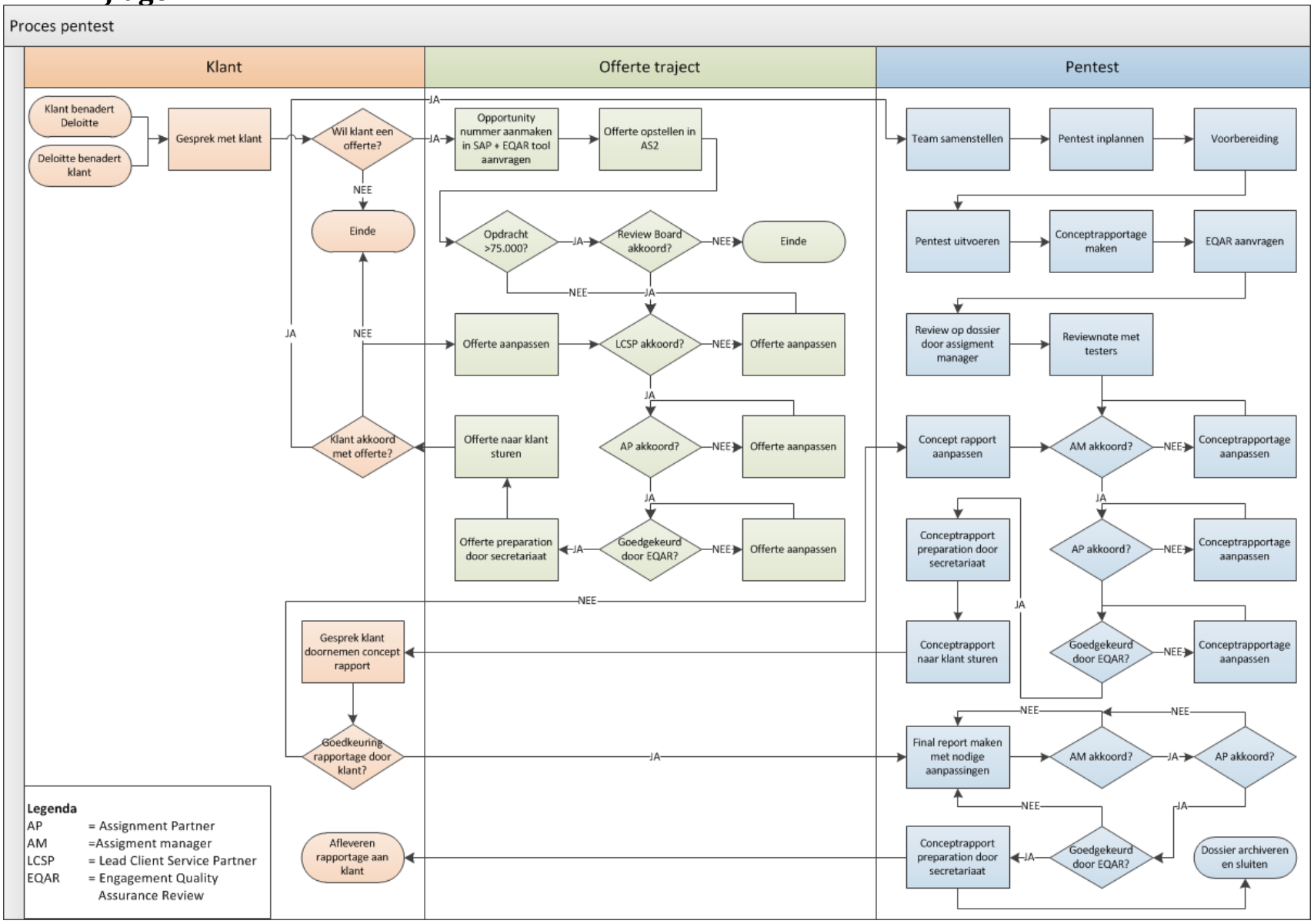
Dit is een lijst van gebruikte bronnen in dit document:

De gebruikte bronnen staan als volgt genoteerd:
[Bron nummer] Achternaam auteur, voorletter(s) of Titel van het document / de website. *Organisatie*. [Bron soort] Publicatiejaar of update. [Geopend op.] URL van website.

1. **Wikipedia.** Penetration test. *Wikipedia.* [Online] 15 December 2011. [Citaat van: 16 December 2011.] http://en.wikipedia.org/wiki/Penetration_test.
2. **Jonathan Gershater, Puneet Mehta.** What is Penetration Testing? *SecPoint.* [Online] [Citaat van: 16 December 2011.] http://www.secpoint.com/what-is-penetration-testing.html.
3. Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010. *GovCERT.* [Online] GovCERT, November 2010. http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/trendrapporten/trendrapport-2010.html.
4. **ISIS.** ISIS - MKB ICT Onderzoek 2009. *consultancy.nl.* [Online] ISIS, September 2009. http://www.consultancy.nl/rapporten/deloitte/mkb-ict-onderzoek-2009.
5. **Young, Ernst &.** ICT Barometer over. *ICT barometer.* [Online] Ernst & Young, 2011. http://www.ict-barometer.nl/_files-cms/File/Rapport%20onderzoeksresultaten%20ICT%20Barometer%20over%20cybercrime%202011.pdf.
6. **Symantec.** Symantec 2010 SMB Information Protection Survey. *Symantec.* [Online] Symantec, November 2010. http://www.symantec.com/content/en/us/about/media/pdfs/SMB_ProtectionSurvey_2010.pdf.
7. **Metro.** Kleine bedrijven dupe cybercrime. *Metro.* [Online] Metro, 16 November 2010. http://www.metronieuws.nl/nieuws/kleine-bedrijven-dupe-cybercrime/SrZjkp!OqunuyNweMAbo/.
8. Informatiebeveiliging. *Wikipedia.* [Online] 30 December 2011. http://nl.wikipedia.org/wiki/Informatiebeveiliging.
9. **Infosecurity.** Mkb stuwt wereldwijde vraag naar security. *Infosecurity.* [Online] 22 December 2011. http://www.infosecurity.net/Nieuws/77952/Mkb-stuwt-wereldwijde-vraag-naar-security.
10. **EMC.** EMC GEEFT DE 10 IT-TRENDS AAN VOOR 2012. *Binnenlands Bestuur.* [Online] 3 Januari 2012. http://www.binnenlandsbestuur.nl/digitaal-besturen/partners/emc/emc-geeft-de-10-it-trends-aan-voor-2012.3427400.lynkx.
11. **Gartner.** Gartner's Top Predictions for IT Organizations and Users, 2012 and Beyond: Control Slips Away. *Gartner.* [Online] Gartner, 2012. http://www.gartner.com/technology/innovation/it-predictions-2012.jsp?prm=TW_CHINNV.
12. **Group, SMB.** 2012 Top 10 SMB Technology Market Predictions. *SMB Group.* [Online] 2012.
13. **Bueters, Philip.** De IT trends van 2012. *Management Team.* [Online] 30 December 2011. http://www.mt.nl/95/54709/ict/de-it-trends-van-2012.html.
14. **Week, Information.** 4 Tech Trends For SMBs In 2012. *Information Week.* [Online] 14 December 2012. http://www.informationweek.com/news/smb/ebusiness/232300521.
15. **Young, Ernst &.** ICT Barometer over . *ict-barometer.nl.* [Online] Ernst & Young, Februari 2011. http://www.ict-barometer.nl/_files-cms/File/ICT%20Barometer%20-%20Business%20Process%20Outsourcing.pdf.

16. **Security.nl.** 4.000 gehackte WordPress blogs vergiftigen Google. *Security.nl.* [Online] Augustus 2011. http://www.security.nl/artikel/38043/4.000_gehackte_WordPress_blogs_vergiftigen_Google.html.
17. **Stansberry, Glen.** Top 10 Most Usable Content Management Systems. *Glen Stansberry.* [Online] Net Tuts, Augustus 2009. http://net.tutsplus.com/articles/web-roundups/top-10-most-usable-content-management-systems/.
18. **Lazaris, Bryan.** 10 best Ecommerce dominant shopping cart applications. *Webgranth.* [Online] September 2011. http://www.webgranth.com/10-best-ecommerce-dominant-shopping-cart-applications.
19. **Mosher, Barb.** SharePoint Portal Alternatives - A Credible List. *cmswire.* [Online] cmswire, Maart 2010. http://www.cmswire.com/cms/enterprise-cms/sharepoint-portal-alternatives-a-credible-list-005080.php.
20. Trendstudie MKB en . *Ondernemerschap.* [Online] ondernemerschap, Maart 2011. http://www.ondernemerschap.nl/sys/cftags/assetnow/design/widgets/site/ctm_getFile.cfm?file=A201103.pdf&perId=596.

Bijlage A


Proces pentest
Klant
Offerte traject
Pentest
Klant benadert Deloitte
Deloitte benadert klant
Gesprek met klant
Wil klant een offerte?
JA
NEE
Einde
Opportunity nummer aanmaken in SAP + EQAR tool aanvragen
Offerte opstellen in AS2
Opdracht >75.000?
Review Board akkoord?
Offerte aanpassen
LCSP akkoord?
AP akkoord?
Goedgekeurd door EQAR?
Offerte preparation door secretariaat
Offerte naar klant sturen
Klant akkoord met offerte?
Gesprek klant doornemen concept rapport
Goedkeuring rapportage door klant?
Afleveren rapportage aan klant
Team samenstellen
Pentest inplannen
Voorbereiding
Pentest uitvoeren
Conceptrapportage maken
EQAR aanvragen
Review op dossier door assigment manager
Reviewnote met testers
Concept rapport aanpassen
AM akkoord?
Conceptrapportage aanpassen
Conceptrapport preparation door secretariaat
Conceptrapport naar klant sturen
Final report maken met nodige aanpassingen
Conceptrapport preparation door secretariaat
Dossier archiveren en sluiten
Legenda
AP = Assignment Partner
AM =Assigment manager
LCSP = Lead Client Service Partner
EQAR = Engagement Quality Assurance Review

Deloitte.

Pentest Report
<company>

Amstelveen

Maart 2012

Deloitte Accountants B.V.
Risk Services
Laan van Kronenburg 2
1183 AS Amstelveen
Postbus 175
1180 AD Amstelveen

Tel: +31 (0) 88 288 28 88
Fax: +31 (0) 88 288 97 11
www.deloitte.nl

Vertrouwelijk en uitsluitend voor intern gebruik

Dit document is verstrekt aan <Klant> door Deloitte Accountants BV (Deloitte). Onze algemene voorwaarden, beschreven in “Offerte <titel offerte>” (ref. <referentie>) d.d. <datum offerte>, zijn van toepassing op dit document.

Deze rapportage is gebaseerd op onze werkzaamheden en is enkel bedoeld voor intern gebruik bij <klant> voor het in de onderzoeksvraag opgenomen doel. Verspreiding naar derden is slechts toegestaan na voorafgaande schriftelijke toestemming van Deloitte.

Dit rapport bevat geen conclusies of een andere vorm van zekerheid over de financiële huishouding, interne beheersing maatregelen of het voldoen aan wet- en regelgeving van <klant>.

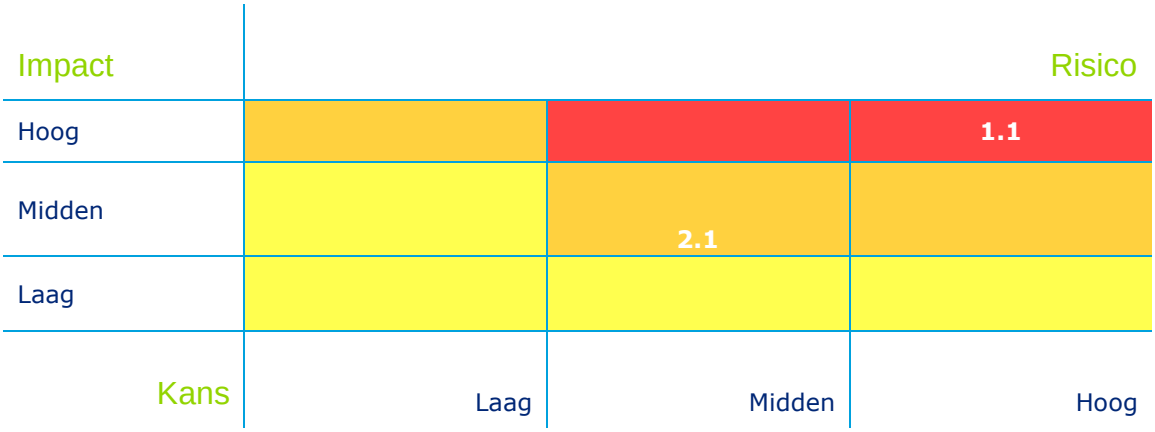
Management Samenvatting

In opdracht van <klant> heeft Deloitte een MKB Security Test uitgevoerd op [naam infrastructuur] [naam web applicatie] [naam mobiele applicatie] van <klant>. Dit rapport bevat een overzicht van de observaties op basis van onze MKB Security Test die is uitgevoerd in de tijdsperiode <start – eind>.

Tijdens onze MKB Security Test voor <klant> hebben wij een aantal kwetsbaarheden geïdentificeerd. Onderstaande opsomming geeft een overzicht van de belangrijkste geïdentificeerde kwetsbaarheden:

- <Omschrijving kwetsbaarheid 1>
- <Omschrijving kwetsbaarheid 2>

In onderstaande tabel is een overzicht gemaakt van de verschillende aangetroffen kwetsbaarheden en het risico dat de kwetsbaarheid met zich meebrengt.



NB: Bijna dagelijks verschijnen nieuwe kwetsbaarheden in IT componenten. De werkzaamheden zijn in een korte periode uitgevoerd en betreffen een momentopname. Derhalve hebben wij tijdens de werkzaamheden uitsluitend getest op kwetsbaarheden die ten tijde van de werkzaamheden bij ons bekend waren en hebben wij uitsluitend systemen getest die op het moment van testen benaderbaar waren. Daar wij de tests in beperkte tijd hebben uitgevoerd, kunnen wij geen zekerheid geven dat wij alle tekortkomingen in de benaderbare aangegeven IP adressen hebben opgemerkt.

1. Project Overzicht

Introtext

1.1 Achtergrond en opdrachtformulering

<Klant> heeft Deloitte gevraagd om een MKB Security Test uit te voeren op [naam infrastructuur] [naam web applicatie] [naam mobiele applicatie]. Doel van de MKB Security Test was aan te geven waar eventuele tekortkomingen zijn in de beveiliging.

1.2 Aanpak

Infrastructuur

Wij hebben een security test uitgevoerd op de IP adressen en poorten zoals aan ons ter beschikking gesteld. Door middel van deze test hebben wij een aanval gesimuleerd van een kwaadwillende persoon op de internetomgeving. Als onderdeel van onze werkzaamheden hebben wij getracht kwetsbaarheden te identificeren in beveiligingsmaatregelen getroffen op het niveau van netwerk, firewall en besturingssysteem van het onderliggende systeem.

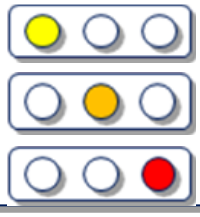
Applicatie

Wij hebben een een applicatie security test uitgevoerd op de webapplicatie vanuit het gezichtspunt van zowel een niet-geautoriseerde bezoeker als een geautoriseerde gebruiker. De test geeft inzicht in veel voorkomende web applicatie kwetsbaarheden, zoals SQL-injectie, Cross-site scripting (XSS), input validatie en kwetsbare management interfaces. Bovendien geeft deze test inzicht in tekortkomingen op het gebied van rechten binnen de applicatie (bijvoorbeeld: kan ik andermans gegevens inzien?).

De kwetsbaarheden en bijbehorende risico's die tijdens de security scan worden gevonden, zullen wij in een rapportage aan UVIT opleveren. Deze rapportage zal ook specifieke aanbevelingen geven ter voorkoming / beperking van de kwetsbaarheden.

1 Zwak Wachtwoordbeleid

Betreffende host(s)	
.	Kans Impact Risico



Observatie

We hebben vastgesteld dat het mogelijk is een zwak wachtwoord te kiezen voor gebruiker accounts. Geen strikt wachtwoordbeleid is aanwezig dat gebruikers verplicht om een sterk wachtwoord te kiezen. We hebben vastgesteld dat het mogelijk was een wachtwoord met een lengte van slechts één karakter, zoals enkel de letter „a" te kiezen. Zwakke wachtwoorden zijn makkelijker te raden of te kraken door middel van een bruteforce-aanval.

Kans

Impact

In het geval van een succesvolle aanval heeft de aanvaller toegang tot functionaliteiten waartoe individuele gebruikers- of beheerdersaccounts zijn geautoriseerd.

Aanbeveling

We bevelen aan strikte wachtwoordinstellingen te implementeren voor de gebruikers accounts van de <applicatie>. De wachtwoordinstellingen zouden een minimum lengte en complexiteit moeten afdwingen.

Deze observatie is gerelateerd aan OWASP Top-10 issue A3 – Broken Authentication and Session Management.

1.1 Screenshot

Call-out omschrijving belangrijkste onderdelen.

Bijlage 1 – Deloitte Risico Definities

Dit overzicht beschrijft de attributen van de zwakheden zoals benoemd in dit rapport.

Kans

Hoog: De kwetsbaarheid is gemakkelijk te exploiteren. Weinig informatie is vereist om dit probleem te exploiteren of een instrument voor de exploitatie is gemakkelijk te verkrijgen en te gebruiken. Geen effectieve maatregelen zijn getroffen om te voorkomen dat het probleem plaatsvindt.
Gemiddeld: De kwetsbaarheid is lastiger te exploiteren. Meer informatie is vereist of kennis is nodig voor het gebruiken van exploitatie instrumenten om misbruik te maken van de kwetsbaarheid. Een paar effectieve maatregelen zijn getroffen om te voorkomen dat het probleem plaatsvindt. Echter, het niveau van de maatregelen laat ruimte over voor verbetering.

Laag: De kwetsbaarheid is moeilijk te exploiteren. Exploitatie vereist specialistische kennis of gedetailleerde kennis van de technische implementatie door de organisatie. Daarnaast zijn effectieve maatregelen getroffen om te voorkomen dat het probleem plaatsvindt.

Impact

Hoog: Gebeurtenissen die een directe dreiging zouden vormen voor de discretie en integriteit van financiële en/of persoonlijke informatie van een groot aantal personen als ze plaatsvinden. Het geïdentificeerde probleem kan de organisatie zowel financieel als juridisch schaden en daarnaast kan het leiden tot imagoverlies.
Gemiddeld: Gebeurtenissen die een directe dreiging zouden vormen voor de discretie en integriteit van financiële en/of persoonlijke informatie van een klein aantal personen als ze plaatsvinden; of exploitatie van het probleem voorziet de inbreker van ongeautoriseerde toegang tot systemen of andere middelen wat ondersteuning biedt bij het uitvoeren van verdere aanvallen.
Laag: Het probleem leidt tot publicatie van technische informatie of het verhoogt de kans op succesvolle aanvallen. Dit probleem leidt niet direct tot ongeautoriseerde toegang, noch vormt het een directe dreiging voor de discretie en integriteit van financiële en/of persoonlijke informatie.

Afleiden van Risiconiveau

Het risico van observaties is gebaseerd op de Kans en Impact rating van de observatie. Hierin is gekozen om de impact zwaarder te laten wegen dan de kans in de bepaling van het risico.

Deloitte Risiconiveau	=	Kans	x	Impact
Hoog	=	Hoog	x	Hoog
Hoog	=	Gemiddeld	x	Hoog
Gemiddeld	=	Hoog	x	Gemiddeld
Gemiddeld	=	Gemiddeld	x	Gemiddeld
Gemiddeld	=	Laag	x	Hoog
Laag	=	Hoog	x	Laag
Laag	=	Gemiddeld	x	Laag
Laag	=	Laag	x	Gemiddeld
Laag	=	Laag	x	Laag

Deloitte Risiconiveau

Hoog: IT Management wordt direct geïnformeerd over de observatie, mogelijke aanvallen en mitigerende scenario's.
Gemiddeld: IT Management wordt regelmatig geïnformeerd over de observaties en mitigatie van de observaties.
Laag: IT Management wordt geïnformeerd als onderdeel van de volledige rapportage van de observaties en tracking.

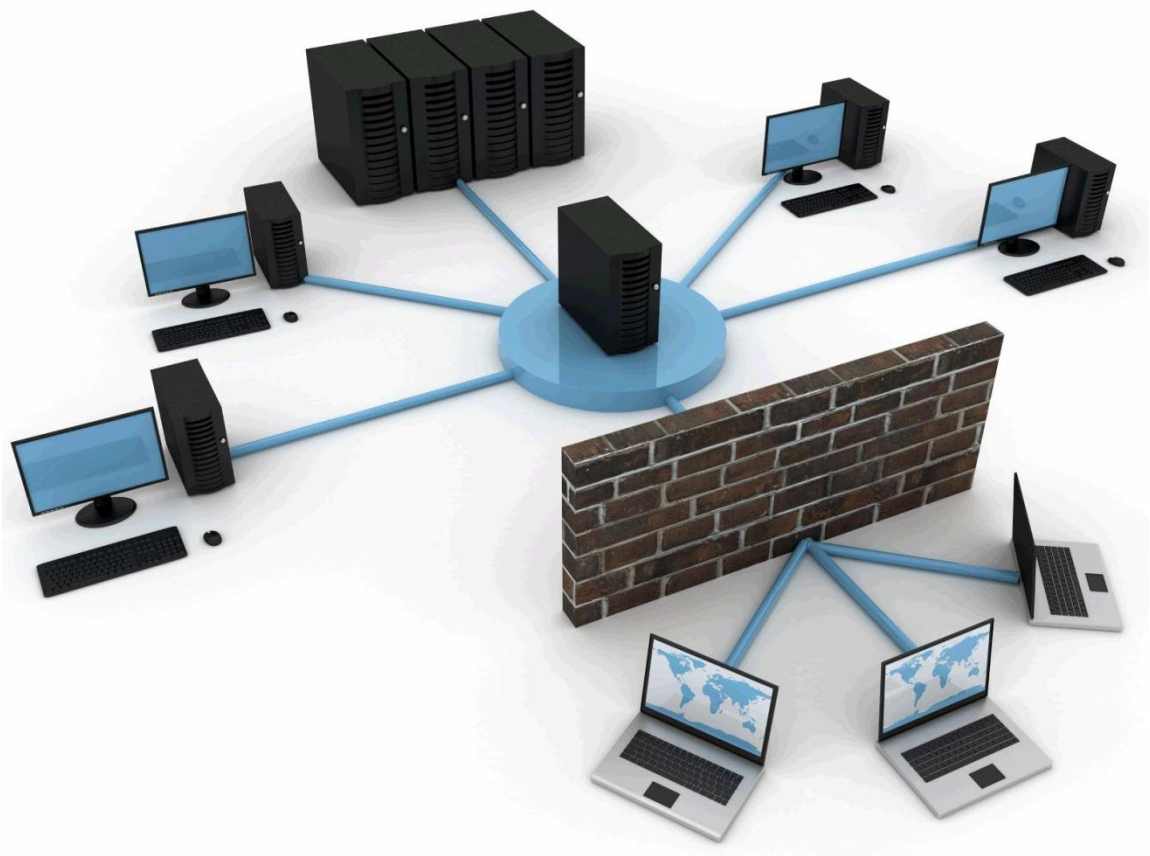
www.deloitte.nl

Requirements analyse

Ontwikkeling MKB pentestproduct

Naam: Werner Alsemgeest
Studentnummer: 08022488
Instituut: De Haagse Hogeschool
Opleiding: Information Security Management
Afstudeerstage bedrijf: Deloitte
Begeleider Hogeschool: Ellen Wesselingh
Begeleider Deloitte: Tom Schuurmans

Datum: 20 januari 2012
Versie: 0.3



Versiehistorie

Versienummer	Versiedatum	Controle door:	Wijzigingen
0.1 (Concept)	09-12-2011	Werner Alsemgeest	Opzet concept
0.2	19-12-2011	Werner Alsemgeest	Wijzigingen na feedback Tom Schuurmans
0.3	09-01-2012	Werner Alsemgeest	Wijziging na feedback Mark Van Zwam

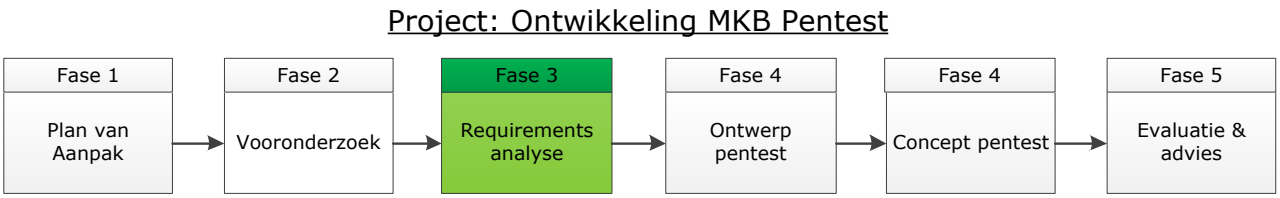
Distributielijst

Versienummer	Datum	Naam	Organisatie
0.1	12-12-2011	Tom Schuurmans	Deloitte
0.2	19-12-2011	Tom Schuurmans	Deloitte

Inhoud

1. Inleiding

Dit document is een onderdeel van het project "Ontwikkeling MKB pentest" in opdracht van Deloitte Nederland te Amstelveen. Dit document bevat fase 3 van het project. In de onderstaande schematische weergave is de plek van dit document (groen gekleurd) in het projectoverzicht weergegeven. Voor meer informatie over het project zie het document "Plan van Aanpak".



Met behulp van de requirements analyse zijn de wensen en eisen in kaart gebracht voor de nog te ontwikkelen pentest voor het MKB. De wensen en eisen komen van de mensen die betrokken zijn bij de ontwikkeling van de pentest voor het MKB. Mensen die waardevolle input geleverd hebben zijn:

Naam	**Rol in het project**
Marko Van Zwam	opdrachtgever
Vojtech Brtnik	pentest expert
Tom Schuurmans	begeleider
Nick Kirtley	pentest expert
Derk Wieringa	Belanghebbende

De scope van de requirements beperken zich tot de wensen en eisen van mensen die betrokken zijn bij het project voor het ontwikkelen van een MKB pentest product.

In hoofdstuk twee worden de kernwaarden voor de MKB pentest beschreven. In het hoofdstuk daarna worden de wensen en eisen in kaart gebracht voor de MKB pentest.

2. Kernwaarden

Voor de MKB pentest zijn een aantal kernwaarden opgesteld. Deze kernwaarden zijn de belangrijkste doelen die behaald dienen te worden met de MKB pentest.

- **Korte doorlooptijd**
  Deloitte en de klant zijn beide gebaat bij een kortere doorlooptijd van de pentest. Hoe langer de pentest duurt hoe meer het gaat kosten voor beide partijen.
- **Lage kosten**
  De meeste MKB organisaties hebben kleinere budgeten voor IT security dan Enterprise organisaties. Een MKB organisatie zal eerder een pentest afnemen wanneer er een laag prijskaartje aan de pentest hangt.
- **Kwalitatief goed**
  Ook al wordt er op de doorlooptijd en de kosten ingekort toch moet de kwaliteit van de pentest hoog blijven. Wanneer dit niet gebeurd zal het imago van Deloitte geschaad kunnen worden. Tevens hechte de meeste klanten veel waarde aan de resultaten van een pentest. Wanneer bijvoorbeeld de bevindingen niet op orde zijn, kan de klant onterecht denken dat zijn informatiesysteem veilig is. Het dient een rapportage te worden waarin zowel technisch aspecten als risico's helder beschreven worden.

In de volgende tabel is te zien hoe er met behulp van de requirements aan de kernwaardes gewerkt gaat worden. Een beschrijving van de requirements is te vinden in het volgende hoofdstuk.

Requierement/Kernwaarde	**Korte doorlooptijd**	**Lage kosten**	**Kwalitatief goed**
Automatische rapportage	✓	✓	
Portaal	✓	✓	
Werkprogramma voor het MKB			✓
Veilige opslag van informatie			✓
Bijwerken standaard observaties			✓
Pentest meer automatiseren	✓	✓	
Aanpassen rapportage			✓
Benchmark database			

3. Requirements

De requirements zijn verdeeld in twee categorieën de "must have's" en "nice to have's". De must have's zijn punten die in de MKB pentest dienen te komen. De nice te have's zijn punten die handig zijn om te hebben in het product, maar niet benodigd zijn voor het behalen van de doelstellingen van de MKB pentest.

Must have

- **Automatische rapportage**
  Het maken van een pentest rapport kost veel werk, dit kan voor een groot deel geautomatiseerd worden om tijd (en geld) te besparen.
- **Portaal**
  Bij een normale pentest vinden er verschillende gesprekken plaats (bijvoorbeeld een intakegesprek of een presentatie van de rapportage) tussen de klant en Deloitte. Om dit proces te versnellen en kosten te besparen dient het mogelijk te worden om deze stappen digitaal uit te voeren. Klanten dien in te kunnen loggen op een digitaal portaal om o.a. een aanvraag te doen voor een pentest, pentest rapportages te bekijken, voortgang van informatie beveiliging te monitoren enz.
- **Werkprogramma voor MKB pentest**
  Het huidige werkprogramma voor een pentest kost te veel tijd om volledig uit te voeren in de beperkte tijd die beschikbaar is voor een MKB pentest. Het werkprogramma dient ingekort te worden en te worden toegespitst op MKB organisaties. Afhankelijk van de wensen van de klant wordt een deel van het werkprogramma uitgevoerd (bijvoorbeeld alleen een infrastructuur pentest). Tevens moet de kwaliteit van de pentest gewaarborgd worden met behulp van het werkprogramma.
- **Veilige opslag van rapportages en klantgegevens**
  Wanneer klantgegevens & vertrouwelijke informatie (pentestrapportage) op het online portaal komen te staan dient deze informatie goed beveilig te worden.

Nice te have

- **Bijwerken standaard observaties**
  Door meer gebruik te maken van standaard observaties kan er tijd bespaard worden. Er is in april 2011 een opzet gemaakt voor standaard observaties, deze dienen bijgewerkt te worden. Tevens moeten de standaard observaties naar het Nederlands vertaald worden.
- **De pentest meer automatiseren**
  Er kan nog meer tijd worden bespaard wanneer en deel van de uitvoering van een pentest geautomatiseerd wordt. Alleen dit automatiseren moet zorgvuldig gebeuren omdat pentest software nog veel "false positives" vindt.
- **Aanpassen rapportage**
  De pentest rapportage dient krachtiger, bondiger en minder technisch te worden voor MKB organisaties. Er kan bijvoorbeeld op één pagina een bondige samenvatting met "heatmap" worden gemaakt. Ook dient er te worden uitgezocht of een (Word)document de beste manier is om de resultaten te presenteren.
- **Benchmark database**
  Met een benchmark database kunnen de pentest resultaten van verschillende klanten vergeleken worden. De resultaten kunnen bijvoorbeeld per branche worden ingedeeld zodat de klant kan zien hoe hij scoort ten opzichte van andere organisaties.

MKB Security Test

Hoe vatbaar zijn uw Internetomgeving en website voor cybercriminaliteit? Laat een MKB Security Test uitvoeren om security kwetsbaarheden bloot te leggen en geef hackers geen kans!

AANVRAGEN

De kranten staan de laatste tijd vol met nieuwsberichten over organisaties die zijn gehackt. Gaten in de beveiliging van IT infrastructuur en applicaties worden benut door hackers om toegang te krijgen tot uw systemen. Diverse keurmerken voor beveiliging worden uitgegeven, maar garanderen niet dat systemen niet worden gehackt. Hoe veilig zijn uw bedrijfskritische systemen nu echt?

De MKB Security Test simuleert een hackersaanval op uw infrastructuur, website of mobiele applicatie. Hierbij wordt vanaf Internet door onze "ethische hackers" op gestructureerde wijze gezocht naar de meest voorkomende security kwetsbaarheden in uw systemen. Resultaat van de MKB Security Test is een getailleerd inzicht in de "lekken" en concrete aanbevelingen om die te dichten. De MKH Security Test is beschikbaar in drie varianten:

Website	Mobiel	Infrastructuur
		
Security Test voor uw websites	Security Test voor uw mobiele applicaties	Security Test voor uw Internet infrastructuur
Voorbeeld: • Bedrijfswebsite • Webshop	Voorbeeld: • Urenregistratie app • Webshop app	Voorbeeld: • Mail server • VPN server
Prijs: € 2000,- **Eenheid:** 1 website	**Prijs:** € 2500,- **Eenheid:** 1 mobiele app	**Prijs:** € 2000,- **Eenheid:** max 20 IP's

Voordelen MKB Security Test

- Speciaal voor het MKB ontwikkelde test op meest voorkomende security kwetsbaarheden
- Realistische test van de beveiliging van uw systemen door "ethische hackers"
- Gedetailleerd inzicht in kwetsbaarheden in uw kritische systemen
- Een begrijpbare en op maat gesneden rapportage

Meer wensen?

Wilt u een op maat gemaakt Security Test? Neem dan contact op.

Deel deze dienst

Deel deze dienst met anderen via: 

Pentest Aanvraagformulier (velden)

- Bedrijfsnaam
- Naam
- E-mailadres
- Telefoonnummer
- Soort pentest (Web, Mobile, infra)
- Aantal eenheden
- Opmerking

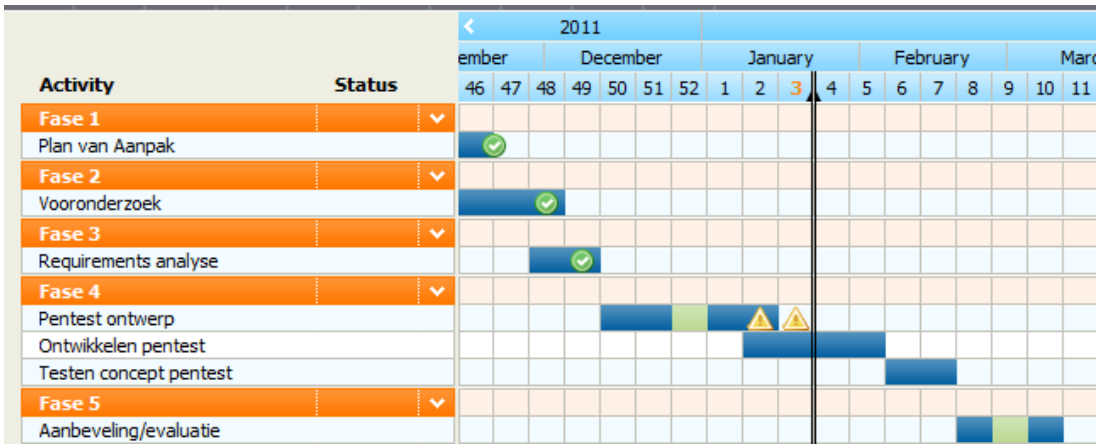
Voortgangsverslag (januari)

Inleiding
Door middel van dit document wordt de voortgang van de afstudeerstage weergegeven van student Werner Alsemgeest. De afstudeerstage wordt uitgevoerd bij Deloitte Nederland te Amstelveen. Het onderwerp van de afstudeerstage betreft het ontwikkelen van een pentestproduct voor het MKB. De afstudeerstage is gestart op 11 november 2011 en duurt +/- 18 werken. Het project bestaat uit vijf fases, welke gedefineerd staan in het plan van aanpak. De (door de begeleider van Deloitte) goedgekeurde documentatie is te vinden in het online portfolio op BlackBoard.

Afgeronde fases:
Op het moment van schrijven zijn de eerste drie fases afgerond.

- **Fase 1**
  Betreft het plan van aanpak van het project. Hierin staan o.a. de probleemstelling, doelstelling en planning beschreven. Deze fase is volgens planning afgerond.
- **Fase 2**
  In fase 2 is een vooronderzoek op het gebied van pentesting uitgevoerd. In dit onderzoek is o.a. onderzocht wat voor soorten pentests er zijn, hoe een pentest uitgevoerd kan worden en hoe het pentestproces bij Deloitte eruit ziet. Er is geen document gemaakt voor het vooronderzoek. Een deel van de resultaten van het vooronderzoek is meegenomen in de documentatie van fase 4. Deze fase is volgens planning afgerond.
- **Fase 3**
  Fase 3 bevat de requirements analyse van het project. In deze fase zijn de wensen en eisen in kaart gebracht van belanghebbenden voor de MKB pentest. De requirements staan beschreven in het document "requirements analyse". Deze fase is volgens planning afgerond, maar er is na de afronding van de fase nog een extra requirements toegevoegd. Dit had geen gevolgen voor het project.

Planning
In het onderstaande schema is de planning van dit project weergegeven. De planning is bijgewerkt tot de verticale zwarte streep. Een groene "vink" betekent afgerond en goedgekeurd. Bij een geel "uitroepteken" kan niet aan de planning worden voldaan.



Op het moment bezig met:

Fase 4
Fase 4 bestaat uit drie onderdelen. Op dit moment wordt er aan twee van de drie onderdelen gewerkt.

- **Pentest ontwerp**
  In het pentest ontwerp staat (in hoofdlijnen) beschreven hoe de MKB pentest eruit moet zien en uit welke onderdelen de pentest zal bestaan. Ook is in dit document een deel van de resultaten van het vooronderzoek inbegrepen. Dit om achtergrondinformatie over pentests te geven en te beschrijven hoe momenteel een pentest wordt uitgevoerd binnen Deloitte.
  Deze fase is nog niet afgerond en is buiten de planning gelopen. Dit heeft twee redenen:
  - 1) Controle
    Het pentest ontwerp is uitgewerkt en opgeleverd aan de toegewezen begeleider van Deloitte. Het document is nog niet volledig nagekeken en goedgekeurd door de begeleider i.v.m. drukte. De planning is dat de begeleider het document op 20-01-2012 op het einde van de dag volledig heeft nagekeken.
  - 2) Presentatie
    Het idee was om in week 3 een presentatie te houden over het MKB pentestontwerp aan belanghebbenden zoals de opdrachtgever, begeleider, een aantal managers en een aantal pentesters. Tijdens deze presentatie zal duidelijk worden gemaakt hoe de MKB pentest uitgevoerd zal worden en uit welke onderdelen de pentest zal bestaan. Aan het einde van de presentatie zal er ruimte zijn voor feedback en discussie over het ontwerp. Deze feedback zal gebruikt worden voor de ontwikkeling van de MKB pentest.
    Ondanks het tijdig aanvragen en inplannen (in week 52) van de presentatie was het niet haalbaar voor iedereen om tijd vrij te maken in de agenda en is daarom verplaatst naar week 5.

  De gevolgen van het uitlopen zijn beperkt. Er is besproken met de begeleider van Deloitte dat er al begonnen kan worden aan het volgende onderdeel van fase 4 (de ontwikkeling). Om de kwaliteit, doelstelling en te tevredenheid van de opdrachtgever te waarborgen wordt de feedback (op het pentest ontwerp) van de begeleider gebruikt. De feedback die de mensen na de presentatie zullen geven zal alleen worden verwerkt als dit geen gevolgen heeft voor de totale planning van het project. Er is een mogelijkheid om fase 4 een week langer door te laten lopen om de feedback te verwerken.
- **Ontwikkelen pentest**
  Deze fase bevat het ontwikkelen van het MKB pentest ontwerp. Deze fase is volgens planning gestart. Er wordt op dit moment o.a. gewerkt aan het werkprogramma voor de MKB pentest en "tooling" om automatisch een pentest rapportage te creëren.